Come abilitare StorageGRID nel tuo ambiente

How to enable StorageGRID in your environment

NetApp
April 18, 2025

Sommario

Come abilitare StorageGRID nel tuo ambiente

Procedura per accedere al software di valutazione StorageGRID

Queste istruzioni sono destinate alla vendita di NetApp, ai partner e ai prospect impegnati in NetApp.

Registrati per un account

1. Registrati per ottenere un account su "Sito di supporto NetApp" utilizzando il tuo indirizzo e-mail aziendale.
   a. Assicurati di non aver effettuato l'accesso con l'account appena creato.
   b. Se si dispone già di un account, assicurarsi di non aver effettuato l'accesso e procedere con il passaggio successivo.
2. Creare un caso di supporto non tecnico per elevare i livelli di accesso al "potenziale cliente". A tale scopo, fare clic sul ""Segnala un problema"collegamento " nel piè di pagina del sito Web.
3. Selezionare "problema di registrazione" come categoria di feedback.
4. Nella sezione dei commenti, scrivi: "Il mio indirizzo e-mail del cliente è *il vostro-indirizzo-e-mail*. Vorrei ottenere l'accesso al potenziale cliente per scaricare il software di valutazione StorageGRID."
   a. Citare il nome della persona interna di NetApp che ha suggerito la richiesta di accesso al prospect.

Scarica StorageGRID

1. Dopo aver esaminato e approvato il tuo caso di supporto, il supporto NetApp ti informerà via e-mail che al tuo account è stato concesso l'accesso ai prospect.
2. Scaricare "Software di valutazione StorageGRID".

Il file di licenza di valutazione si trova all'interno del file zip. Si tratta di StorageGRID-webscale-<version>\vsphere\NLF000000.txt una volta decompresso.

Il download del software è un processo che prevede misure di conformità commerciale per rispettare i requisiti legali. Per garantire la conformità, gli utenti devono creare un account e aprire un caso di supporto prima di poter accedere. Questo processo ci aiuta a mantenere il controllo e la documentazione corretti, fornendo ai potenziali clienti il software pronto per la produzione di cui hanno bisogno.

Forniamo la versione "pronta per la produzione" di StorageGRID, che non è una versione open-source o alternativa. È importante notare che **il supporto non viene fornito** a meno che il potenziale cliente non effettui l'aggiornamento a una licenza di produzione.

Contattare StorageGRID.Feedback@netapp.com per eventuali problemi con i passaggi precedenti.

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 11,9

Le seguenti soluzioni di terze parti sono state convalidate per l'utilizzo con StorageGRID 11,9. + 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
- Snapshot Elasticsearch (incluso il Tier "frozen")
- 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
- Starburst
- Lo storage diventa semplice
- Trino
- Verniciare Enterprise 6.0.4
- Veeeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 e versioni successive
- 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
- Rubrik
- Veeeam 12
- Veritas Enterprise Vault 15,1
- 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

Responsabili delle chiavi supportati su StorageGRID

Queste soluzioni sono state testate.

- Controllo chiave Entrust 10,2

- Vault Hashiorp 1.15.0
- Thales CipherTrust Manager 2,0
- Thales CipherTrust Manager 2,1
- Thales CipherTrust Manager 2,2
- Thales CipherTrust Manager 2,3
- Thales CipherTrust Manager 2,4
- Thales CipherTrust Manager 2,8
- Thales CipherTrust Manager 2,9
- Thales CipherTrust Manager 2,10
- Thales CipherTrust Manager 2,11
- Thales CipherTrust Manager 2,12
- Thales CipherTrust Manager 2,13
- Thales CipherTrust Manager 2,14

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
- Snapshot Elasticsearch (incluso il Tier "frozen")
- 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
- Starburst
- Lo storage diventa semplice
- Trino
- Verniciare Enterprise 6.0.4
- Veeeam 12

- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 e versioni successive
- 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
- Rubrik
- Veeeam 12
- Veritas Enterprise Vault 15,1
- 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

Responsabili delle chiavi supportati su StorageGRID

Queste soluzioni sono state testate.

- Controllo chiave Entrust 10,2
- Vault Hashiorp 1.15.0
- Thales CipherTrust Manager 2,0
- Thales CipherTrust Manager 2,1
- Thales CipherTrust Manager 2,2
- Thales CipherTrust Manager 2,3
- Thales CipherTrust Manager 2,4
- Thales CipherTrust Manager 2,8
- Thales CipherTrust Manager 2,9
- Thales CipherTrust Manager 2,10
- Thales CipherTrust Manager 2,11
- Thales CipherTrust Manager 2,12
- Thales CipherTrust Manager 2,13
- Thales CipherTrust Manager 2,14

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
- Snapshot Elasticsearch (incluso il Tier "frozen")
- 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 10.1.1 e versioni successive
- 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
- Rubrik
- 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

Responsabili delle chiavi supportati su StorageGRID

Queste soluzioni sono state testate.

- Thales CipherTrust Manager 2,0
- Thales CipherTrust Manager 2,1
- Thales CipherTrust Manager 2,2
- Thales CipherTrust Manager 2,3
- Thales CipherTrust Manager 2,4
- Thales CipherTrust Manager 2,8
- Thales CipherTrust Manager 2,9

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

Raggiungimento di un RPO pari a zero con StorageGRID: Una guida completa alla replica multisito

Questo report tecnico fornisce una guida completa all'implementazione delle strategie di replica di StorageGRID per ottenere un recovery point objective (RPO) pari a zero in caso di guasto di un sito. Il documento descrive in dettaglio le varie opzioni di implementazione per StorageGRID, tra cui la replica sincrona multisito e la replica asincrona multi-grid. Spiega in che modo è possibile configurare le policy ILM (Information Lifecycle Management) di StorageGRID per garantire la conservazione e la disponibilità dei dati in più sedi. Inoltre, il rapporto prende in esame considerazioni sulle prestazioni, scenari di errore e processi di ripristino per garantire operazioni ininterrotte dei client. L'obiettivo di questo documento è fornire le informazioni necessarie per garantire che i dati rimangano accessibili e coerenti, anche in caso di guasto completo del sito, sfruttando tecniche di replica sincrone e asincrone.

Panoramica di StorageGRID

NetApp StorageGRID è un sistema storage basato su oggetti che supporta l'API Amazon Simple Storage Service (Amazon S3) standard di settore.

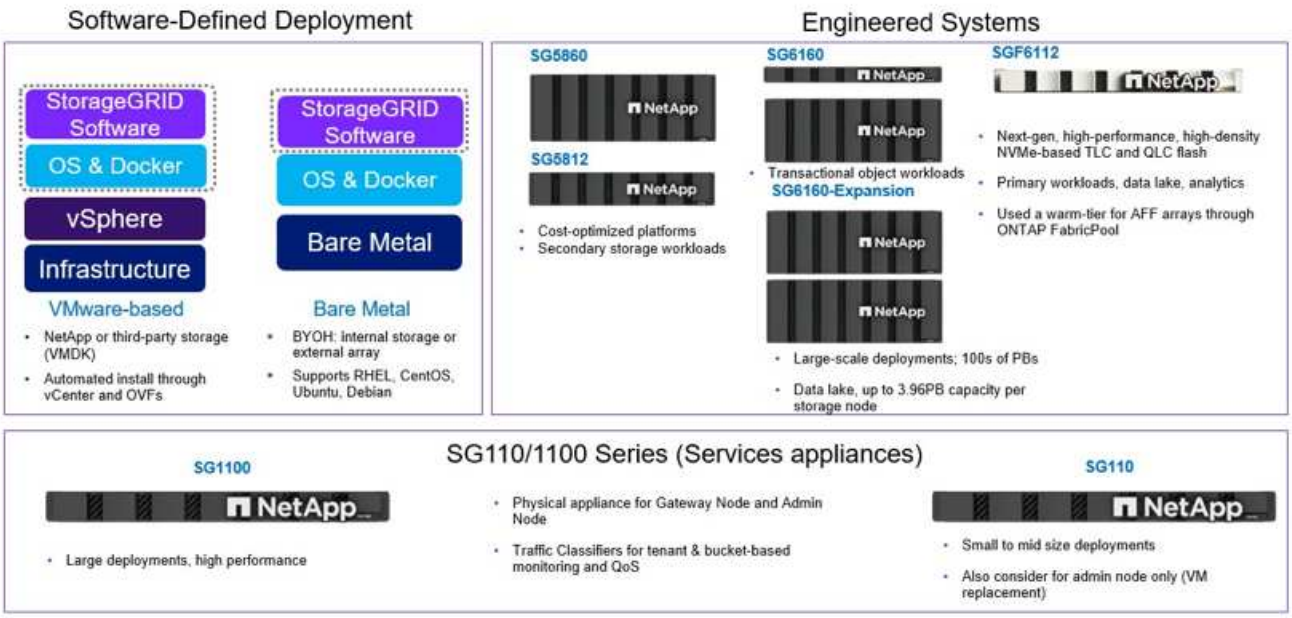
StorageGRID offre un namespace singolo in siti multipli con livelli di servizio variabili determinati da policy di Information Lifecycle Management (ILM). Con queste policy del ciclo di vita puoi ottimizzare la posizione dei dati durante il loro ciclo di vita.

StorageGRID garantisce durata e disponibilità configurabili dei tuoi dati in soluzioni locali e geodistribuito. Sia che i dati risiedano on-premise o in un cloud pubblico, i flussi di lavoro del cloud ibrido integrato consentono alla tua azienda di sfruttare servizi cloud come Amazon Simple Notification Service (Amazon SNS), Google Cloud, Microsoft Azure Blob, Amazon S3 Glacier, Elasticsearch e altri ancora.

Scala StorageGRID

È possibile implementare StorageGRID con soli 3 nodi storage e un singolo grid può crescere fino a 200 nodi. È possibile implementare una singola griglia come singolo sito o estenderla fino a 16 siti. Un grid minimo è costituito da un nodo amministrativo e da 3 nodi storage in un singolo sito. Il nodo admin contiene l'interfaccia di gestione, un punto centrale per le metriche e il logging e mantiene la configurazione dei componenti StorageGRID. Il nodo admin contiene anche un bilanciamento del carico integrato per l'accesso API S3. StorageGRID può essere implementato come software-only, come appliance per macchine virtuali VMware o come appliance costruite ad hoc.

È possibile implementare un nodo StorageGRID solo come nodo di metadati che massimizza il numero di oggetti, un nodo di storage a oggetti che massimizza lo spazio di oggetti o un nodo combinato di metadati e storage a oggetti che aggiunge sia il numero di oggetti che lo spazio degli oggetti. Ciascun nodo storage può scalare fino a raggiungere una capacità di diversi petabyte per lo storage a oggetti, permettendo di creare un namespace singolo nelle centinaia di petabyte. StorageGRID fornisce anche un bilanciatore di carico integrato per operazioni API S3 chiamate nodo di gateway.



StorageGRID consiste di una raccolta di nodi posizionati in una topologia di sito. Un sito in StorageGRID può essere una posizione fisica univoca o risiedere in una posizione fisica condivisa come altri siti nella griglia come costrutto logico. Un sito StorageGRID non deve occupare più posizioni fisiche. Un sito rappresenta un'infrastruttura LAN condivisa.

StorageGRID e domini di errore

StorageGRID contiene diversi livelli di domini di errore da prendere in considerazione per decidere come progettare la soluzione, come archiviare i dati e dove archiviare i dati per mitigare i rischi di guasti.

- Livello griglia - Una griglia costituita da più siti può presentare guasti o isolamento del sito e i siti accessibili possono continuare a funzionare come rete.
- Livello sito - i guasti all'interno di un sito possono influire sulle operazioni del sito, ma non sul resto della griglia.
- Livello nodo - il guasto di Un nodo non influisce sul funzionamento del sito.
- Livello disco - un guasto del disco non influisce sul funzionamento del nodo.

Dati e metadati di oggetti

Con lo storage a oggetti, l'unità di storage è un oggetto, piuttosto che un file o un blocco. A differenza della gerarchia ad albero di un file system o di uno storage a blocchi, lo storage a oggetti organizza i dati in un layout piatto e non strutturato. Lo storage a oggetti separa la posizione fisica dei dati dal metodo utilizzato per memorizzare e recuperare tali dati.

Ogni oggetto in un sistema di storage basato su oggetti ha due parti: Dati oggetto e metadati oggetto.

- I dati oggetto rappresentano i dati sottostanti effettivi, ad esempio una fotografia, un filmato o una cartella clinica.
- I metadati degli oggetti sono informazioni che descrivono un oggetto.

StorageGRID utilizza i metadati degli oggetti per tenere traccia delle posizioni di tutti gli oggetti nella griglia e gestire il ciclo di vita di ciascun oggetto nel tempo.

I metadati dell'oggetto includono informazioni come:

- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3, il nome o l'ID dell'account tenant, le dimensioni logiche dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.
- Posizione dello storage corrente di ogni replica dell'oggetto o frammento sottoposto a erasure coding.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto
- Per oggetti segmentati e multiparte, identificatori di segmenti e dimensioni dei dati.

I metadati degli oggetti sono personalizzabili ed espandibili, il che lo rende flessibile per l'utilizzo da parte delle applicazioni. Per informazioni dettagliate su come e dove StorageGRID archivia i metadati degli oggetti, visitare il sito "Gestire lo storage dei metadati degli oggetti".

Il sistema Information Lifecycle management (ILM) di StorageGRID viene utilizzato per orchestrare il posizionamento, la durata e il comportamento di acquisizione per tutti i dati degli oggetti nel sistema StorageGRID. Le regole ILM determinano il modo in cui StorageGRID archivia gli oggetti nel tempo utilizzando repliche degli oggetti o erasure coding dell'oggetto nei nodi e nei siti. Questo sistema ILM è responsabile della coerenza dei dati degli oggetti all'interno di una griglia.

Erasure coding

StorageGRID offre la possibilità di sottoporre a erasure coding i dati a diversi livelli. Le appliance StorageGRID eliminano i dati memorizzati su ciascun nodo su tutti i dischi con RAID, garantendo la protezione contro guasti ai dischi multipli e causando interruzioni o perdita di dati. Inoltre, StorageGRID può utilizzare gli schemi di erasure coding per memorizzare i dati degli oggetti nei nodi di un sito o distribuiti in 3 o più siti nel sistema StorageGRID attraverso le regole ILM di StorageGRID.

L'erasure coding fornisce un layout dello storage resiliente ai guasti dei nodi con overhead ridotto, mentre la replica può fare la stessa cosa, con più overhead. Tutti gli schemi di erasure coding StorageGRID sono implementabili in un singolo sito, a condizione che il numero minimo di nodi necessari per memorizzare le porzioni di dati sia soddisfatto. Ciò significa che per uno schema EC di 4+2 è necessario disporre di un minimo di 6 nodi disponibili per ricevere i dati.

Erasure-coding scheme (*k+m*)	Minimum number of deployed sites	Recommended number of Storage Nodes at each site	Total recommended number of Storage Nodes	Site loss protection?	Storage overhead
4+2	3	3	9	Yes	50%
6+2	4	3	12	Yes	33%
8+2	5	3	15	Yes	25%
6+3	3	4	12	Yes	50%
9+3	4	4	16	Yes	33%
2+1	3	3	9	Yes	50%
4+1	5	3	15	Yes	25%
6+1	7	3	21	Yes	17%
7+5	3	5	15	Yes	71%

Coerenza dei metadati

In StorageGRID, i metadati vengono generalmente archiviati con tre repliche per sito, per garantire coerenza e disponibilità. Questa ridondanza contribuisce a mantenere l'integrità e l'accessibilità dei dati anche in caso di errore.

La coerenza predefinita è definita a livello di griglia. Gli utenti possono modificare la coerenza a livello del bucket in qualsiasi momento.

Le opzioni di coerenza delle benne disponibili in StorageGRID sono:

- **Tutti**: Offre il massimo livello di coerenza. Tutti i nodi nella griglia ricevono i dati immediatamente, altrimenti la richiesta non riesce.
- **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-Global V2**: Garantisce coerenza lettura dopo scrittura per tutte le richieste dei clienti in tutti i siti. Offre coerenza per nodi multipli o anche un guasto del sito, se si raggiunge il quorum di replica dei metadati. Ad esempio, è necessario eseguire un minimo di 5 repliche da una griglia a 3 siti con un massimo di 3 repliche all'interno di un sito.
- **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write**(default): Fornisce coerenza lettura-dopo-scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Coerenza dei dati degli oggetti

Mentre i metadati vengono replicati automaticamente all'interno e tra i siti, spetta a te prendere decisioni sul posizionamento dello storage dei dati a oggetti. I dati degli oggetti possono essere memorizzati in repliche all'interno e tra i siti, con erasure coding all'interno o tra i siti, o in una combinazione o repliche e schemi di storage con erasure coding. Le regole ILM possono essere applicate a tutti gli oggetti o filtrate per applicarsi solo a determinati oggetti, bucket o tenant. Le regole ILM definiscono il modo in cui gli oggetti vengono memorizzati, le repliche e/o il erasure coding, la durata della memorizzazione degli oggetti in tali posizioni, se il numero di repliche o lo schema di erasure coding deve cambiare o se le posizioni devono cambiare nel tempo.

Ogni regola ILM verrà configurata con uno dei tre comportamenti di acquisizione per la protezione degli oggetti: Dual commit, balanced o Strict.

L'opzione dual commit consente di eseguire immediatamente due copie su due nodi di storage diversi nella griglia, restituendo la richiesta al client con esito positivo. La selezione del nodo tenterà all'interno del sito della richiesta, ma in alcune circostanze potrebbe utilizzare i nodi di un altro sito. L'oggetto viene aggiunto alla coda ILM da valutare e posizionato in base alle regole ILM.

L'opzione Balanced valuta immediatamente l'oggetto rispetto al criterio ILM e posiziona l'oggetto in modo sincrono prima che la richiesta venga restituita correttamente al client. Se non è possibile soddisfare immediatamente la regola ILM a causa di un'interruzione del servizio o di uno storage non adeguato per soddisfare i requisiti di posizionamento, verrà utilizzato il dual commit. Una volta risolto il problema, ILM posizionerà automaticamente l'oggetto in base alla regola definita.

L'opzione Strict valuta immediatamente l'oggetto rispetto al criterio ILM e posiziona l'oggetto in modo sincrono prima che la richiesta venga restituita correttamente al client. Se non è possibile soddisfare immediatamente la regola ILM a causa di un'interruzione o di uno storage inadeguato per soddisfare i requisiti di posizionamento, la richiesta non viene accettata e il client deve riprovare.

Bilanciamento del carico

StorageGRID può essere implementato con accesso client tramite i nodi gateway integrati, un bilanciatore di carico esterno di 3e parti, round robin DNS o direttamente in un nodo storage. È possibile implementare diversi nodi di gateway in un sito e configurarli in gruppi a disponibilità elevata per offrire failover e failback automatici in caso di black-out di un nodo di gateway. È possibile combinare metodi di bilanciamento del carico in una soluzione per fornire un unico punto di accesso per tutti i siti in una soluzione.

Per impostazione predefinita, i nodi di gateway bilanciano il carico tra i nodi storage nel sito in cui si trova il nodo gateway. StorageGRID può essere configurato in modo da consentire ai nodi di gateway di bilanciare il carico utilizzando nodi da più siti. Questa configurazione aggiungerebbe la latenza tra questi siti alla latenza di risposta alle richieste del client. Questa impostazione deve essere configurata solo se la latenza totale è accettabile per i client.

Come ottenere un RPO pari a zero con StorageGRID

Per raggiungere l'obiettivo RPO (Recovery Point Objective) zero in un sistema storage a oggetti, è fondamentale che al momento del guasto:

- Sia i metadati che i contenuti degli oggetti sono sincronizzati e considerati coerenti
- I contenuti degli oggetti rimangono accessibili nonostante il guasto.

Per un'implementazione multi-sito, strong Global V2 è il modello di coerenza preferito per garantire che i metadati siano sincronizzati in tutti i siti, il che lo rende essenziale per soddisfare il requisito di RPO pari a zero.

Gli oggetti nel sistema storage sono archiviati in base alle regole ILM (Information Lifecycle Management), che stabiliscono come e dove i dati vengono archiviati per tutto il loro ciclo di vita. Per la replica sincrona si può considerare tra esecuzione rigorosa o esecuzione bilanciata.

- Per un RPO pari a zero è necessaria un'esecuzione rigorosa di queste regole ILM, in quanto assicura che gli oggetti vengano posizionati nelle posizioni definite senza alcun ritardo o fallback, mantenendo la disponibilità e la coerenza dei dati.
- Il comportamento di acquisizione ILM di StorageGRID offre un equilibrio tra alta disponibilità e resilienza, consentendo agli utenti di continuare ad acquisire i dati anche in caso di guasto del sito.

In alternativa, è possibile ottenere un RTO di zero con una combinazione di bilanciamento del carico locale e globale. Per garantire un accesso ininterrotto ai client è necessario il bilanciamento del carico delle richieste dei client. Una soluzione StorageGRID può contenere molti nodi di gateway e gruppi di alta disponibilità in ogni sito. Per fornire accesso ininterrotto ai client di qualsiasi sito, anche in caso di guasti, è necessario configurare una soluzione di bilanciamento del carico esterna in combinazione con i nodi di gateway StorageGRID. Configurare i gruppi di high Availability del nodo gateway che gestiscono il carico all'interno di ogni sito e utilizzare il bilanciamento del carico esterno per bilanciare il carico tra i gruppi di high Availability. Il bilanciamento del carico esterno deve essere configurato per eseguire un controllo di integrità per garantire che le richieste vengano inviate solo ai siti operativi. Per ulteriori informazioni sul bilanciamento del carico con StorageGRID, vedere "Report tecnico per il bilanciamento del carico di StorageGRID" .

Implementazioni sincrone in siti multipli

Soluzioni multisito: StorageGRID consente di replicare gli oggetti su più siti all'interno della griglia in modo sincrono. Impostando le regole ILM (Information Lifecycle Management) con comportamento equilibrato o rigoroso, gli oggetti vengono posizionati immediatamente nelle posizioni specificate. La configurazione del livello di coerenza del bucket su strong Global v2 garantirà anche la replica sincrona dei metadati. StorageGRID utilizza un singolo Global namespace, archiviando le posizioni di posizionamento degli oggetti come metadati, in modo che ogni nodo sappia dove sono situate tutte le copie o i componenti con erasure coding. Se un oggetto non può essere recuperato dal sito in cui è stata effettuata la richiesta, verrà recuperato automaticamente da un sito remoto senza richiedere le procedure di failover.

Una volta risolto il problema, non è necessario alcun intervento di failback manuale. Le performance di replica dipendono dal sito con il throughput di rete più basso, la latenza più alta e le performance più basse. Le prestazioni di un sito si basano sul numero di nodi, sul numero di core della CPU e sulla velocità, sulla memoria, sulla quantità di unità e sui tipi di unità.

Soluzioni multi-grid: StorageGRID è in grado di replicare tenant, utenti e bucket tra più sistemi StorageGRID utilizzando la replica cross-grid (CGR, Cross-Grid Replication). CGR può estendere i dati selezionati a più di 16 siti, aumentare la capacità utilizzabile dell'archivio di oggetti e fornire il disaster recovery. La replica dei bucket con CGR include oggetti, versioni degli oggetti e metadati e può essere bidirezionale o unidirezionale. L'RPO (Recovery Point Objective) dipende dalle prestazioni di ogni sistema StorageGRID e dalle connessioni di rete tra di essi.

Sommario:

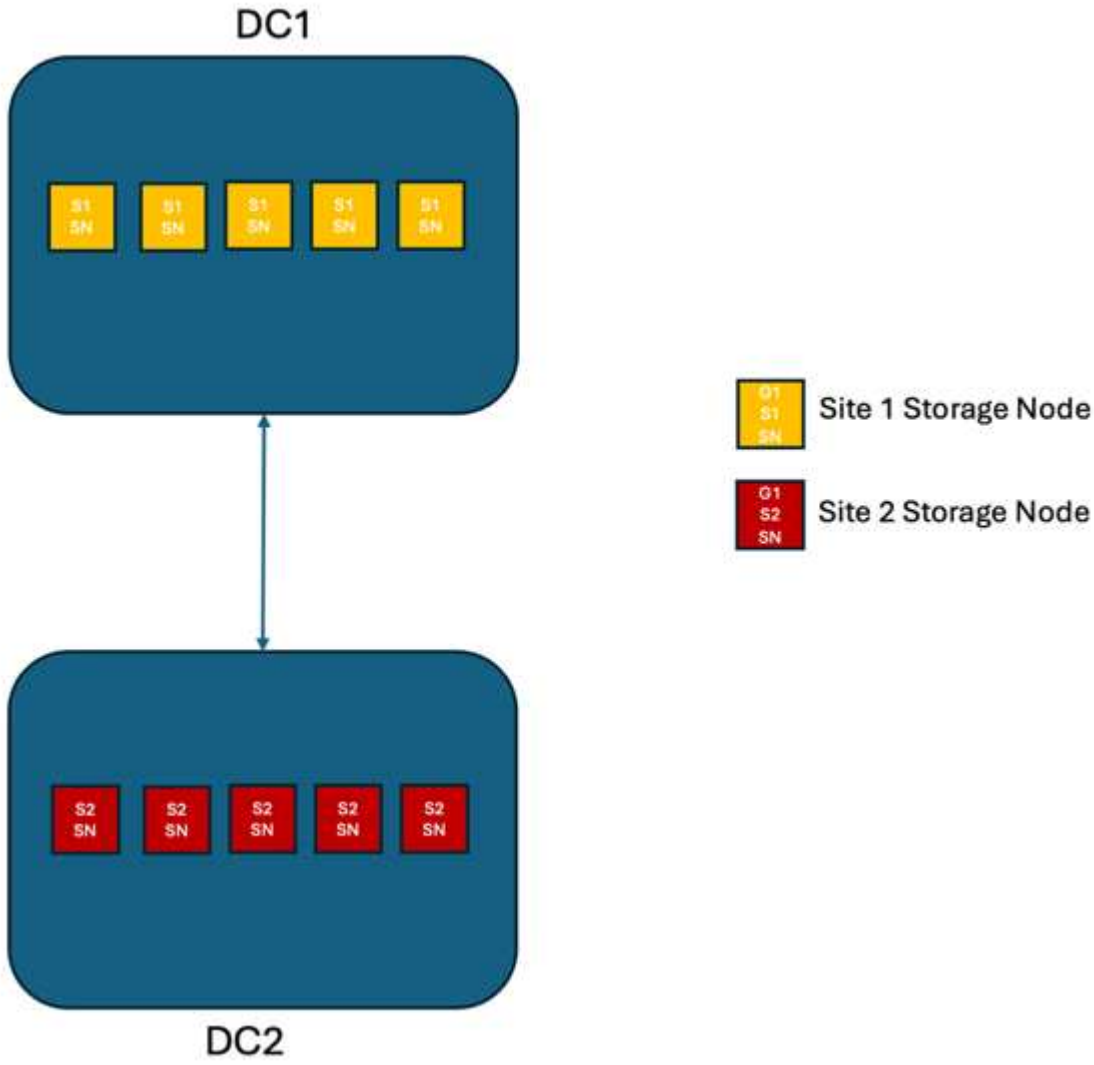
- La replica intra-grid include una replica sincrona e asincrona, configurabile tramite comportamento di acquisizione ILM e controllo della coerenza dei metadati.
- La replica inter-grid è solo asincrona.

Distribuzione multisito Single Grid

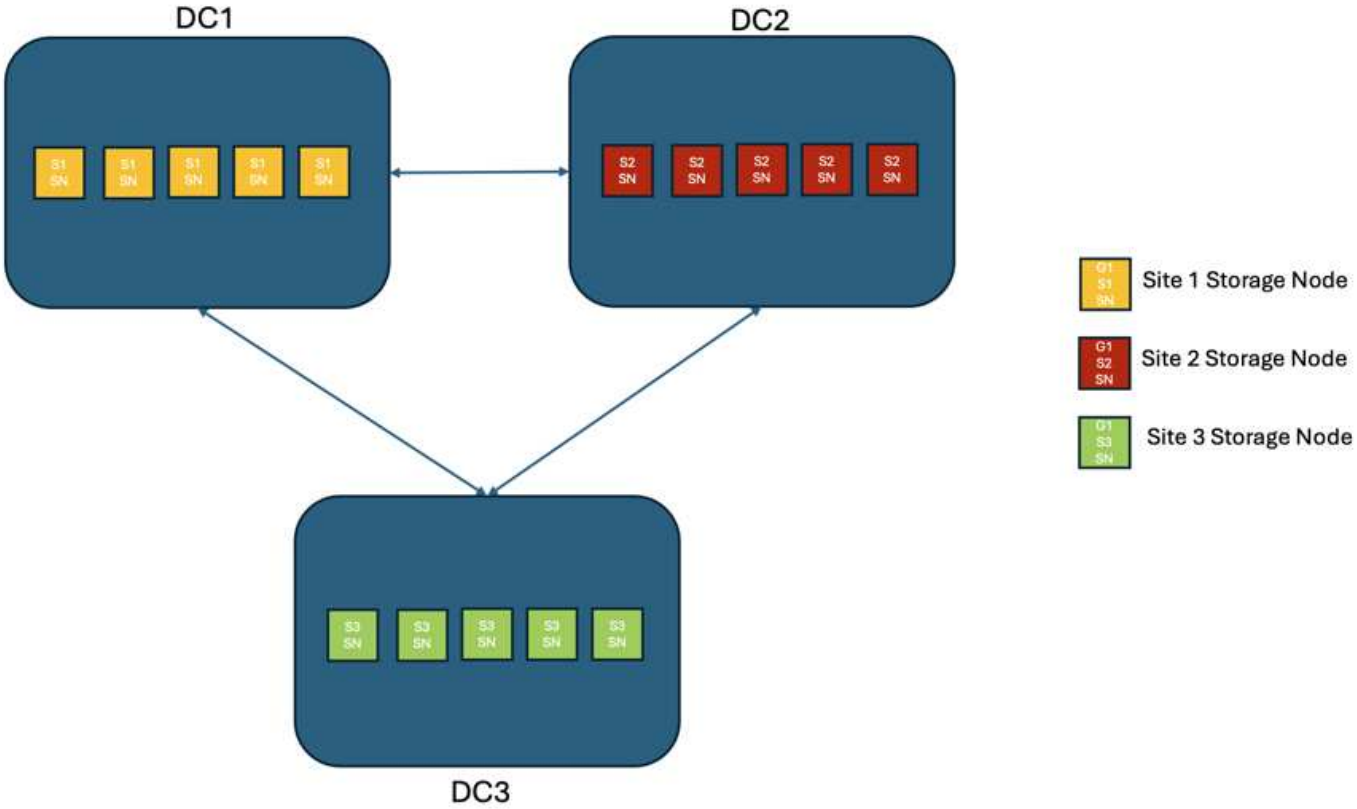
Nei seguenti scenari le soluzioni StorageGRID sono configurate con un bilanciatore di carico esterno opzionale

che gestisce le richieste ai gruppi ad alta disponibilità del bilanciatore di carico integrato. In questo modo si otterrà un RTO di zero oltre a un RPO pari a zero. ILM è configurato con protezione di acquisizione bilanciata per il posizionamento sincrono. Ogni bucket è configurato con il forte modello globale di coerenza v2 per griglie di 3 o più siti e con una forte coerenza globale per meno di 3 siti.

In una soluzione StorageGRID con due siti ci sono almeno due repliche o 3 pezzi EC di ogni oggetto e 6 repliche di tutti i metadati. In caso di errore, gli aggiornamenti dal black-out vengono sincronizzati automaticamente con il sito/i nodi ripristinati. Con solo 2 siti è improbabile che raggiunga un RPO pari a zero negli scenari di guasto oltre alla perdita dell'intero sito.



In una soluzione StorageGRID di tre o più siti ci sono almeno 3 repliche o 3 pezzi EC di ogni oggetto e 9 repliche di tutti i metadati. In caso di errore, gli aggiornamenti dal black-out vengono sincronizzati automaticamente con il sito/i nodi ripristinati. Con tre o più siti è possibile ottenere un RPO pari a zero.



Scenari di guasti su più siti

Guasto	Esito a 2 siti	risultato di 3 o più siti
Guasto al disco a nodo singolo	Ogni appliance utilizza gruppi di dischi multipli e può sostenere almeno 1 dischi per gruppo di guasti senza interruzioni o perdita di dati.	Ogni appliance utilizza gruppi di dischi multipli e può sostenere almeno 1 dischi per gruppo di guasti senza interruzioni o perdita di dati.
Guasto a un singolo nodo in un sito	Nessuna interruzione delle operazioni o perdita di dati.	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a più nodi in un solo sito	Interruzione delle operazioni dei client dirette a questo sito senza perdita di dati. Le operazioni dirette all'altro sito rimangono senza interruzioni e non perdono dati.	Le operazioni vengono dirette a tutti gli altri siti mantenendo interruzioni e senza perdita di dati.

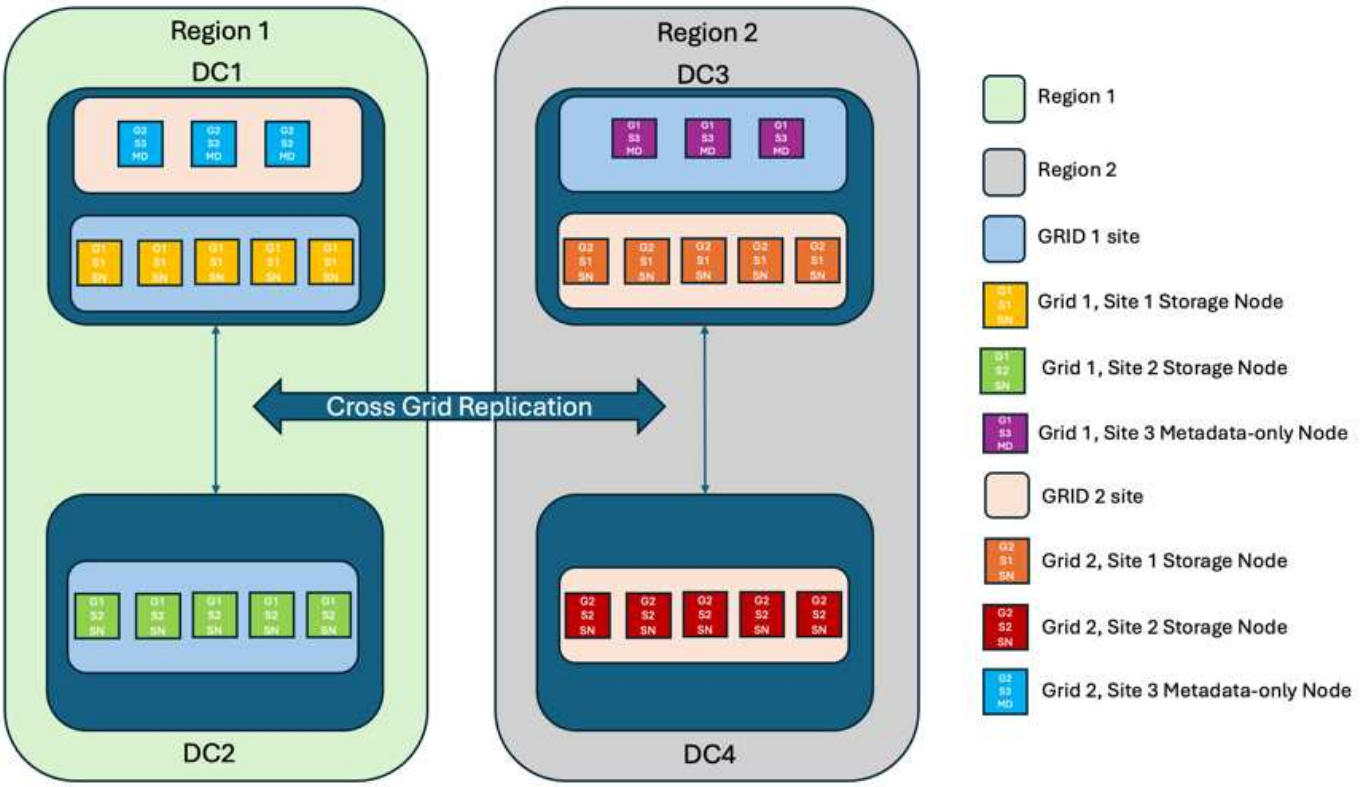
Guasto	Esito a 2 siti	risultato di 3 o più siti
Guasto a nodo singolo in più siti	Nessuna interruzione o perdita di dati se: • Nella griglia esiste almeno una singola replica • Nella griglia sono presenti frammenti EC sufficienti Operazioni interrotte e rischio di perdita di dati se: • Nessuna replica esistente • Presenza di mandrini EC insufficienti	Nessuna interruzione o perdita di dati se: • Nella griglia esiste almeno una singola replica • Nella griglia sono presenti frammenti EC sufficienti Operazioni interrotte e rischio di perdita di dati se: • Nessuna replica esistente • Non esistono chucks EC sufficienti per recuperare l'oggetto
Guasto a un singolo sito	le operazioni del client verranno interrotte fino a quando l'errore non viene risolto, oppure finché la coerenza del bucket non viene ridotta a un sito sicuro o inferiore per garantire il successo delle operazioni senza alcuna perdita di dati.	Nessuna interruzione delle operazioni o perdita di dati.
Guasti a un singolo sito e a un nodo singolo	le operazioni del client verranno interrotte fino a quando il guasto non viene risolto o la coerenza del bucket viene ridotta a lettura dopo nuova scrittura o a un livello inferiore per consentire la riuscita delle operazioni e l'eventuale perdita di dati.	Nessuna interruzione delle operazioni o perdita di dati.
Singolo sito più un nodo da ciascun sito rimanente	le operazioni del client verranno interrotte fino a quando il guasto non viene risolto o la coerenza del bucket viene ridotta a lettura dopo nuova scrittura o a un livello inferiore per consentire la riuscita delle operazioni e l'eventuale perdita di dati.	Le operazioni verranno interrotte se non è possibile soddisfare il quorum della replica dei metadati e la possibile perdita di dati.
Guasto multi-sito	Nessun sito operativo resterà in gioco se non sarà possibile ripristinare completamente almeno 1 sito.	Le operazioni verranno interrotte se non è possibile soddisfare il quorum della replica dei metadati. Nessuna perdita di dati finché rimane almeno 1 sito.

Guasto	Esito a 2 siti	risultato di 3 o più siti
Isolamento della rete di un sito	le operazioni del client verranno interrotte fino a quando l'errore non viene risolto, oppure finché la coerenza del bucket non viene ridotta a un sito sicuro o inferiore per garantire il successo delle operazioni, senza tuttavia alcuna perdita di dati	Le operazioni verranno interrotte per il sito isolato, senza alcuna perdita di dati Nessuna interruzione delle operazioni nei siti rimanenti e nessuna perdita di dati

Distribuzione multi-sito multi-grid

Per aggiungere un ulteriore livello di ridondanza, questo scenario prevede l'utilizzo di due cluster StorageGRID e la replica cross-grid per mantenerli sincronizzati. Per questa soluzione ogni cluster StorageGRID avrà tre siti. Saranno utilizzati due siti per lo storage a oggetti e i metadati, mentre il terzo sito sarà utilizzato esclusivamente per i metadati. Entrambi i sistemi verranno configurati con una regola ILM bilanciata per memorizzare in modo sincrono gli oggetti utilizzando l'erasure coding in ciascuno dei due siti di dati. I bucket verranno configurati con il forte modello di coerenza globale v2. Ogni griglia verrà configurata con replica cross-grid bidirezionale su ogni bucket. In questo modo viene eseguita la replica asincrona tra le regioni. In via opzionale, è possibile implementare un bilanciamento del carico globale per gestire le richieste ai gruppi ad alta disponibilità del bilanciatore del carico integrato di entrambi i sistemi StorageGRID per raggiungere un RPO pari a zero.

La soluzione utilizzerà quattro posizioni equamente suddivise in due regioni. La regione 1 conterrà i 2 siti di memorizzazione della griglia 1 come griglia primaria della regione e il sito di metadati della griglia 2. La regione 2 conterrà i 2 siti di memorizzazione della griglia 2 come griglia primaria della regione e il sito di metadati della griglia 1. In ogni regione la stessa posizione può ospitare il sito di archiviazione della griglia primaria della regione e il sito di sola metadati della griglia delle altre regioni. L'utilizzo dei soli nodi di metadati come il terzo sito fornirà la coerenza richiesta per i metadati, non duplicando lo storage degli oggetti in tale posizione.



Questa soluzione con quattro ubicazioni separate offre ridondanza completa di due sistemi StorageGRID separati che mantengono un RPO di 0 e sfrutteranno sia la replica sincrona multi-sito che la replica asincrona multi-grid. È possibile guastare qualsiasi sito mantenendo operazioni client senza interruzioni su entrambi i sistemi StorageGRID.

Questa soluzione prevede quattro copie sottoposte a erasure coding per ciascun oggetto e 18 repliche di tutti i metadati. Ciò consente più scenari di errore senza impatto sulle operazioni dei client. In caso di errore, gli aggiornamenti del ripristino dal black-out verranno sincronizzati automaticamente con il sito/i nodi guasti.

Scenari di guasto multisito e multi-grid

Guasto	**Risultato**
Guasto al disco a nodo singolo	Ogni appliance utilizza gruppi di dischi multipli e può sostenere almeno 1 dischi per gruppo di guasti senza interruzioni o perdita di dati.
Guasto a un singolo nodo in un sito in un grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo nodo in un sito in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto di più nodi in un sito in una griglia	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a più nodi in un sito in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo nodo in più siti in un grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo nodo in più siti in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo sito in una griglia	Nessuna interruzione delle operazioni o perdita di dati.
Guasto a un singolo sito in ciascun grid	Nessuna interruzione delle operazioni o perdita di dati.
Guasti a un singolo sito e a un nodo in un grid	Nessuna interruzione delle operazioni o perdita di dati.
Singolo sito più un nodo da ciascun sito rimanente in un singolo grid	Nessuna interruzione delle operazioni o perdita di dati.
Errore di singola posizione	Nessuna interruzione delle operazioni o perdita di dati.
Errore di singola posizione in ciascuna griglia DC1 e DC3	Le operazioni verranno interrotte fino a quando il guasto non verrà risolto o la coerenza del bucket non verrà ridotta; ogni grid avrà perso 2 siti Tutti i dati sono ancora presenti in 2 postazioni
Errore di singola posizione in ciascuna griglia DC1 e DC4 o DC2 e DC3	Nessuna interruzione delle operazioni o perdita di dati.

Guasto	Risultato
Errore di singola posizione in ciascuna griglia DC2 e DC4	Nessuna interruzione delle operazioni o perdita di dati.
Isolamento della rete di un sito	Le operazioni per il sito isolato verranno interrotte, ma nessun dato andrà perso Nessuna interruzione delle operazioni nei siti rimanenti o perdita di dati.

Conclusione

L'obiettivo di zero recovery point objective (RPO) con StorageGRID è un obiettivo critico per garantire la conservazione e la disponibilità dei dati in caso di guasti del sito. Sfruttando le solide strategie di replica di StorageGRID, tra cui la replica sincrona multisito e la replica asincrona multi-grid, le organizzazioni possono mantenere operazioni ininterrotte dei client e garantire la coerenza dei dati in più posizioni. L'implementazione delle policy ILM (Information Lifecycle Management) e l'utilizzo di nodi basati solo sui metadati migliorano ulteriormente la resilienza e le prestazioni del sistema. Con StorageGRID, le aziende possono gestire con sicurezza i propri dati, sapendo che rimangono accessibili e coerenti anche in caso di complessi scenari di guasto. Questo approccio completo alla gestione e alla replica dei dati sottolinea l'importanza di una pianificazione e di un'esecuzione meticolose per il raggiungimento di un RPO pari a zero e la salvaguardia di informazioni preziose.

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 NetApp StorageGRID con il servizio Amazon OpenSearch o Elasticsearch on-premise.

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.

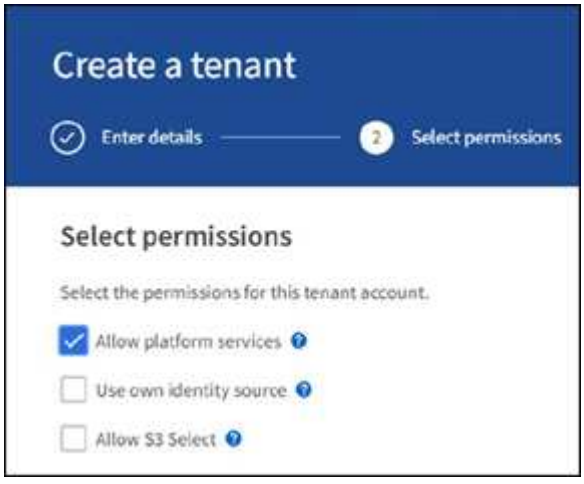
I servizi della piattaforma vengono configurati dal tenant S3 tramite l'interfaccia utente di Tenant Manager. Per ulteriori informazioni, vedere "Considerazioni sull'utilizzo dei servizi della piattaforma".

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

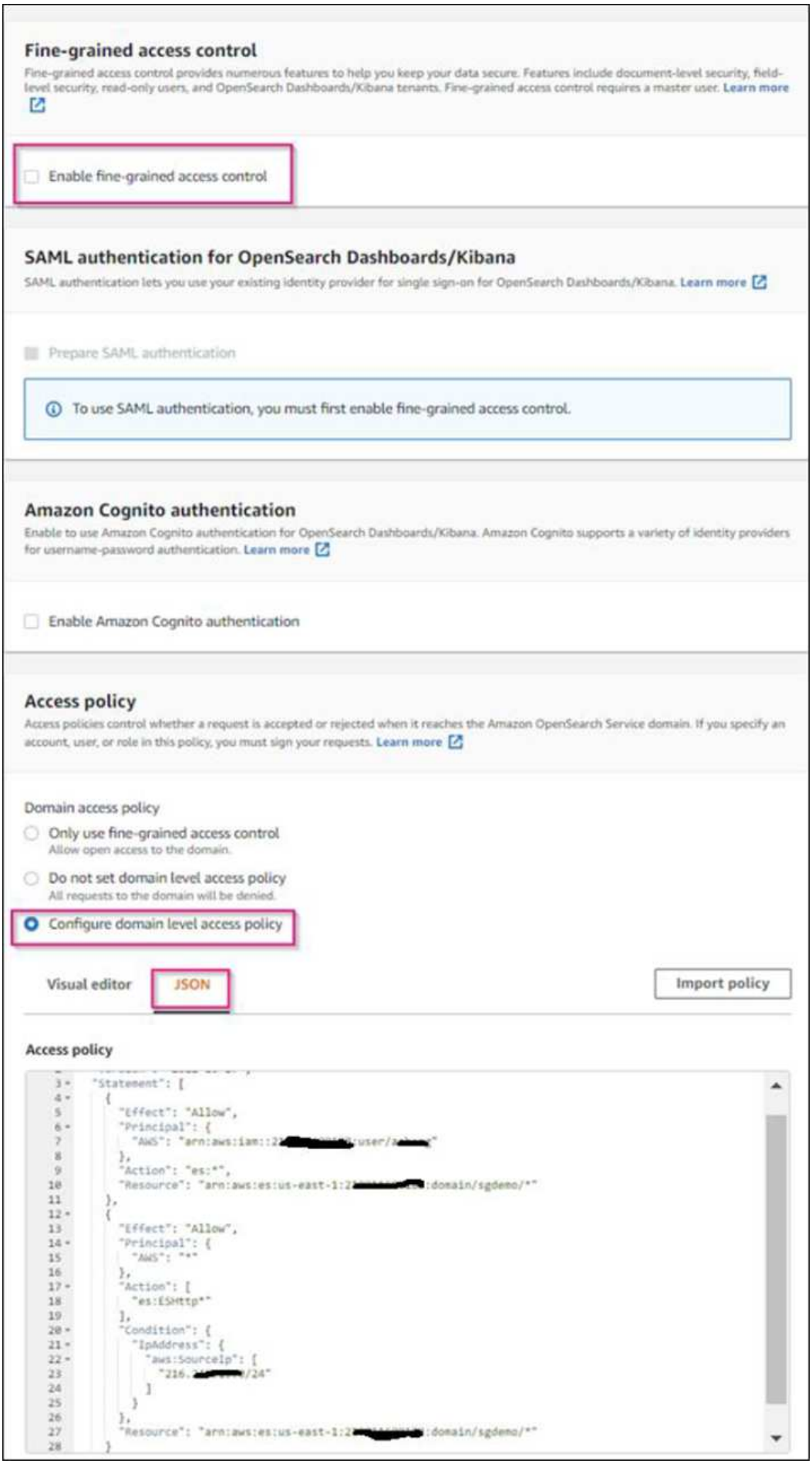
Configurazione del servizio Amazon OpenSearch (precedentemente chiamato Elasticsearch)

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.

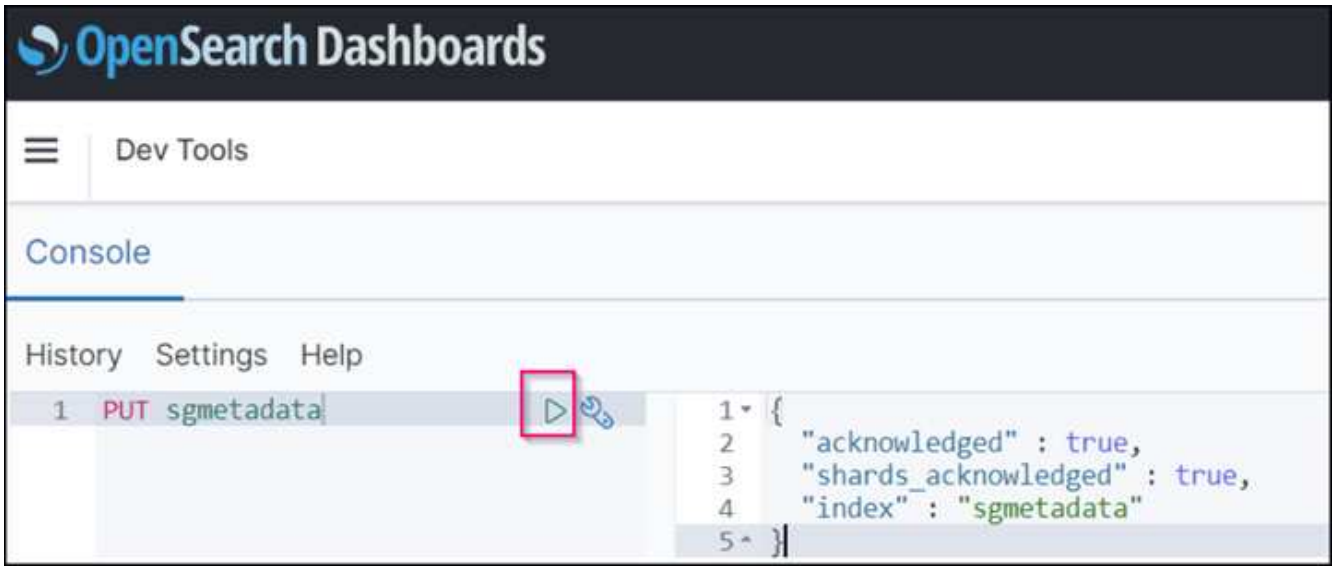
1. Creare un nuovo dominio utilizzando le istruzioni fornite da "Guida introduttiva al servizio AWS OpenSearch", ad eccezione di:
   - Fase 4. Nome di dominio: Sgdemo
   - Fase 10. Controllo degli accessi dettagliato: Deselezionare l'opzione Enable fine-Grained Access Control (attiva controllo degli 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/*"
        }
    ]
}
```

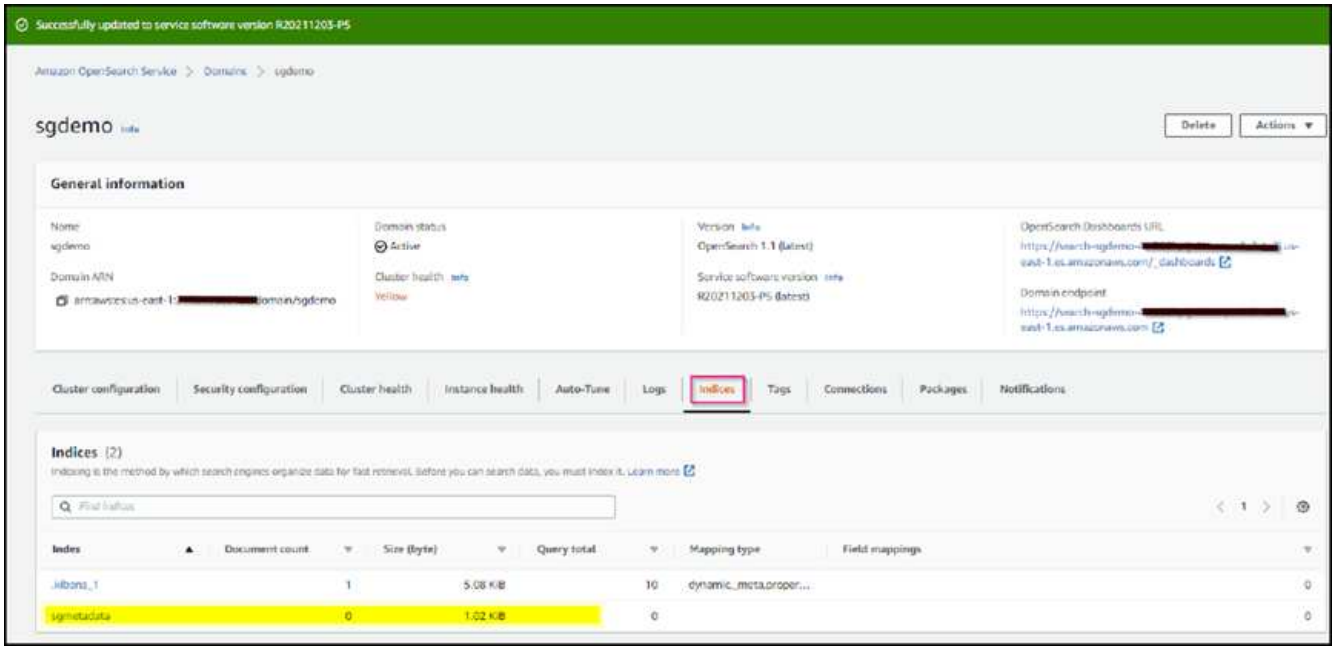

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more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



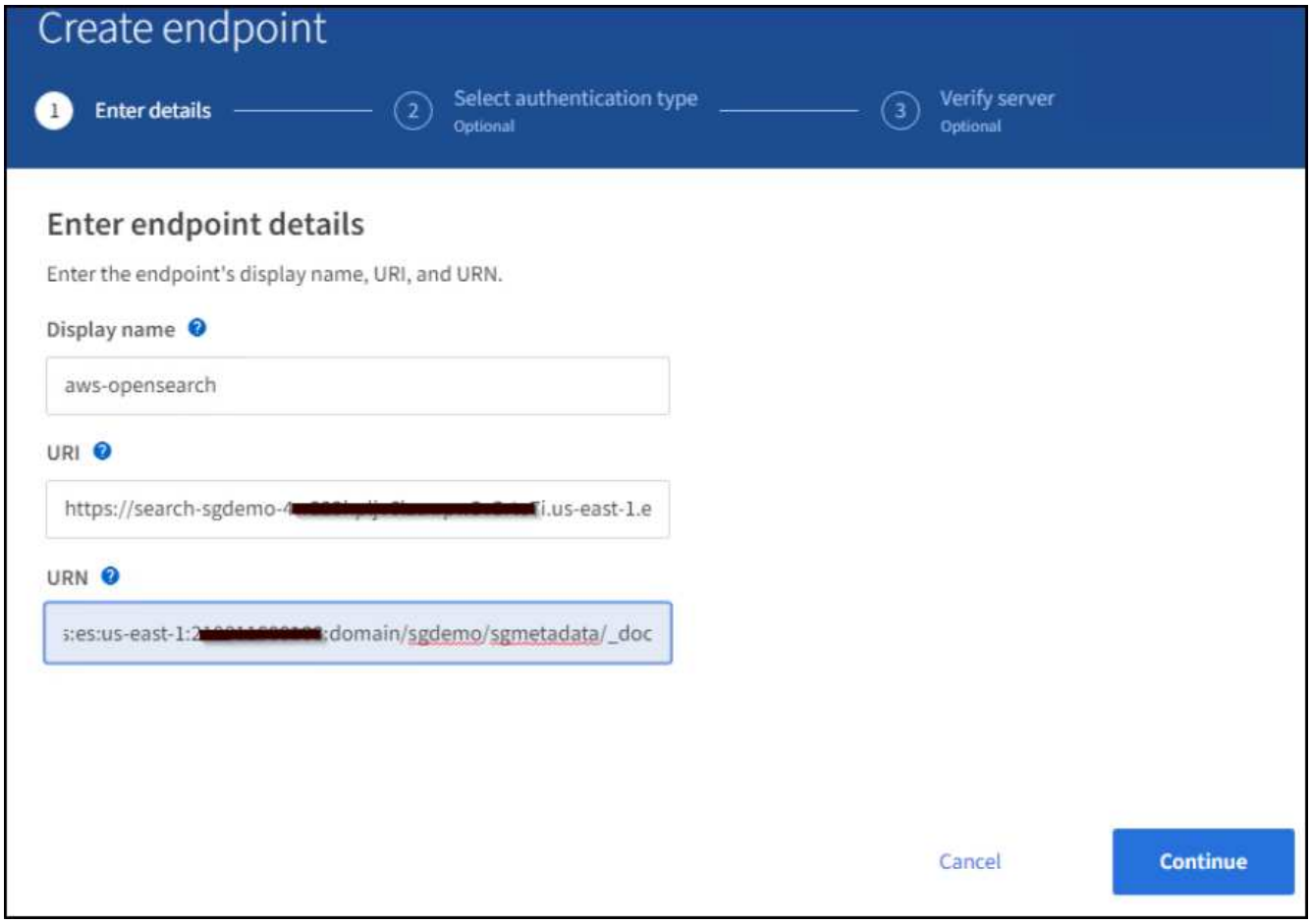
Configurazione degli endpoint dei servizi della piattaforma

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

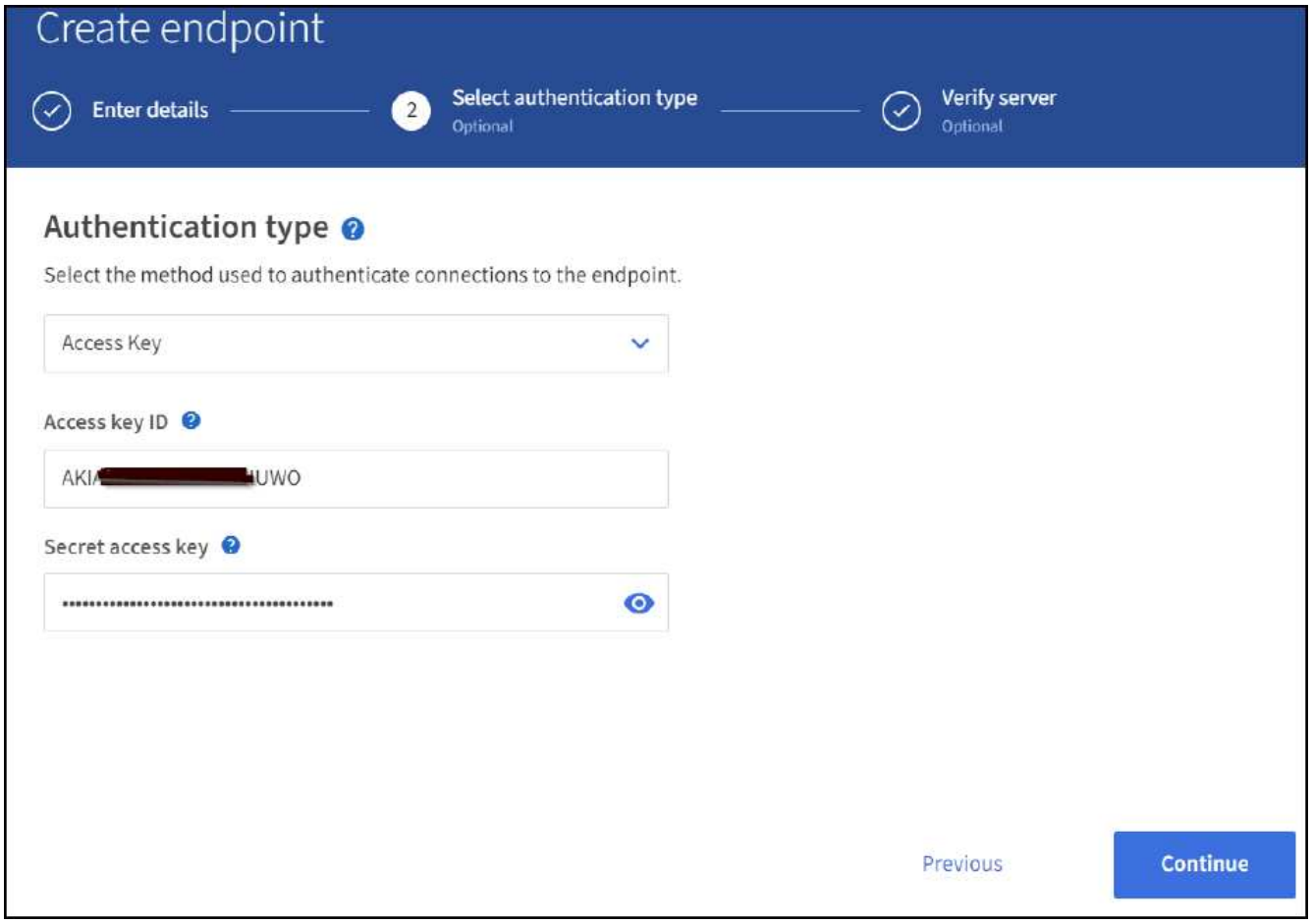
1. In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint.
2. Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):

   - 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.

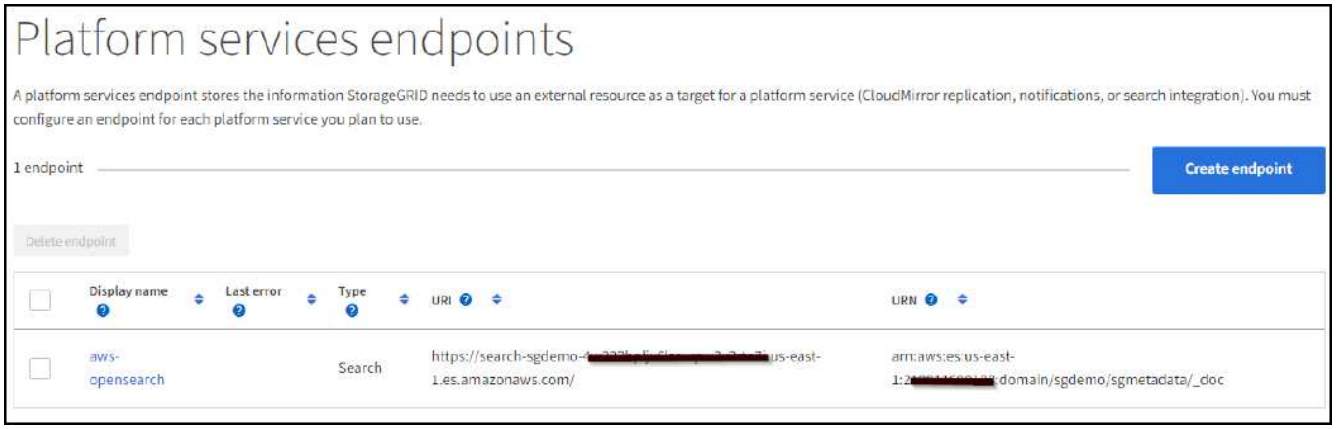
     In questo esempio, URN diventa `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.



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.

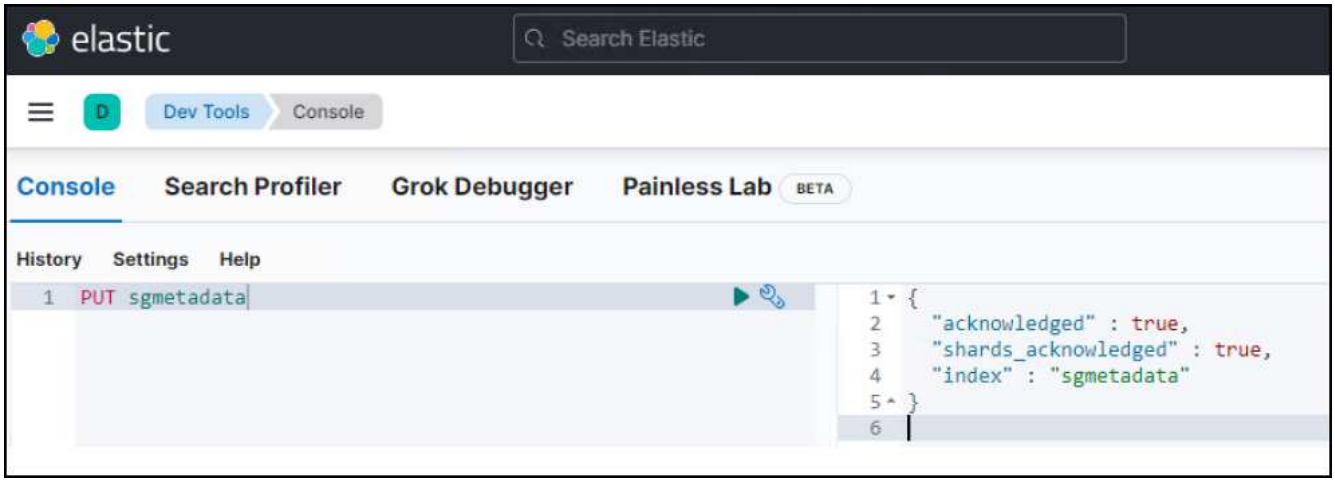
1. In a new terminal session, run:

```
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.

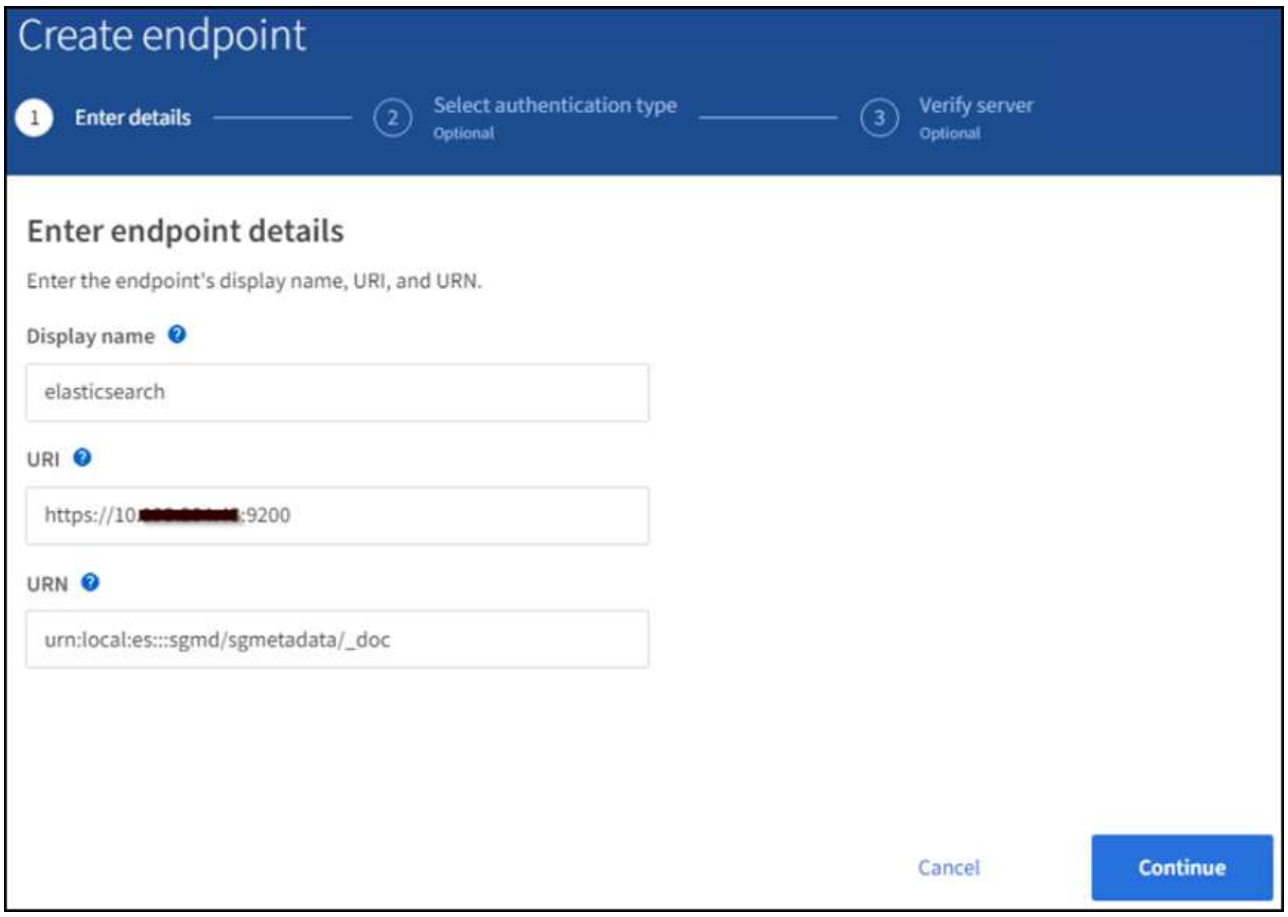
3. Una volta avviato il container Kibana docker, viene visualizzato il link URL `https://0.0.0.0:5601` viene visualizzato nella console. Sostituire 0.0.0.0 con l'indirizzo IP del server nell'URL.
4. Accedere all'interfaccia utente di Kibana utilizzando il nome utente `elastic` E la password generata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



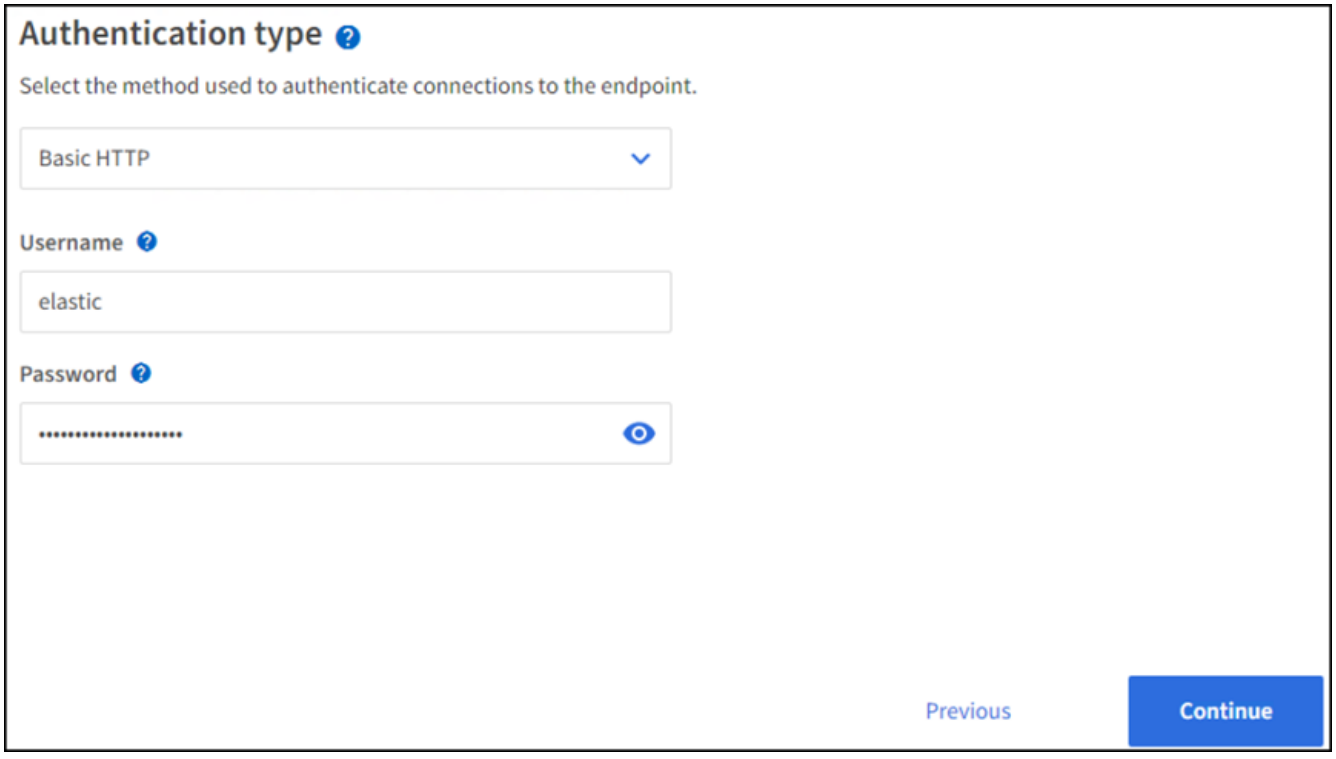
Configurazione degli endpoint dei servizi della piattaforma

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

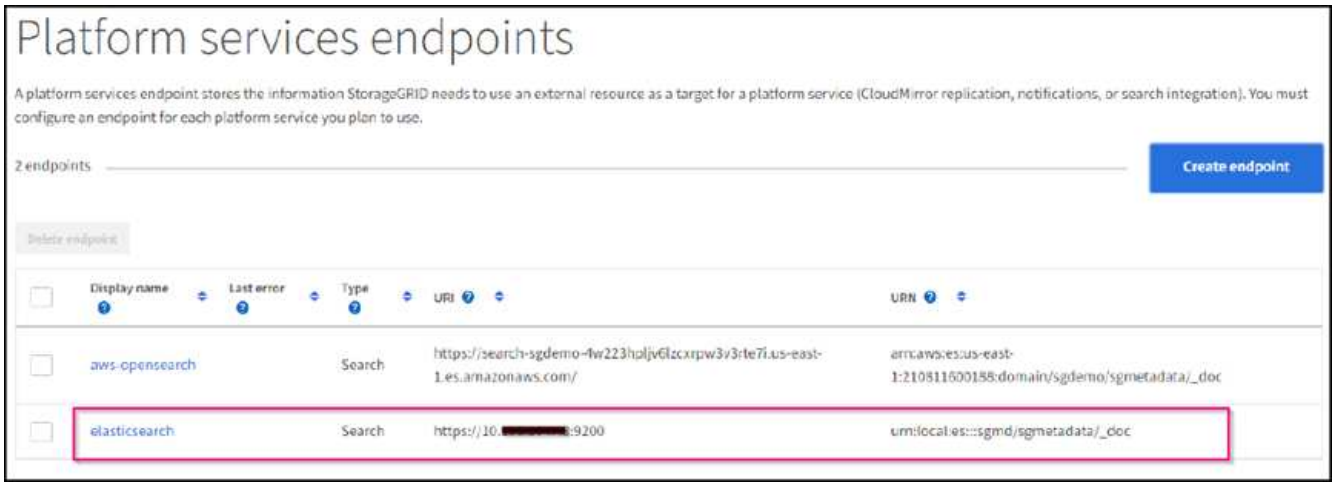
1. In Tenant Manager, andare a STORAGE(S3) > Platform Services Endpoint
2. Fare clic su Create Endpoint (Crea endpoint), immettere quanto segue, quindi fare clic su Continue (continua):
   - Esempio di nome visualizzato: `elasticsearch`
   - URI: `https://<elasticsearch-server-ip or hostname>:9200`
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

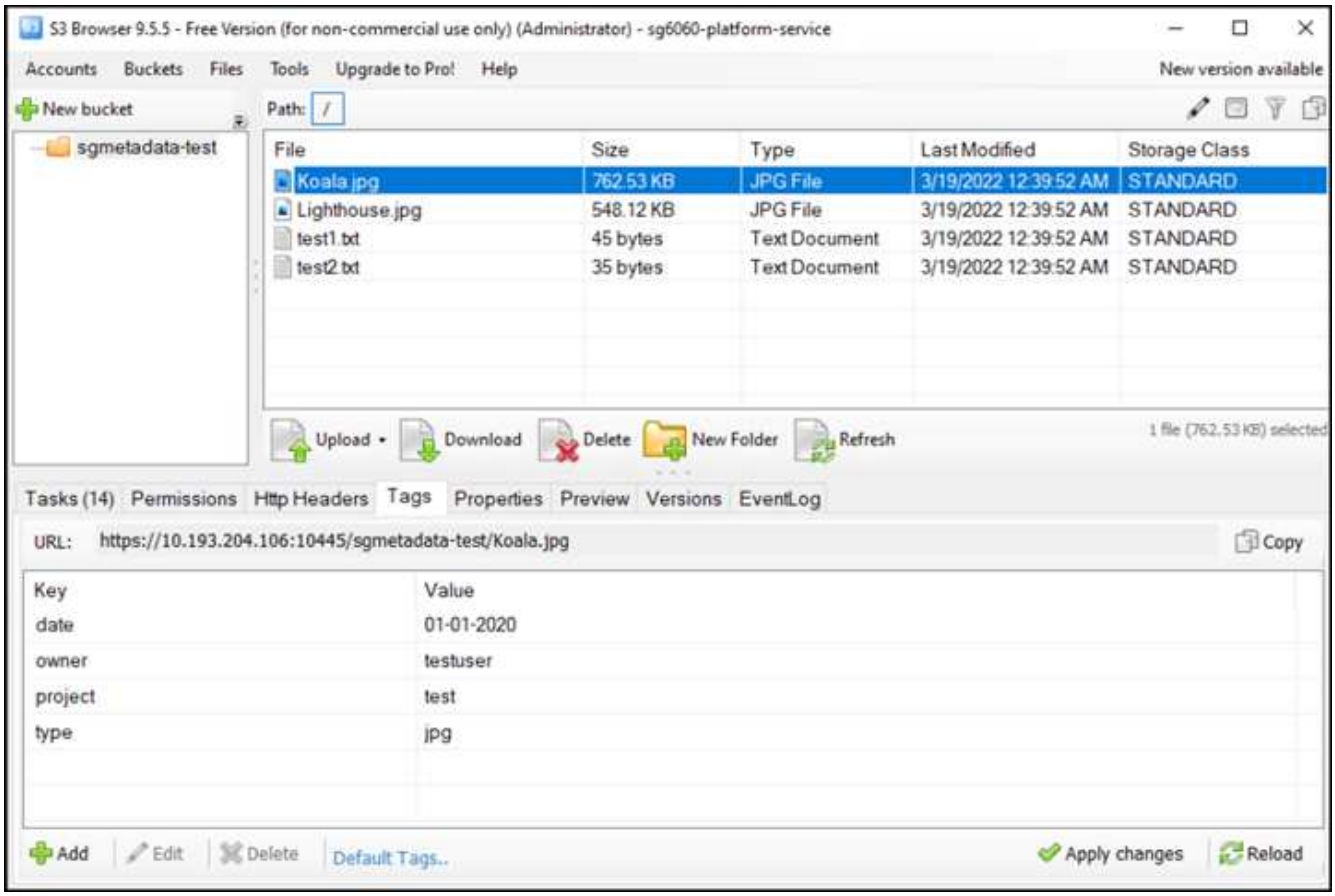
1. In Tenant Manager, andare a STORAGE(S3) > Bucket
2. Fare clic su Create bucket (Crea bucket), inserire il nome del bucket (ad esempio, `sgmetadata-test`) e accettare l'impostazione predefinita `us-east-1` regione.
3. Fare clic su continua > Crea bucket.
4. Per visualizzare la pagina Panoramica del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



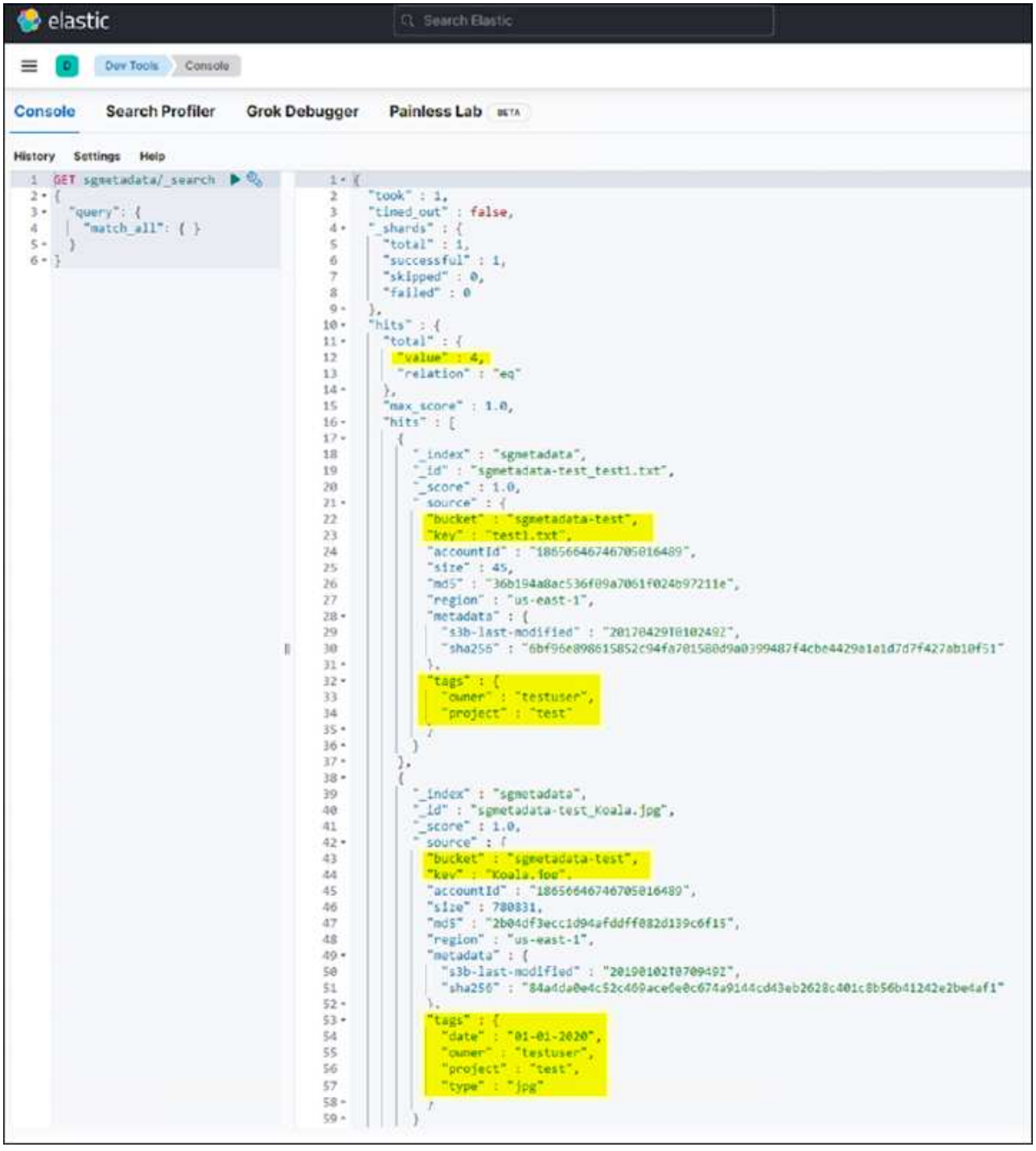
7. Utilizzare l'interfaccia utente di Kibana per verificare che i metadati dell'oggetto siano stati caricati nell'indice di sgmetadata.

   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.

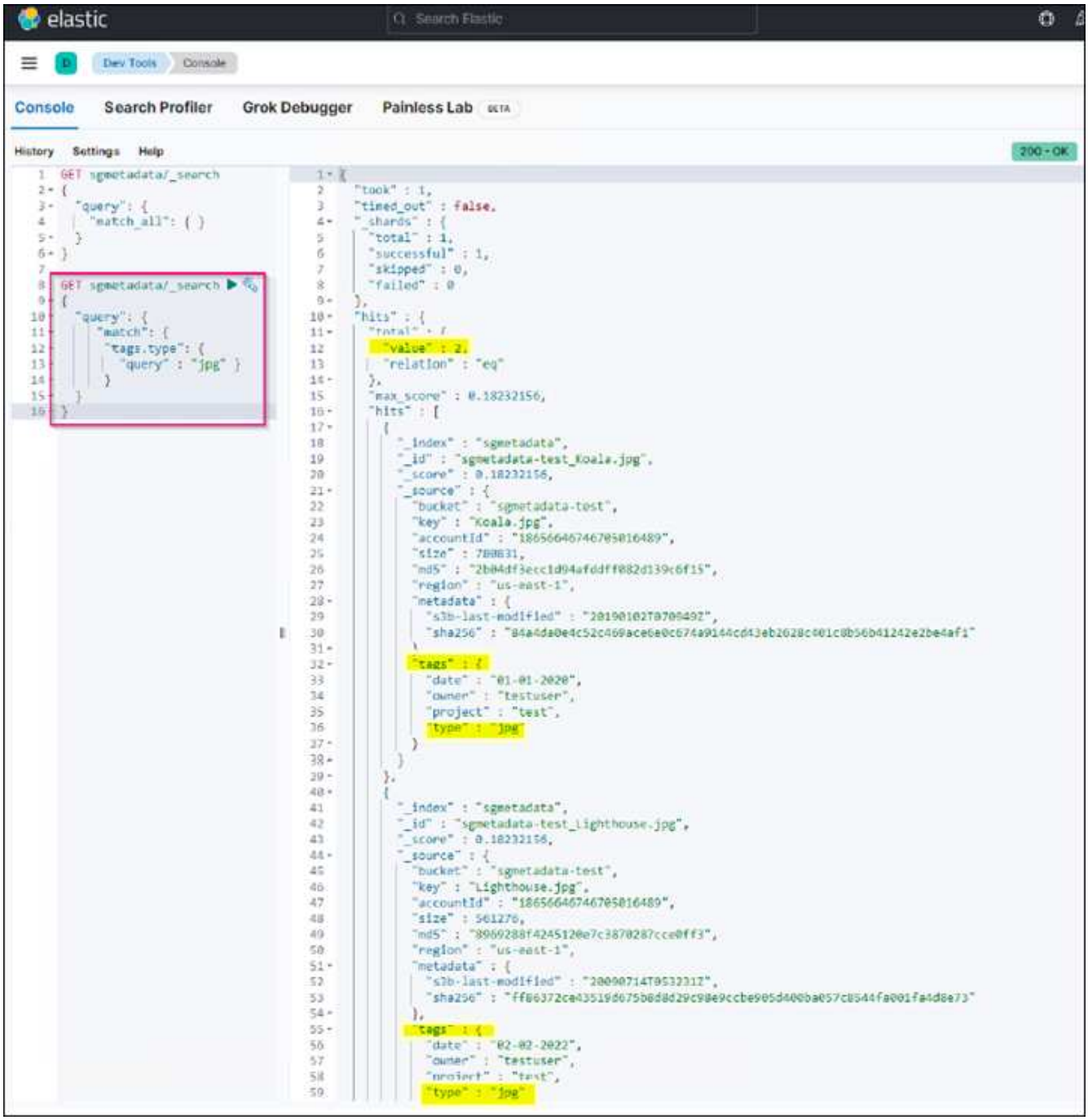
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



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.
- 11,8 e soffietto: Un nodo 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.
  - 11,9: Il limite di 15 giorni è stato rimosso.
- Per un SG6060 o SG6160 con shelf di espansione, è necessario aggiungere al tempo dell'appliance di base il tempo necessario per le dimensioni corrette dello shelf, per ottenere l'intera durata 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/SG5712/SG5812 → 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	Dimensioni dell'unità 22 TB
10 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni	5.5 giorni
25 GB	1 giorno	2 giorni	2.5 giorni	3 giorni	4 giorni	4.5 giorni	5.5 giorni

SG5660 → SG5760/SG5860

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	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	**13,5 giorni**	**15,5 giorni**	**18,5 giorni**
25 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	**13,5 giorni**	**15,5 giorni**	**18,5 giorni**

SG5660 → SG6060/SG6160

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	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	9 giorni	10 giorni	**12 giorni**
25 GB	2 giorni	4 giorni	5 giorni	6 giorni	8 giorni	9 giorni	10 giorni

SG5760/SG5860 → SG5760/SG5860

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	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	**13,5 giorni**	**15,5 giorni**	**18,5 giorni**
25 GB	3.5 giorni	7 giorni	8.5 giorni	10.5 giorni	**13,5 giorni**	**15,5 giorni**	**18,5 giorni**

SG5760/SG5860 → SG6060/SG6160

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	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	9 giorni	10 giorni	**12 giorni**
25 GB	2 giorni	3.5 giorni	4.5 giorni	5.5 giorni	7 giorni	8 giorni	9.5 giorni

SG6060/SG6160 → SG6060/SG6160

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	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	4.5 giorni	5.5 giorni	6.5 giorni	8.5 giorni	9.5 giorni	11.5 giorni
25 GB	2 giorni	3 giorni	4 giorni	4.5 giorni	6 giorni	7 giorni	8.5 giorni

DDP16

SG5760/SG5860 → SG5760/SG5860

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	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	6.5 giorni	8 giorni	9.5 giorni	**12,5 giorni**	**14 giorni**	**17 giorni**
25 GB	3.5 giorni	6.5 giorni	8 giorni	9.5 giorni	**12,5 giorni**	**14 giorni**	**17 giorni**

SG5760/SG5860 → SG6060/SG6160

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	Dimensioni dell'unità 22 TB
10 GB	2.5 giorni	5 giorni	6 giorni	7.5 giorni	10 giorni	11 giorni	**13 giorni**
25 GB	2 giorni	3.5 giorni	4 giorni	5 giorni	6.5 giorni	7 giorni	8.5 giorni

SG6060/SG6160 → SG6060/SG6160

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	Dimensioni dell'unità 22 TB
10 GB	3 giorni	5 giorni	6 giorni	7 giorni	9.5 giorni	10.5 giorni	**13 giorni**
25 GB	2 giorni	3.5 giorni	4.5 giorni	5 giorni	7 giorni	7.5 giorni	9 giorni

Shelf di espansione (aggiunta a oltre SG6060 TB/SG6160 TB 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	Dimensioni dell'unità 22 TB
10 GB	3.5 giorni	5 giorni	6 giorni	7 giorni	9.5 giorni	10.5 giorni	**12 giorni**
25 GB	2 giorni	3 giorni	4 giorni	4.5 giorni	6 giorni	7 giorni	8.5 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

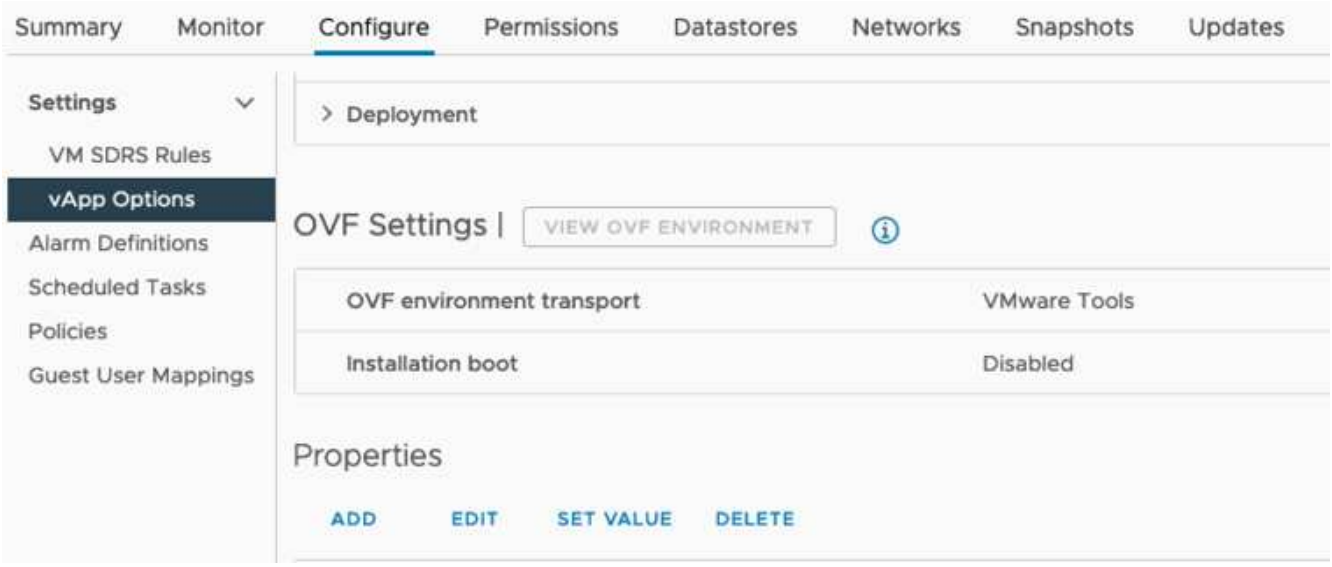
Per distruggere il primo nodo gateway, attenersi alla seguente procedura:

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.

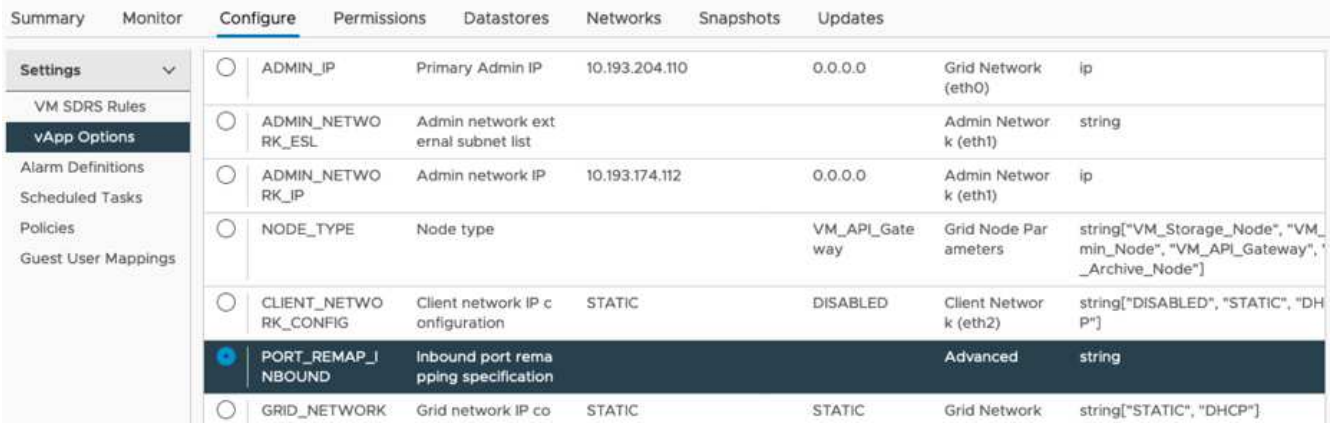
Implementare il nodo gateway sostitutivo

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

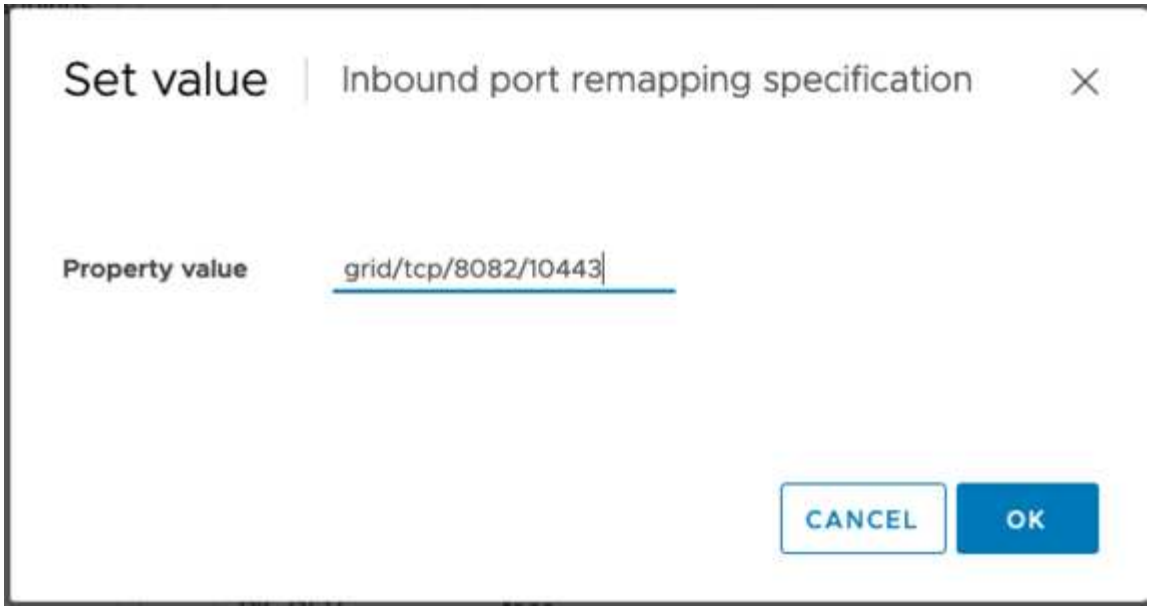


4. Scorrere fino all'inizio dell'elenco Proprietà e fare clic su Modifica

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.

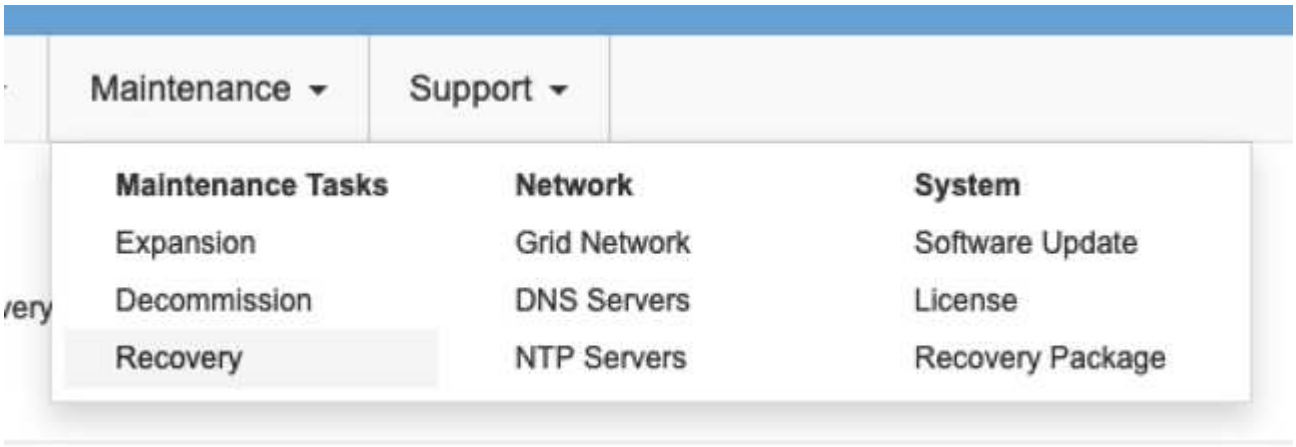


8. Se si utilizzano più reti, utilizzare una virgola (,) per separare le stringhe di rete, ad esempio Grid/tcp/8082/10443,admin/tcp/8082/10443,client/tcp/8082/10443

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`

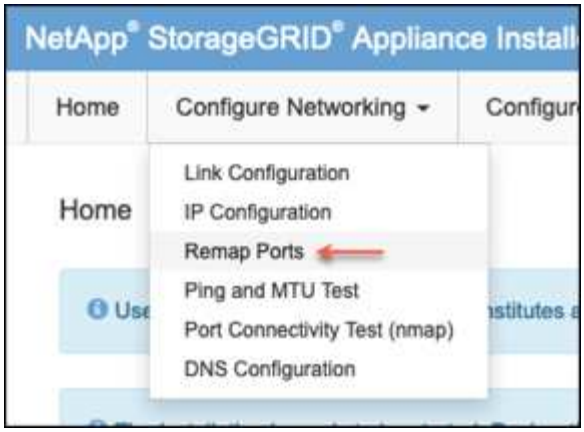
Ricostruire il nodo Admin

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`

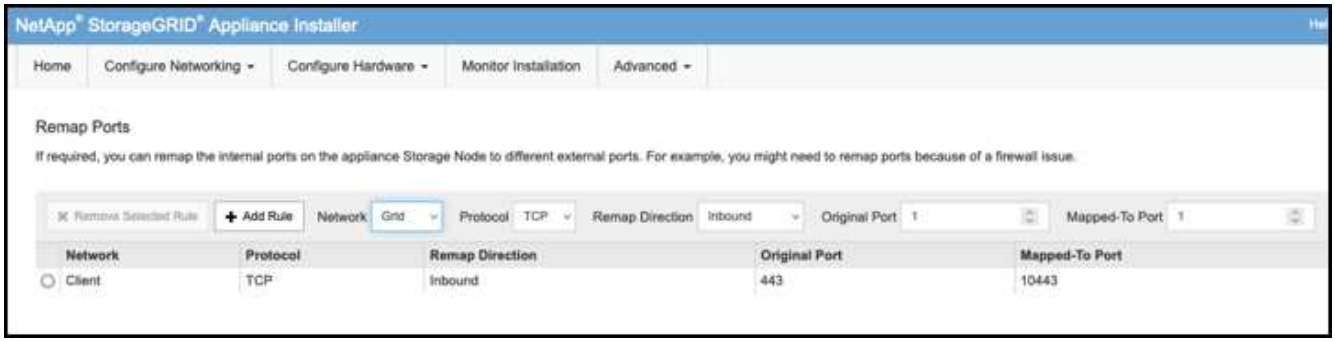
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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.

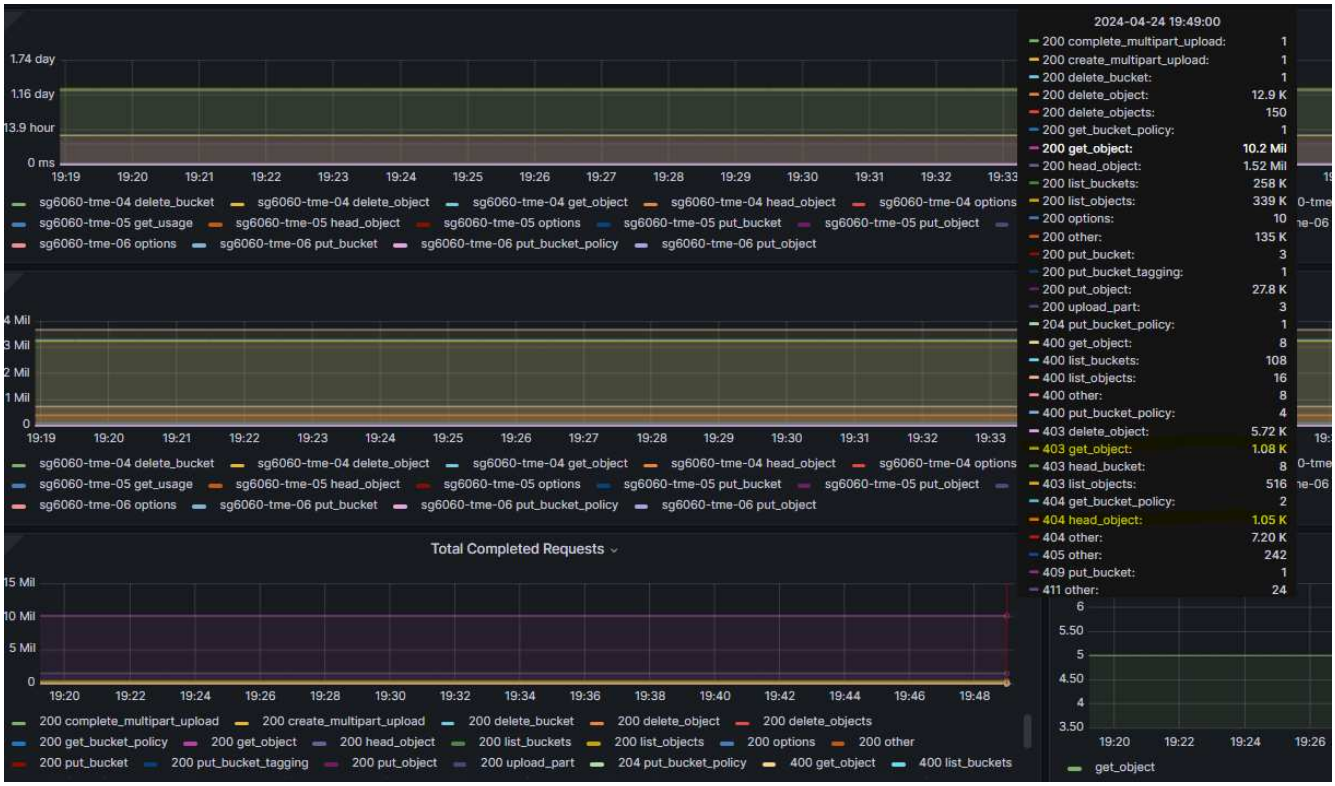
Se è necessario modificare la rete Grid di tutta la griglia, vedere "Modificare gli indirizzi IP per tutti i nodi nella griglia".

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
```

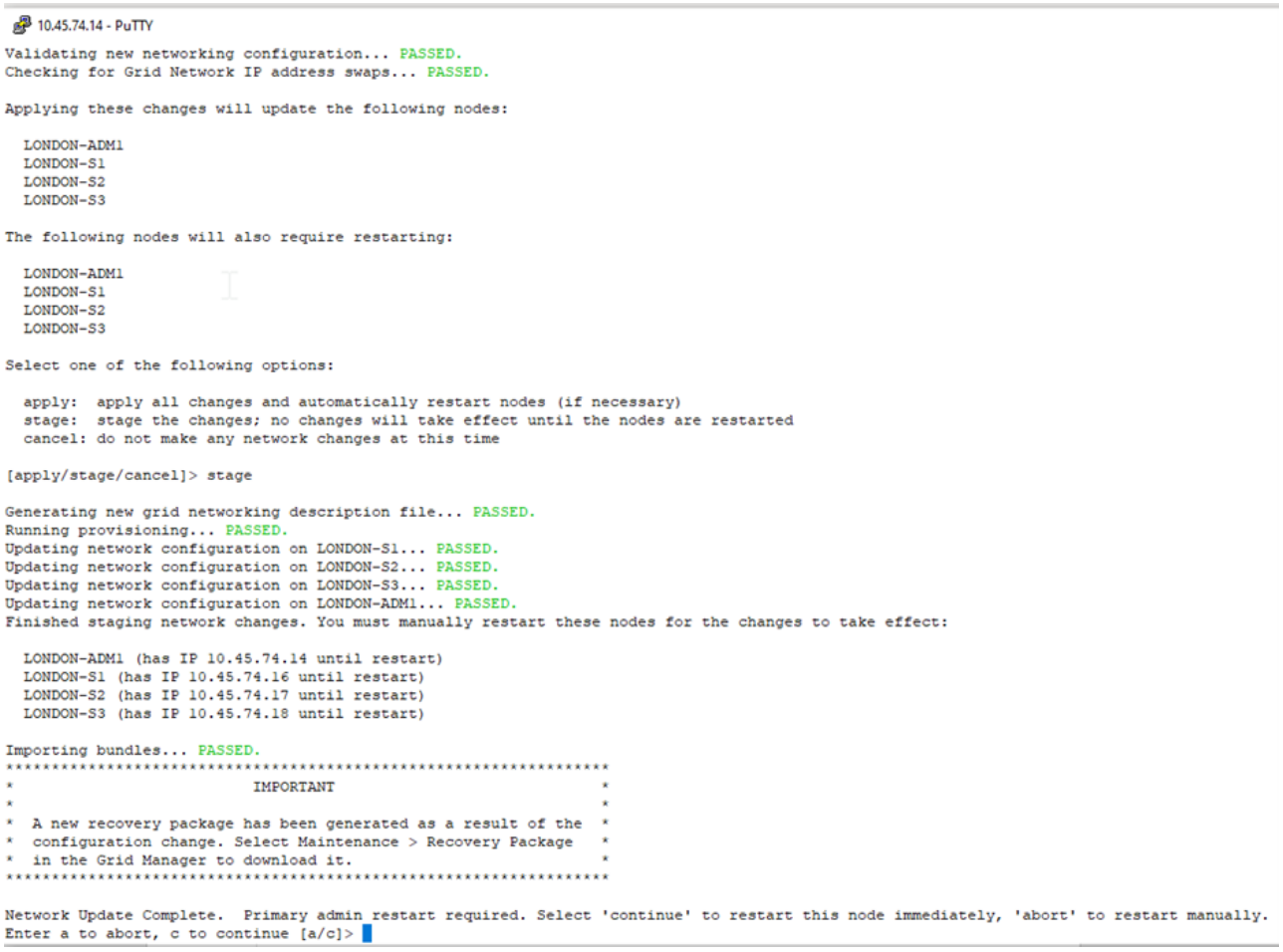
c. selezionare 10 per convalidare e applicare la modifica.

```
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
```

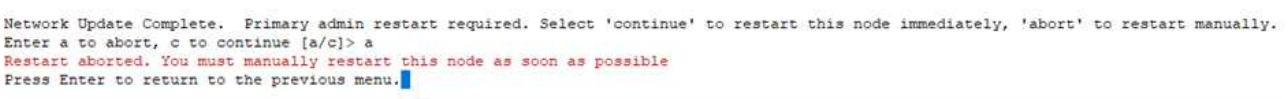
d. In questa fase è necessario selezionare **fase**.

```
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.

Migrazione dello storage a oggetti da ONTAP S3 a StorageGRID

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Demo sulla migrazione

Questa è una dimostrazione sulla migrazione di utenti e bucket da ONTAP S3 a StorageGRID.

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

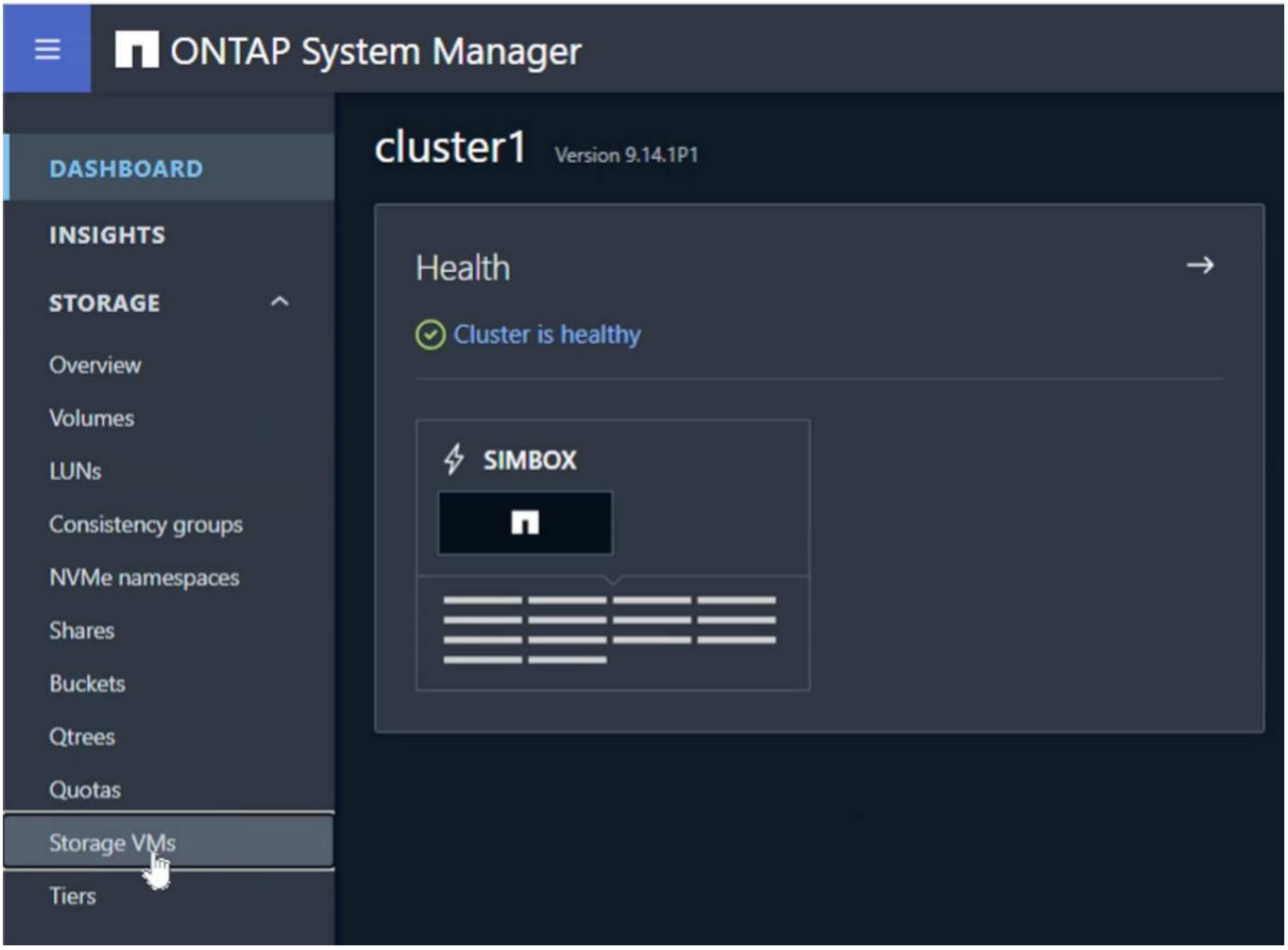
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Preparazione di ONTAP

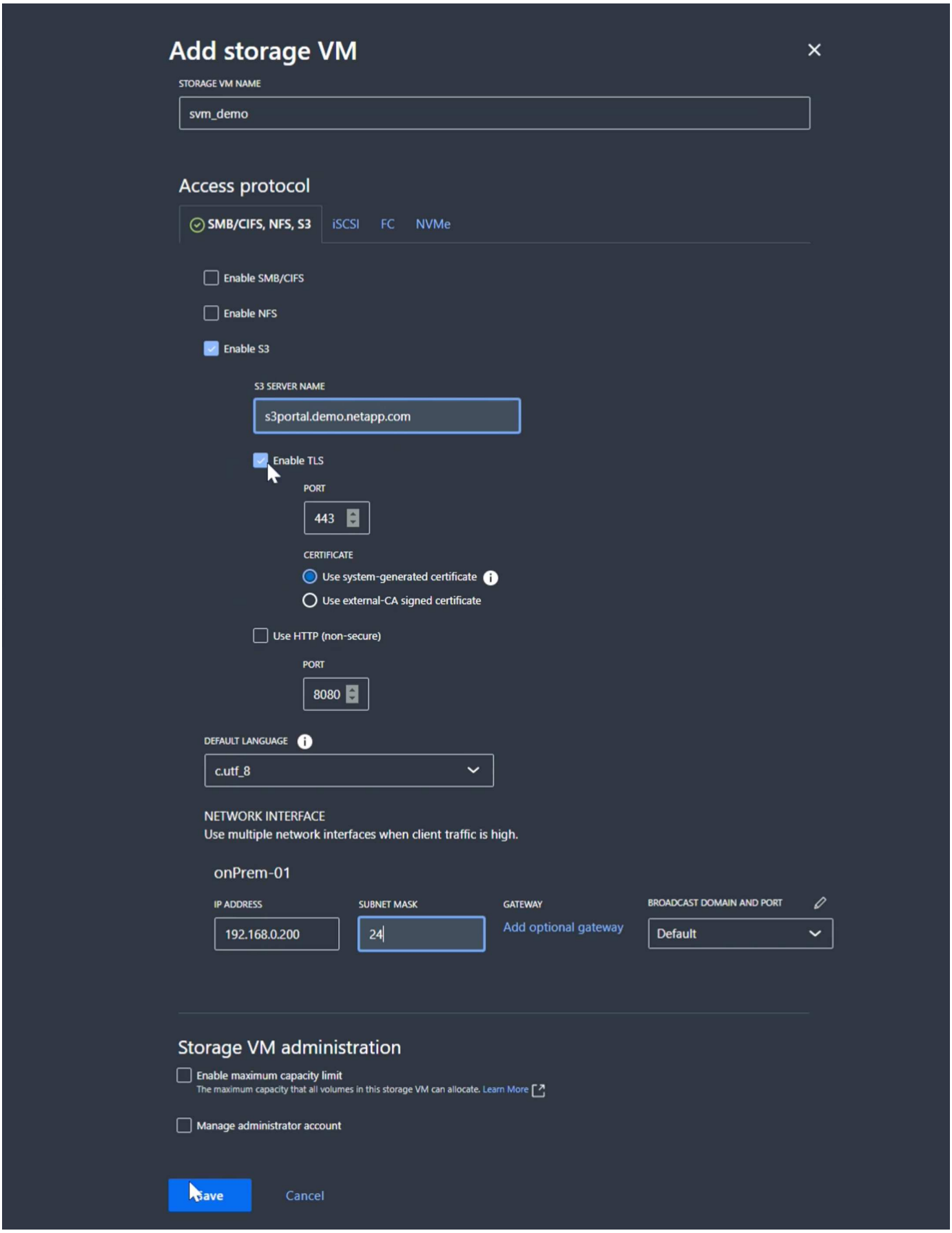
A scopo dimostrativo creeremo un server per archivio di oggetti SVM, un utente, un gruppo, una policy di gruppo e bucket.

Creare la Storage Virtual Machine

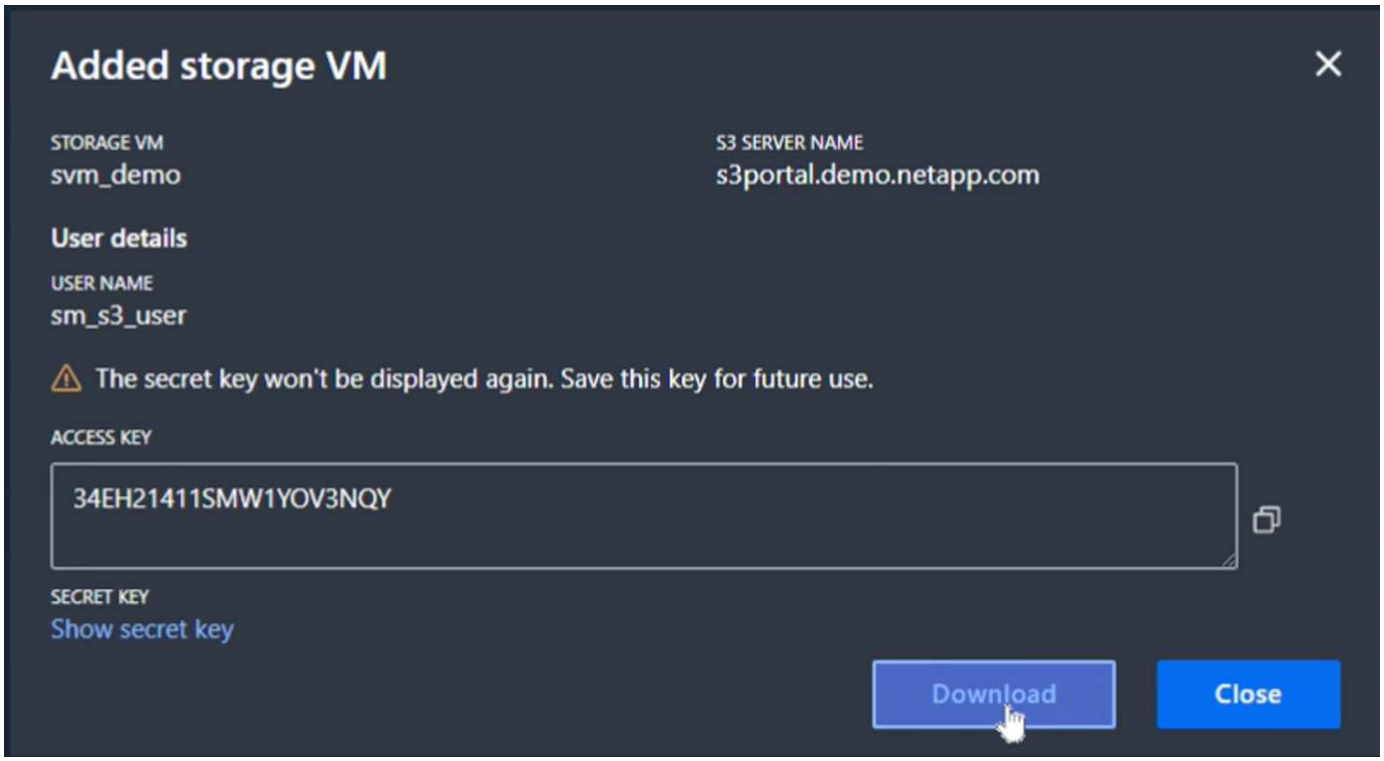
In Gestione sistema di ONTAP, accedere alle VM di archiviazione e aggiungere una nuova VM di archiviazione.



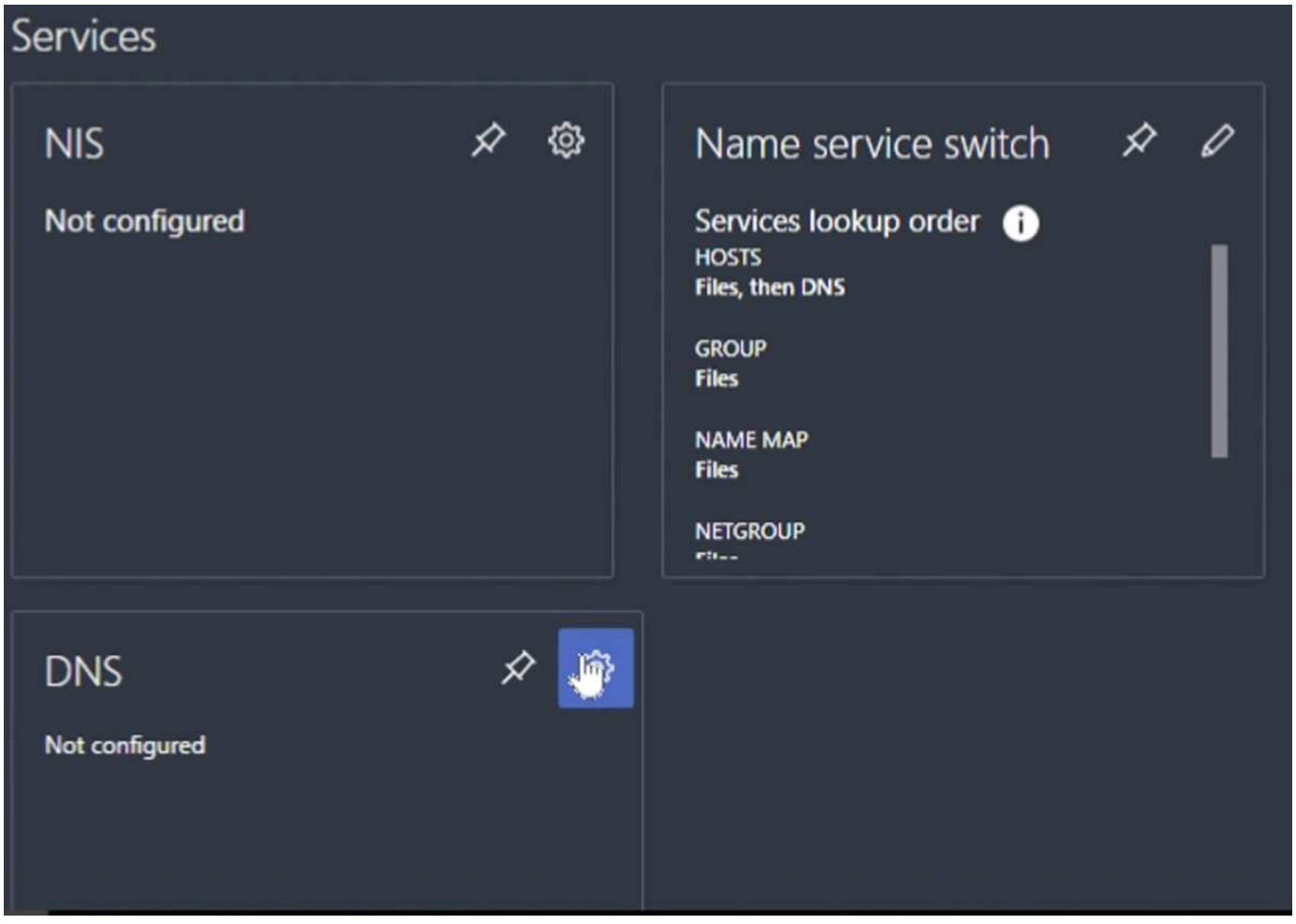
Selezionare le caselle di controllo "Enable" (attiva S3) e "Enable TLS" (attiva TLS) e configurare le porte HTTP(S). Definire l'IP, la subnet mask e definire il gateway e il dominio di broadcast se non si utilizza l'impostazione predefinita o obbligatoria nell'ambiente in uso.



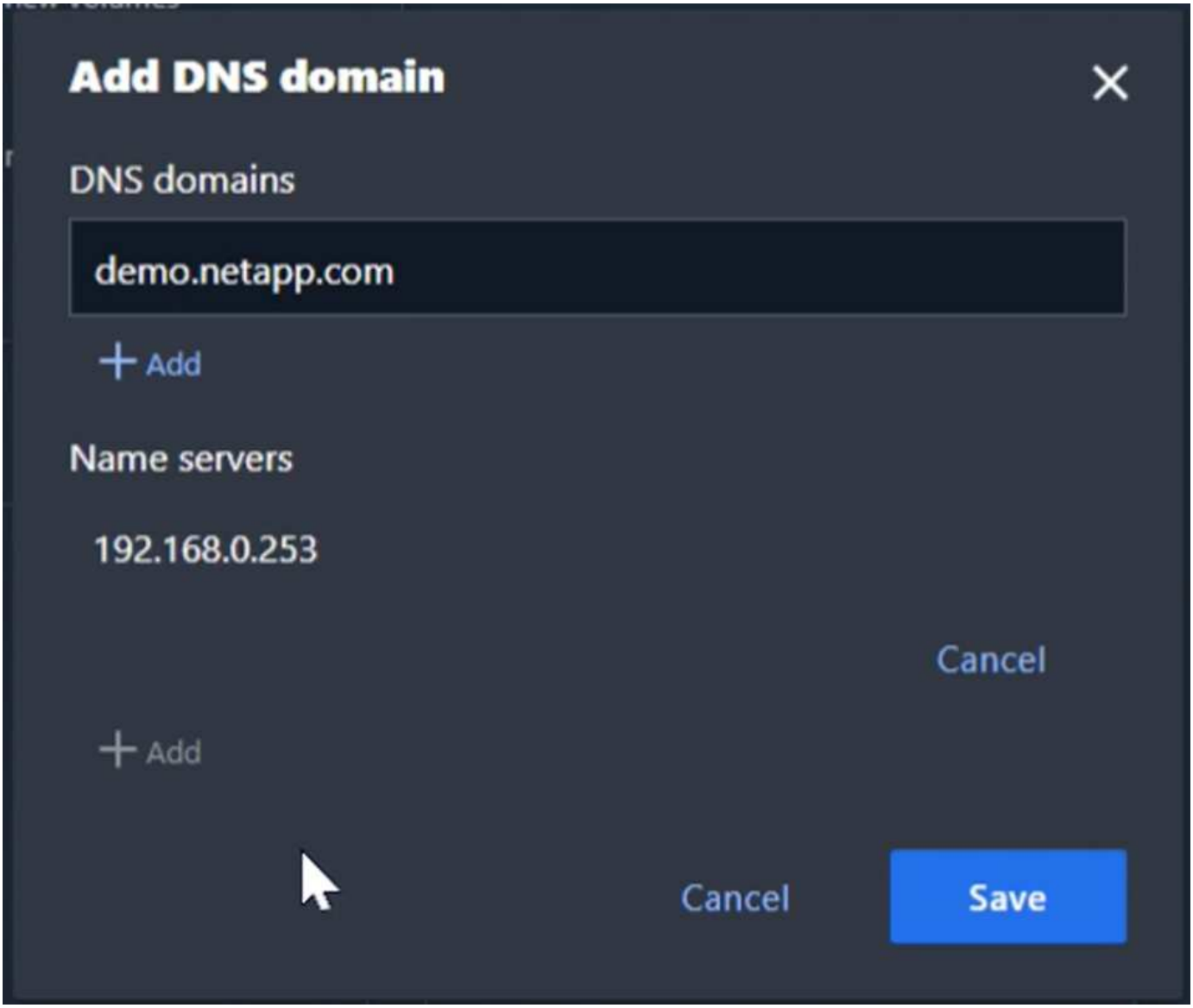
Durante la creazione della SVM verrà creato un utente. Scaricare i S3 tasti per questo utente e chiudere la finestra.



Una volta creata la SVM, edita la SVM e Aggiungi le impostazioni DNS.

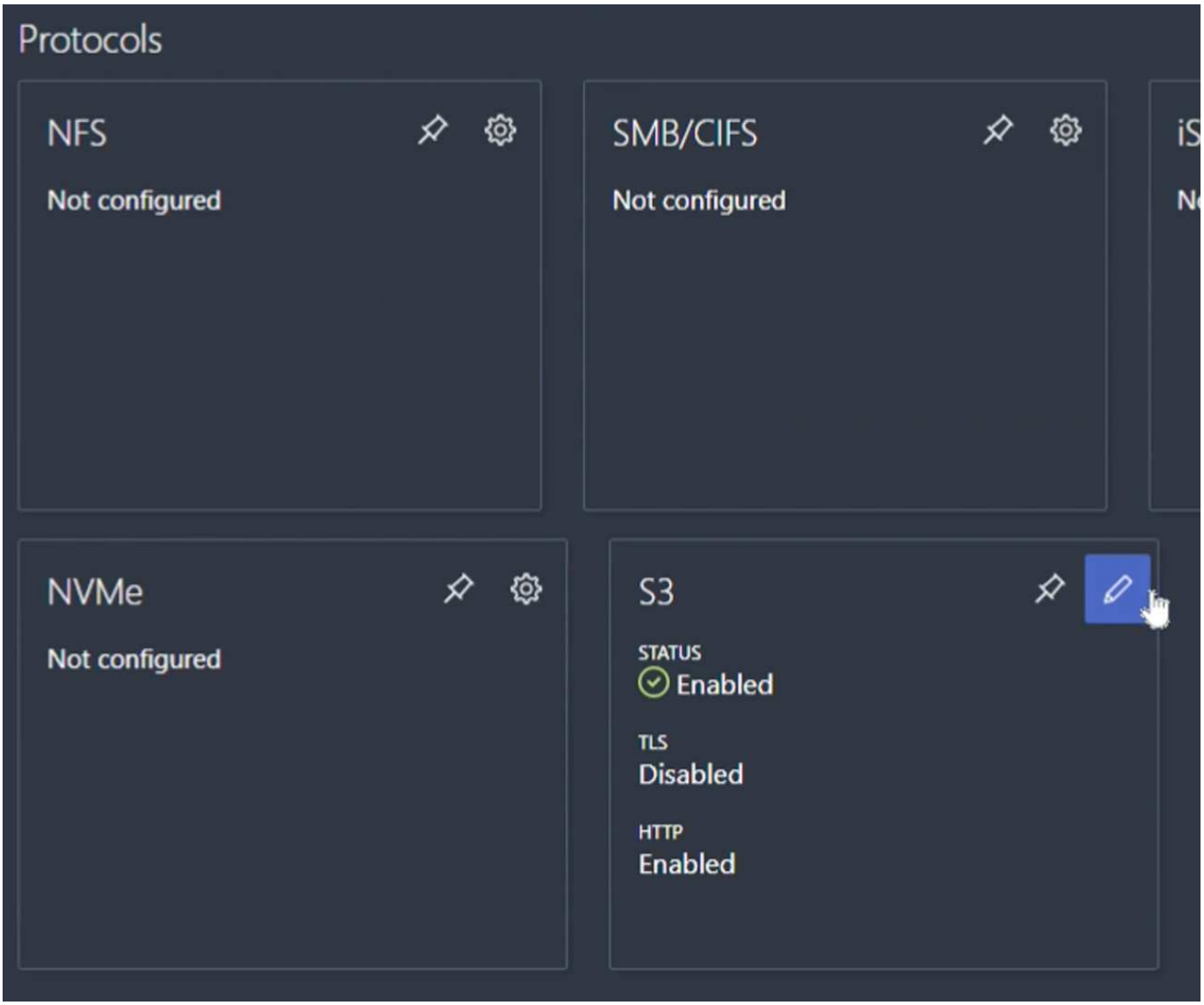


Definire il nome DNS e l'IP.

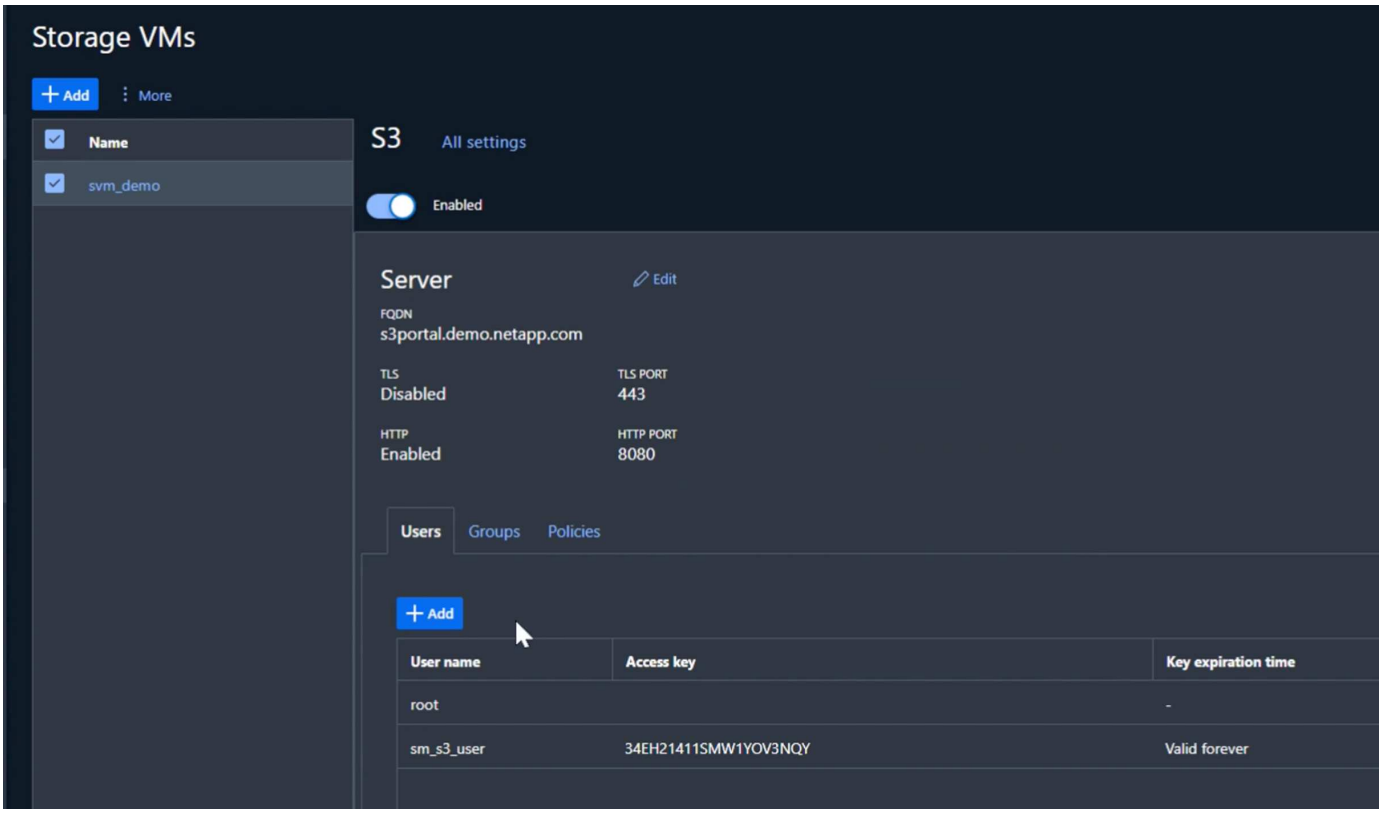


Creare un utente SVM S3

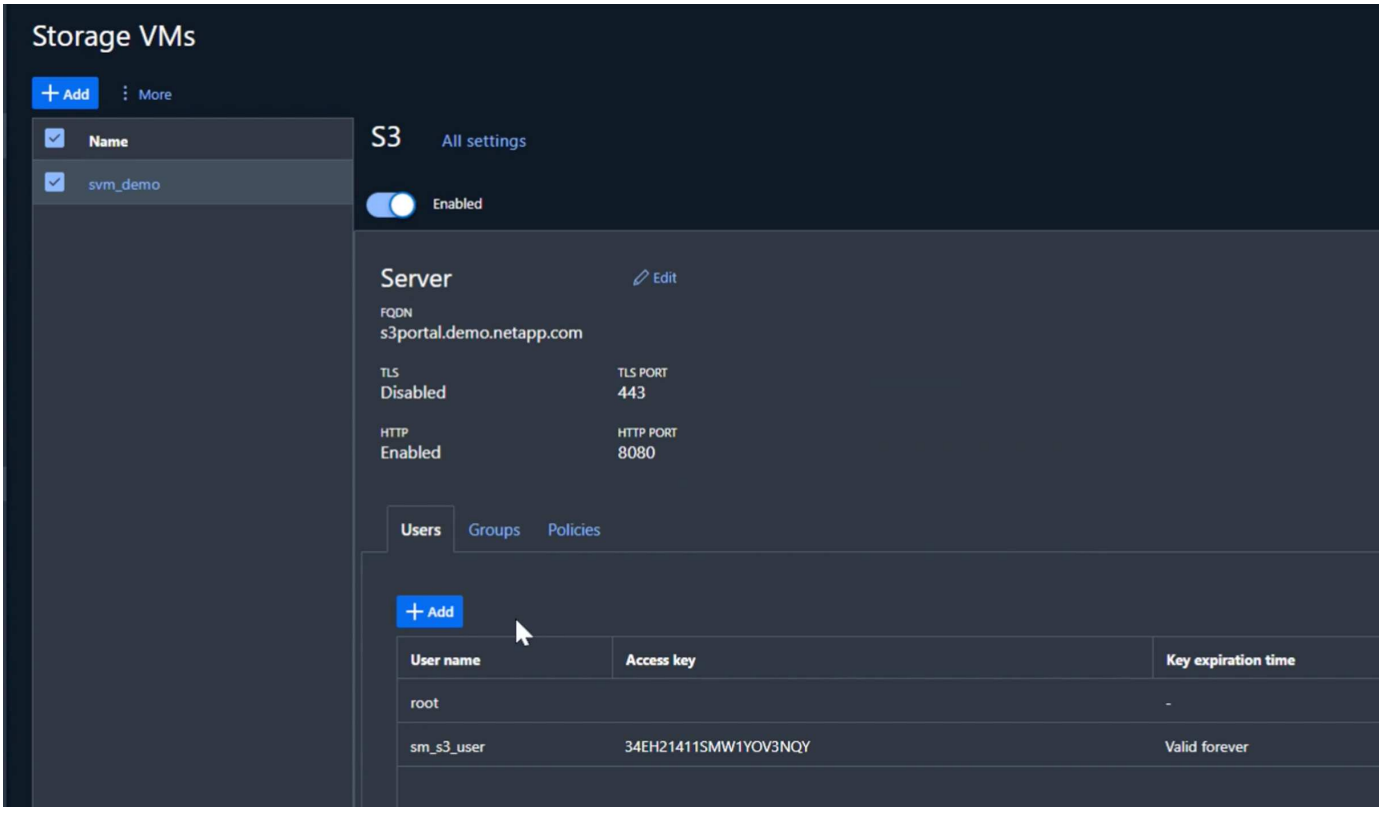
Ora possiamo configurare i S3 utenti e il gruppo. Modificare le impostazioni S3.



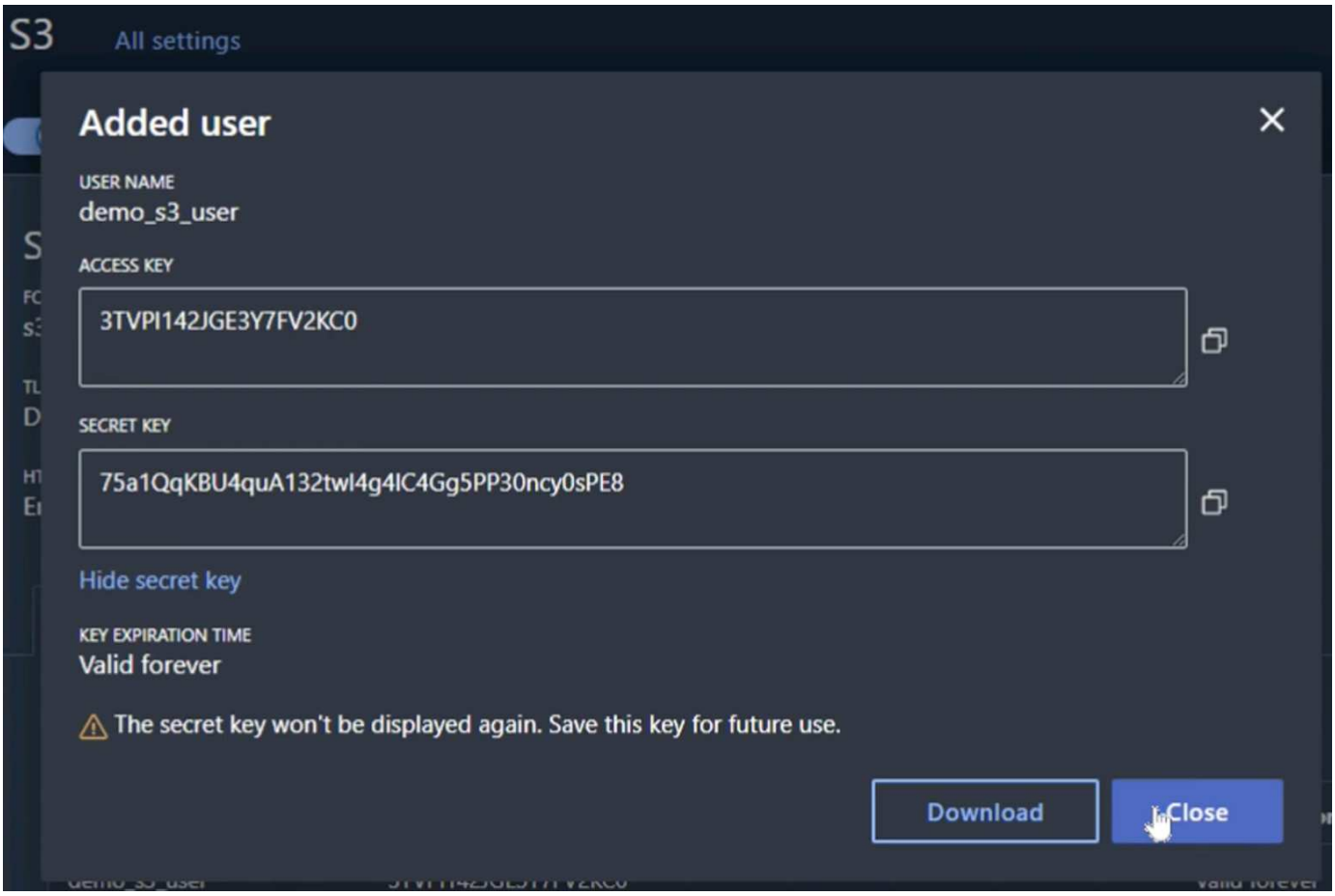
Aggiungere un nuovo utente.



Inserire il nome utente e la scadenza della chiave.

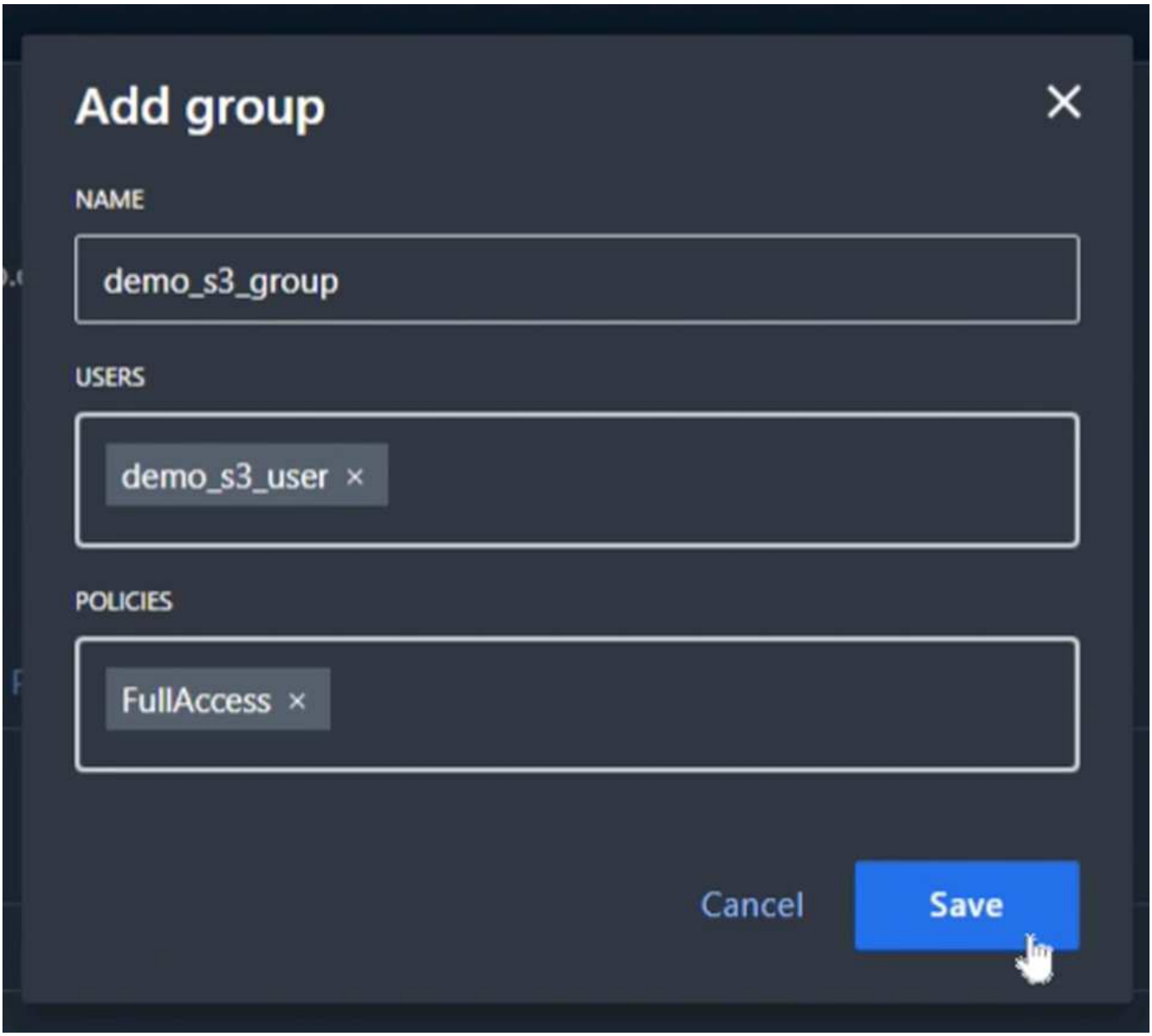


Scaricare i S3 tasti per il nuovo utente.



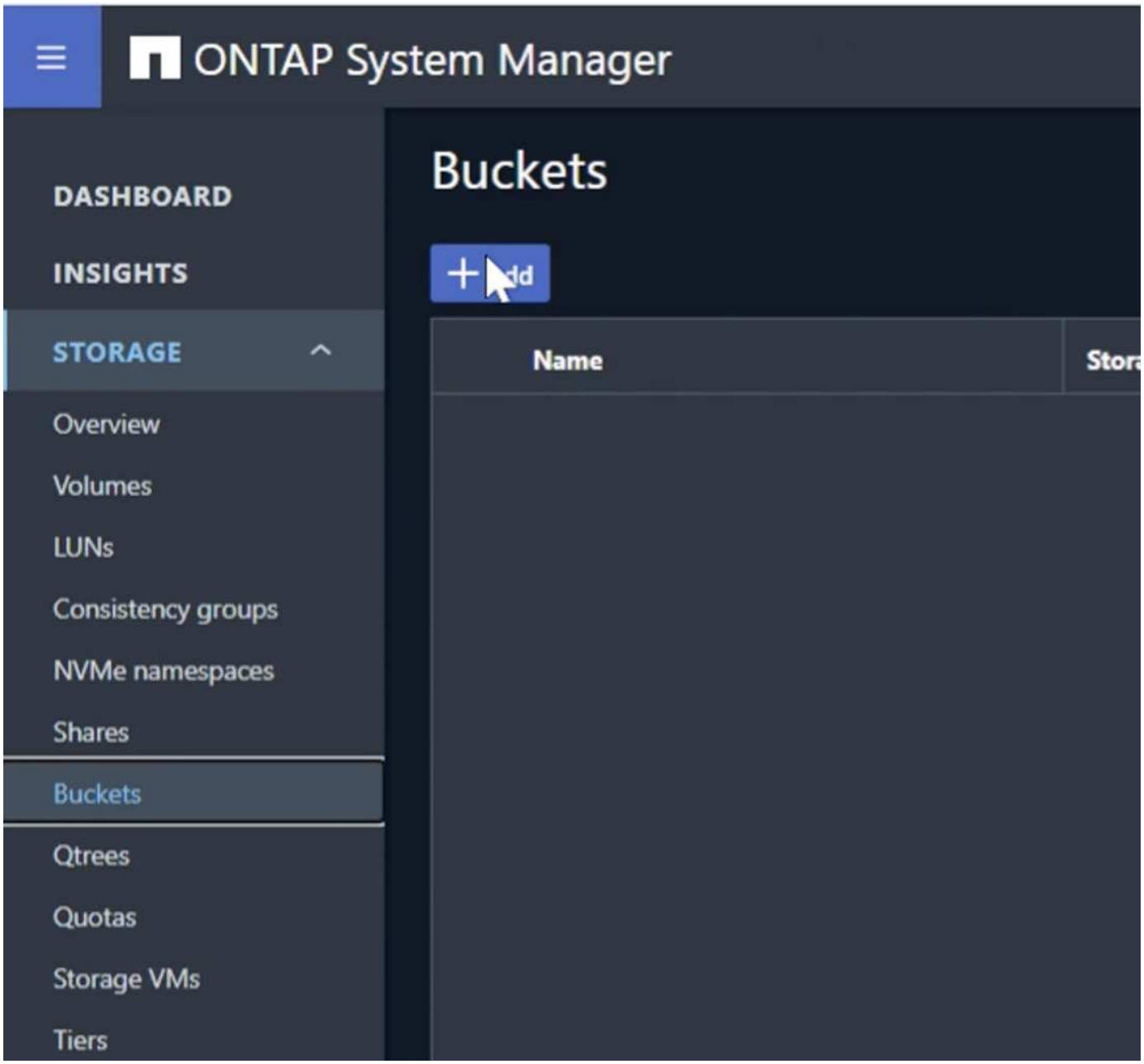
Creare un gruppo SVM S3

Nella scheda Groups (gruppi) delle impostazioni SVM S3, aggiungere un nuovo gruppo con l'utente creato in precedenza e le autorizzazioni FullAccess.

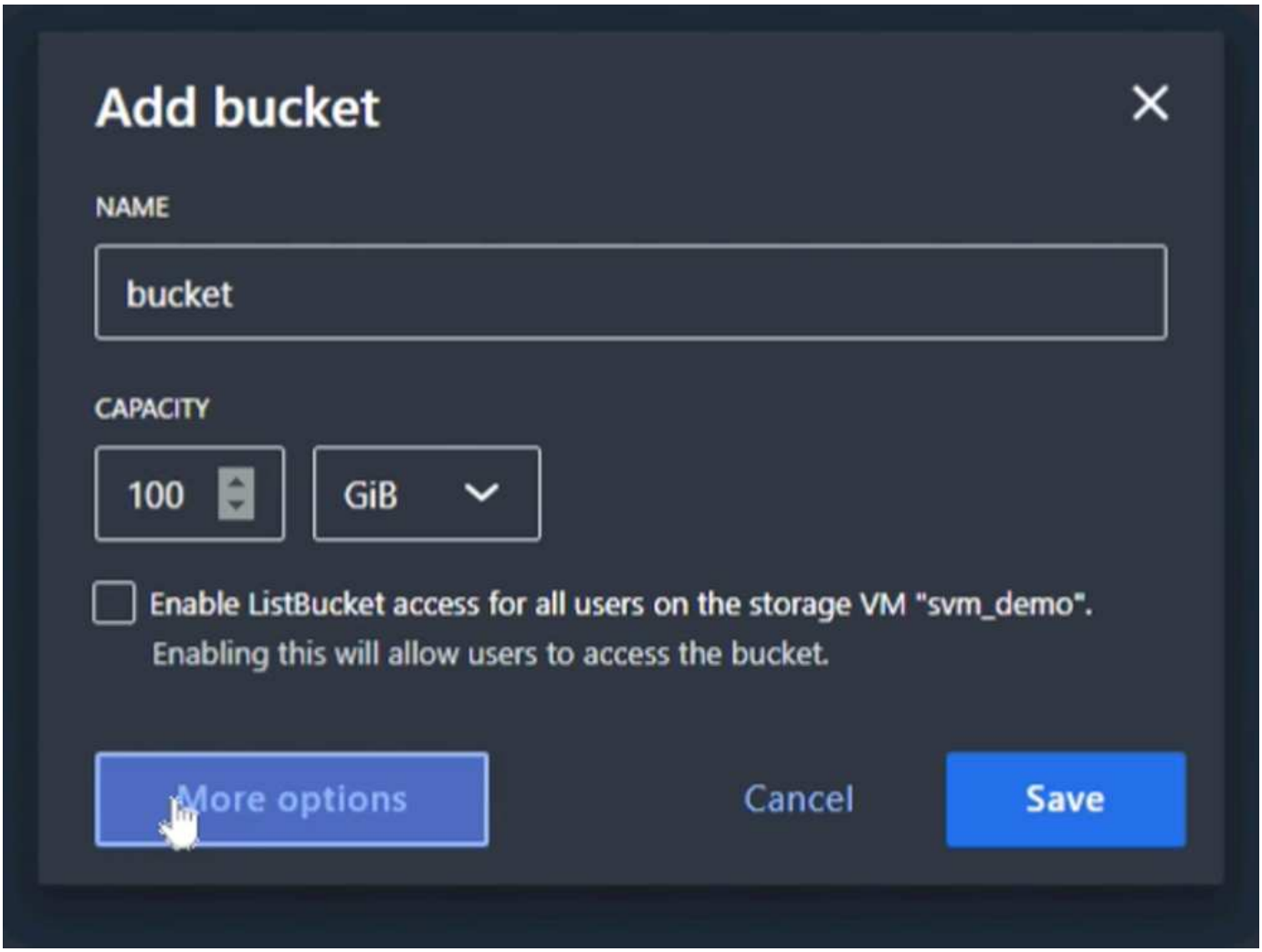


Creare bucket SVM S3

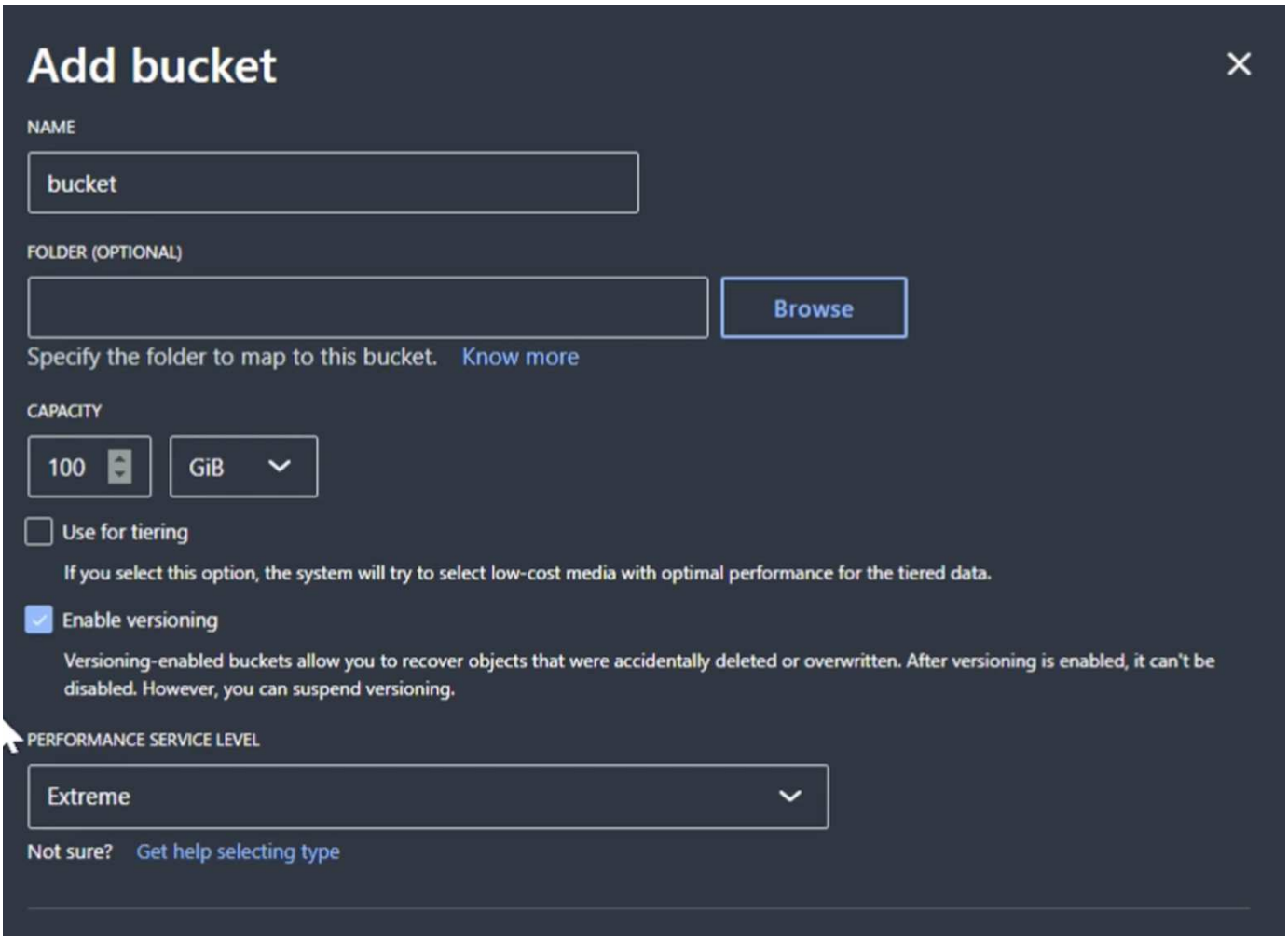
Passare alla sezione benne e fare clic sul pulsante "+Aggiungi".



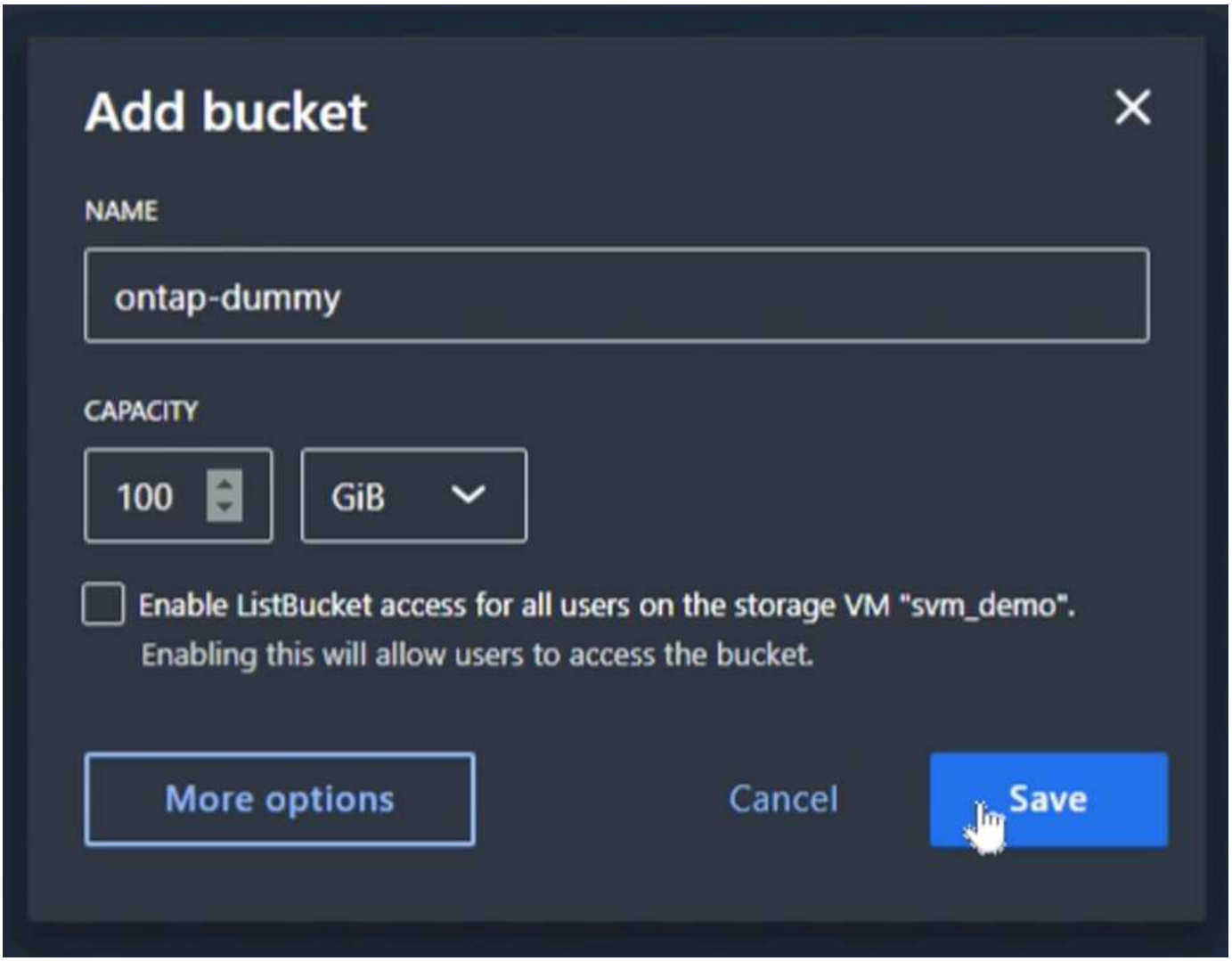
Immettere un nome, una capacità e deselezionare la casella di controllo "Abilita accesso a ListBucket…", quindi fare clic sul pulsante "altre opzioni".



Nella sezione "altre opzioni" selezionare la casella di controllo attiva versione e fare clic sul pulsante "Salva".



Ripetere il processo e creare un secondo bucket senza attivare il controllo delle versioni. Immettere un nome con la stessa capacità del bucket uno e deselezionare la casella di controllo "Abilita accesso a ListBucket…", quindi fare clic sul pulsante "Salva".



Di Rafael Guedes e Aron Klein

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

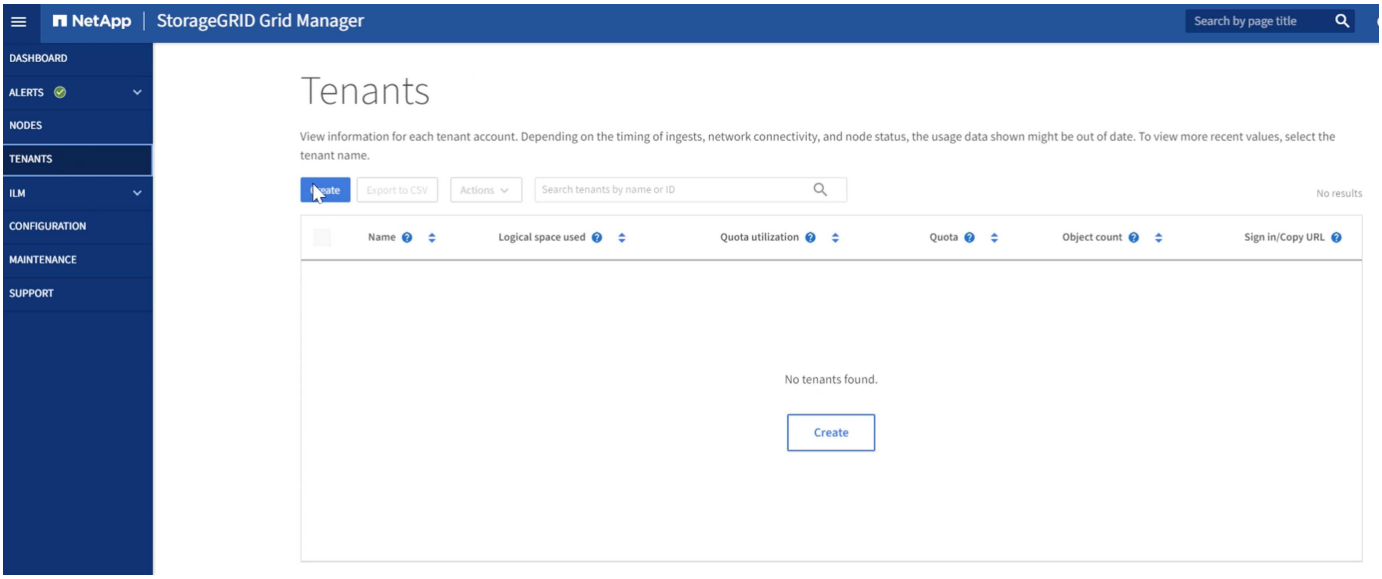
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Preparazione di StorageGRID

Continuando la configurazione per questa demo, creeremo un tenant, un utente, un gruppo di sicurezza, una policy di gruppo e un bucket.

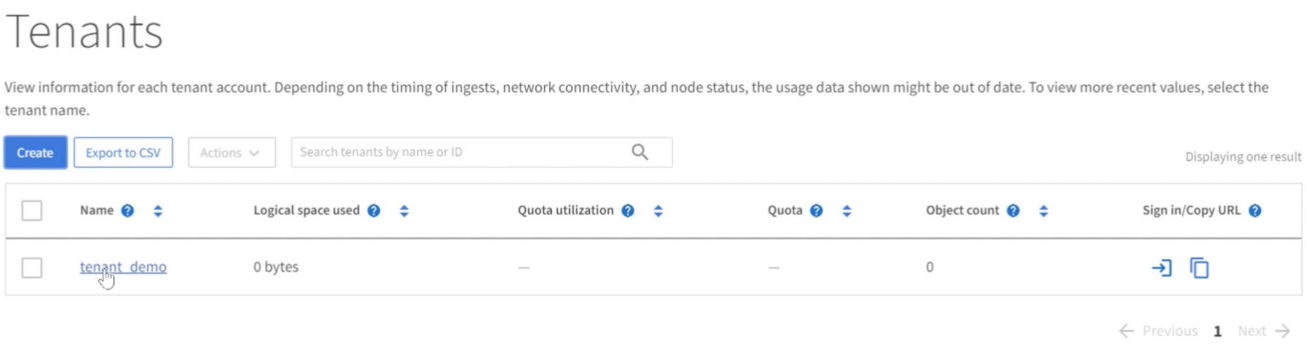
Creare il tenant

Passare alla scheda "inquilini" e fare clic sul pulsante "Crea"

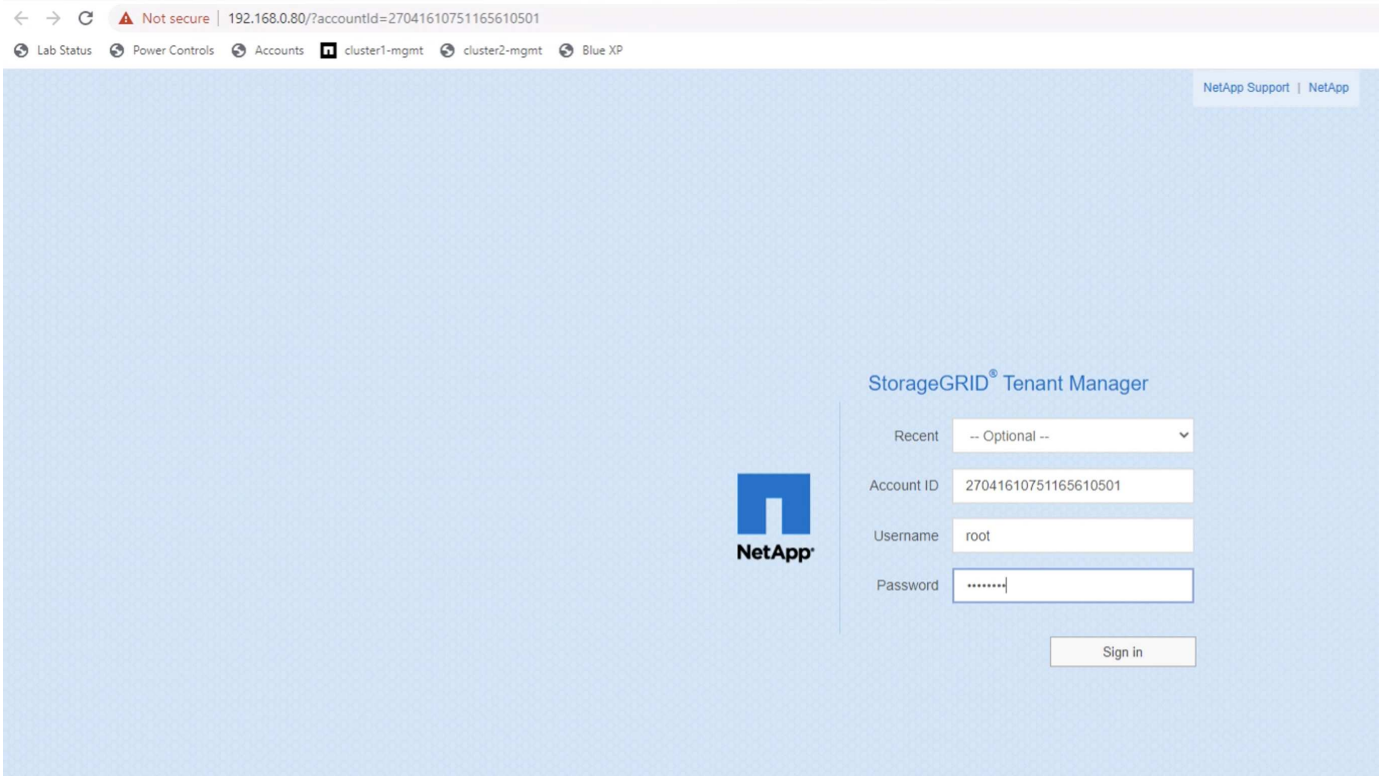


Inserire i dettagli del tenant che fornisce il nome del tenant, selezionare S3 per il tipo di client e non è richiesta alcuna quota. Non è necessario selezionare i servizi della piattaforma o consentire la selezione S3. Se lo si sceglie, è possibile scegliere di utilizzare la propria fonte di identità. Impostare la password principale e fare clic sul pulsante Finish (fine).

Fare clic sul nome del tenant per visualizzare i dettagli del tenant. **In seguito sarà necessario l'ID tenant, quindi copiarlo**. Fare clic sul pulsante Accedi. In questo modo si accede al portale tenant. Salvare l'URL per uso futuro.

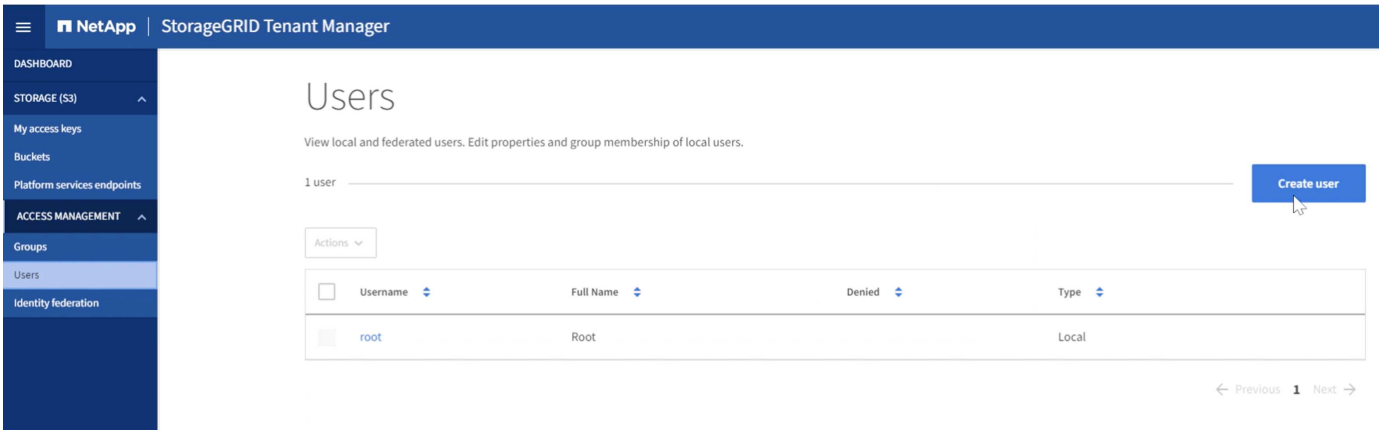


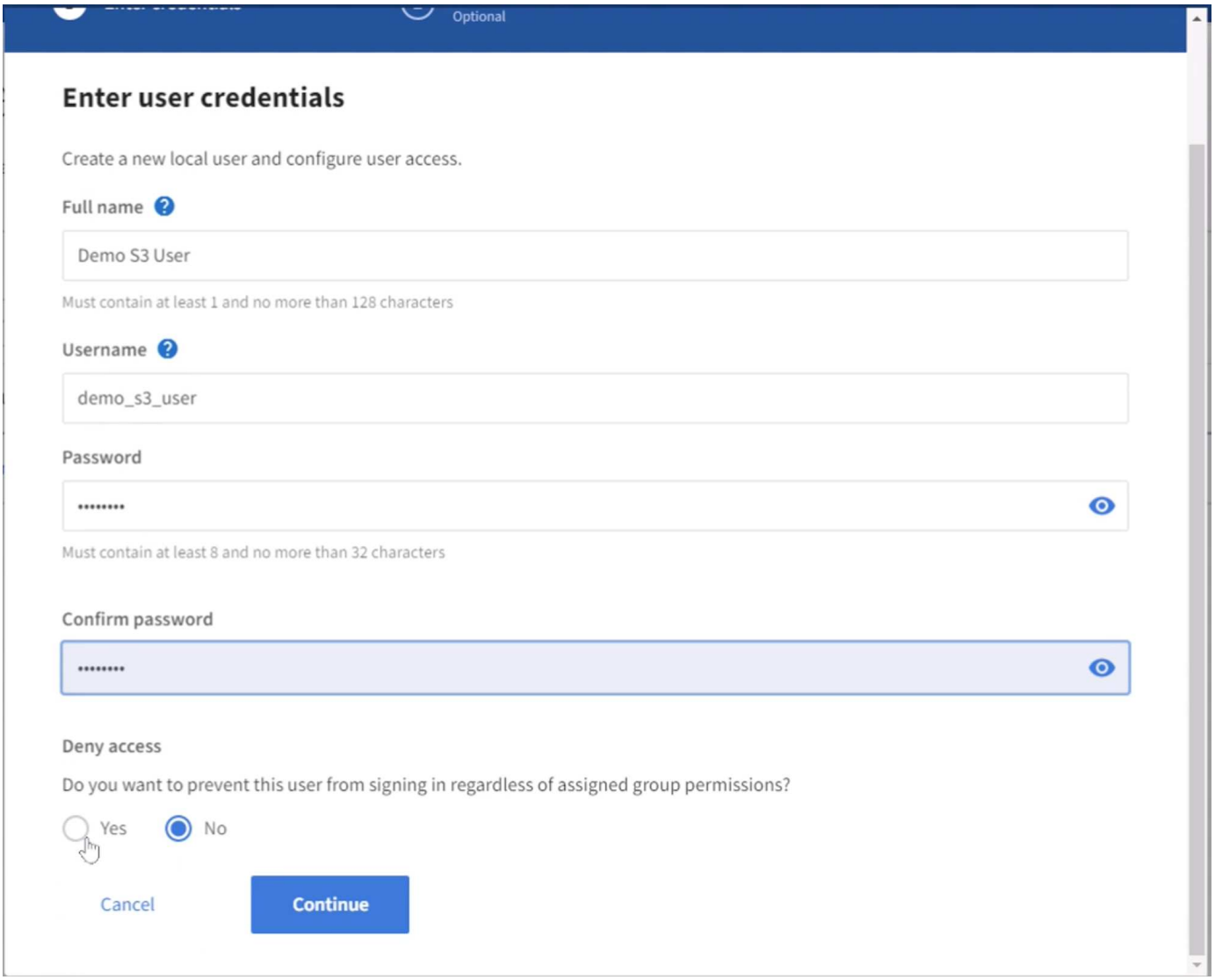
In questo modo si accede al portale tenant. Salvare l'URL per uso futuro e immettere le credenziali dell'utente root.



Creare l'utente

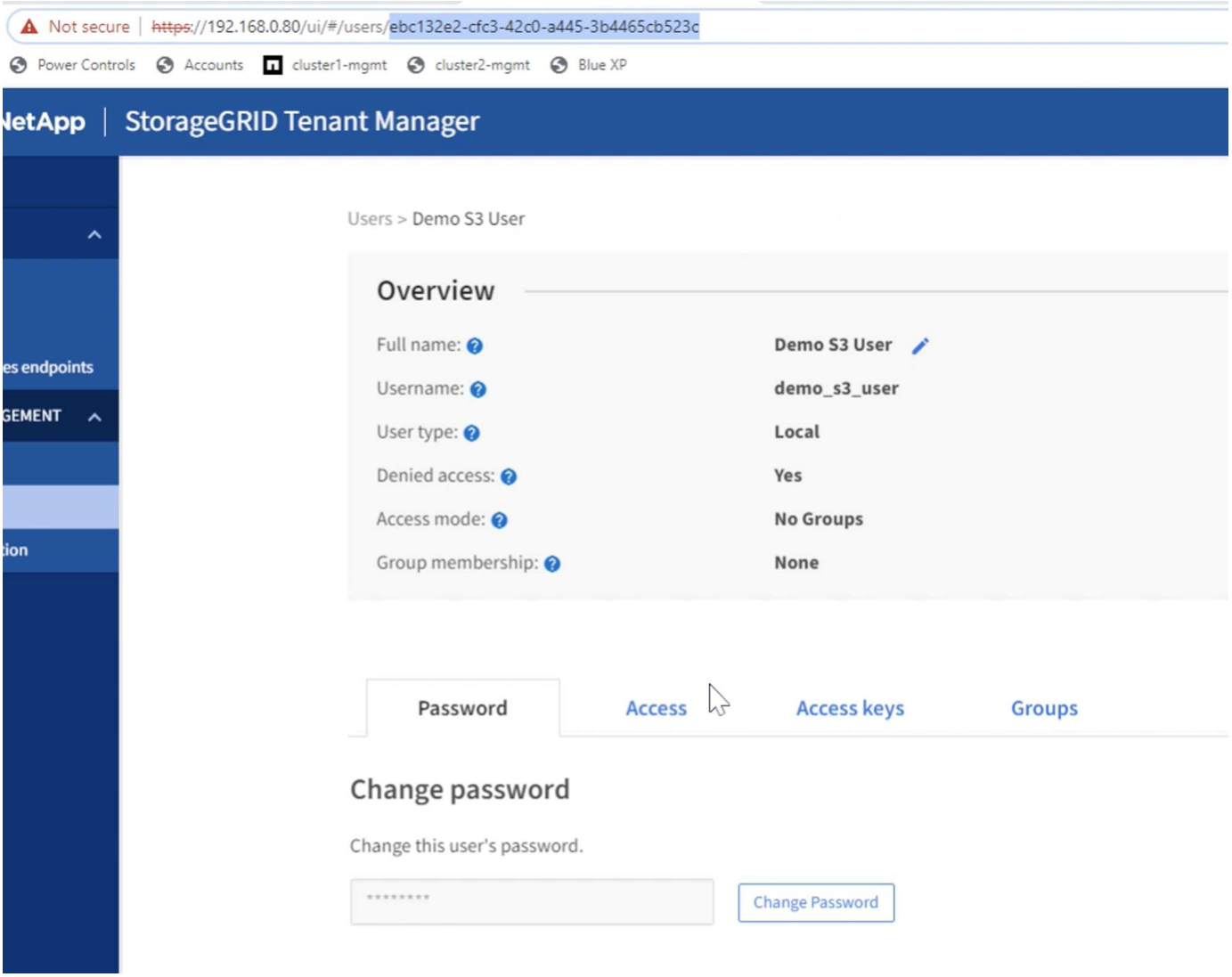
Accedere alla scheda utenti e creare un nuovo utente.



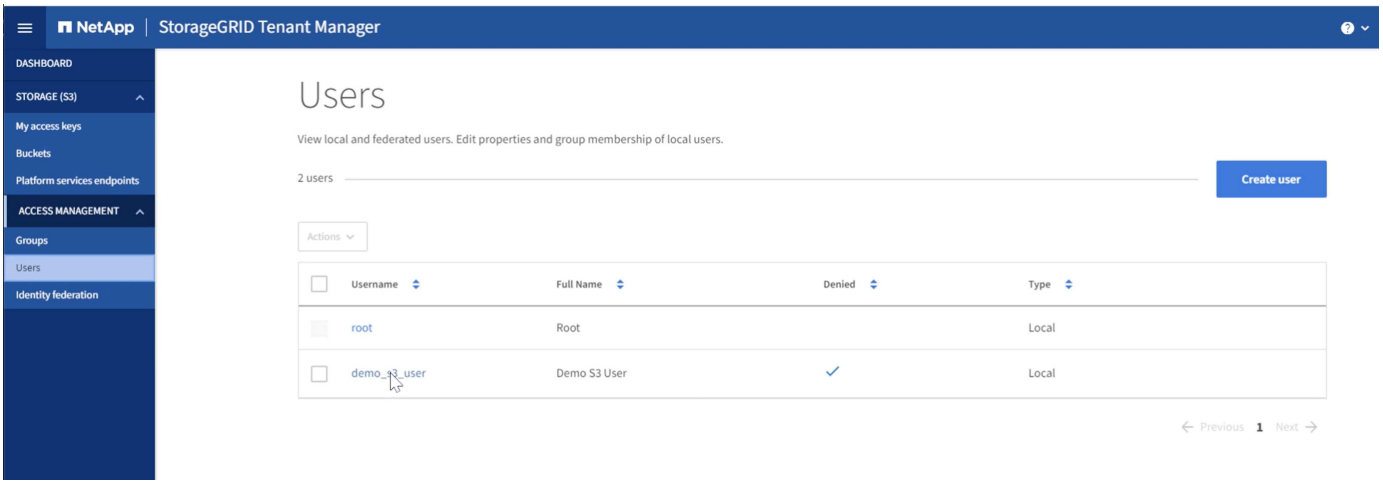


Ora che il nuovo utente è stato creato, fare clic sul nome dell'utente per aprire i dettagli dell'utente.

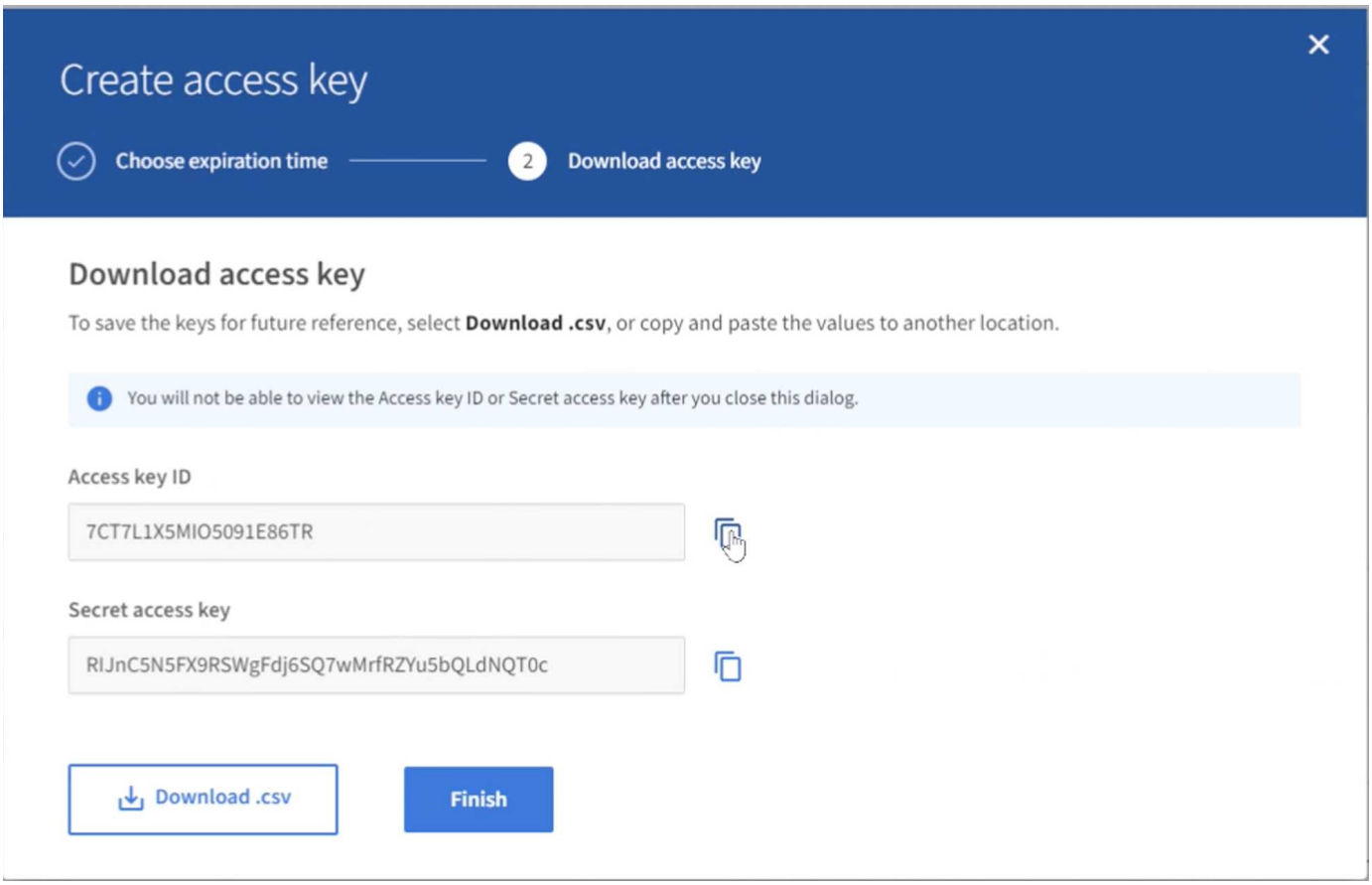
Copiare l'ID utente dall'URL da utilizzare in un secondo momento.



Per creare i tasti S3, fare clic sul nome utente.

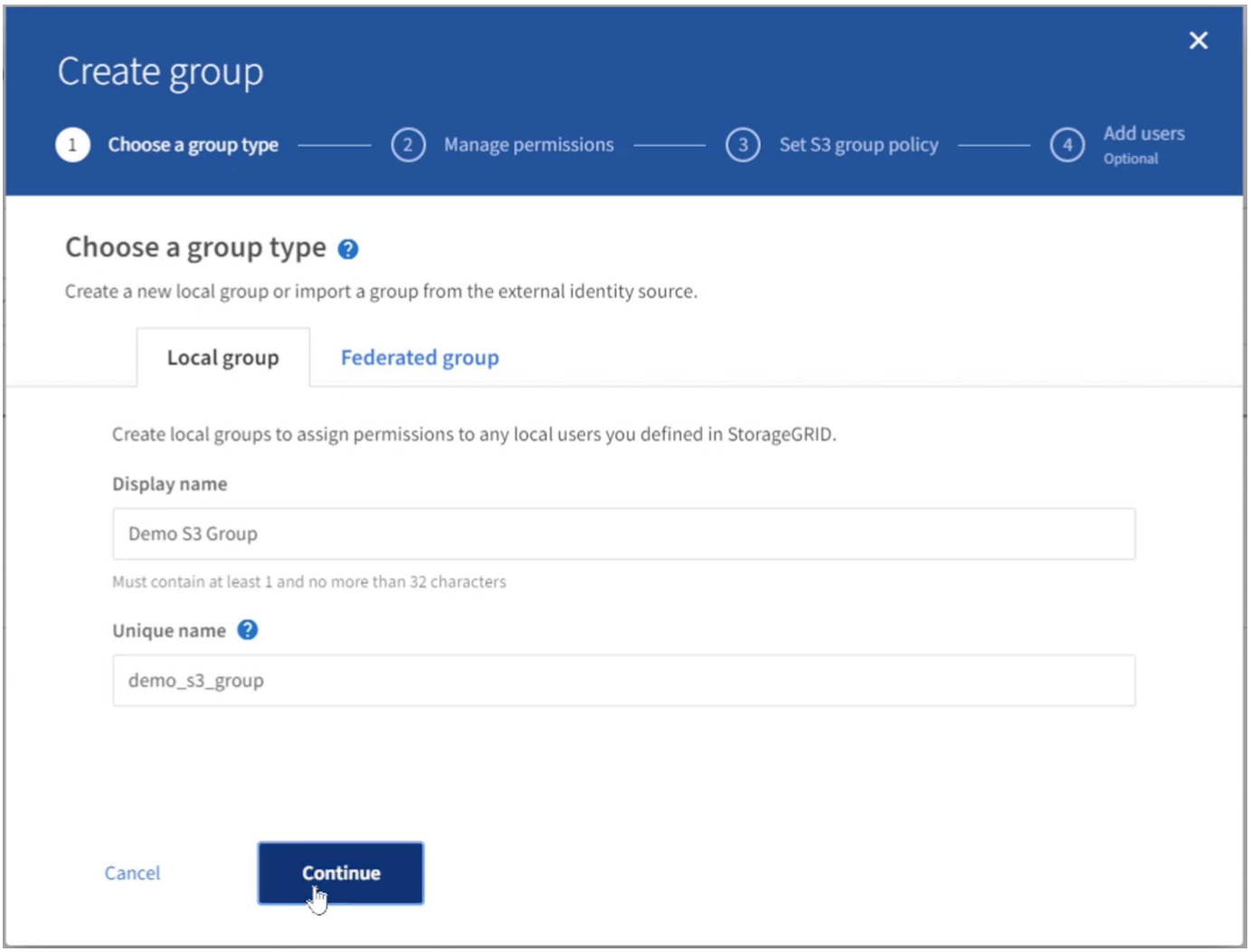


Selezionare la scheda "tasti di accesso" e fare clic sul pulsante "Crea chiave". Non è necessario impostare un'ora di scadenza. Scaricare i S3 tasti in quanto non possono essere richiamati una volta chiusa la finestra.

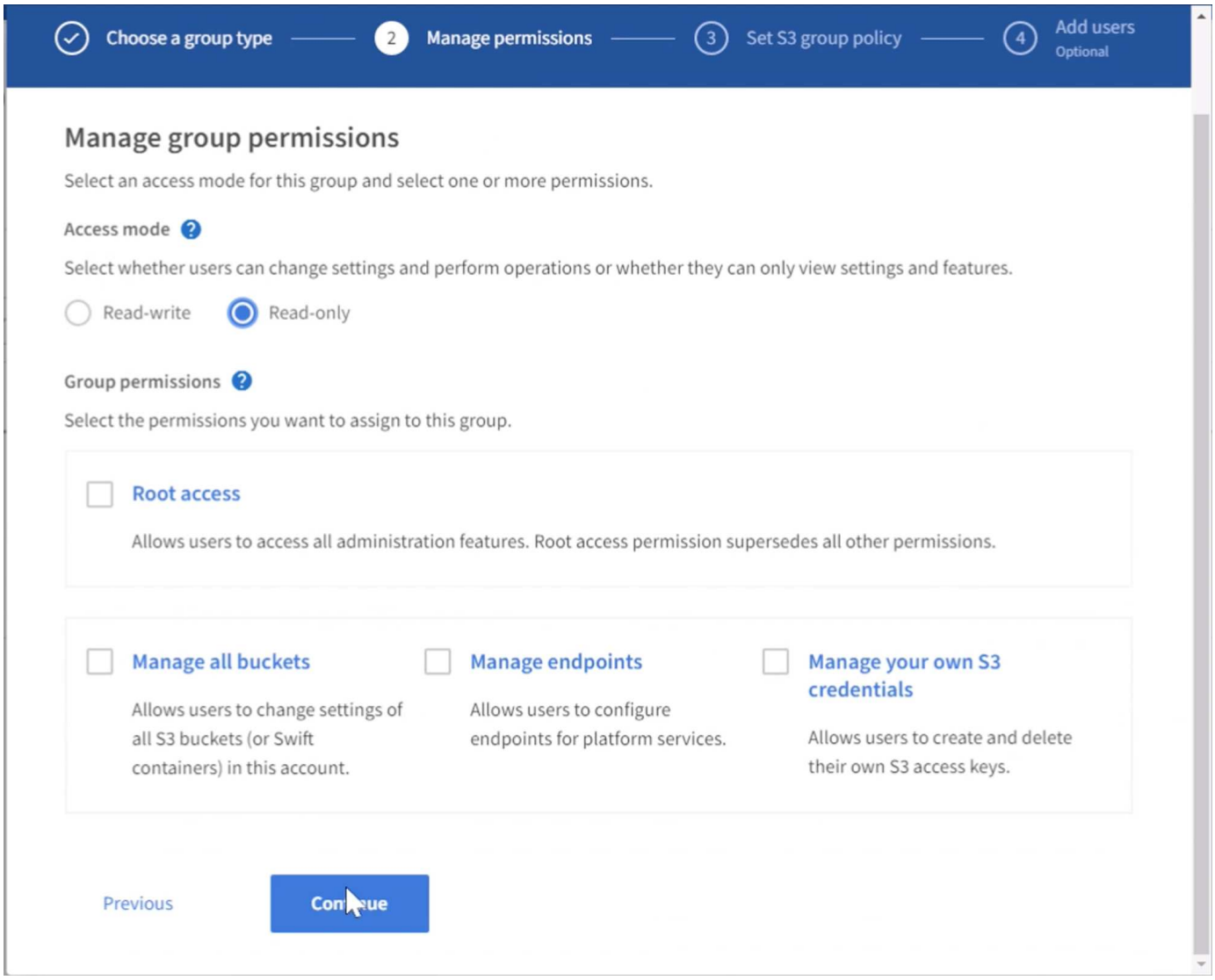


Creare il gruppo di protezione

Andare alla pagina gruppi e creare un nuovo gruppo.

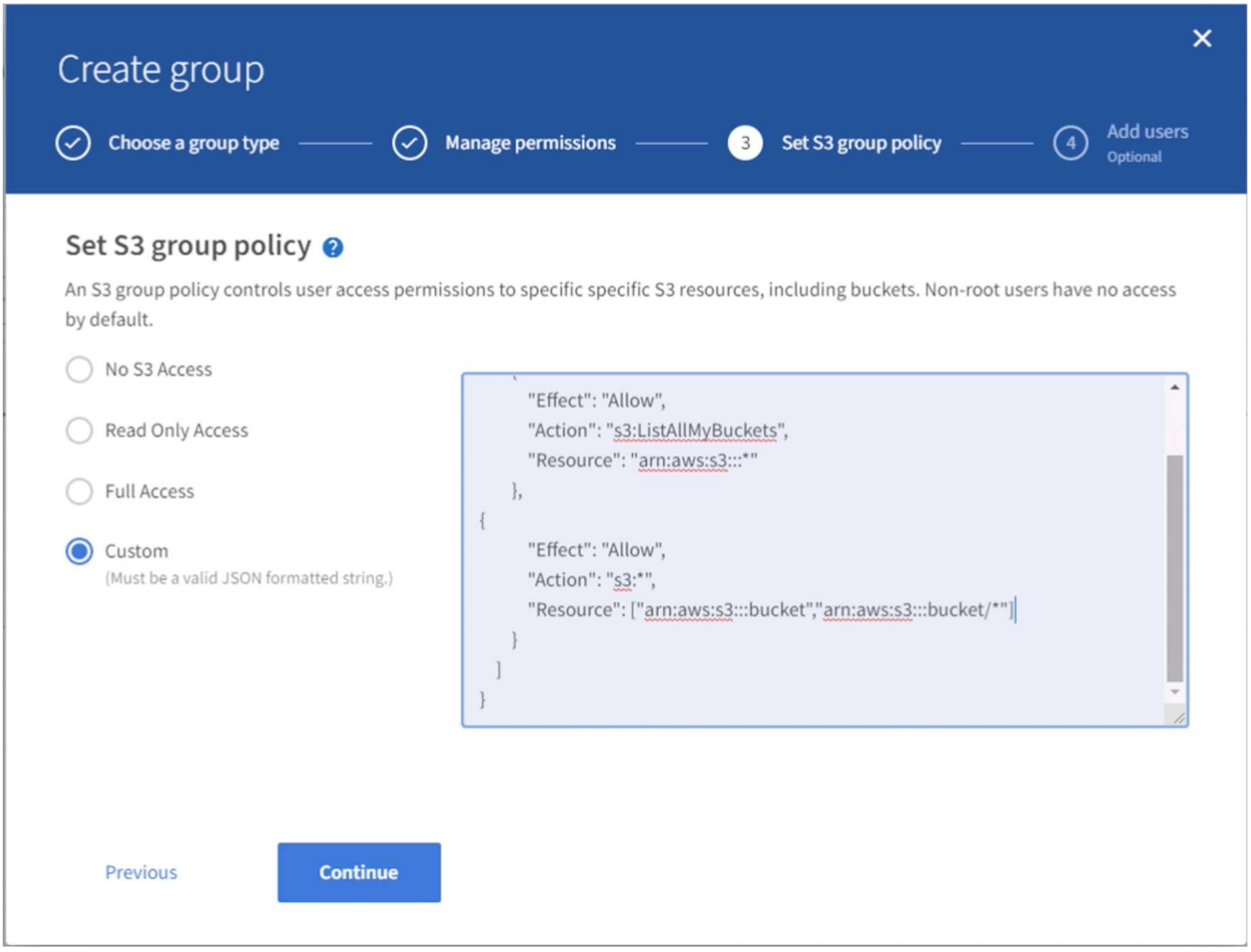


Impostare le autorizzazioni del gruppo su sola lettura. Si tratta delle autorizzazioni dell'interfaccia utente tenant, non delle autorizzazioni S3.

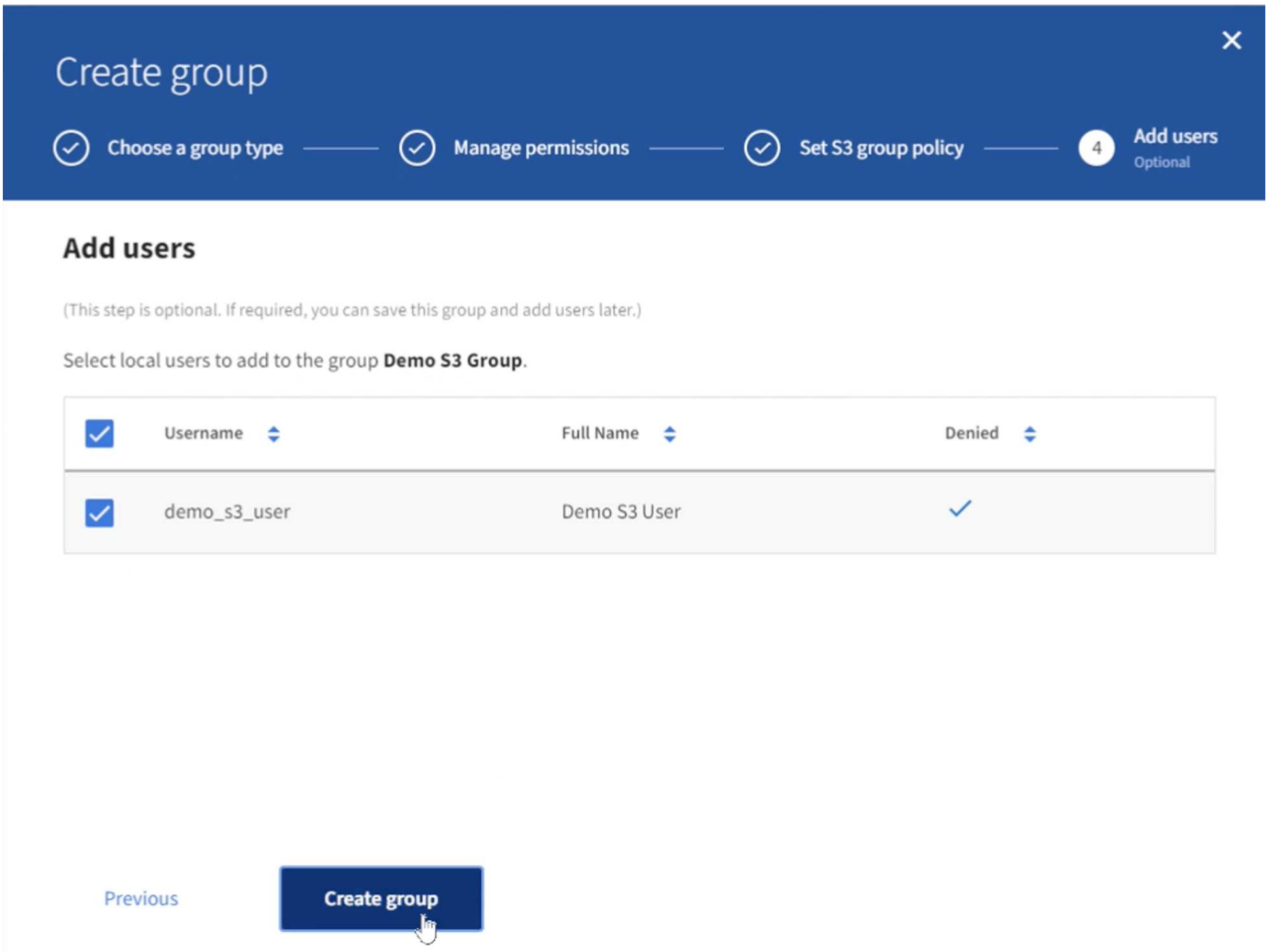


Le autorizzazioni S3 sono controllate con i criteri di gruppo (criteri IAM). Impostare il criterio di gruppo su personalizzato e incollare il criterio json nella casella. Questo criterio consente agli utenti di questo gruppo di elencare i bucket del tenant ed eseguire qualsiasi operazione S3 nel bucket denominato "bucket" o sottocartelle nel bucket denominato "bucket".

```
{
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
        "Action": "s3:*",
        "Resource": ["arn:aws:s3:::bucket","arn:aws:s3:::bucket/*"]
      }
    ]
}
```

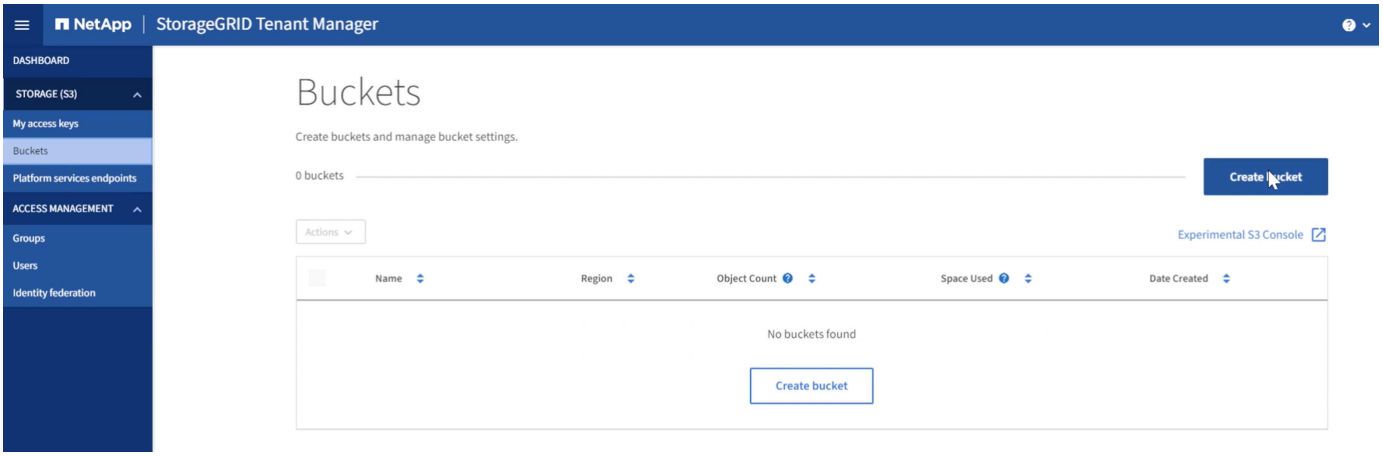


Infine, aggiungere l'utente al gruppo e terminare.

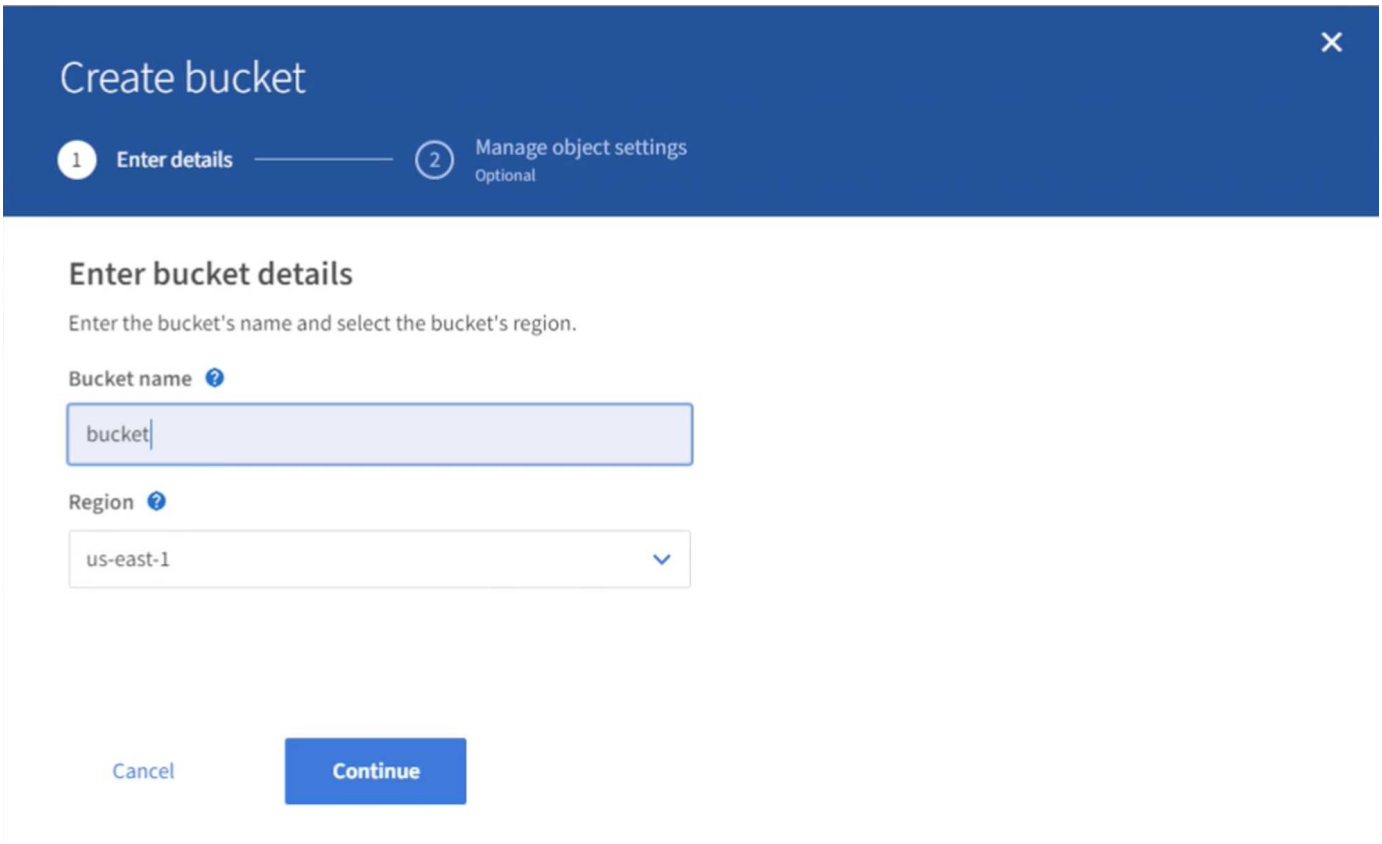


Creare due bucket

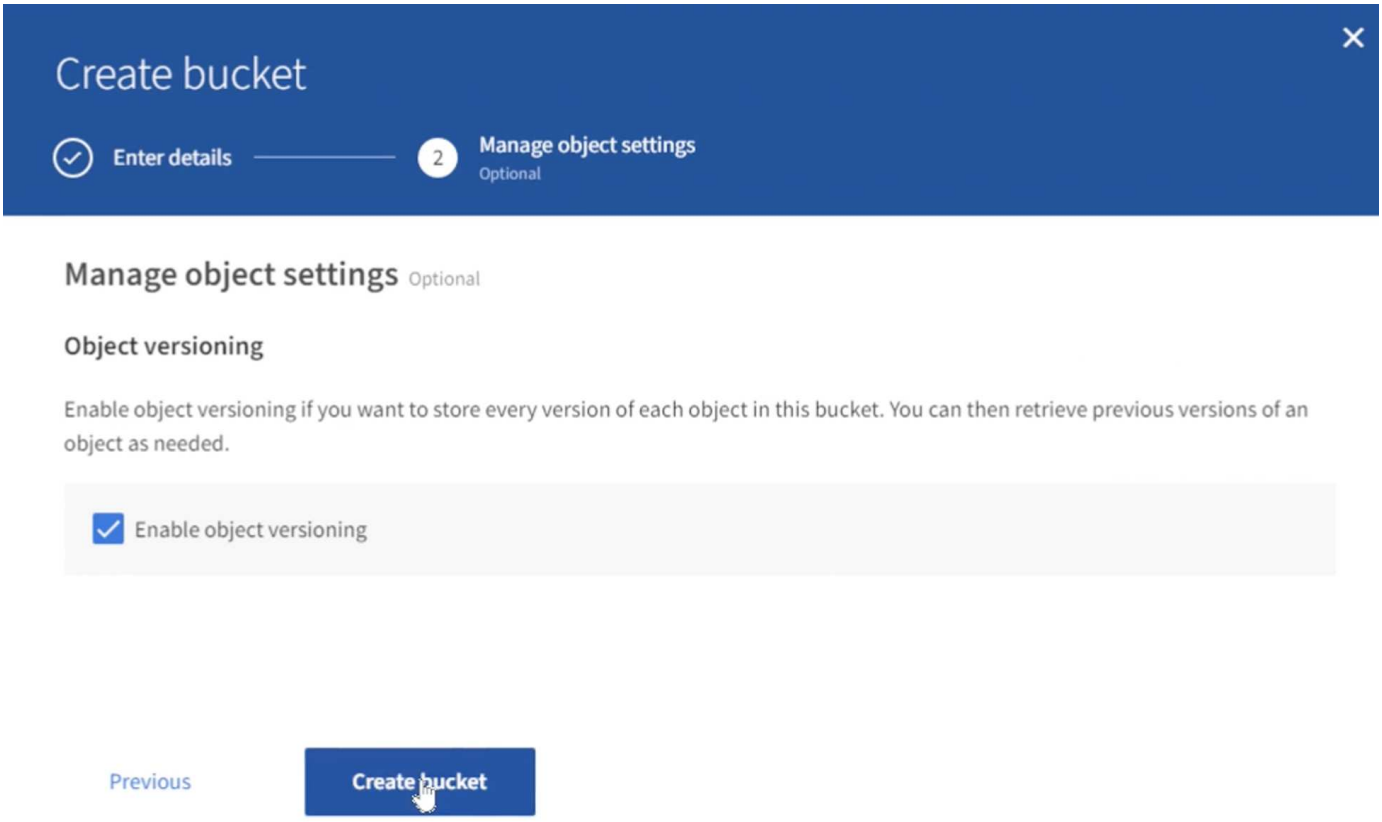
Passare alla scheda bucket e fare clic sul pulsante Crea bucket.



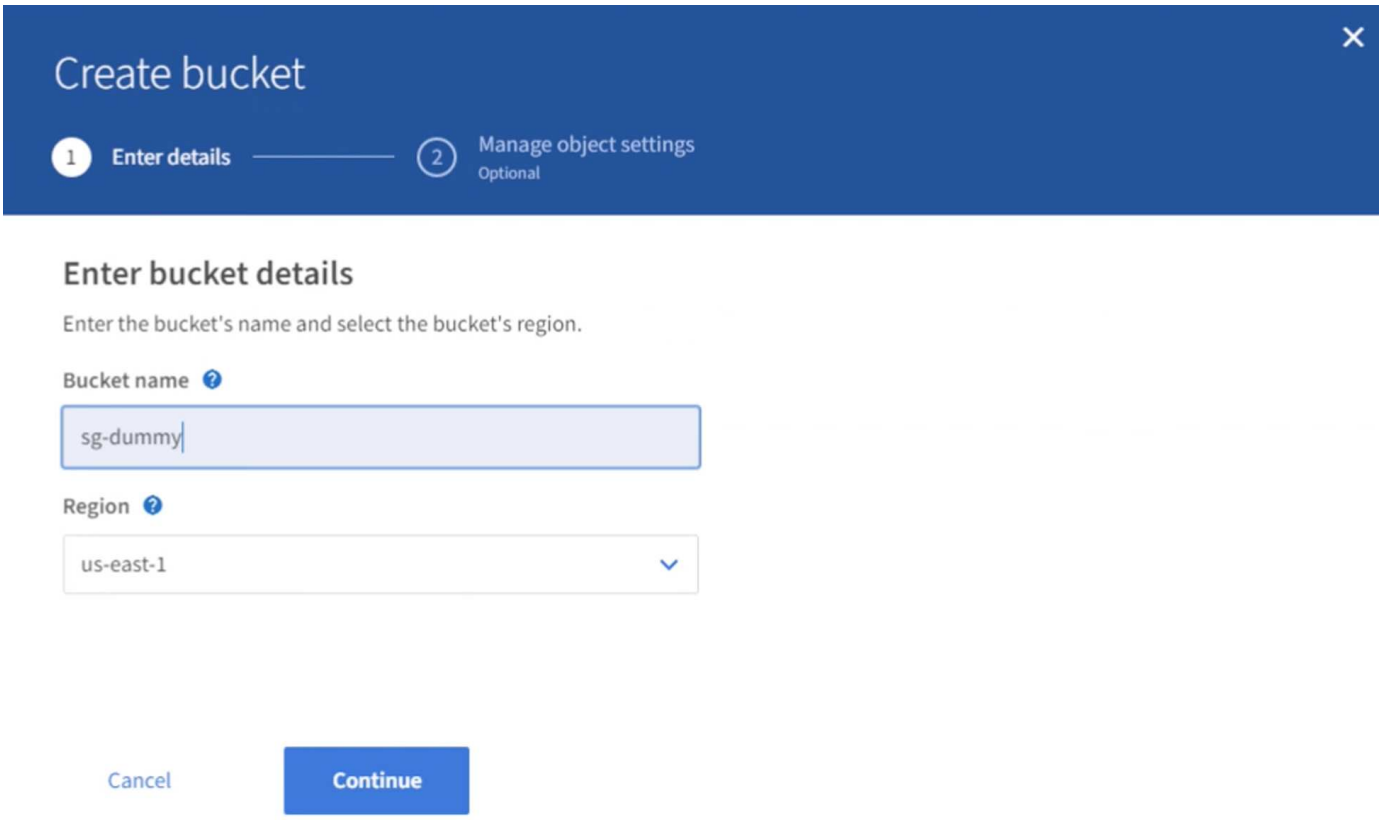
Definire il nome del bucket e la regione.



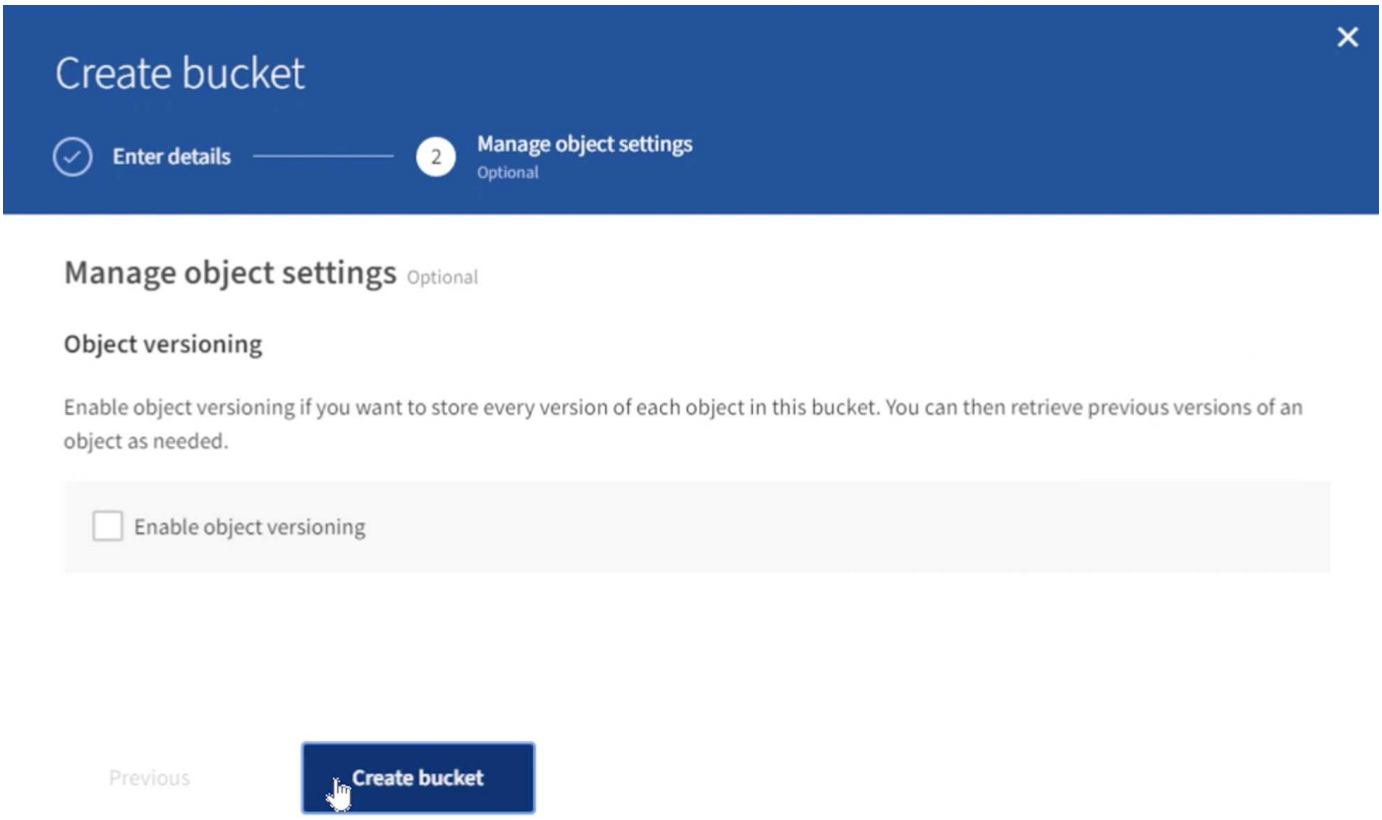
In questo primo bucket abilitare la versione.



Ora creare un secondo bucket senza abilitare il controllo delle versioni.



Non abilitare la versione in questo secondo bucket.



Di Rafael Guedes e Aron Klein

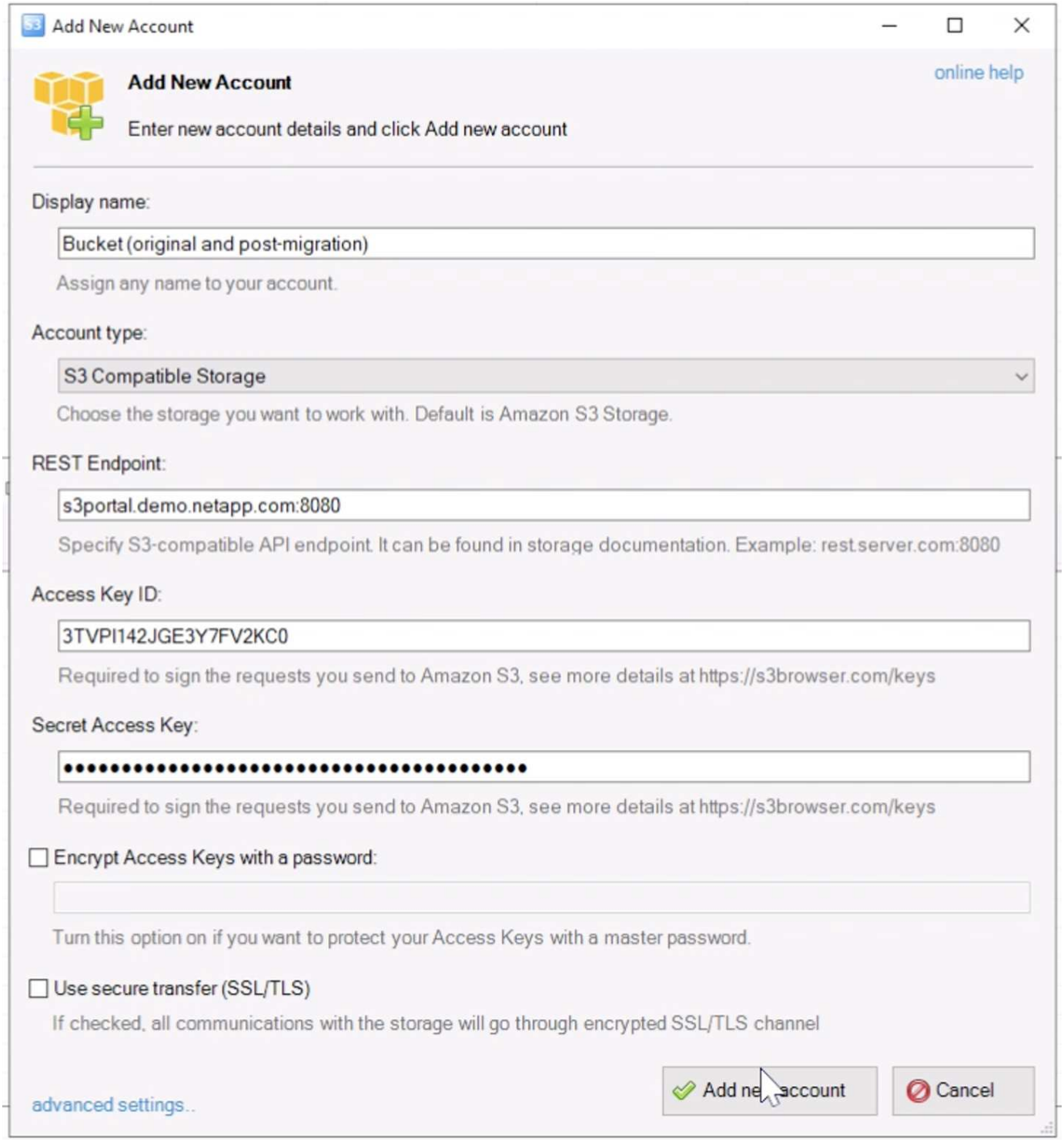
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

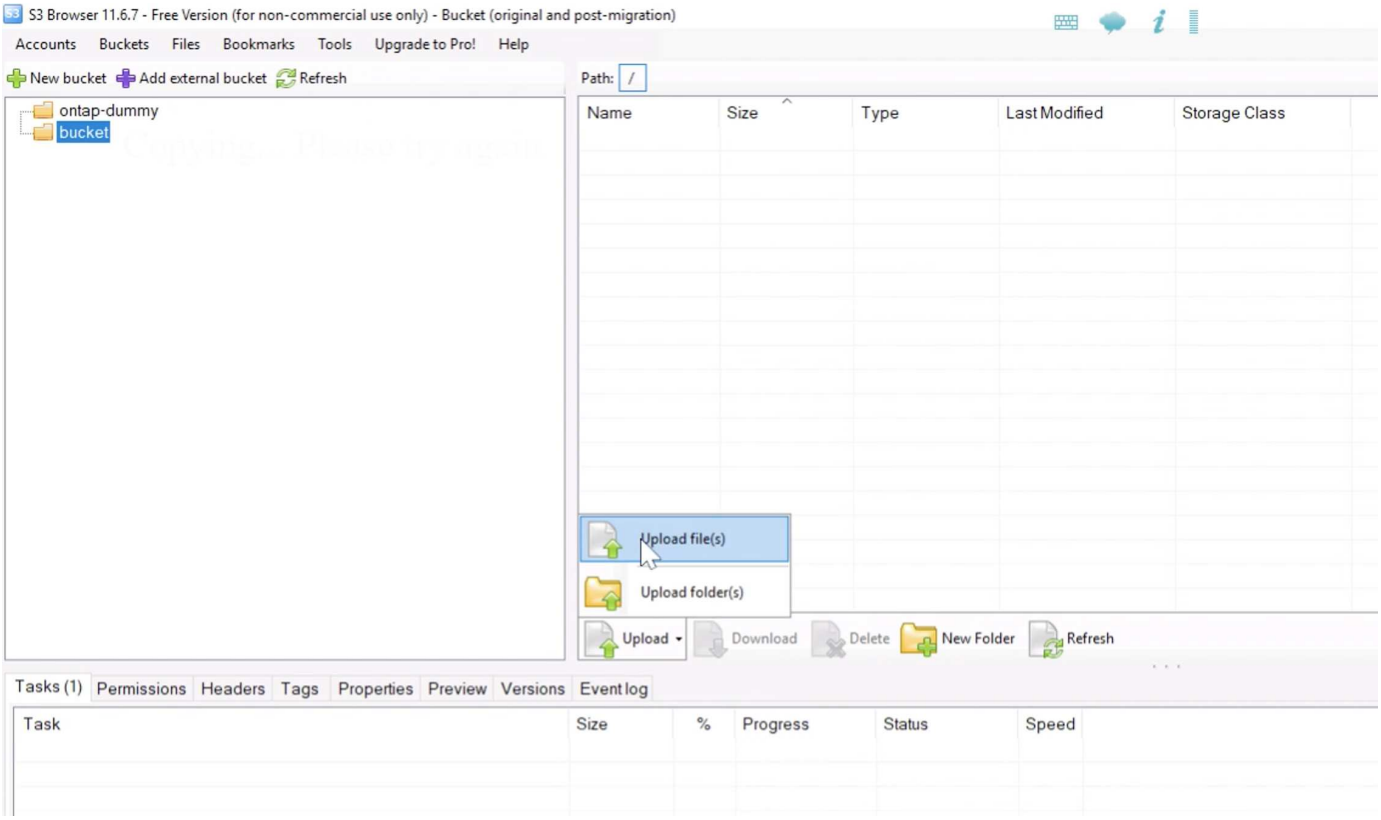
Compilare il bucket Source (origine)

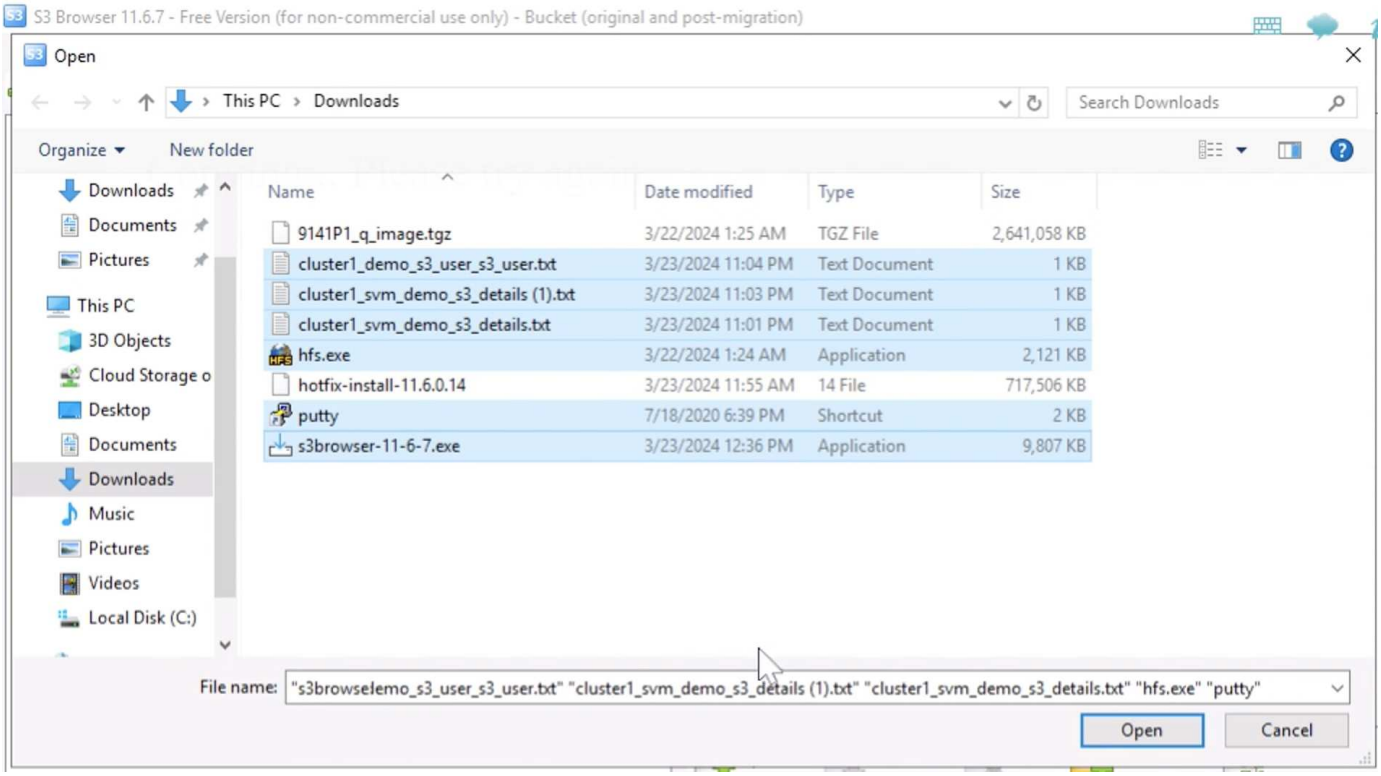
Consente di inserire alcuni oggetti nel bucket ONTAP di origine. Utilizzeremo S3Browser per questa demo, ma puoi usare qualsiasi strumento che ti trovi a tuo agio.

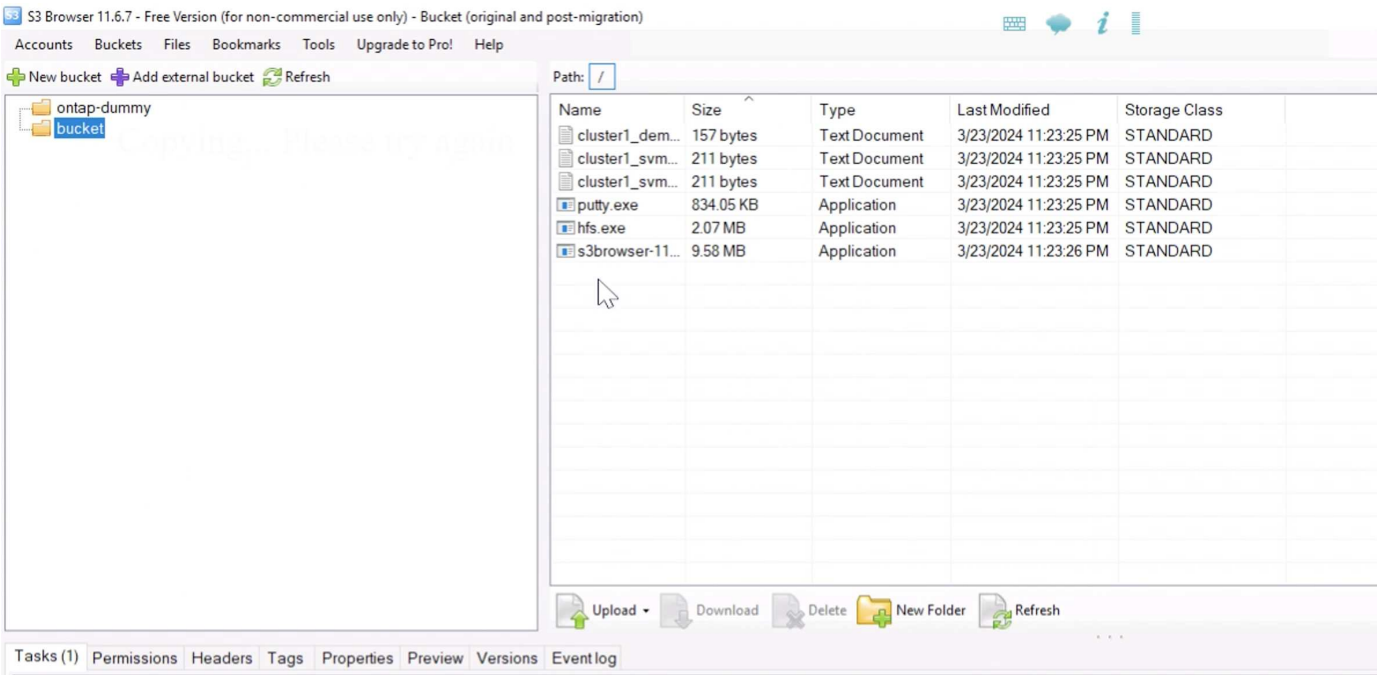
Utilizzando le chiavi S3 dell'utente ONTAP create in precedenza, configurare S3Browser per la connessione al sistema ONTAP.



Ora permette di caricare alcuni file nel bucket abilitato per la versione.

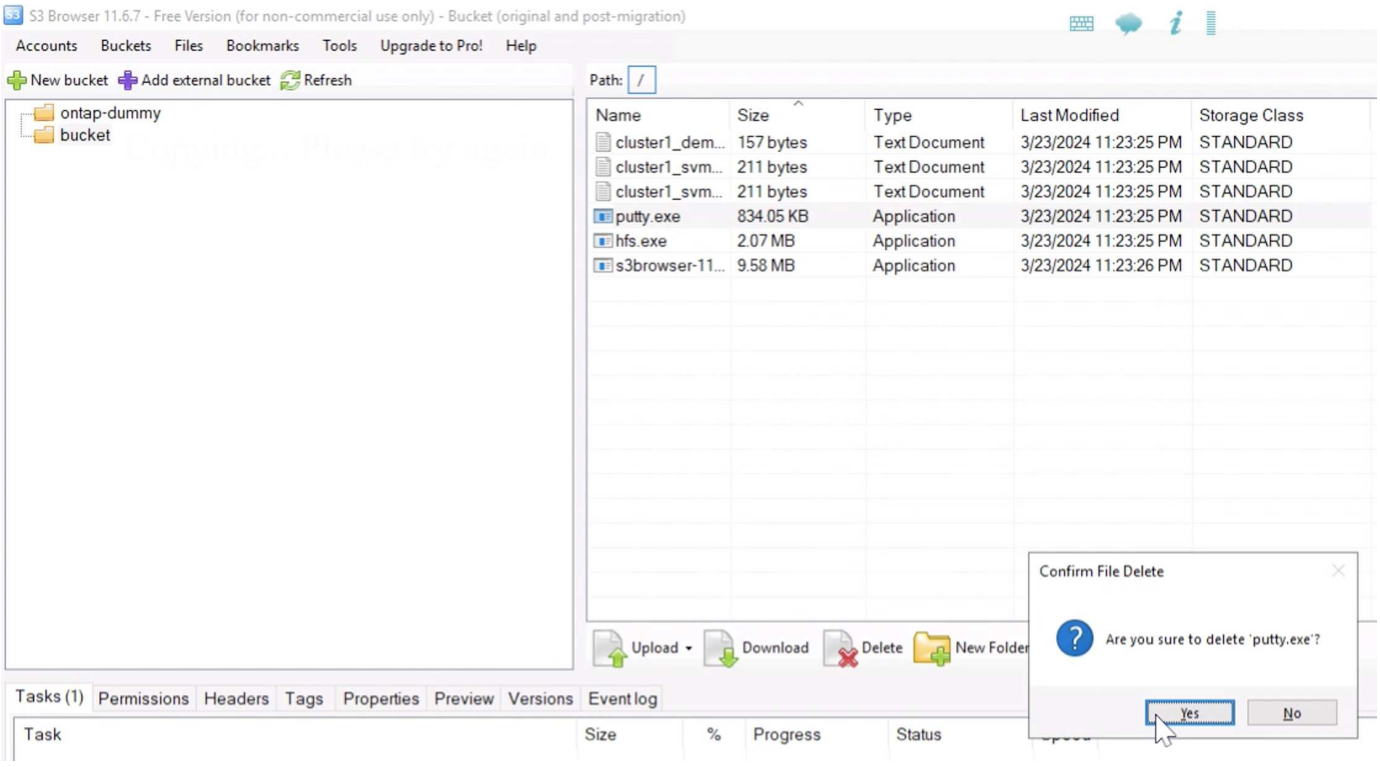

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)
Upload
Download
Delete
New Folder
Refresh
Tasks (1)
Permissions
Headers
Tags
Properties
Preview
Versions
Event log
Task
Size
%
Progress
Status
Speed


S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Open
This PC
Downloads
Search Downloads
Organize
New folder
Downloads
Documents
Pictures
This PC
3D Objects
Cloud Storage o
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
Size
9141P1_q_image.tgz
3/22/2024 1:25 AM
TGZ File
2,641,058 KB
cluster1_demo_s3_user_s3_user.txt
3/23/2024 11:04 PM
Text Document
1 KB
cluster1_svm_demo_s3_details (1).txt
3/23/2024 11:03 PM
Text Document
1 KB
cluster1_svm_demo_s3_details.txt
3/23/2024 11:01 PM
Text Document
1 KB
hfs.exe
3/22/2024 1:24 AM
Application
2,121 KB
hotfix-install-11.6.0.14
3/23/2024 11:55 AM
14 File
717,506 KB
putty
7/18/2020 6:39 PM
Shortcut
2 KB
s3browser-11-6-7.exe
3/23/2024 12:36 PM
Application
9,807 KB
File name:
"s3browselemo_s3_user_s3_user.txt" "cluster1_svm_demo_s3_details (1).txt" "cluster1_svm_demo_s3_details.txt" "hfs.exe" "putty"
Open
Cancel

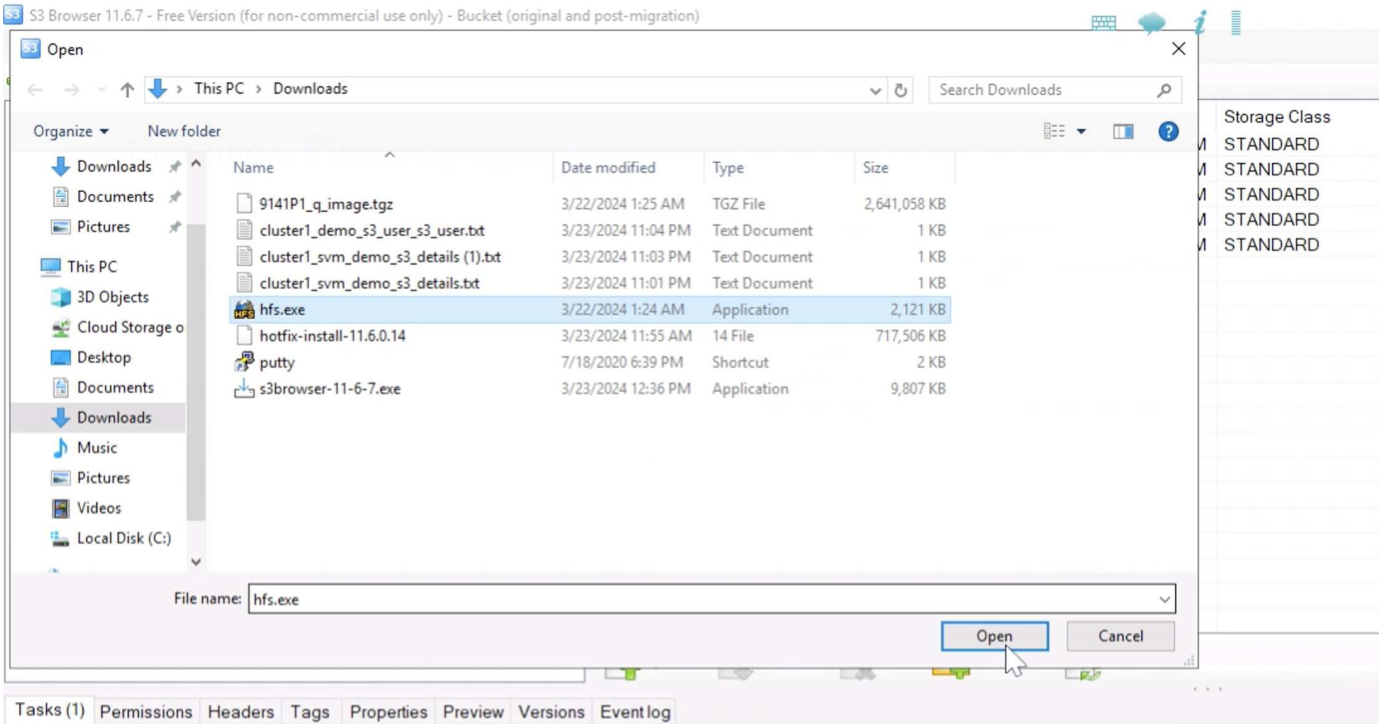


Ora permette di creare alcune versioni di oggetti nel bucket.

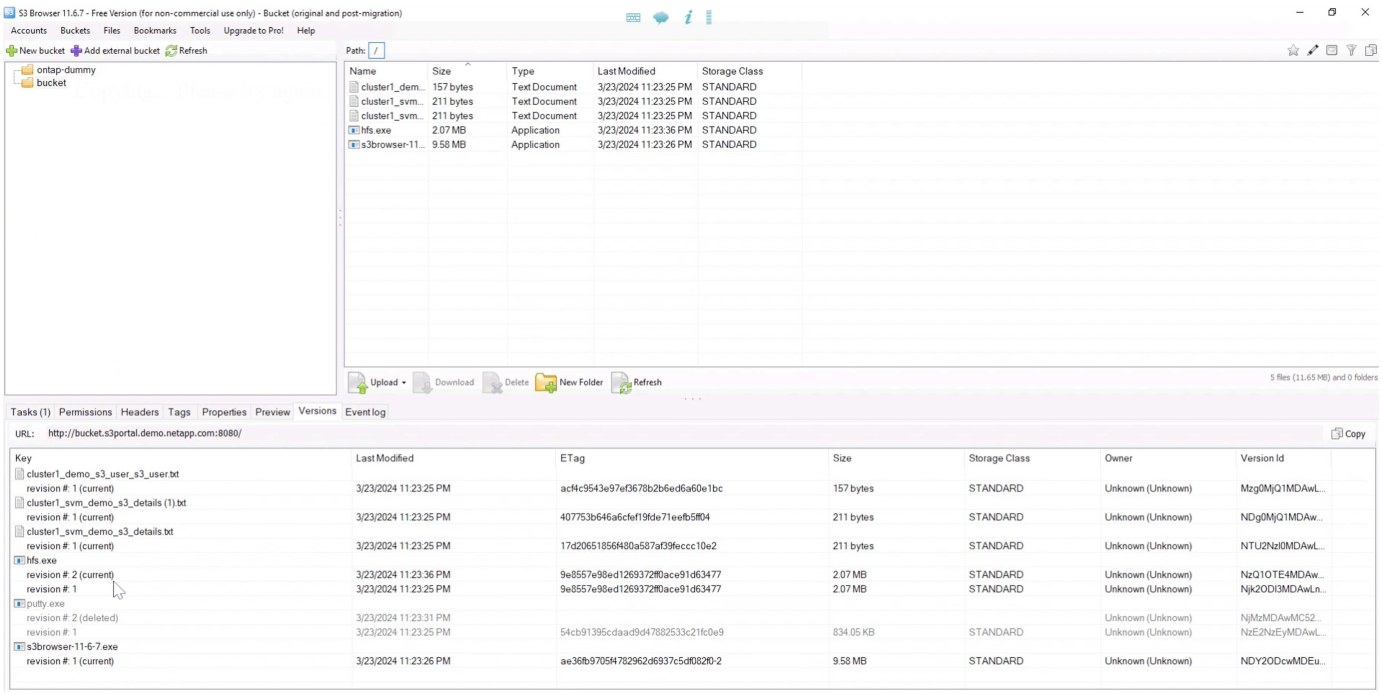
Eliminare un file.



Caricare un file già esistente nel bucket per copiare il file su se stesso e crearne una nuova versione.



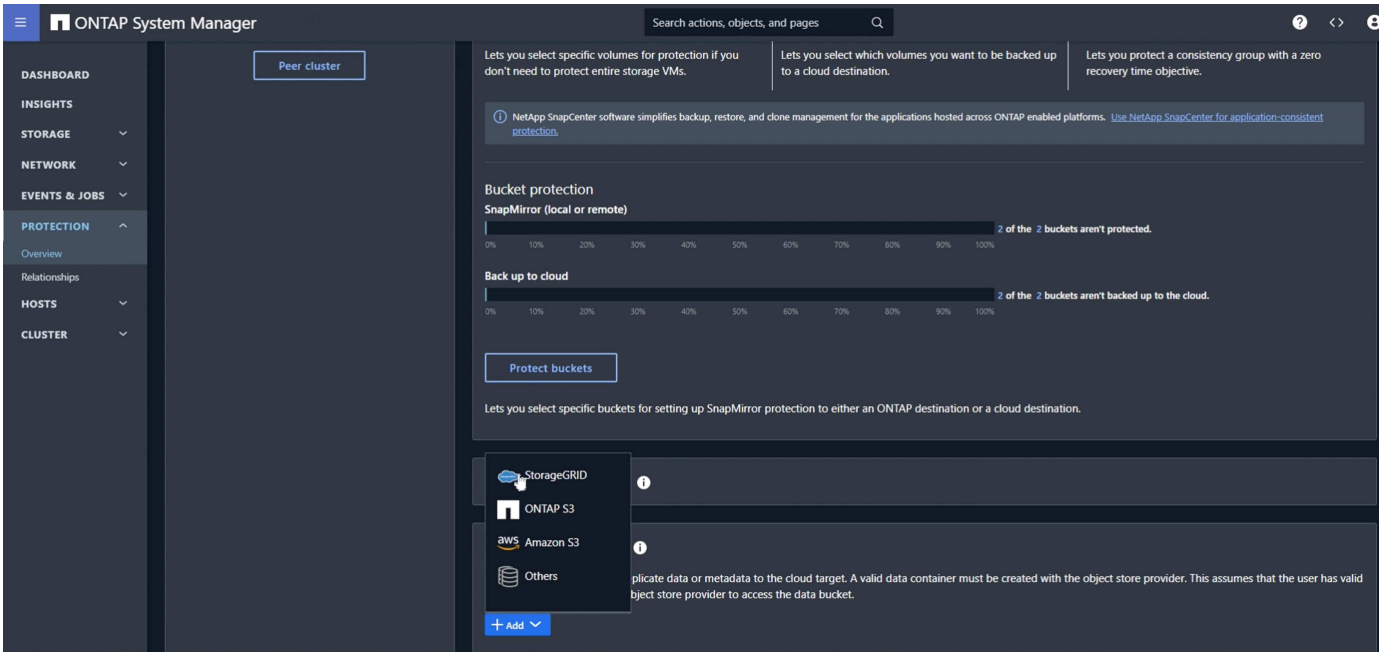
In S3Browser possiamo visualizzare le versioni degli oggetti appena creati.



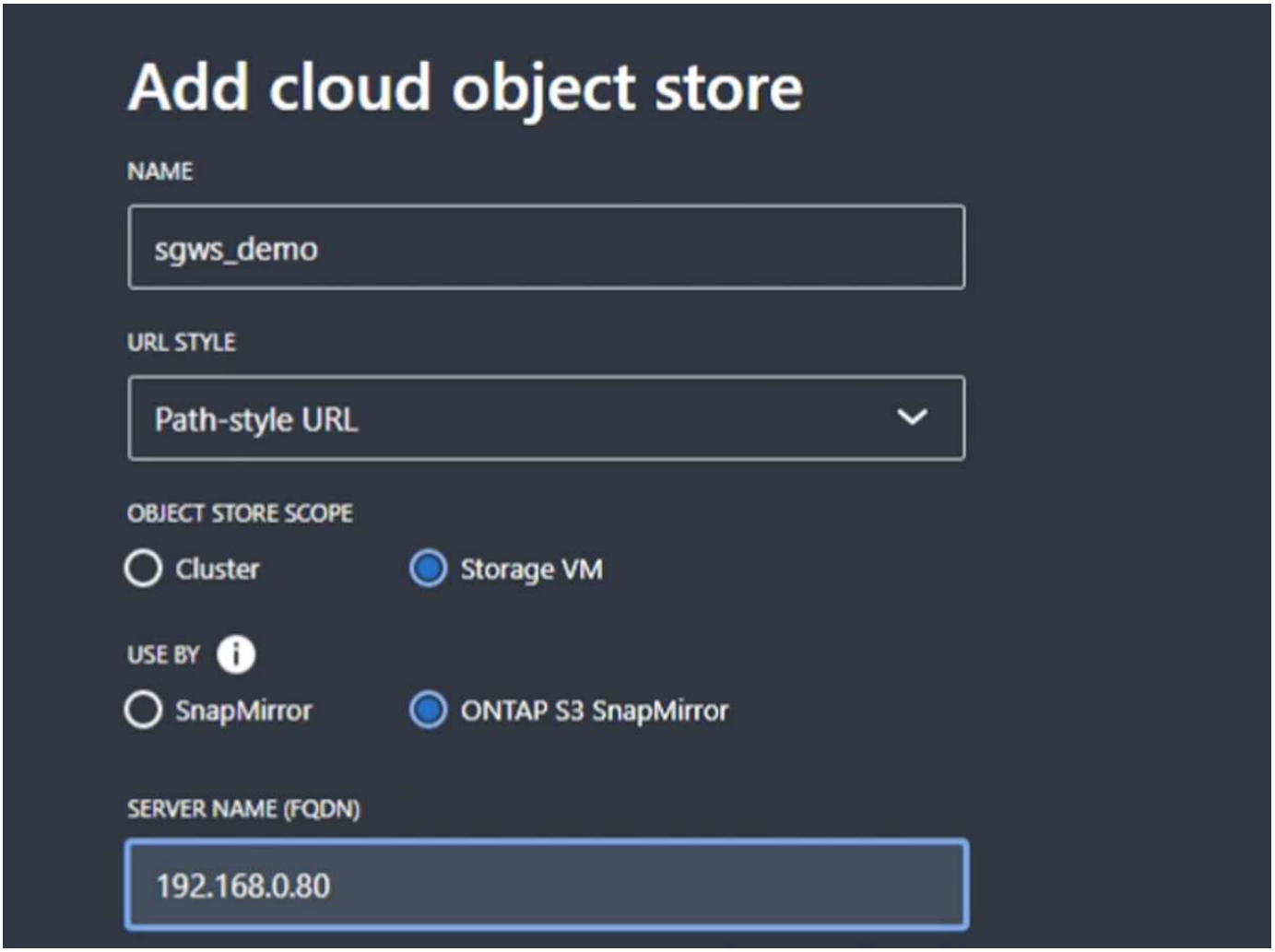
Stabilire la relazione di replica

Consente di iniziare a inviare dati da ONTAP a StorageGRID.

In Gestione di sistema di ONTAP, selezionare "protezione/Panoramica". Scorri verso il basso fino a "Archivio oggetti cloud", quindi fai clic sul pulsante "Aggiungi" e seleziona "StorageGRID".



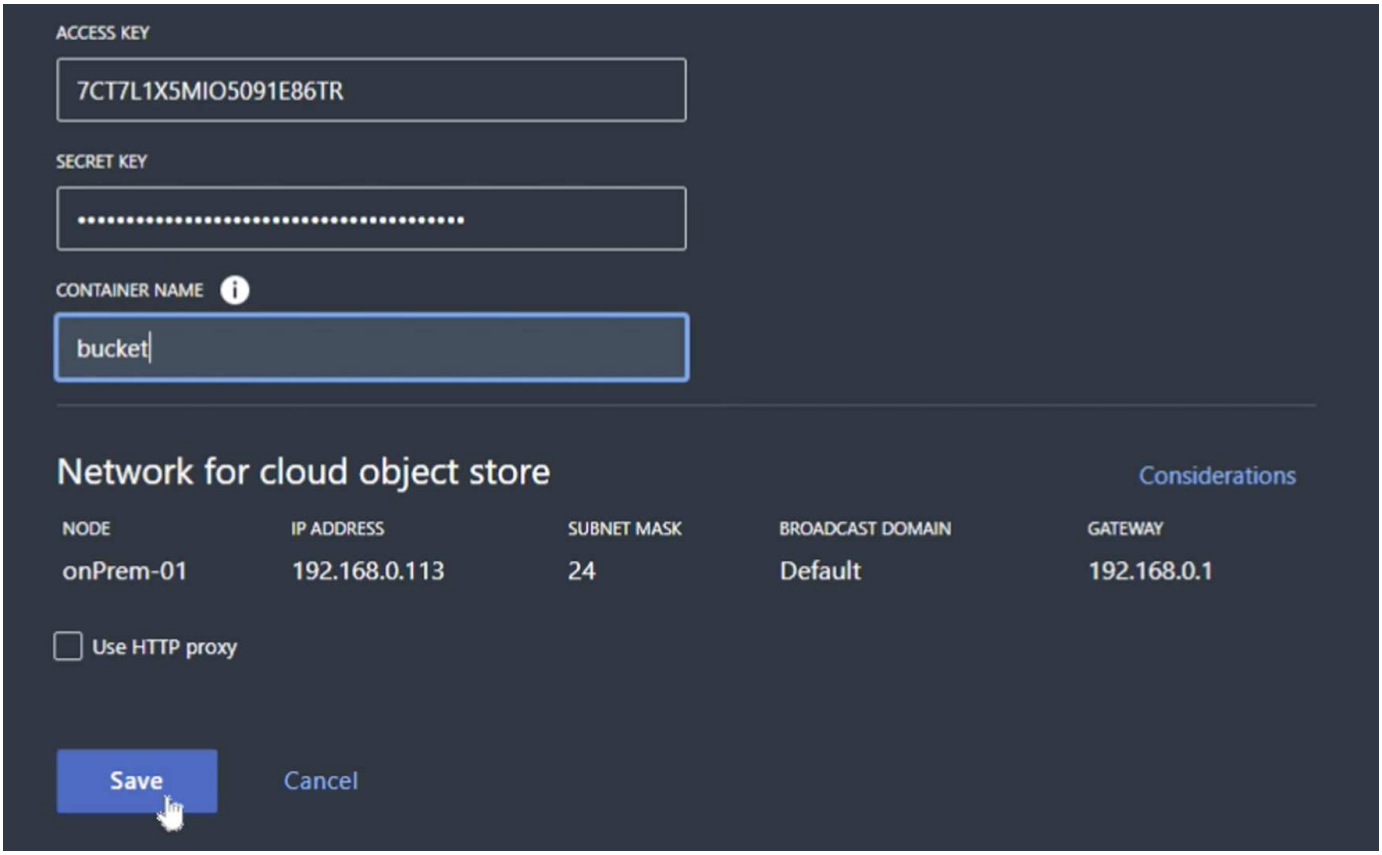
Inserisci le informazioni StorageGRID fornendo un nome, uno stile URL (per questa demo useremo gli URL Path-styl). Impostare l'ambito dell'archivio oggetti su "Storage VM".



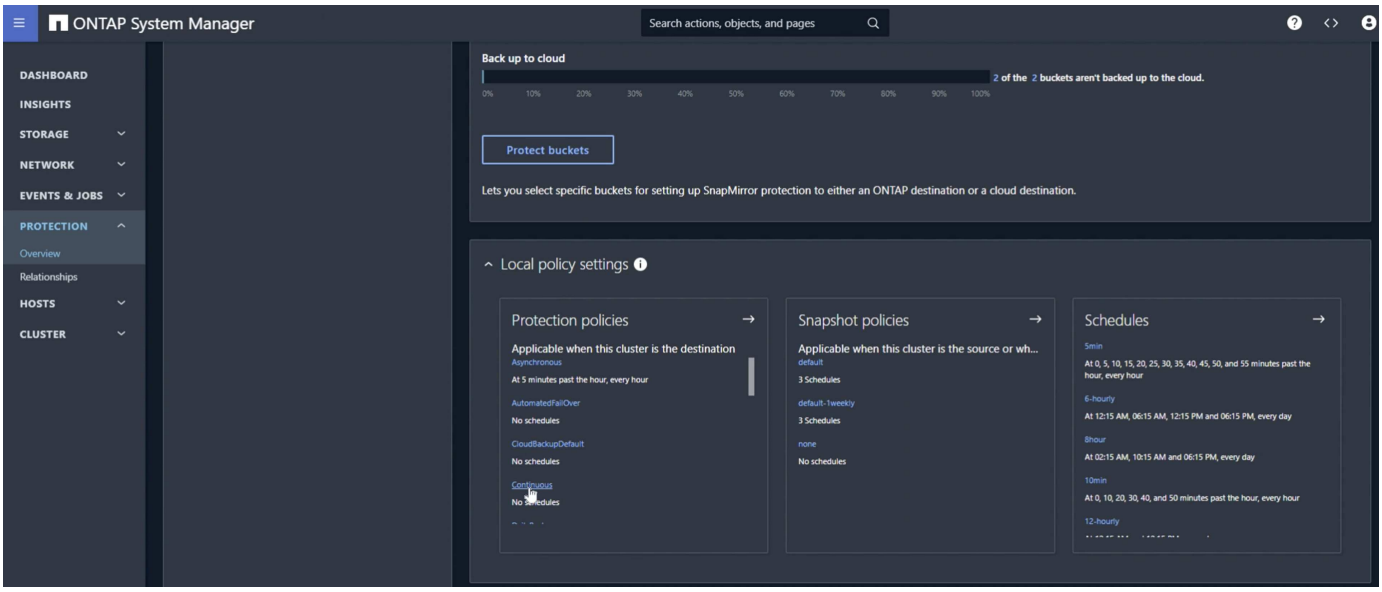
Se si utilizza SSL, impostare la porta dell'endpoint del bilanciamento del carico e copiarla nel certificato

dell'endpoint StorageGRID. Altrimenti deselezionare la casella SSL e immettere la porta dell'endpoint HTTP qui.

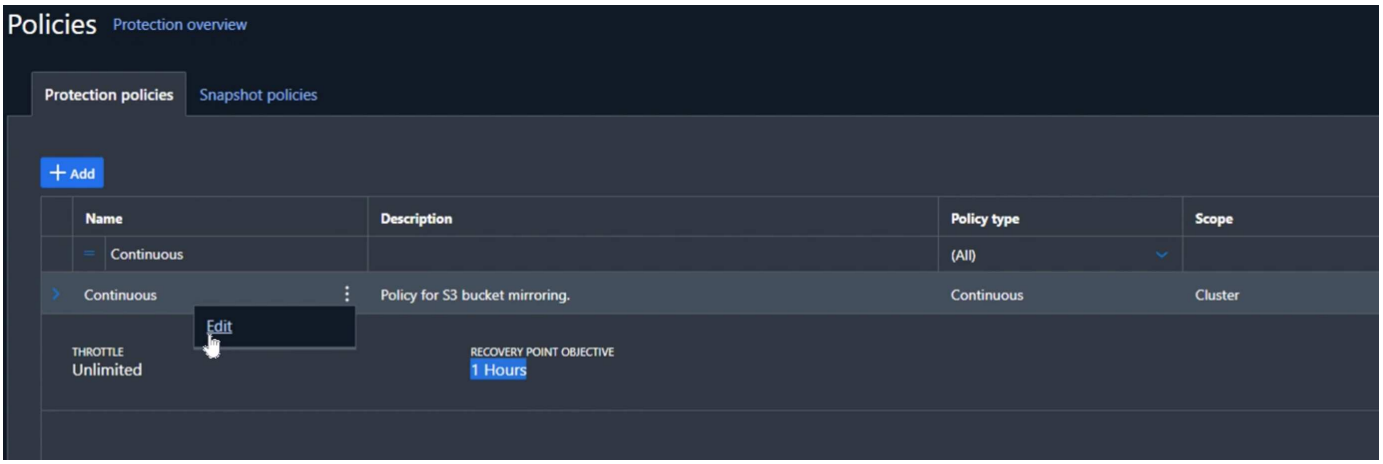
Immettere i tasti S3 dell'utente StorageGRID e il nome del bucket dalla configurazione StorageGRID riportata sopra per la destinazione.



Una volta configurata una destinazione, è possibile configurare le impostazioni dei criteri per la destinazione. Espandere "Impostazioni criteri locali" e selezionare "continuo".



Modificare il criterio continuo e modificare l'obiettivo del punto di ripristino da "1 ore" a "3 secondi".

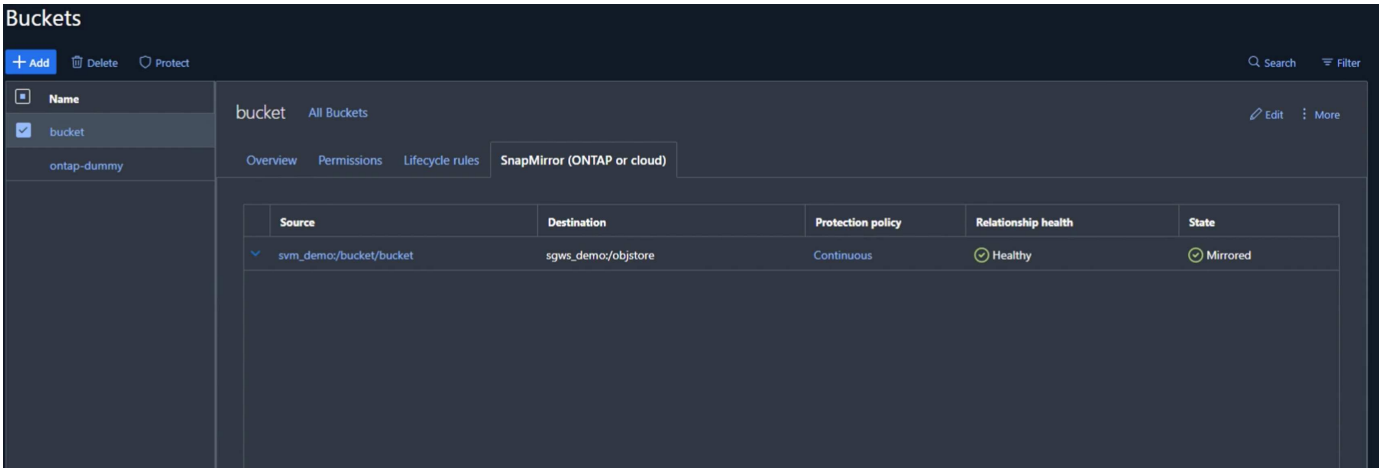


Ora possiamo configurare SnapMirror per replicare il bucket.

```
SnapMirror create -source-path sv_demo: /Bucket/bucket -destination-path sgws_demo: /Objstore -policy Continuous
```

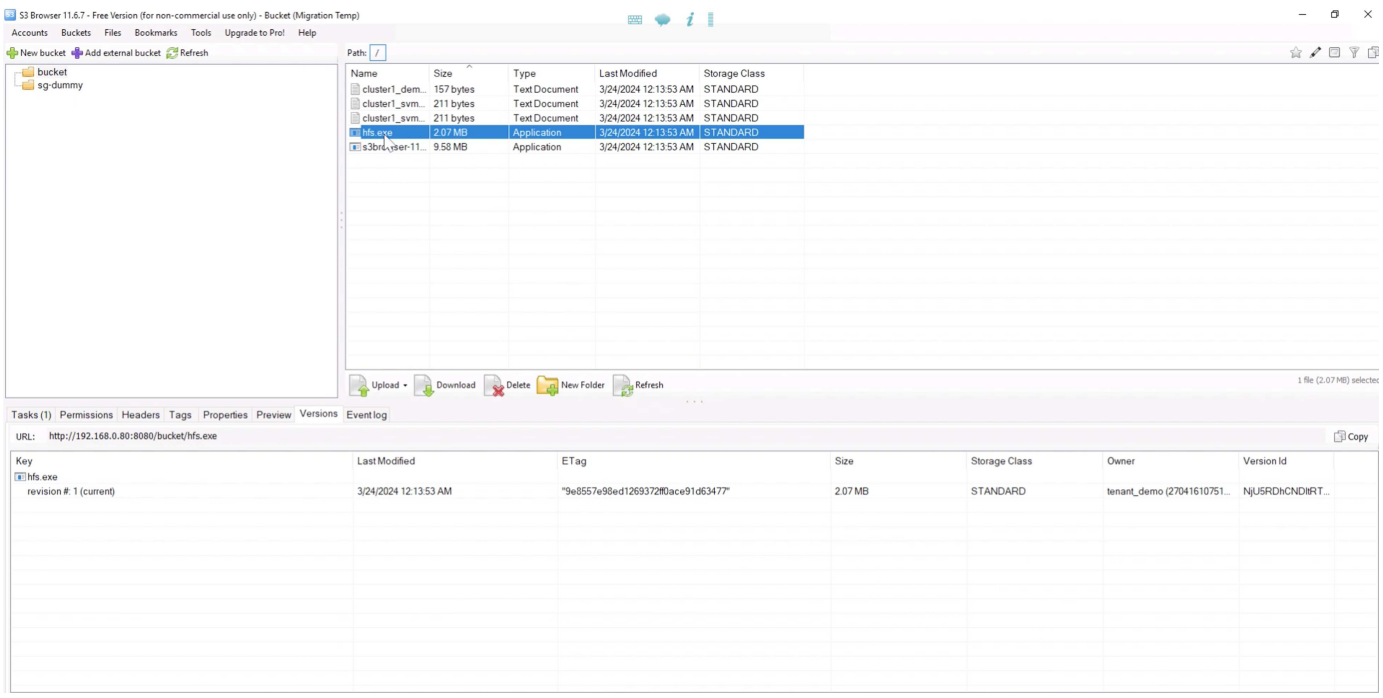
Il bucket mostrerà ora un simbolo di nuvola nell'elenco bucket sotto protezione.

Se si seleziona il bucket e si passa alla scheda "SnapMirror (ONTAP o Cloud)", verrà visualizzato lo stato di spedizione SnapMirror.

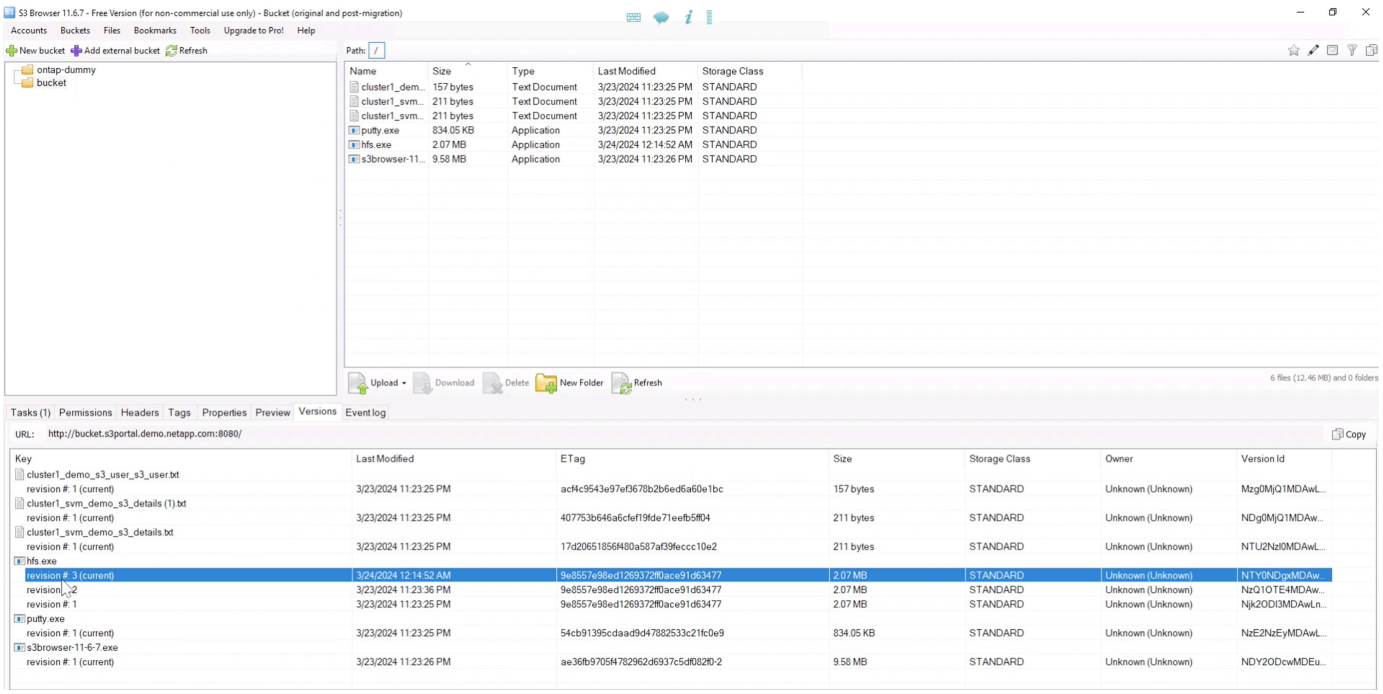


I dettagli della replica

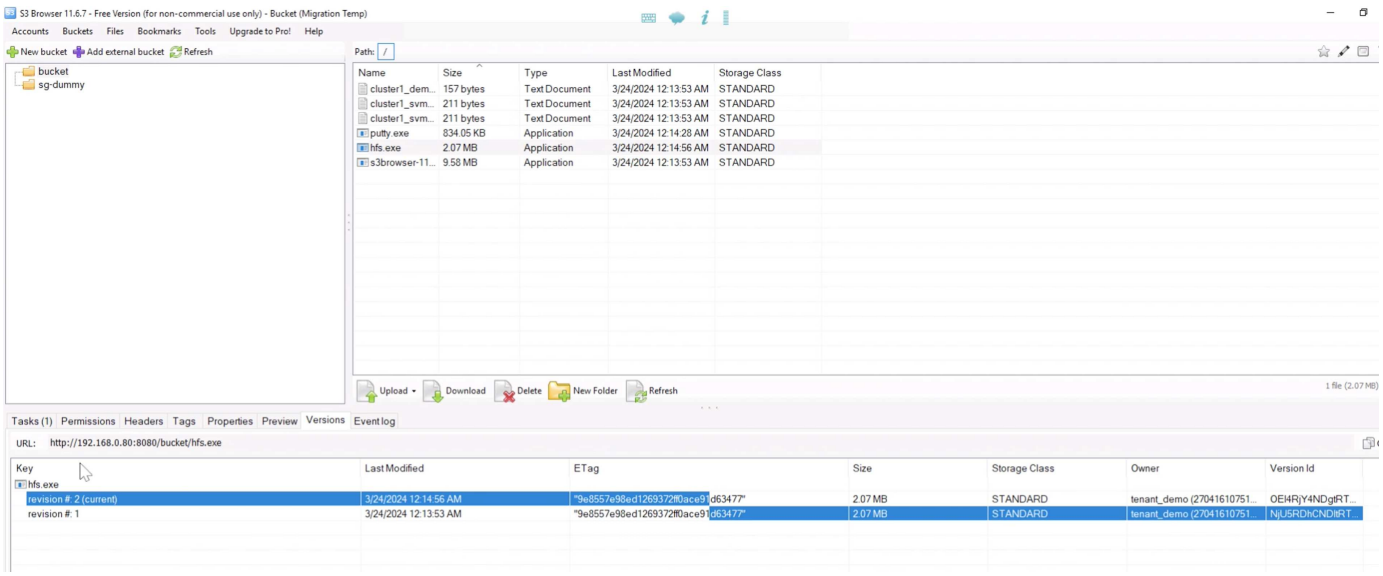
Ora disponiamo di un bucket di replica con successo da ONTAP a StorageGRID. Ma che cosa si replica? La nostra fonte e la nostra destinazione sono entrambi bucket in versione. Anche le versioni precedenti vengono replicate nella destinazione? Se guardiamo al nostro bucket StorageGRID con S3Browser vediamo che le versioni esistenti non sono state replicate e l'oggetto eliminato non esiste, né un marcatore di eliminazione per quell'oggetto. L'oggetto duplicato ha solo la versione 1 nel bucket StorageGRID.



Nel bucket ONTAP, si aggiunge una nuova versione allo stesso oggetto utilizzato in precedenza e si osserva come viene replicata.



Se guardiamo al lato StorageGRID vediamo che è stata creata anche una nuova versione in questo bucket, ma manca la versione iniziale da prima della relazione SnapMirror.



Questo perché il processo di ONTAP SnapMirror S3 replica solo la versione corrente dell'oggetto. Ecco perché abbiamo creato un bucket di versione sul lato StorageGRID per essere la destinazione. In questo modo StorageGRID può mantenere una cronologia delle versioni degli oggetti.

Di Rafael Guedes e Aron Klein

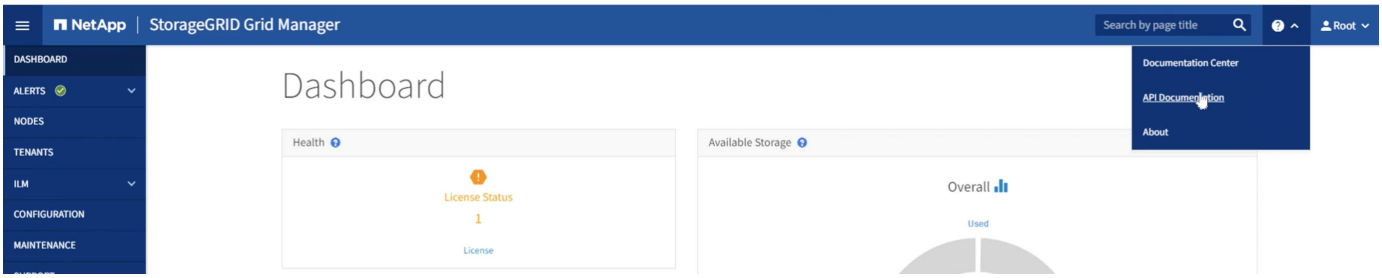
Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

Offerta di S3 Enterprise mediante la migrazione perfetta dello storage basato su oggetti da ONTAP S3 a StorageGRID

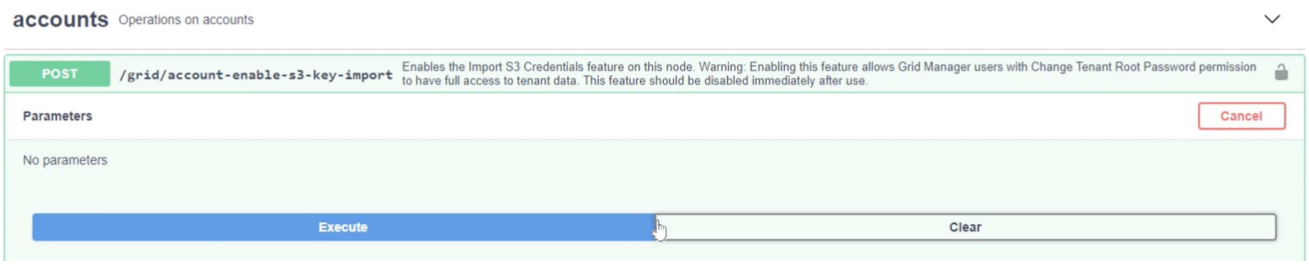
Migrare S3 chiavi

Per una migrazione, la maggior parte del tempo si desidera migrare le credenziali per gli utenti invece di generare nuove credenziali sul lato di destinazione. StorageGRID fornisce api per consentire l'importazione di S3 chiavi per un utente.

Accedendo all'interfaccia utente di gestione di StorageGRID (non all'interfaccia utente di gestione tenant), aprire la pagina dello swap della documentazione API.

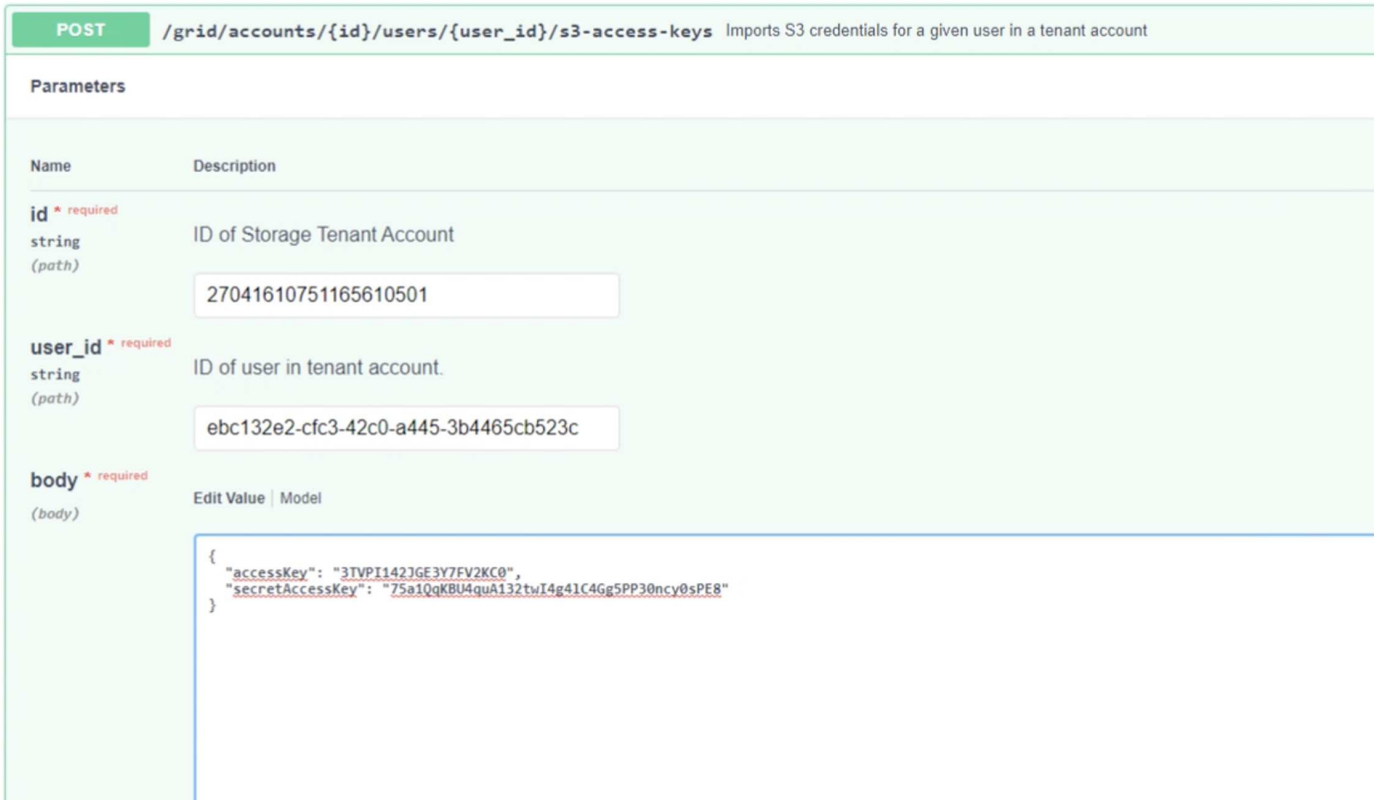


Espandere la sezione "account", selezionare "POST /grid/account-enable-S3-key-import", fare clic sul pulsante "prova", quindi fare clic sul pulsante "Esegui".

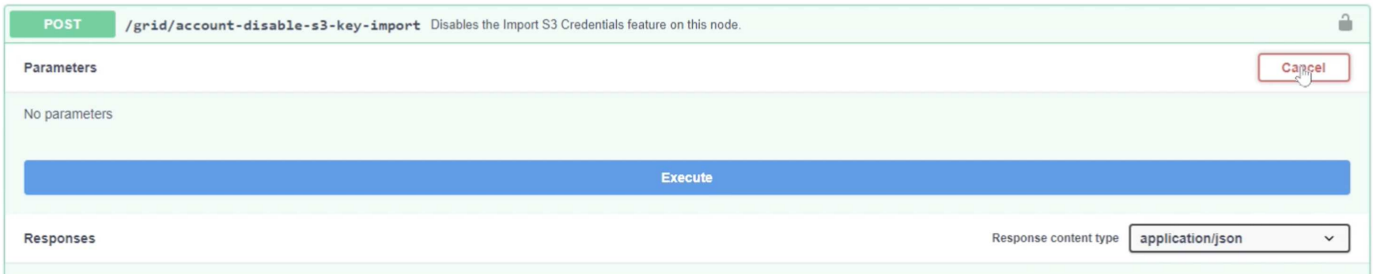


Ora scorri verso il basso ancora sotto "Accounts" fino a "POST /grid/accounts/{id}/users/{user_id}/S3-access-keys"

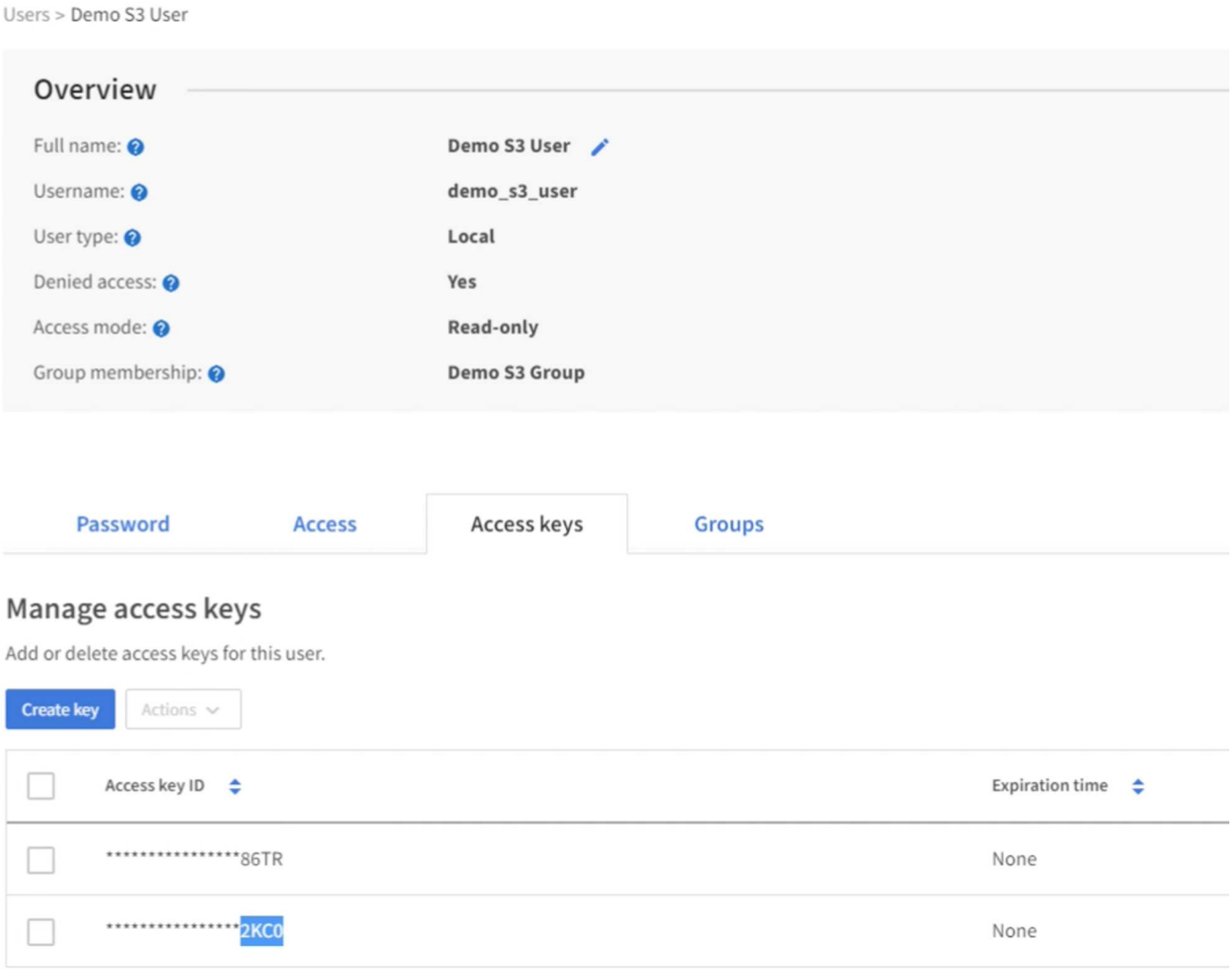
Qui è dove stiamo andando inserire l'ID del inquilino e l'ID dell'account utente che abbiamo raccolto in precedenza. Compilare i campi e le chiavi del nostro utente ONTAP nella casella json. È possibile impostare la scadenza delle chiavi, o rimuovere il " , "expires": 123456789" e fare clic su execute.



Una volta completate tutte le importazioni della chiave utente, disabilitare la funzione di importazione della chiave in "account" "POST /grid/account-disable-S3-key-import"



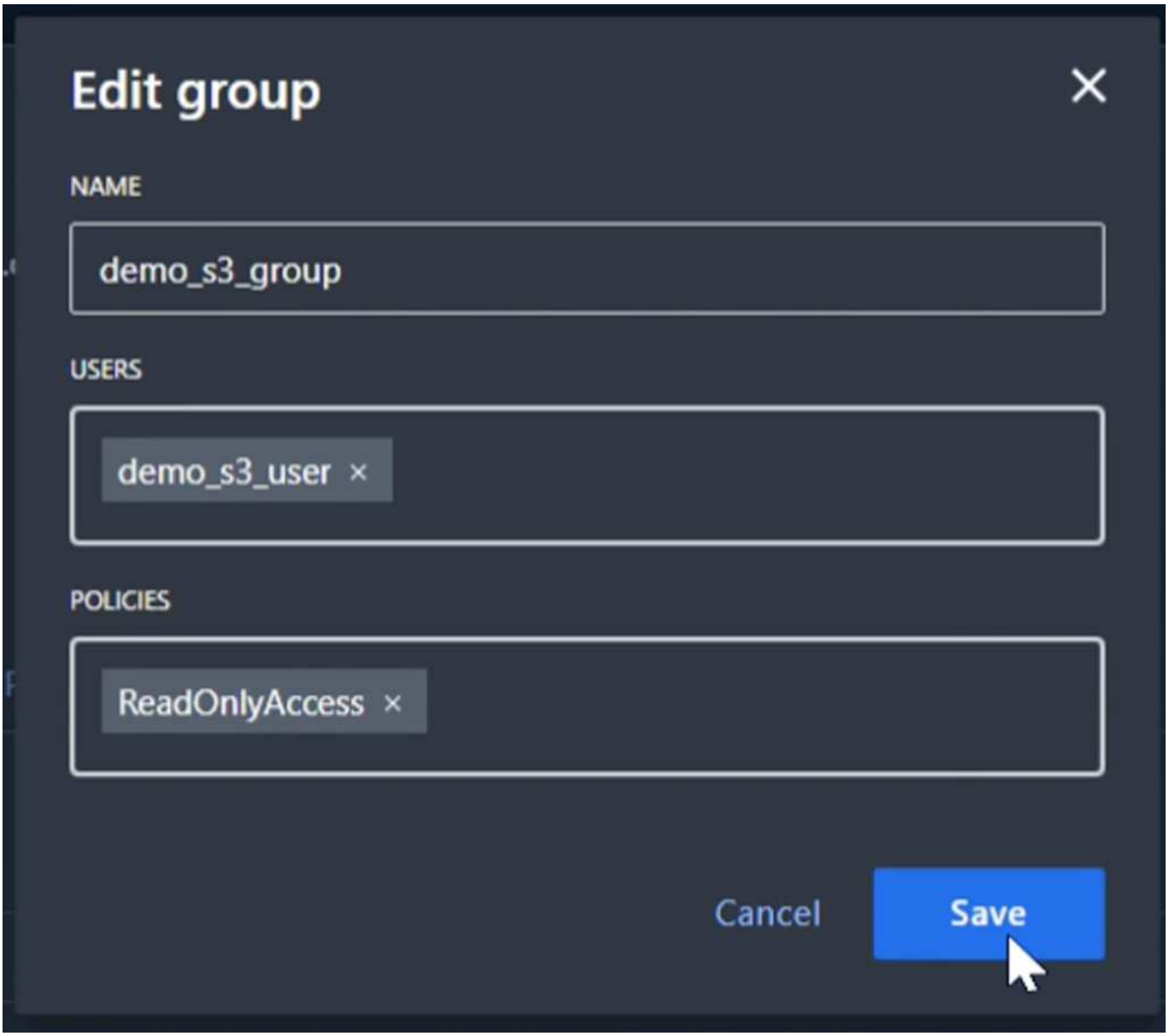
Se guardiamo l'account utente nell'interfaccia utente del gestore tenant, possiamo vedere che è stata aggiunta la nuova chiave.



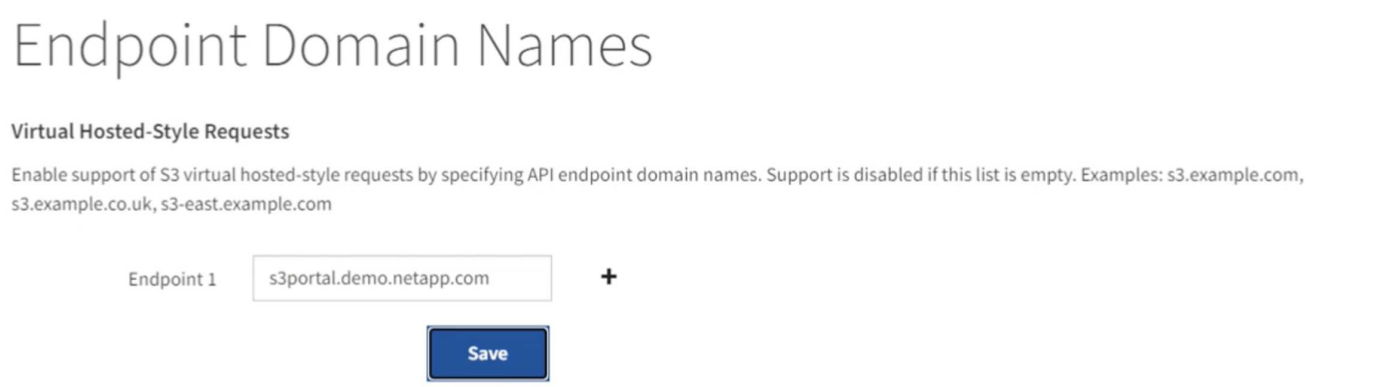
Il taglio finale

Se l'intenzione è quella di avere un bucket a replica perpetua da ONTAP a StorageGRID, puoi finire qui. Se si tratta di una migrazione da ONTAP S3 a StorageGRID, allora è il momento di mettervi fine e tagliare.

In Gestione di sistema di ONTAP, modificare il gruppo S3 e impostarlo su "ReadOnlyAccess". In questo modo gli utenti non potranno più scrivere nel bucket ONTAP S3.



Tutto ciò che resta da fare è configurare il DNS in modo che punti dal cluster ONTAP all'endpoint StorageGRID. Assicurarsi che il certificato dell'endpoint sia corretto e, se sono necessarie richieste di stile ospitate virtuali, aggiungere i nomi di dominio dell'endpoint in StorageGRID



I client dovranno attendere la scadenza del TTL o scaricare il DNS per risolvere il problema nel nuovo sistema in modo da poter verificare che tutto funzioni. Resta solo ripulire le chiavi S3 temporanee iniziali utilizzate per verificare l'accesso ai dati StorageGRID (NON alle chiavi importate), rimuovere le relazioni SnapMirror e rimuovere i dati ONTAP.

Di Rafael Guedes e Aron Klein

Guide agli strumenti e alle applicazioni

USA il connettore S3A di Cloudera Hadoop con StorageGRID

Di Angela Cheng

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

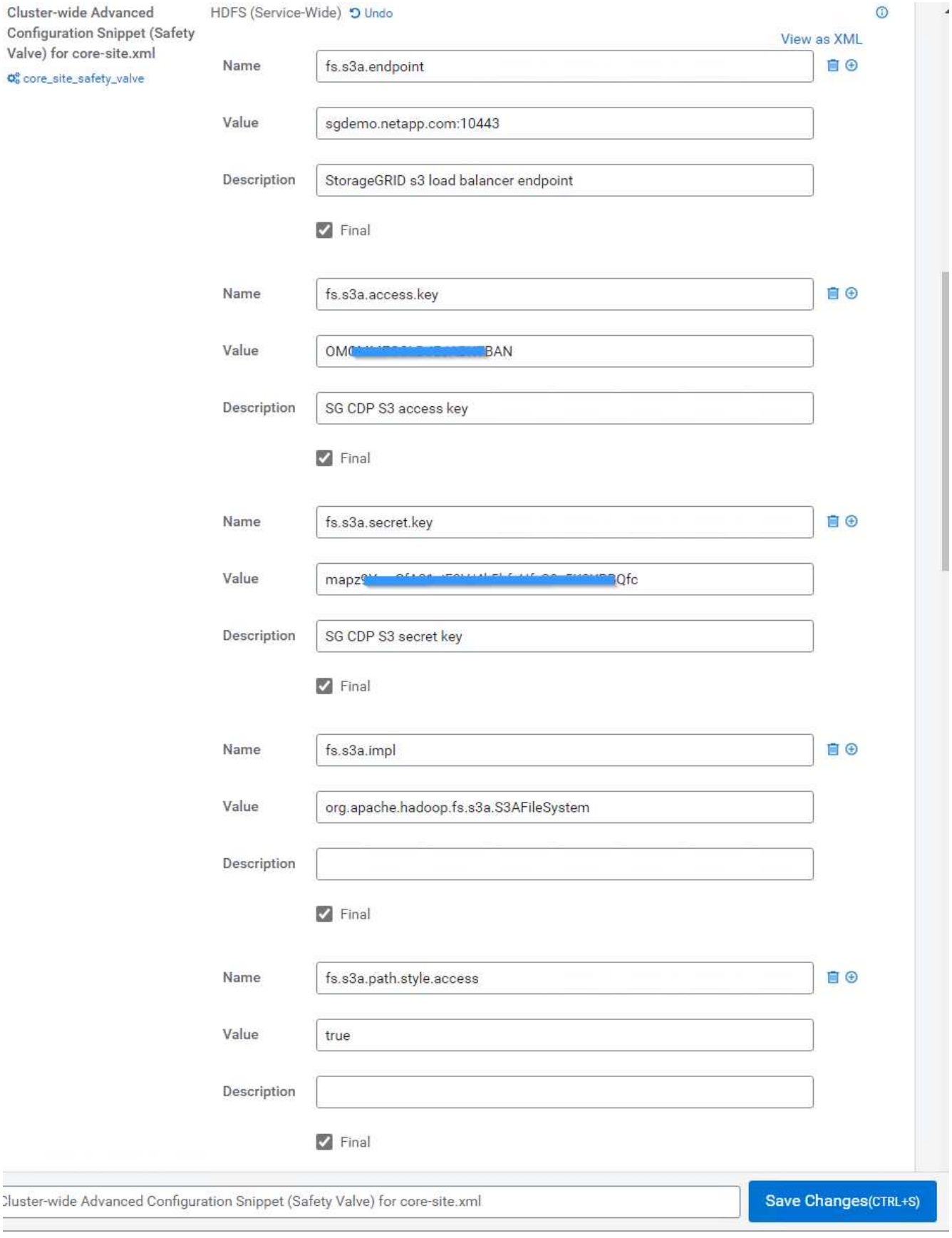
Fasi

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.

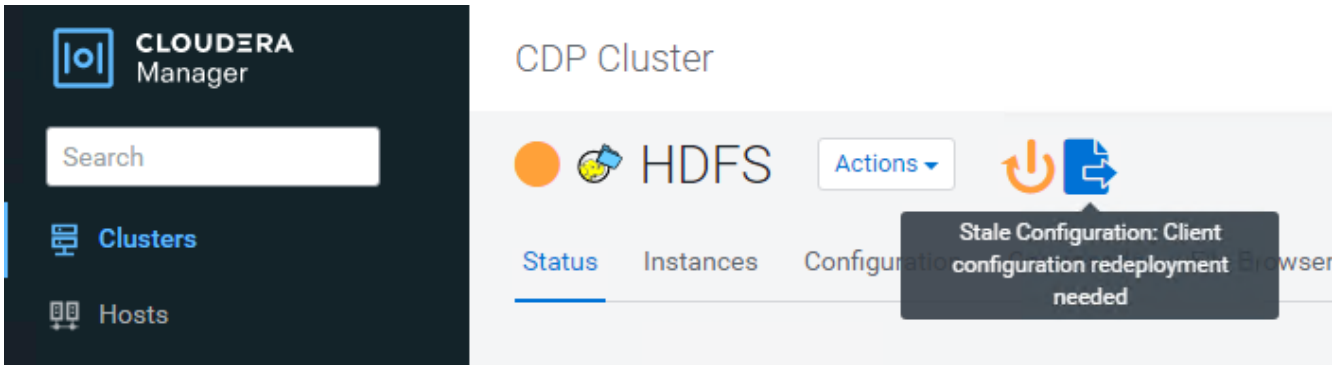
Nome	Valore
fs.s3a.access.key	*<chiave di accesso s3 tenant da StorageGRID>*
fs.s3a.secret.key	*<chiave segreta s3 tenant da StorageGRID>*
fs.s3a.connection.ssl.enabled	[true o false] (l'impostazione predefinita è https se questa voce non è presente)
fs.s3a.endpoint	*<StorageGRID S3 endpoint:porta>*

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

Di Aron Klein

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
```

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

Di Angela Cheng

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.

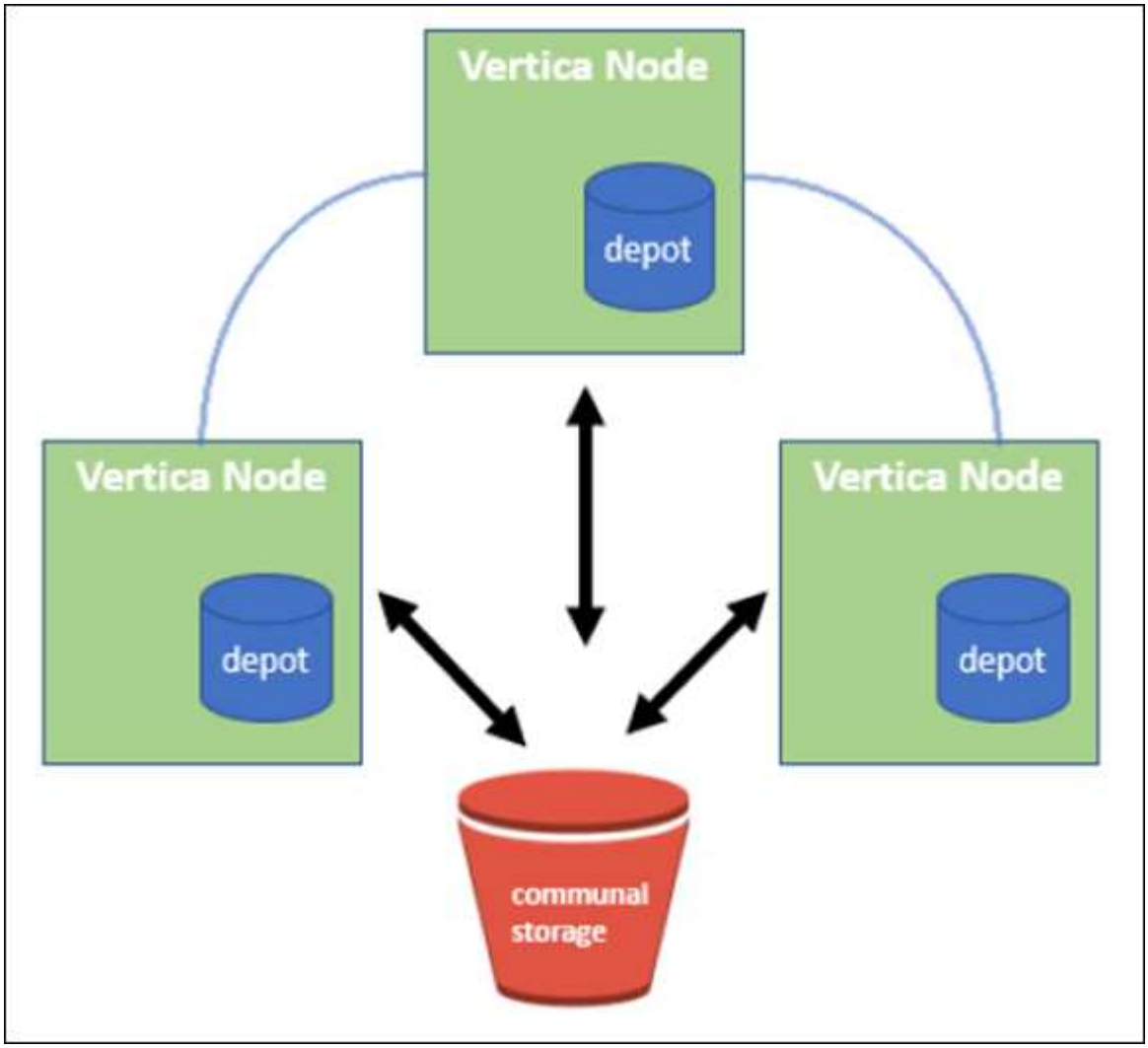
Le modalità EON ed Enterprise si differenziano principalmente per la posizione in cui memorizzano i dati:

- 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

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
145	s3://vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a21_0_0.dfs
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

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
133	s3://vertica/b98/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a4d_0_0.dfs
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/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602.tar
204217344	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610.tar
16109056	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000217e0.tar
12853248	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800.tar
8937984	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a.tar

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
56260608	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000218b2.tar
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

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
2958	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/chkpt_1.cat.gz
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

Dimensione oggetto (byte)	Percorso completo della chiave bucket/oggetto
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
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

Di Angela Cheng

Con la funzione di inoltro syslog di StorageGRID, è possibile configurare un server syslog esterno per raccogliere e analizzare i messaggi di registro StorageGRID. ELK (Elasticsearch, Logstash, Kibana) è diventata una delle soluzioni di analisi dei log più diffuse. Osservare la "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 relativi alle richieste S3 non riuscite. StorageGRID 11,9 supporta l'esportazione del log di accesso agli endpoint del bilanciamento del carico nel server syslog esterno. Guarda questo "Video di YouTube" articolo per saperne di più su questa nuova funzionalità. 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

- "Scaricare il pacchetto file di esempio Logstash 8.x per StorageGRID 11,9" + **md5 checksum** 41272857c4a54600f95995f6ed74800d + **sha256 checksum** 67048e8661052719990851e1ad960d4902fe537a6e135e8600177188da6779c9

Assunzione

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

Istruzioni

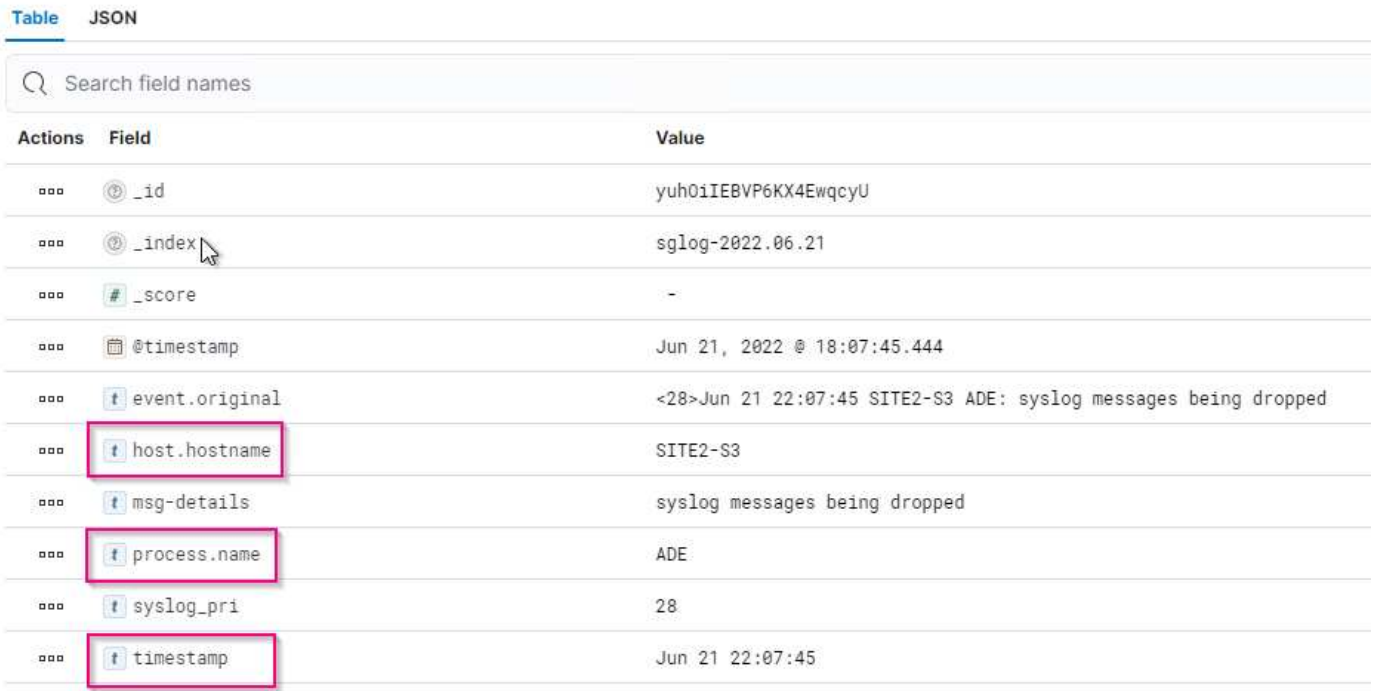
Due versioni di esempio sono fornite a causa delle differenze nei nomi definiti dai modelli grok. Ad esempio, il modello SYSLOGBASE grok nel file di configurazione di Logstash definisce i nomi dei campi in modo diverso a seconda della versione di Logstash installata.

```
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
```

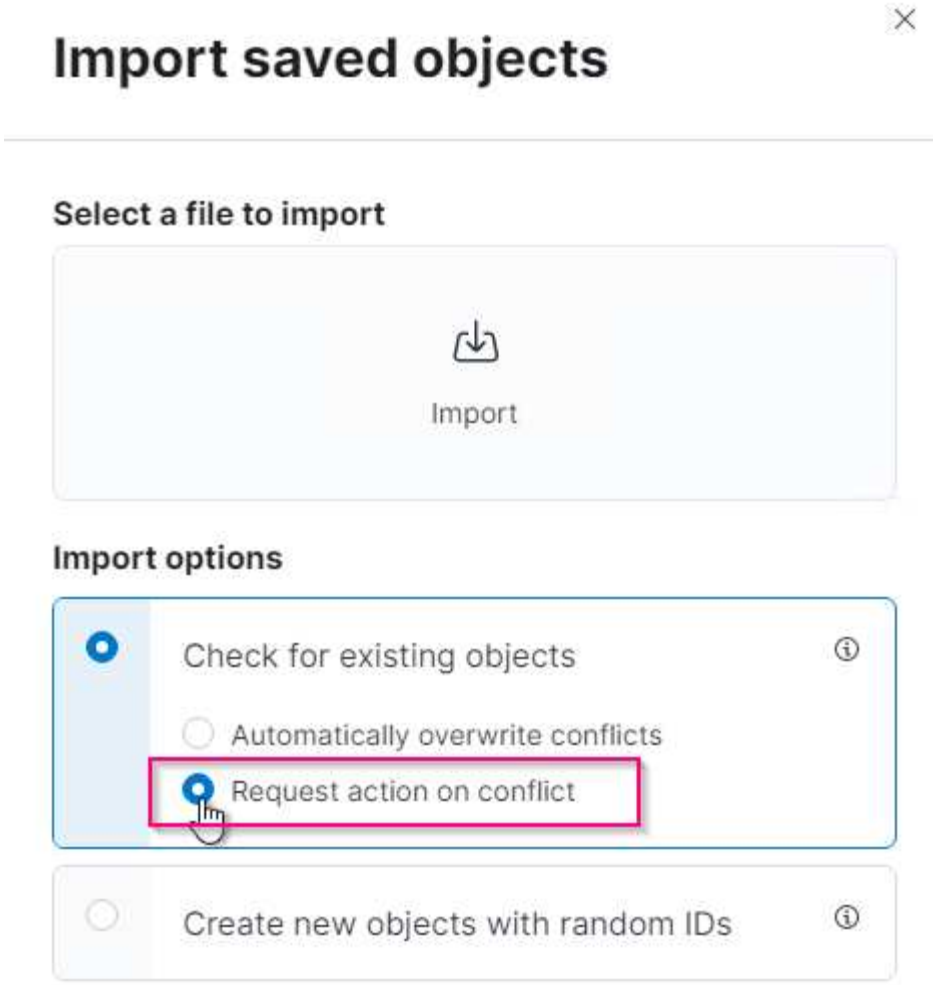
4. Controllare /var/log/logstash/logstash-plain.log e verificare che non ci siano errori durante l'avvio di Logstash con il nuovo file di configurazione.
5. Verificare che la porta TCP sia stata avviata e in attesa. + in questo esempio, viene utilizzata la porta TCP 5000.

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

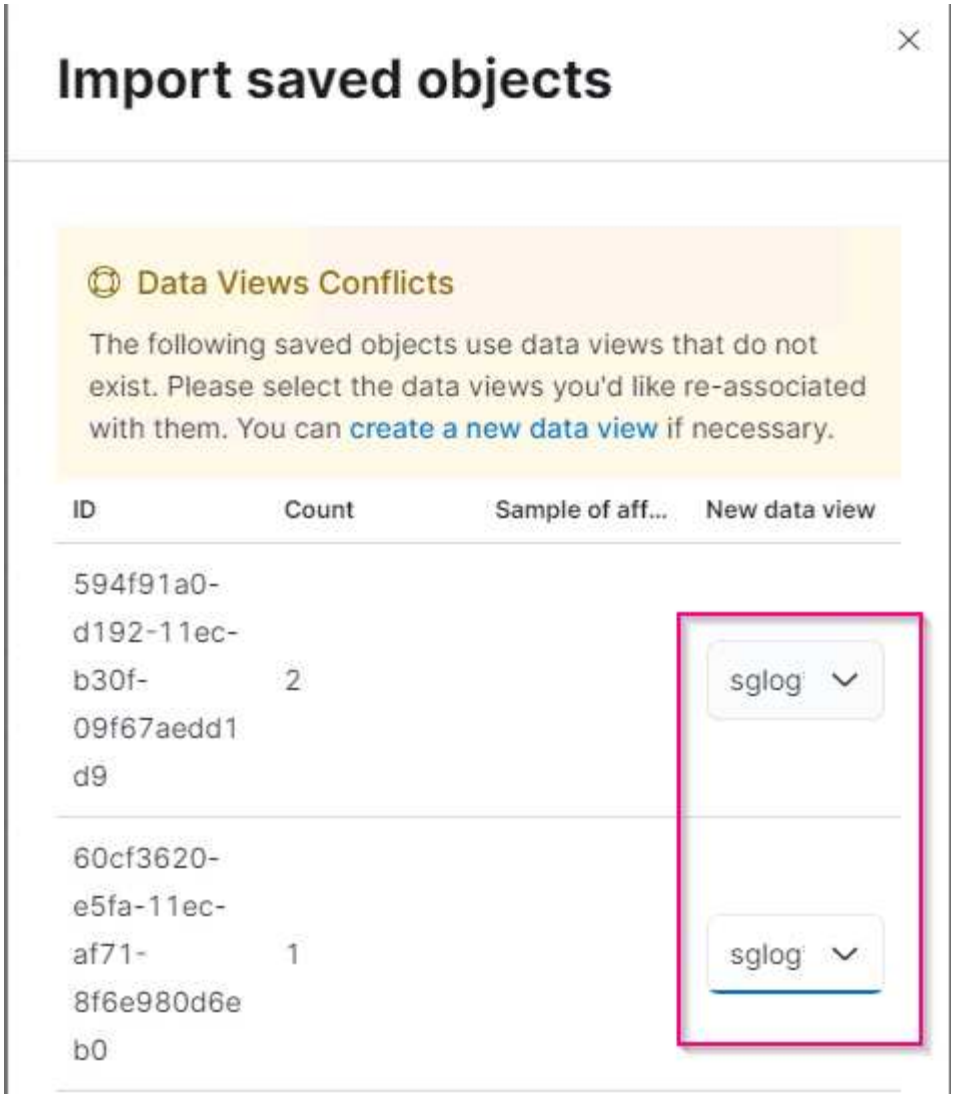
6. Dalla GUI di StorageGRID Manager, configurare il server syslog esterno per l'invio dei messaggi di log a Logstash. Per ulteriori informazioni, fare riferimento alla "video dimostrativo" .
7. È necessario configurare o disattivare il firewall sul server Logstash per consentire la connessione dei nodi 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 + * avviso livello di accesso o superiore + * evento di sicurezza non riuscito + * nginx-gw log di accesso endpoint (disponibile solo in elk8-sample-for-sg119.zip) + **grafico** + * S3 conteggio richieste basato su bycast.log + * Codice di stato HTTP + * tipo di controllo + tempo di risposta medio del dashboard * S3 msg del dashboard * dati di analisi del dashboard * dati del tipo di analisi del dashboard * S3.

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"

Utilizza Prometheus e Grafana per estendere la conservazione delle metriche

Di Aron Klein

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

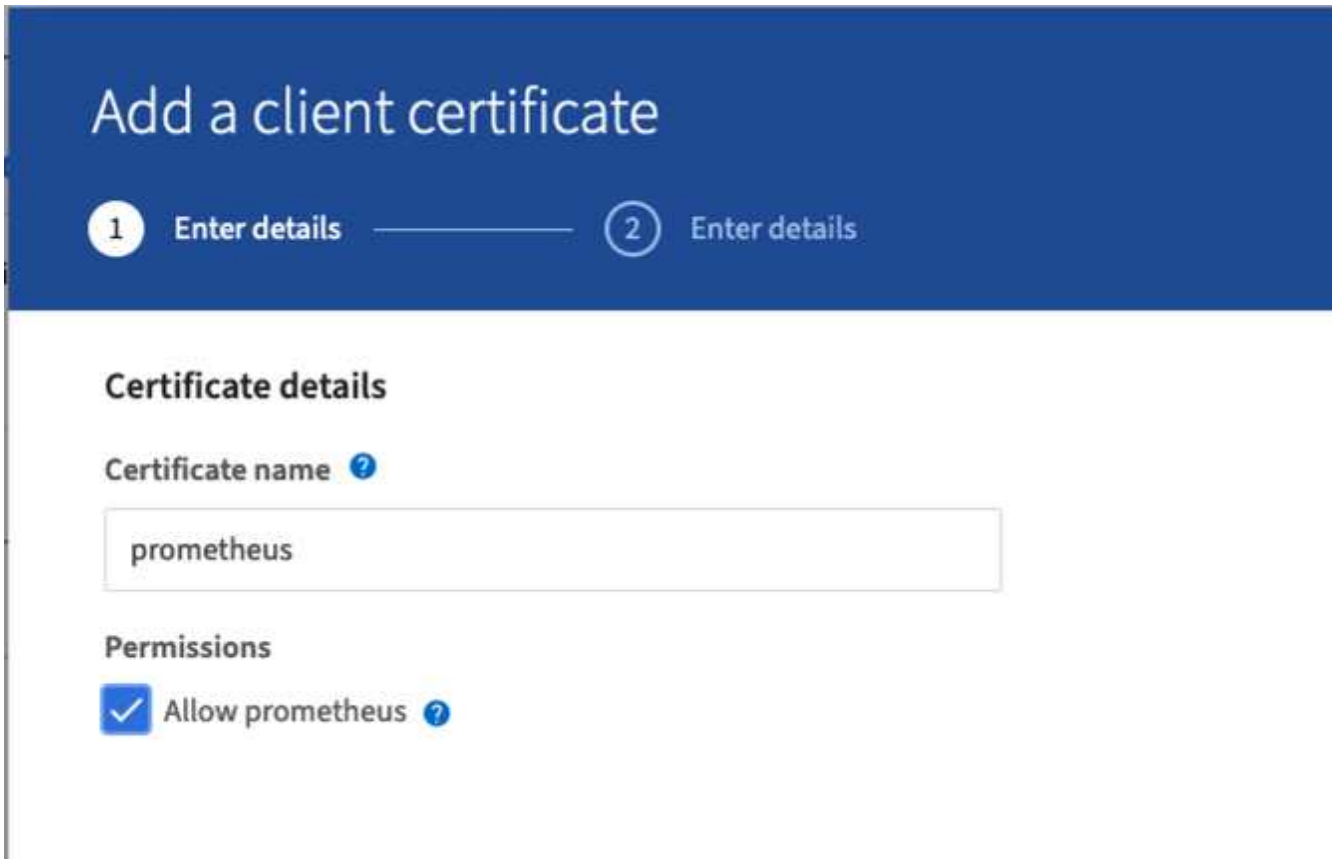
Dettagli del laboratorio

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.

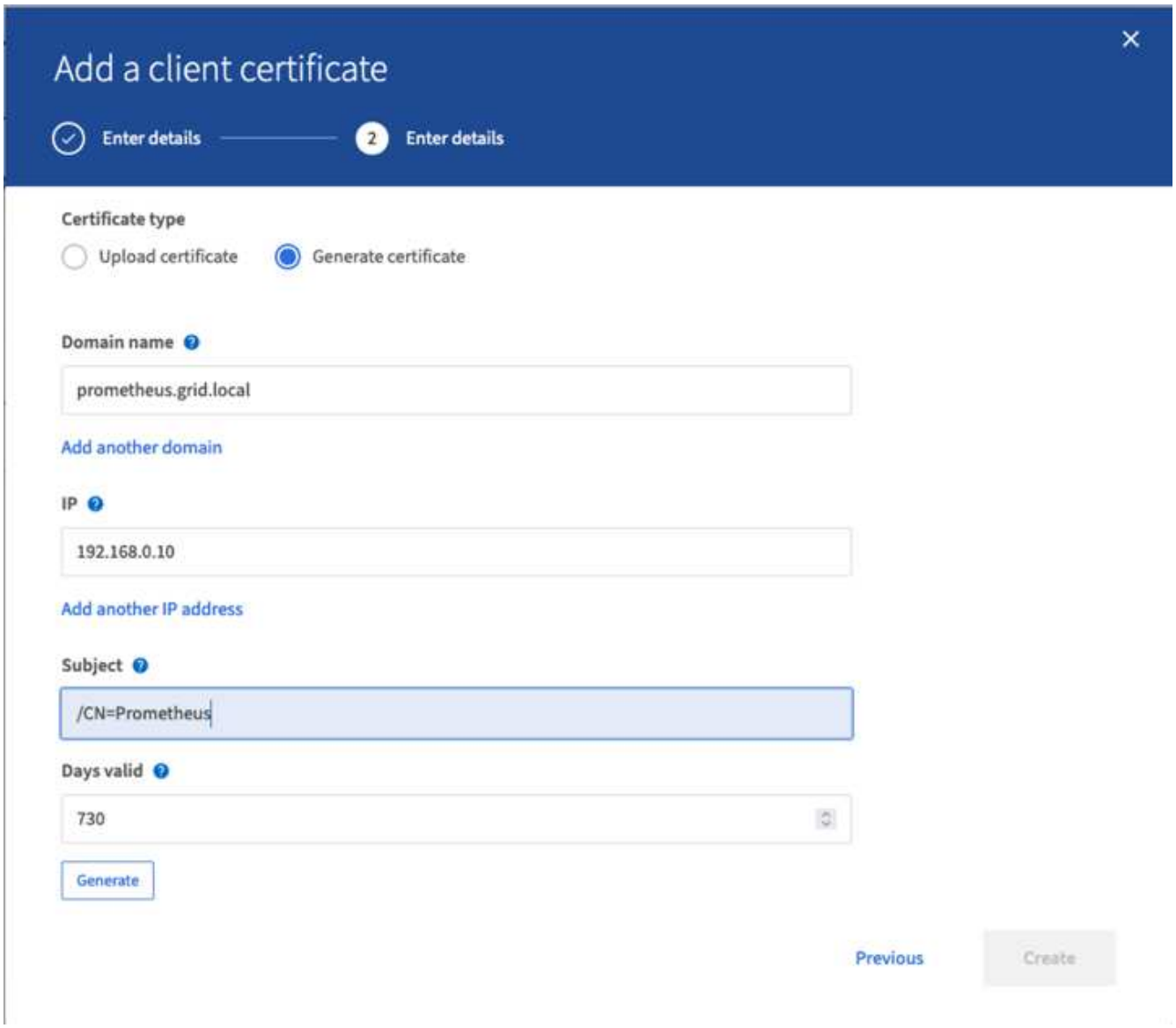
Configurare StorageGRID per l'accesso al client Prometheus

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.

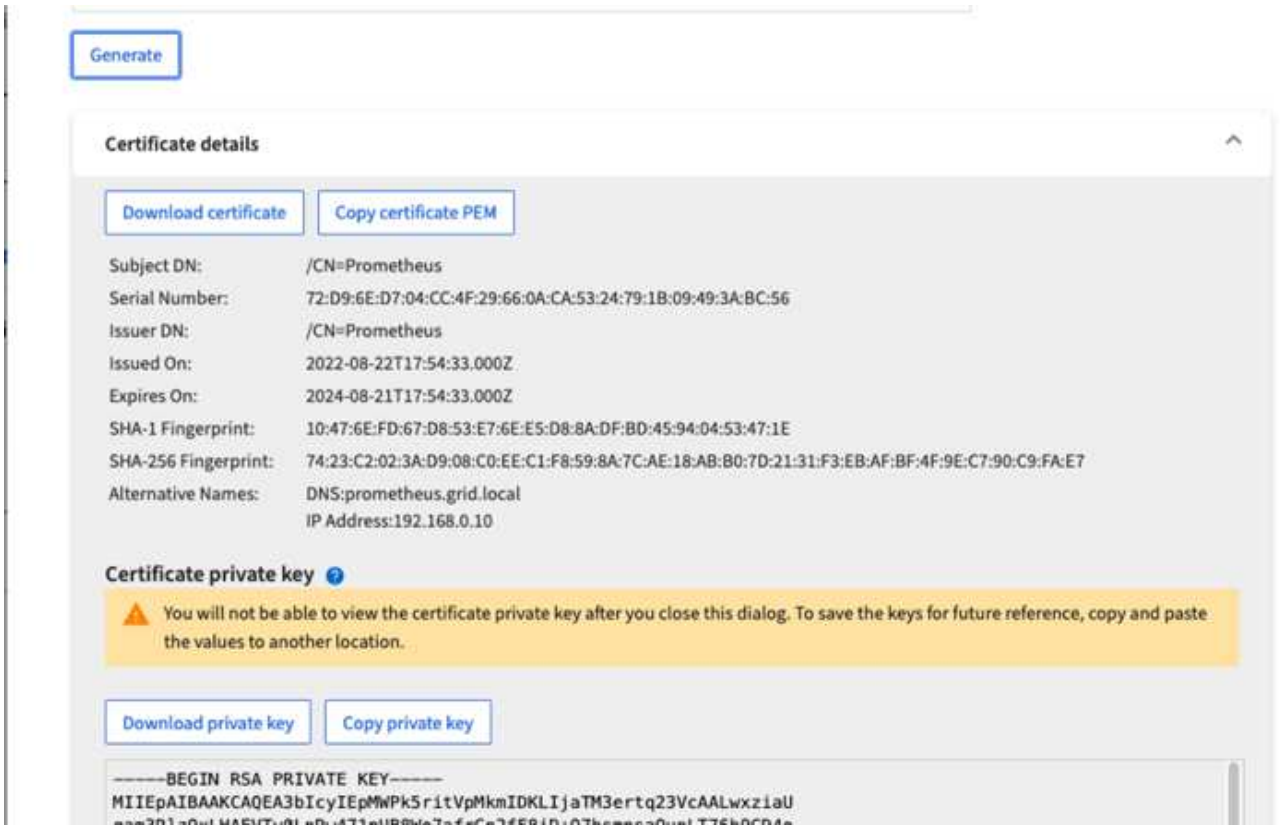


4. Se si dispone di un certificato firmato dalla CA, è possibile selezionare il pulsante di opzione "carica certificato", ma in questo caso StorageGRID genererà il certificato client selezionando il pulsante di opzione "genera certificato". Vengono visualizzati i campi obbligatori da compilare. Inserire 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.

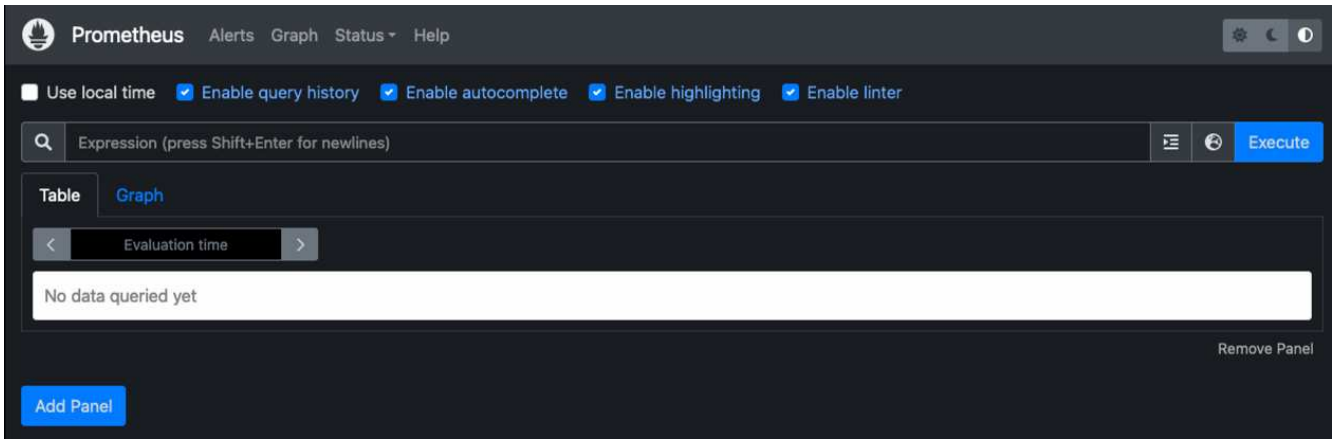
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. Verificare che il servizio sia in funzione correttamente

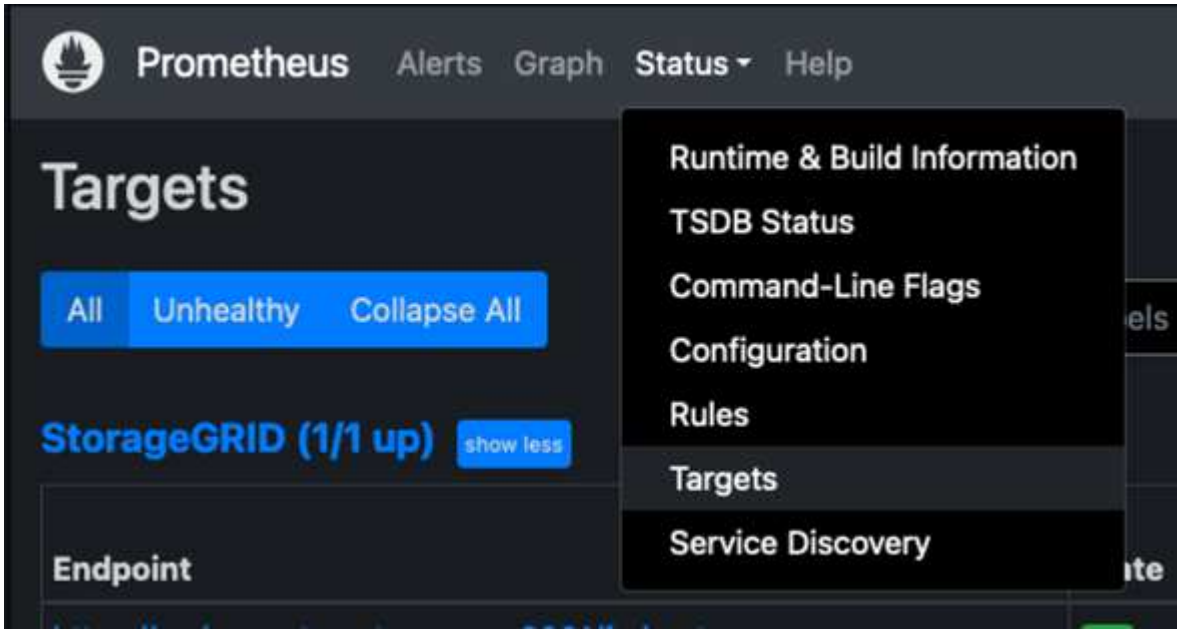
```
sudo systemctl status prometheus
```

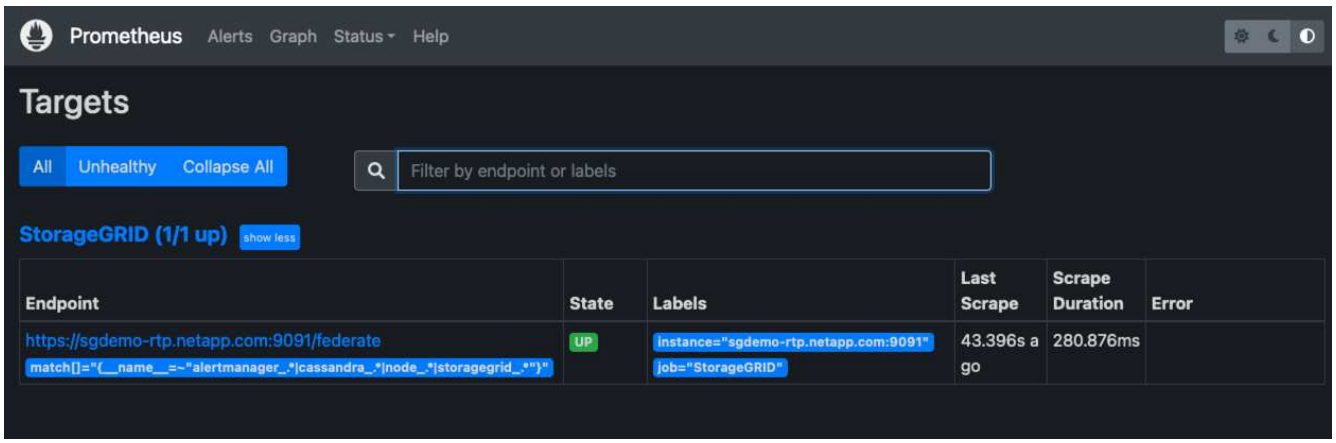
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 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

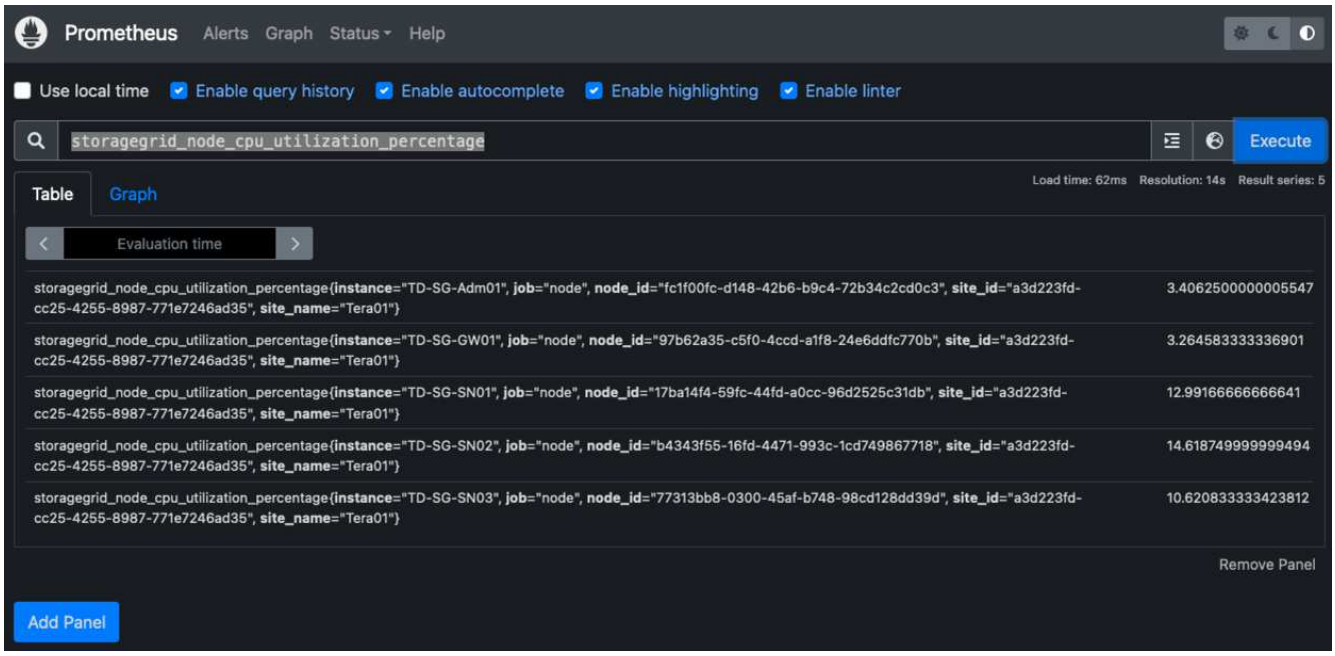


7. Sotto "Stato", è possibile visualizzare lo stato dell'endpoint StorageGRID configurato in prometheus.yml





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.

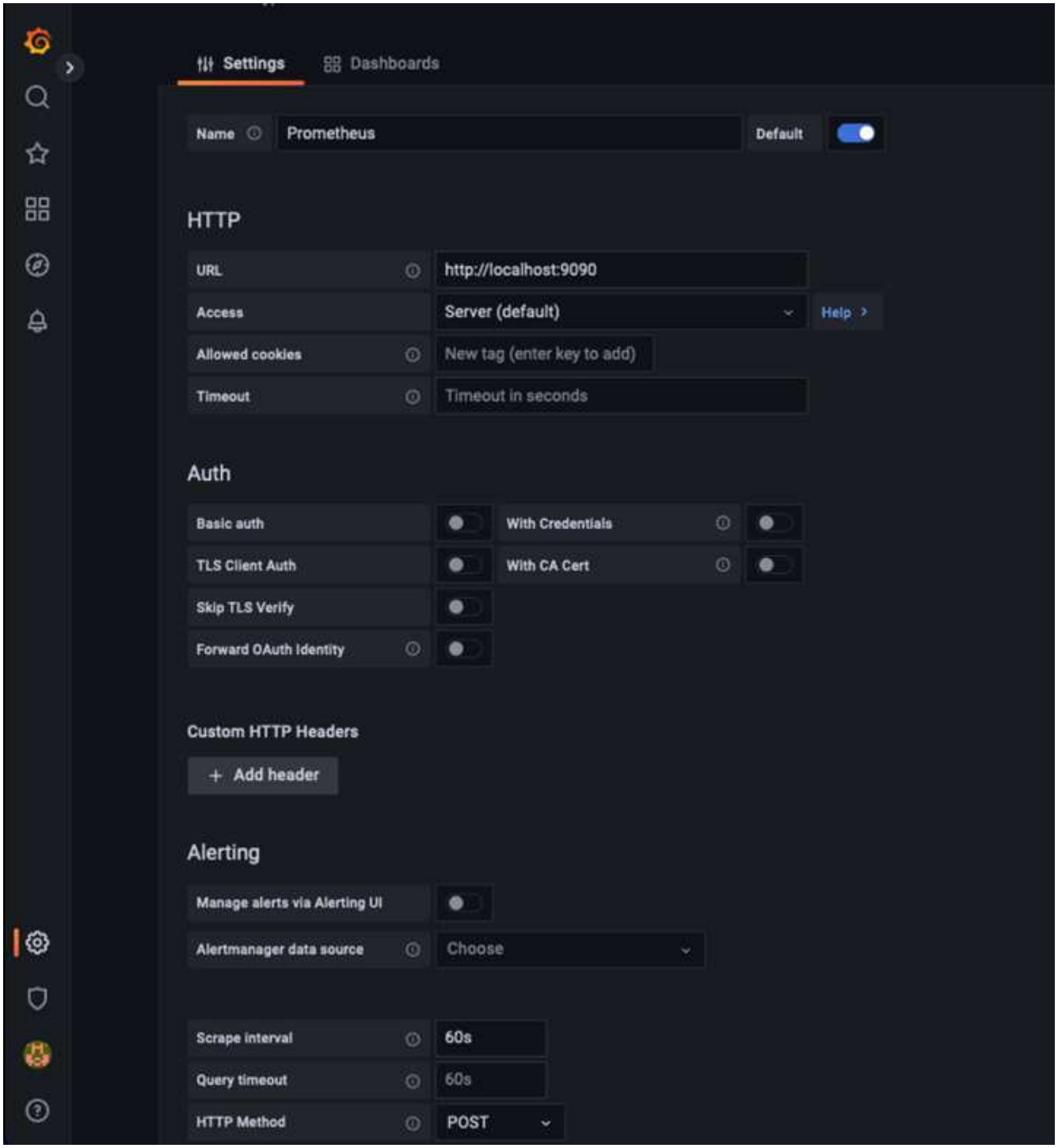
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

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.

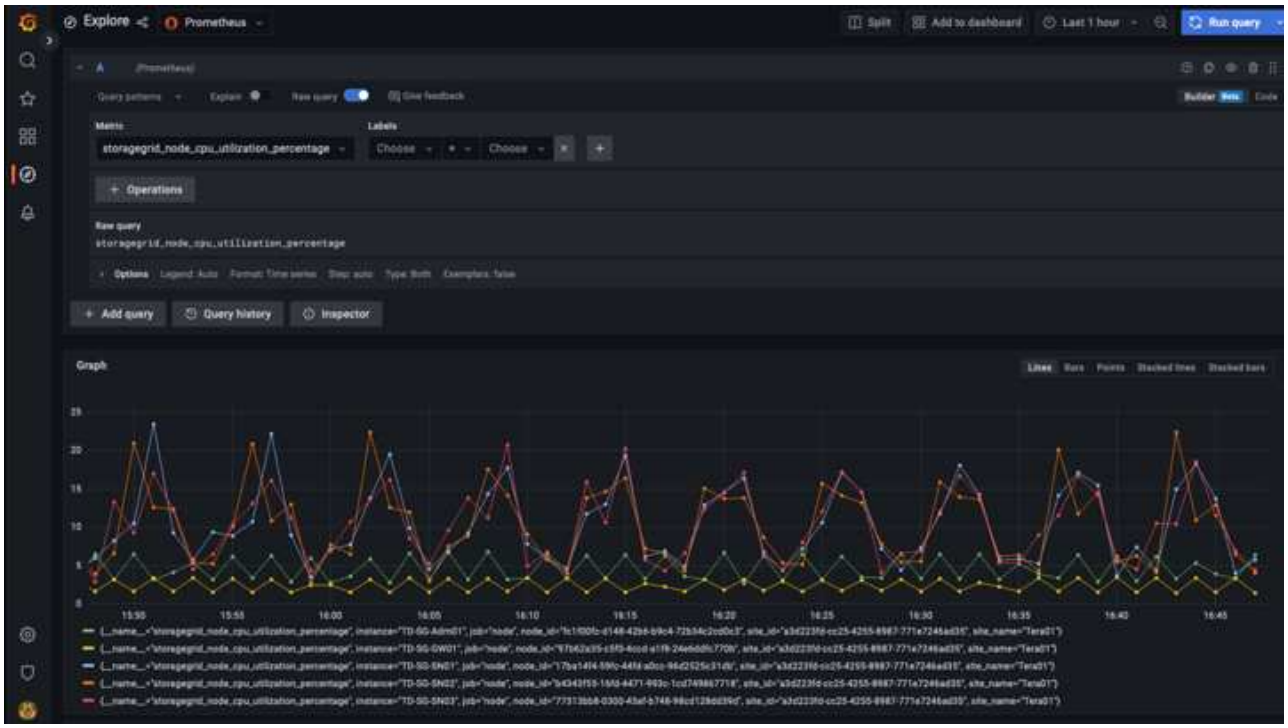
Creare una dashboard Grafana per StorageGRID

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

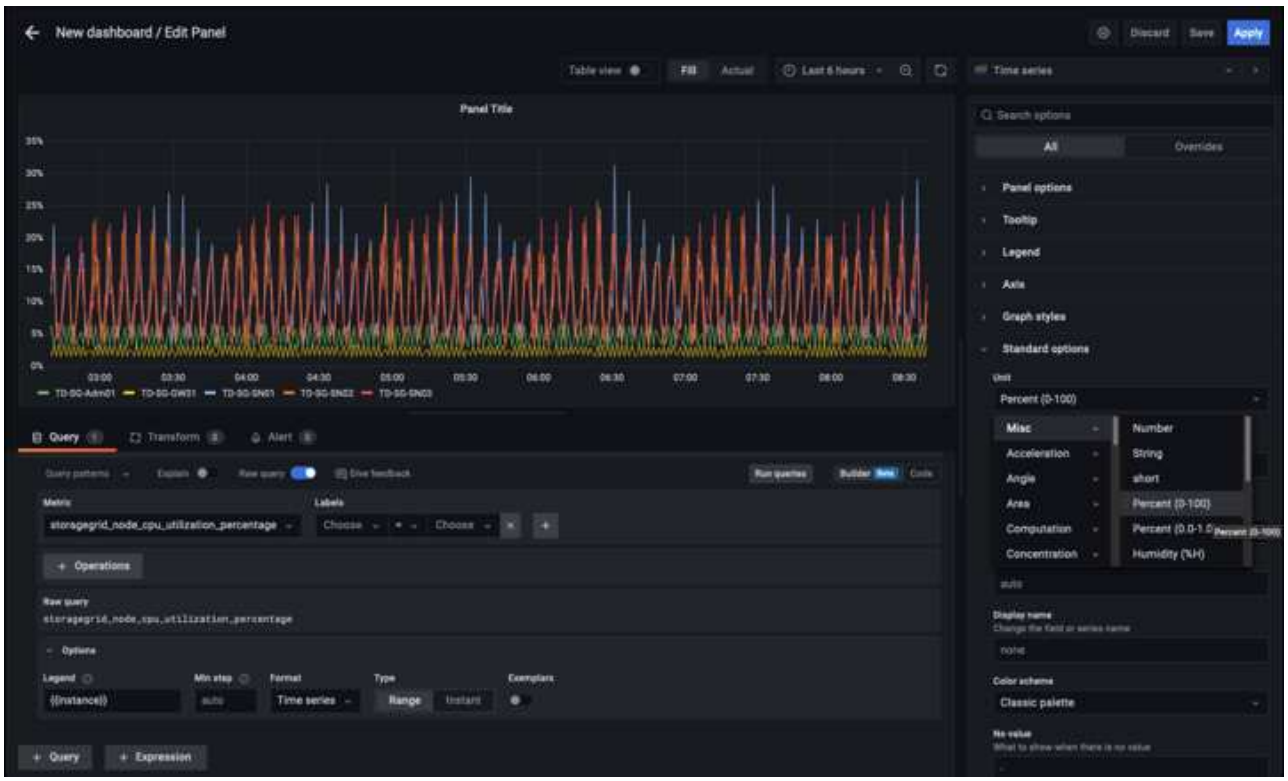
1. Nel riquadro di sinistra, espandere "Configuration" (Configurazione) e selezionare "Data Sources" (origini dati), quindi fare clic sul pulsante "Add Data Source" (Aggiungi origine dati)
2. Prometheus sarà una delle principali fonti di dati tra cui scegliere. In caso contrario, utilizzare la barra 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"



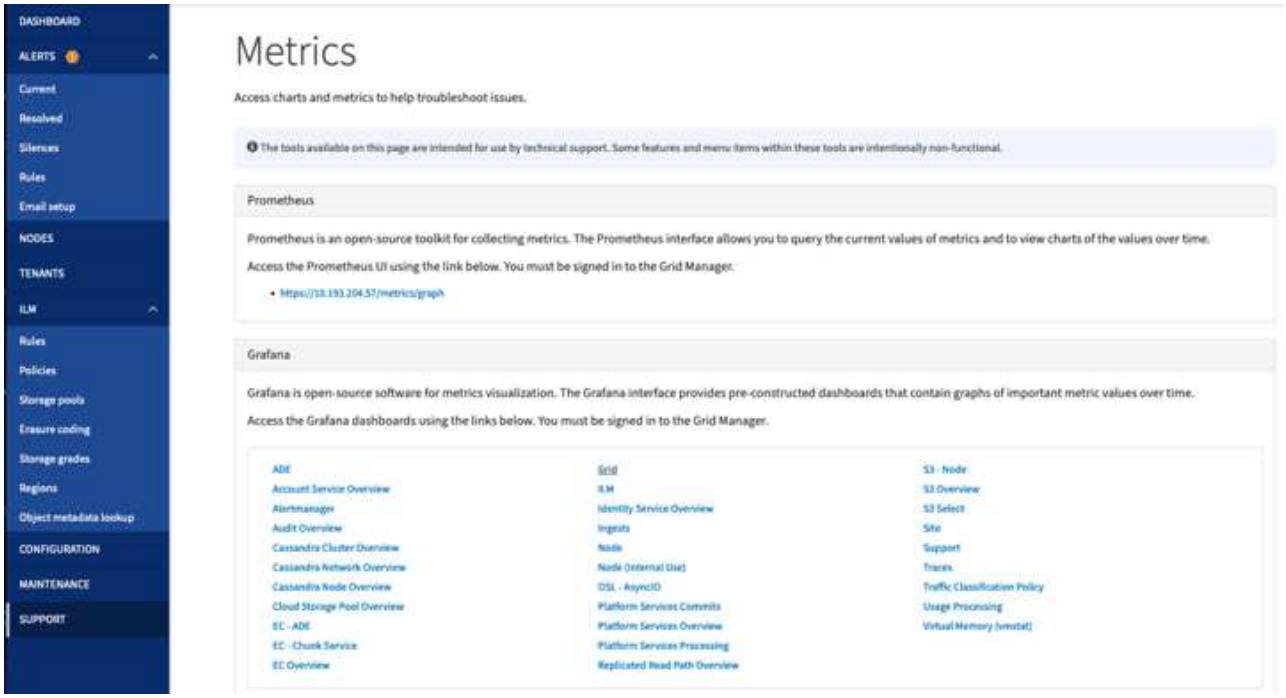
6. Ora che abbiamo configurato l'origine dati, possiamo creare una dashboard.
   a. Nel riquadro di sinistra, espandere "Dashboard" e selezionare "+ new Dashboard"
   b. Seleziona "Aggiungi un nuovo pannello"
   c. Configurare il nuovo pannello selezionando una metrica, di nuovo userò "storagegrid_node_cpu_Utilization_Percent", 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.



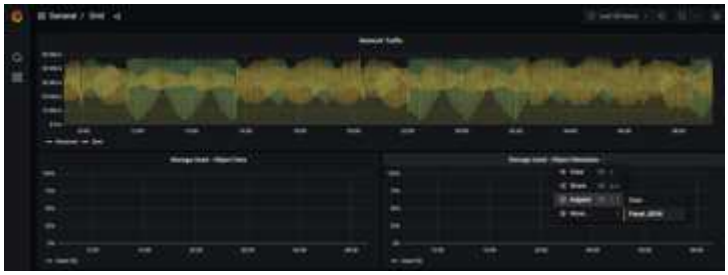
7. Potremmo continuare a costruire la nostra dashboard in questo modo per ogni metrica che vogliamo, ma fortunatamente StorageGRID dispone già di dashboard con pannelli che possiamo copiare nelle nostre dashboard personalizzate.

   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.

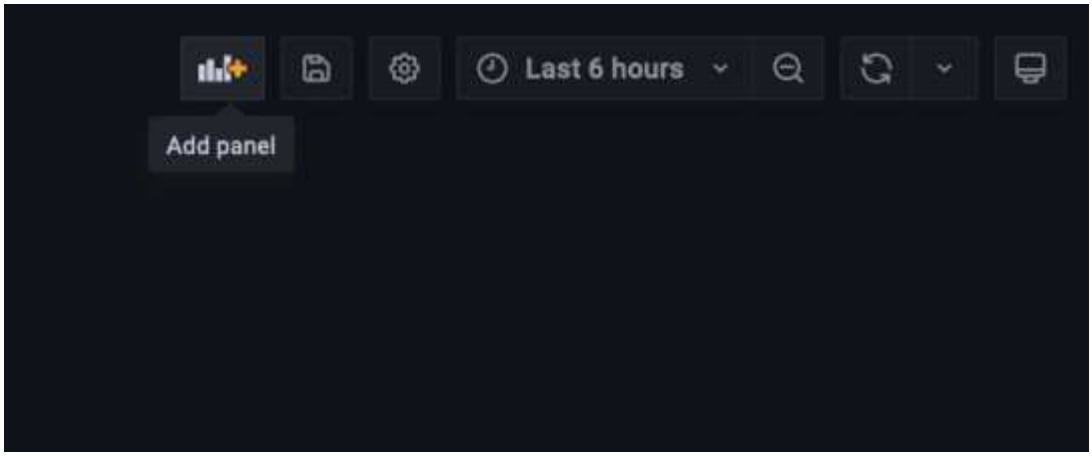


   c. Dalla dashboard della griglia, selezionare il pannello "Storage used - Object Metadata" (Storage utilizzato - metadati oggetto). Fare clic sulla piccola freccia verso il basso e sulla fine del titolo del pannello per visualizzare un menu a discesa. Da questo menu selezionare "Inspect" (ispezione)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



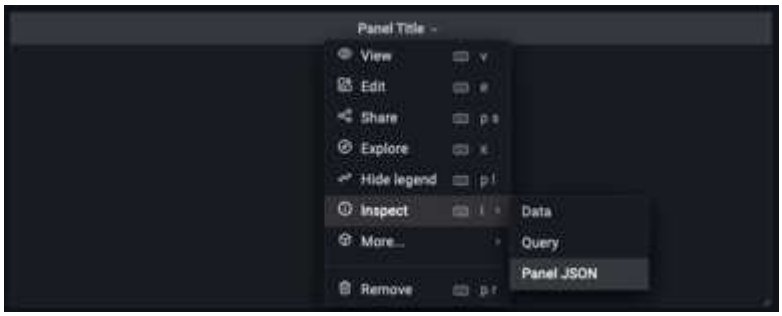
   d. Copiare il codice JSON e chiudere la finestra.

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

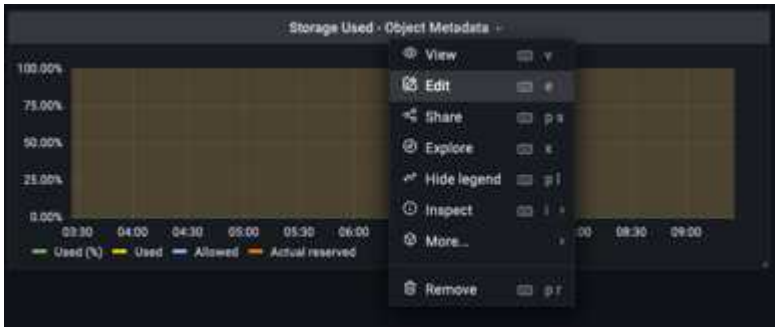


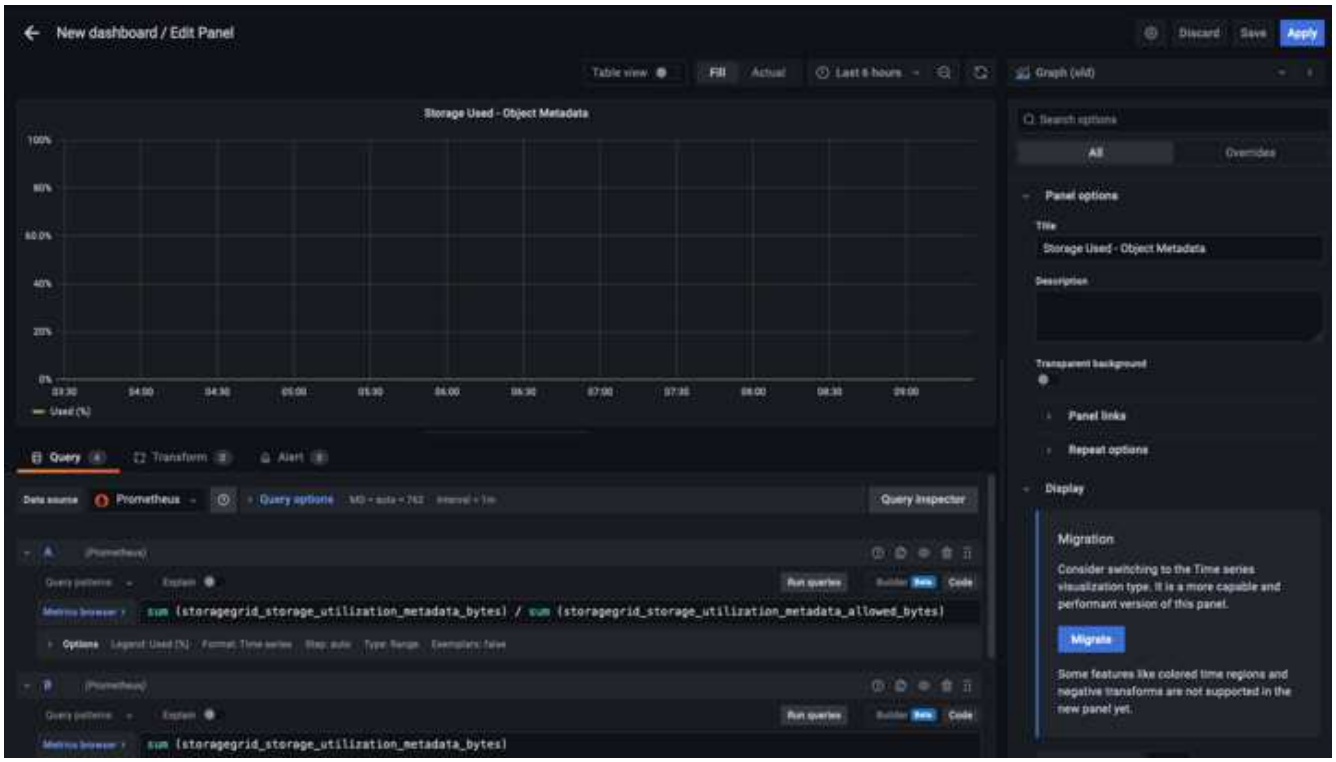
f. Applicare il nuovo pannello senza apportare modifiche

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".

Configurazione SNMP Datadog

Di Aron Klein

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'
```

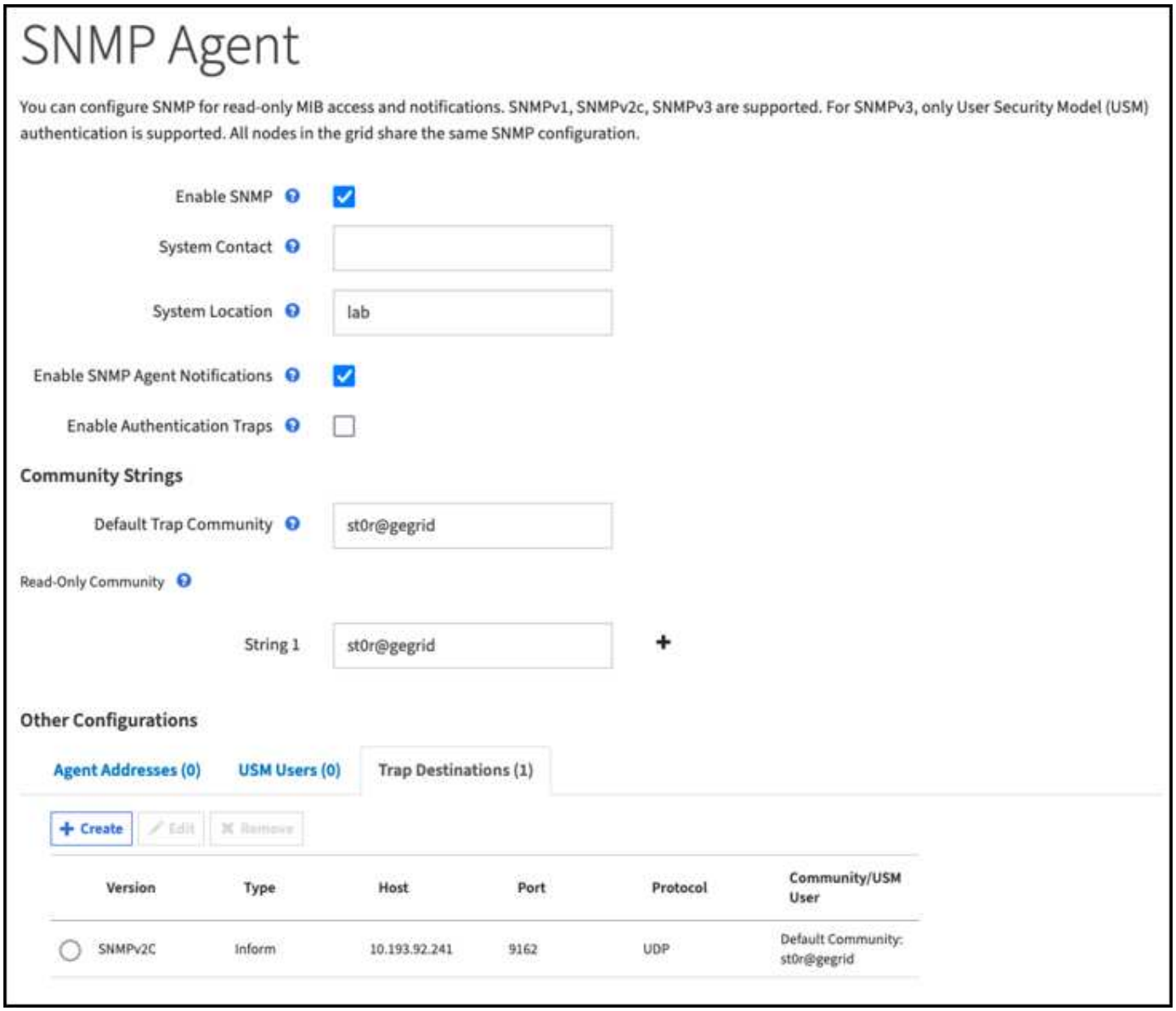
Configurazione SNMP per i trap

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.



Utilizzare rclone per migrare, INSERIRE ed ELIMINARE oggetti su StorageGRID

Di Siegfried Hepp e Aron Klein

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
```

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

Di Oliver Haensel e Aron Klein

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 restare aggiornati e di applicare gli aggiornamenti rapidi più recenti per il sistema Veeam Backup & Replication 12 o 12,1. Attualmente consigliamo almeno di installare Veeam 12 patch 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 11,7 o 11,8 con la correzione rapida più recente sono le versioni consigliate per le implementazioni 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, Loadbalancer.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.

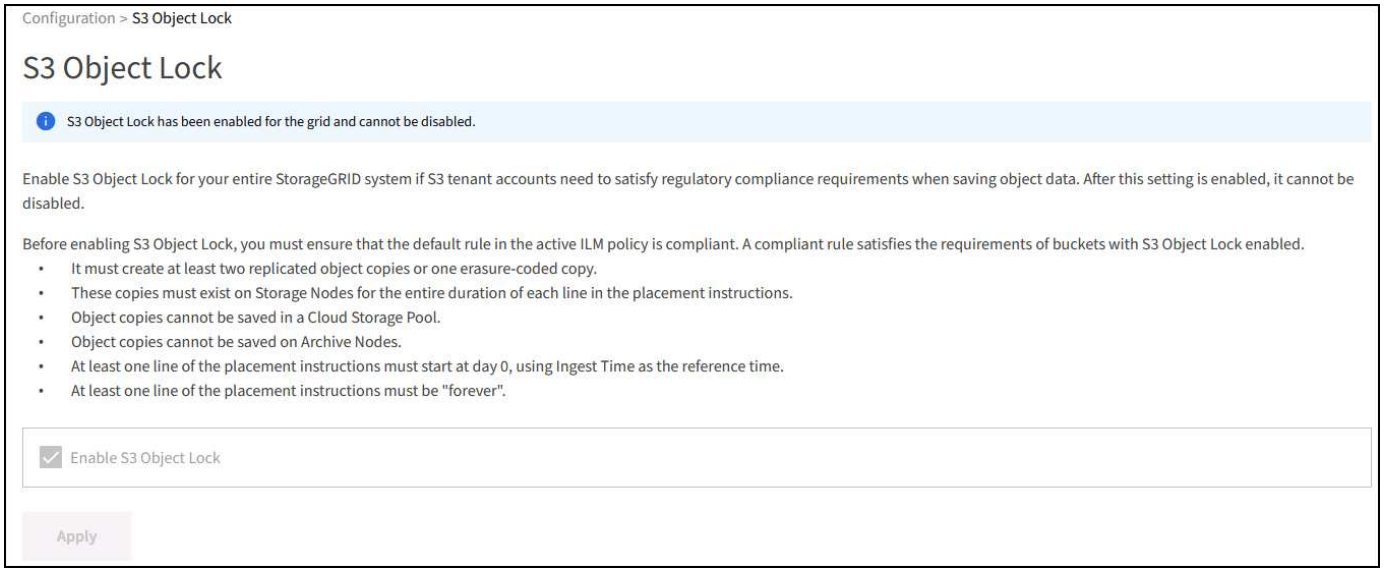
Gestione del ciclo di vita

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.

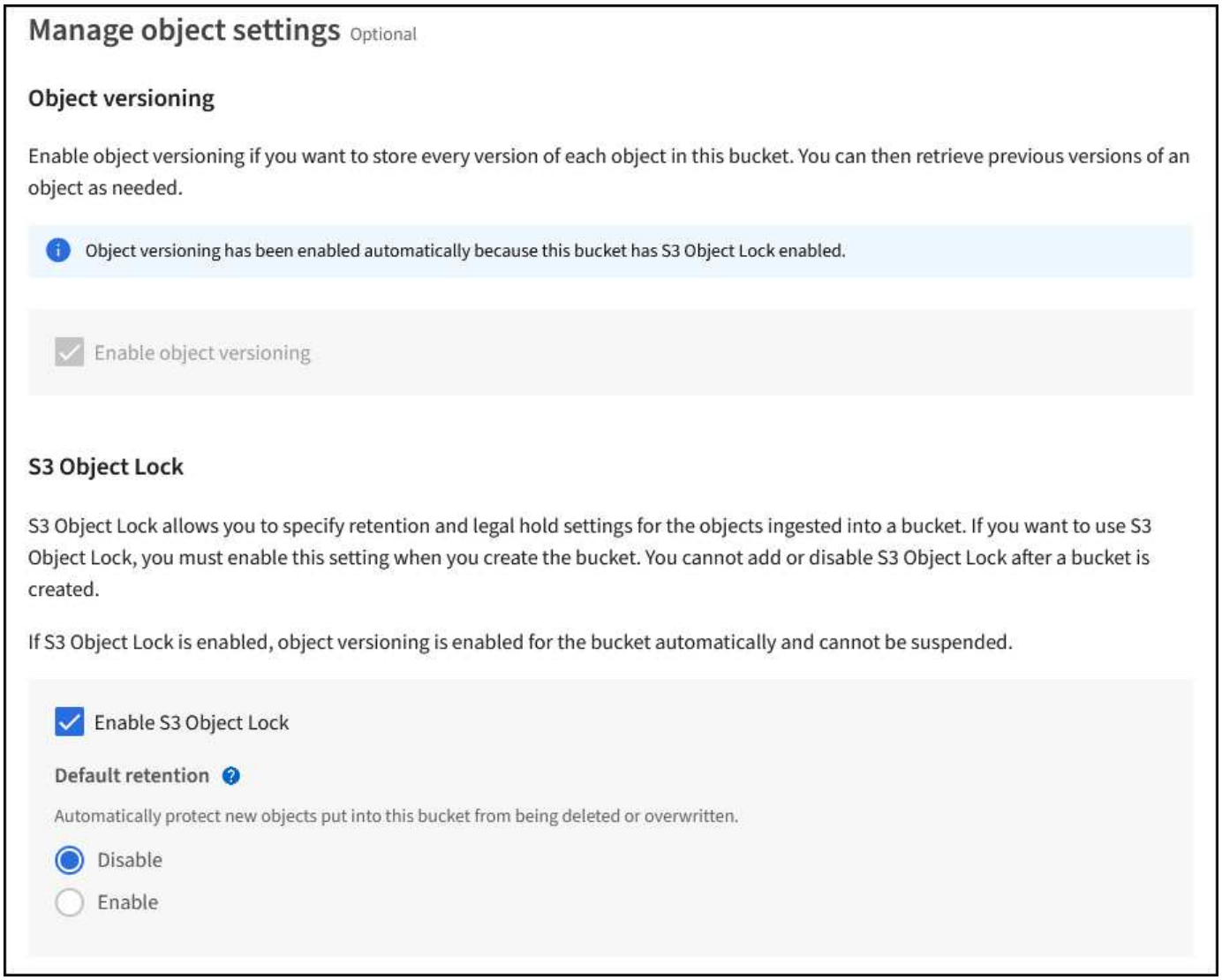
Punti chiave di implementazione

StorageGRID

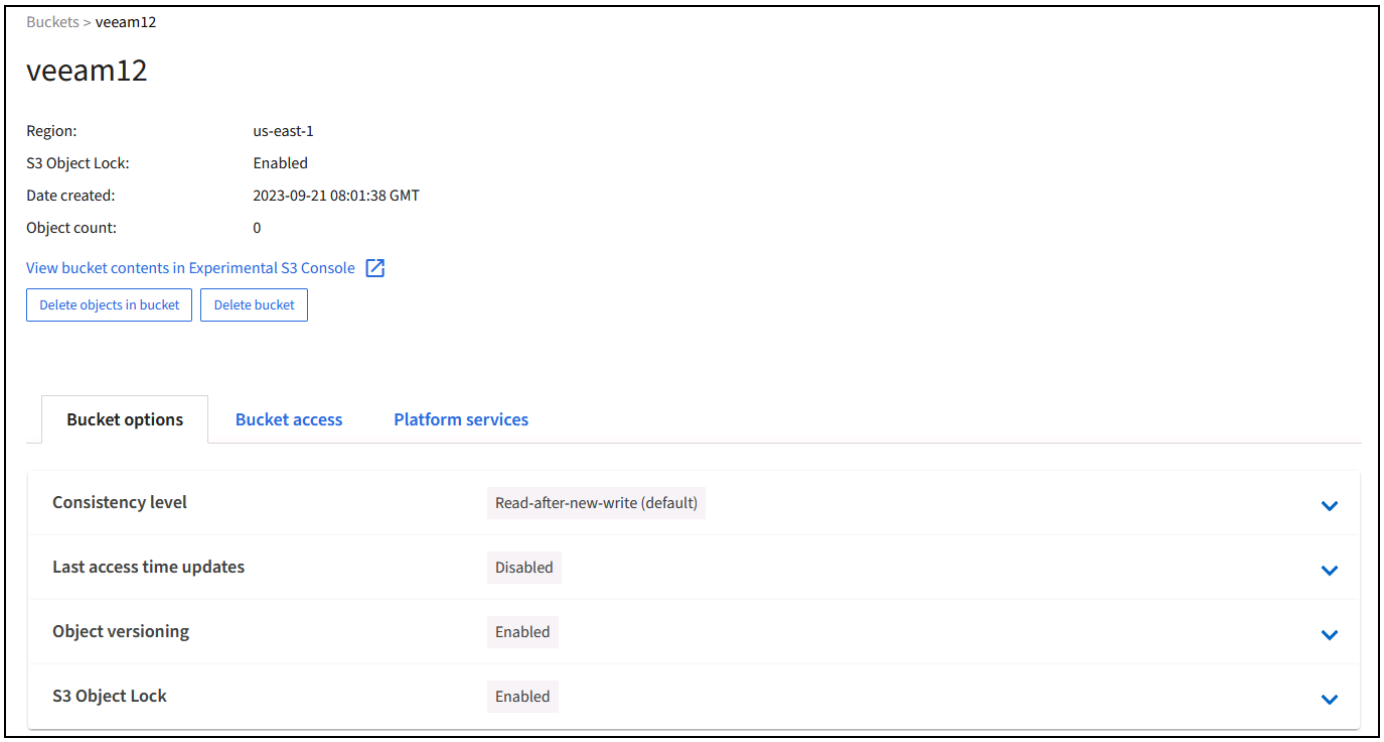
Assicurarsi che blocco oggetti sia attivato sul sistema StorageGRID se è necessaria l'immutabilità. Individuare l'opzione nell'interfaccia utente di gestione in Configurazione/blocco oggetti S3.



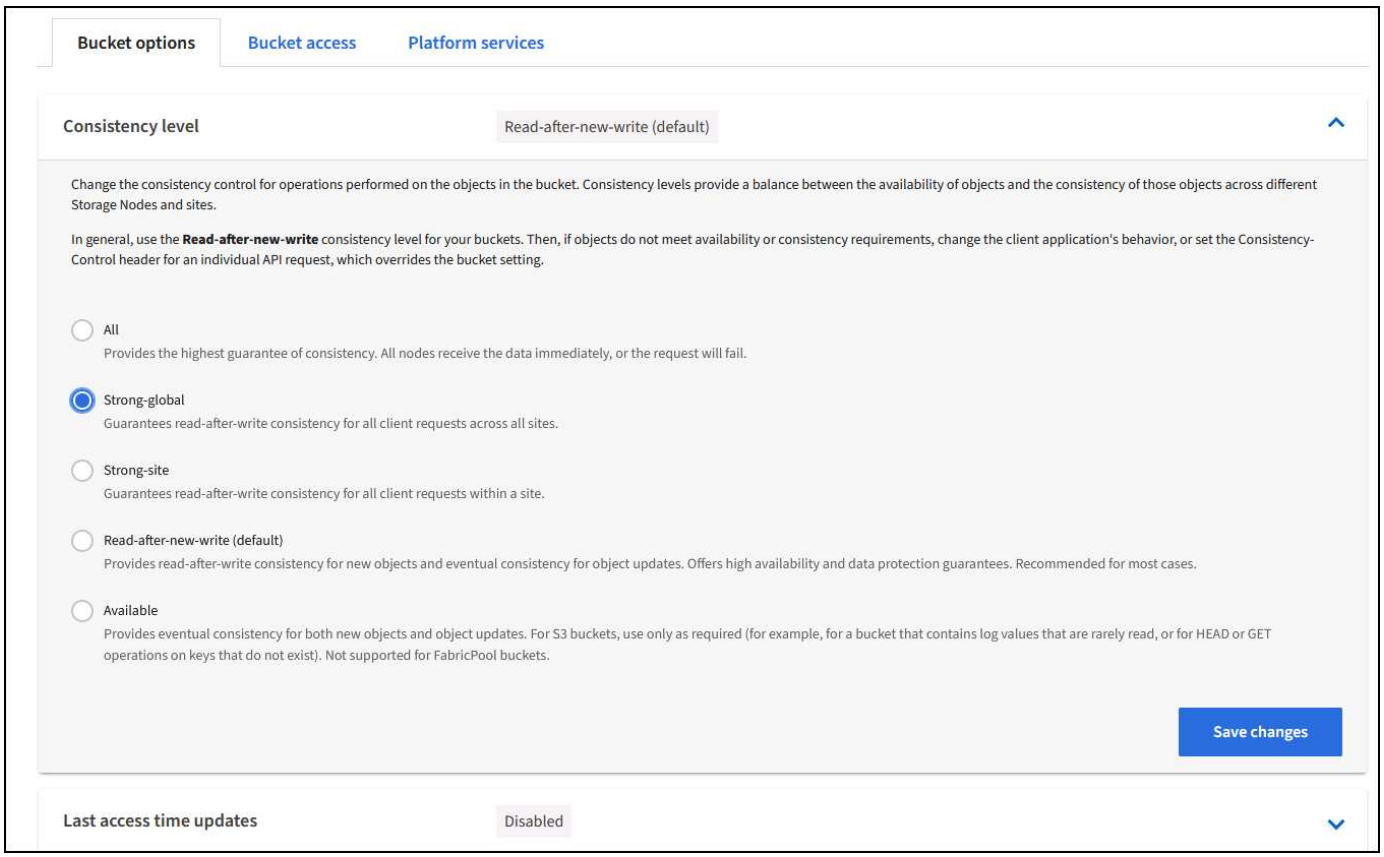
Quando si crea il bucket, selezionare "Enable S3 Object Lock" (attiva blocco oggetti 3D) se questo bucket deve essere utilizzato per i backup di immutabilità. In questo modo si attiva automaticamente la versione bucket. Lasciare disattivata la conservazione predefinita poiché Veeam imposterà esplicitamente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



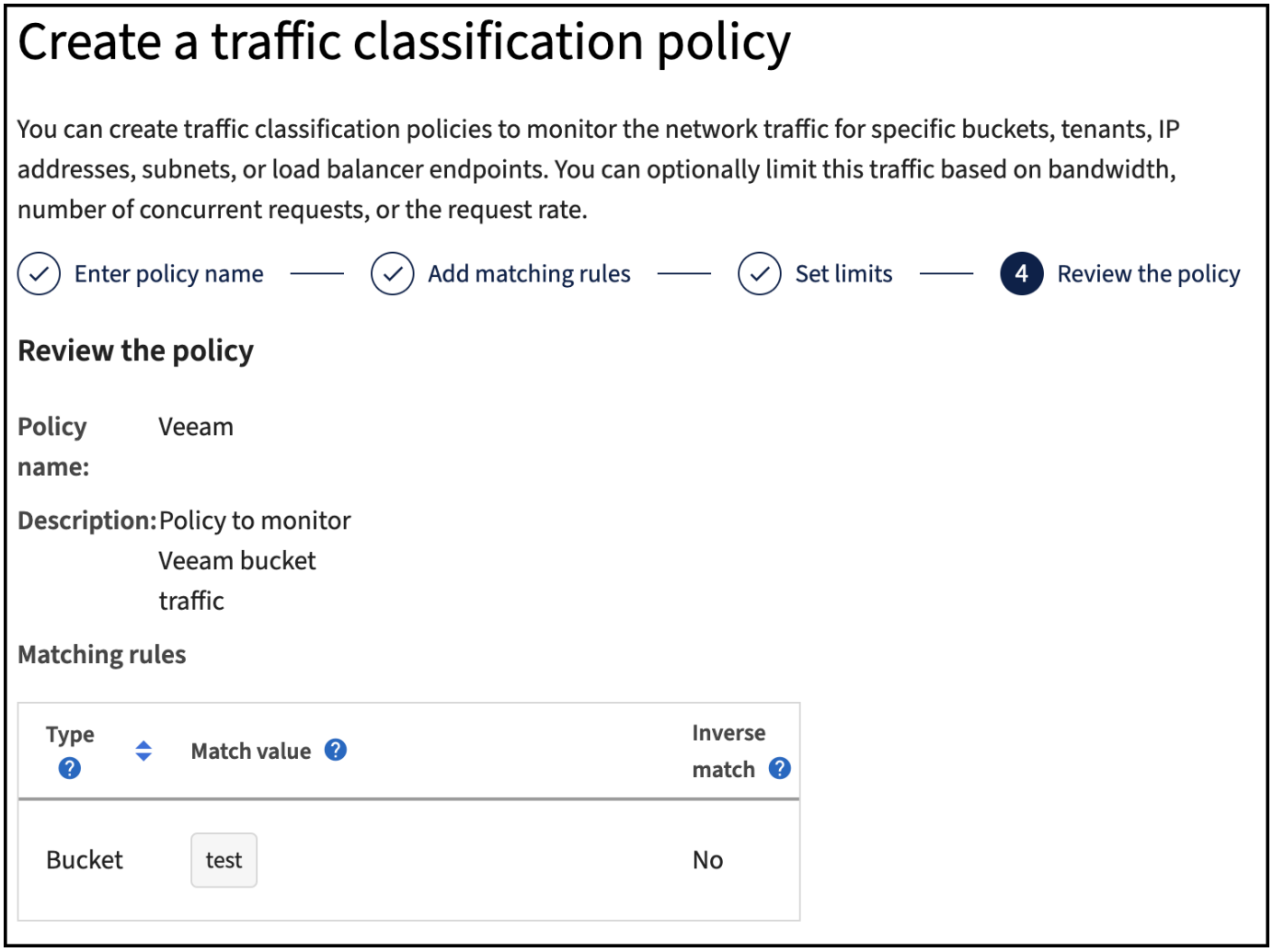
Veeam richiede una forte coerenza per i bucket S3. Quindi, per implementazioni multi-sito con Veeam che accede ai dati da posizioni multiple, seleziona "strong-Global". Se Veeam effettua backup e ripristini solo su un singolo sito, dovrebbe essere impostato su "strong-site". Salvare le modifiche.



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

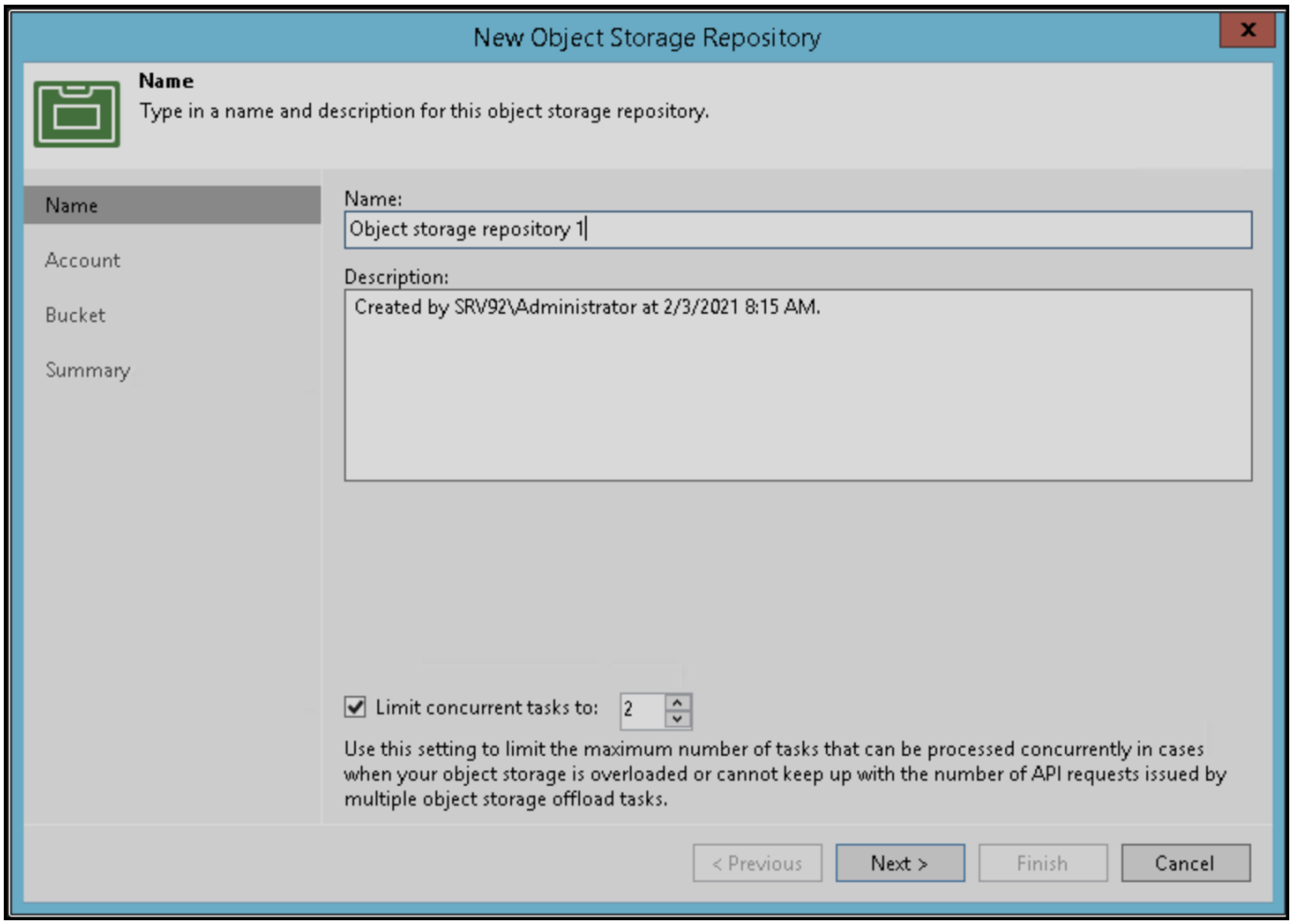
configurare i criteri di classificazione del traffico (QoS). Sebbene vengano utilizzati principalmente per limitare l'impatto di un'applicazione su altri carichi di lavoro dei client o per assegnare priorità a un carico di lavoro rispetto ad altri, forniscono anche un bonus di raccolta di metriche aggiuntive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

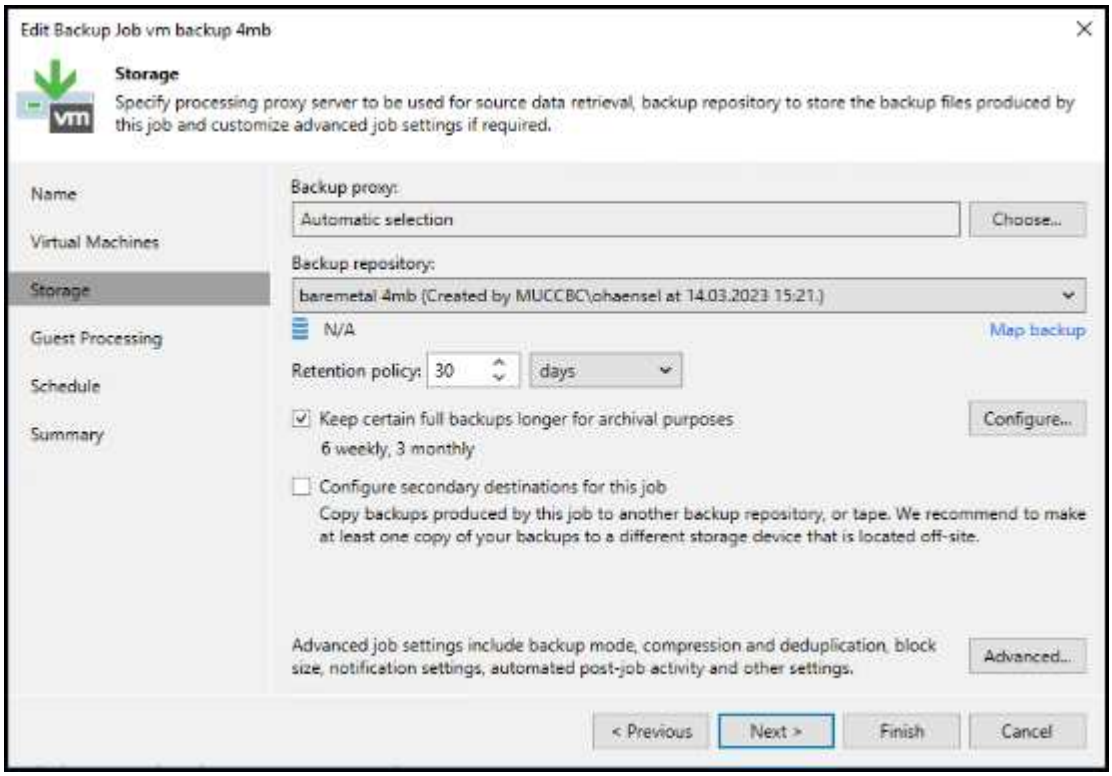


Veeam

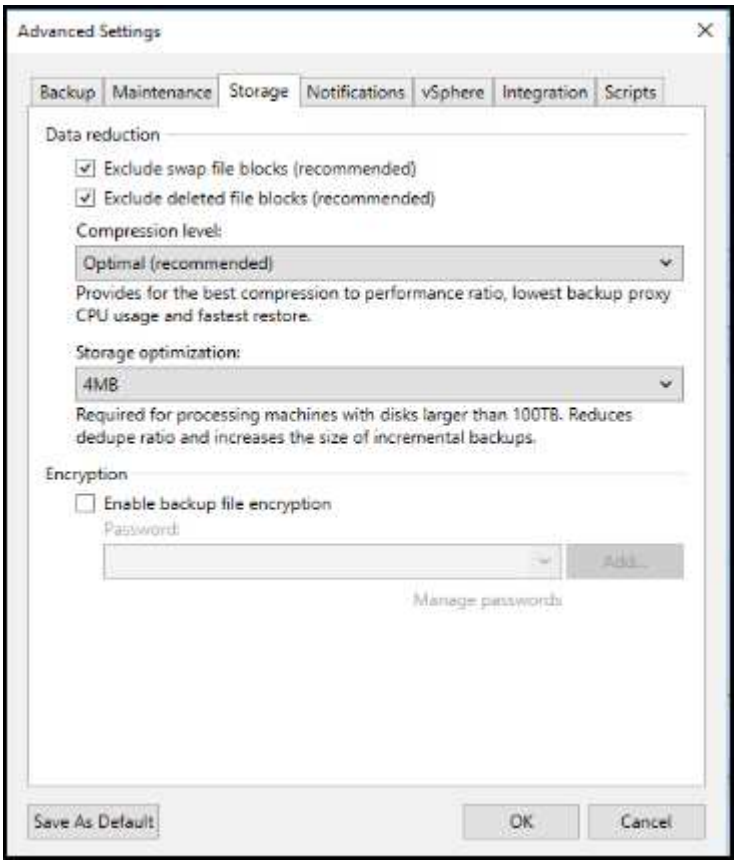
A seconda del modello e della quantità di appliance StorageGRID, potrebbe essere necessario selezionare e configurare un limite al numero di operazioni simultanee nel bucket.



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

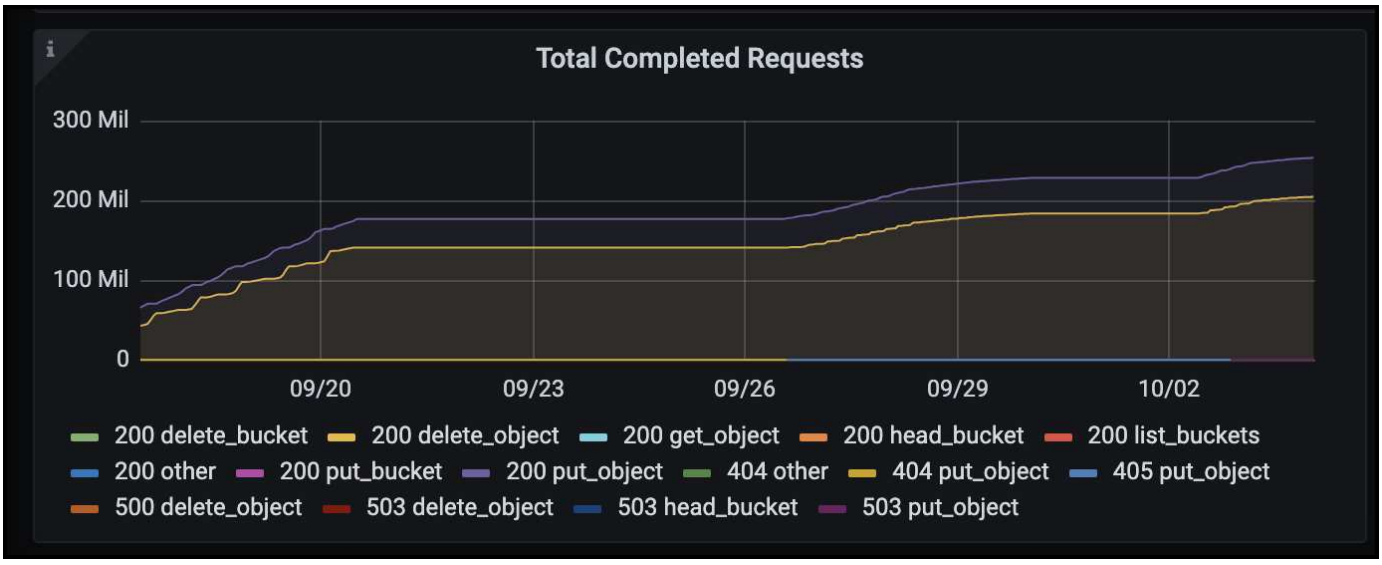
Per avere un quadro completo delle prestazioni congiunte di Veeam e StorageGRID, devi attendere la scadenza del tempo di conservazione dei primi backup. Fino a questo punto il workload Veeam è costituito principalmente da operazioni PUT e non si sono verificati eliminazioni. Una volta che i dati di backup 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 11,9"
- "Backup e replica di Veeam"

Configurare l'origine dati Dremio con StorageGRID

Di Angela Cheng

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

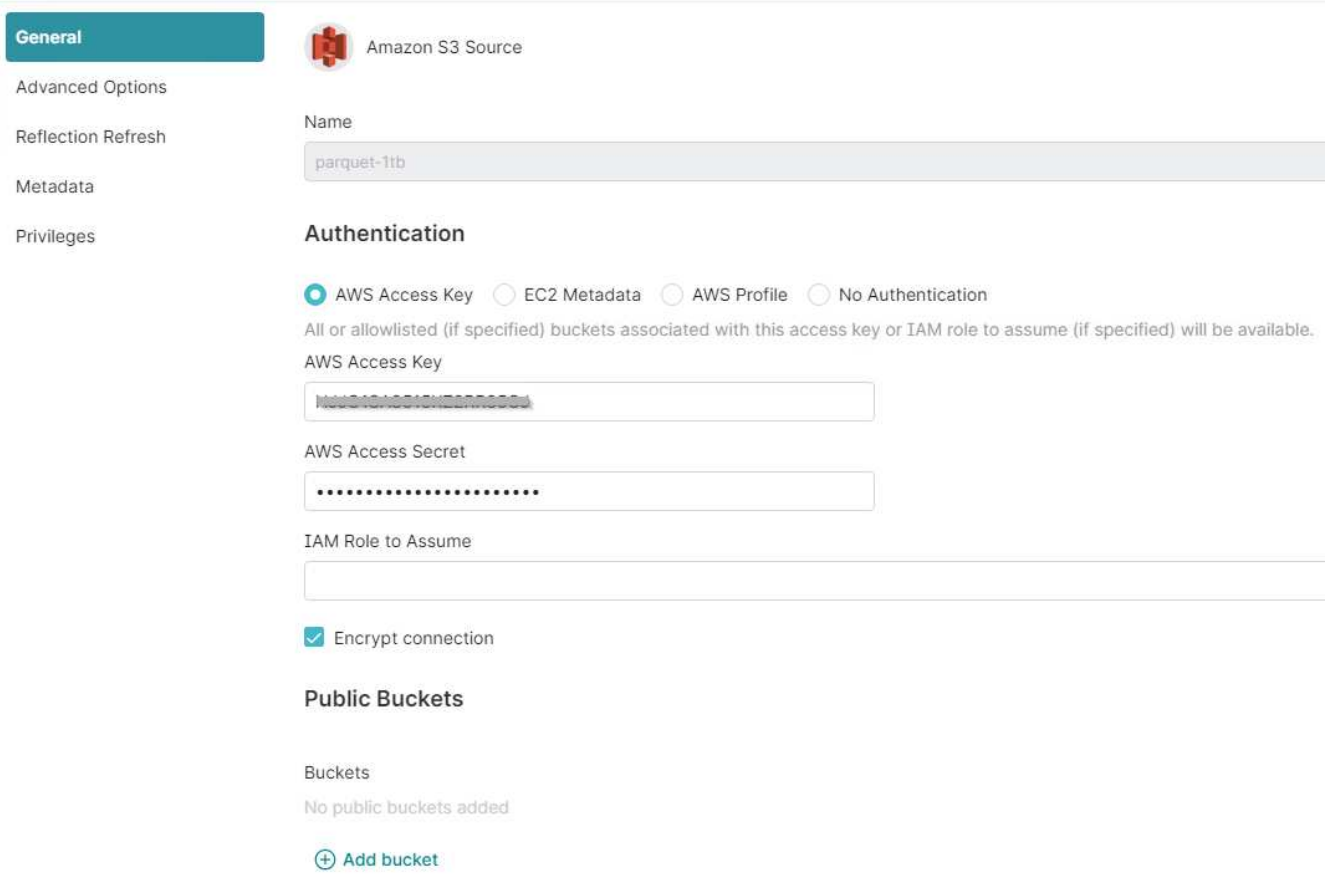
- Un URL dell'endpoint StorageGRID S3, un ID della chiave di accesso tenant S3 e una chiave di accesso segreta.
- Raccomandazione per la configurazione di StorageGRID: Disattivare la compressione (disattivata per impostazione predefinita).
  Dremio utilizza l'intervallo di byte GET per recuperare contemporaneamente 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

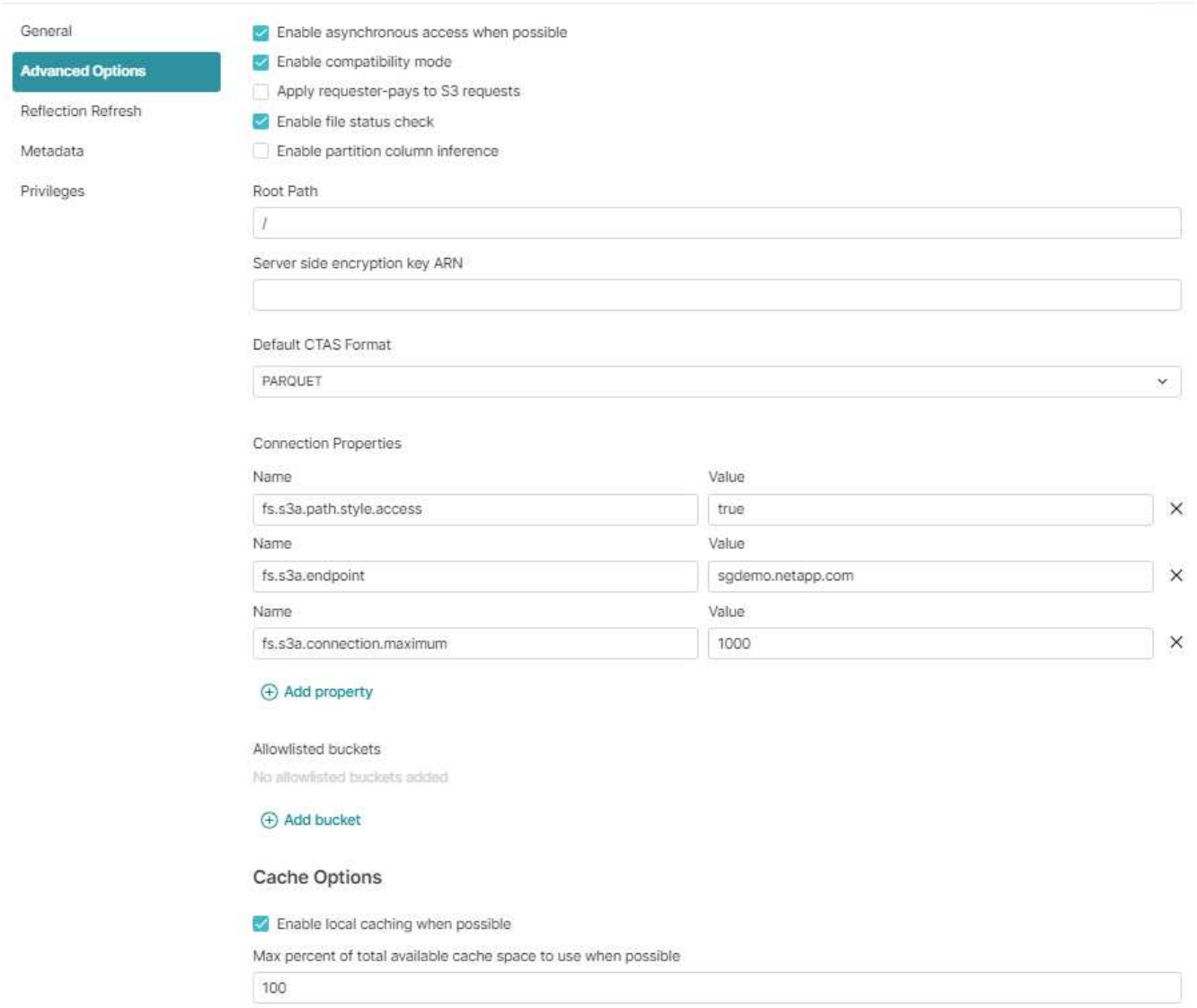
1. Nella pagina Datasets di Dremio, fare clic sul segno + per aggiungere un'origine, selezionare "Amazon S3".
2. Immettere un nome per la nuova origine dati, l'ID della chiave di accesso tenant StorageGRID S3 e la chiave di accesso segreta.
3. Selezionare la casella 'Crittografa connessione' se si utilizza 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



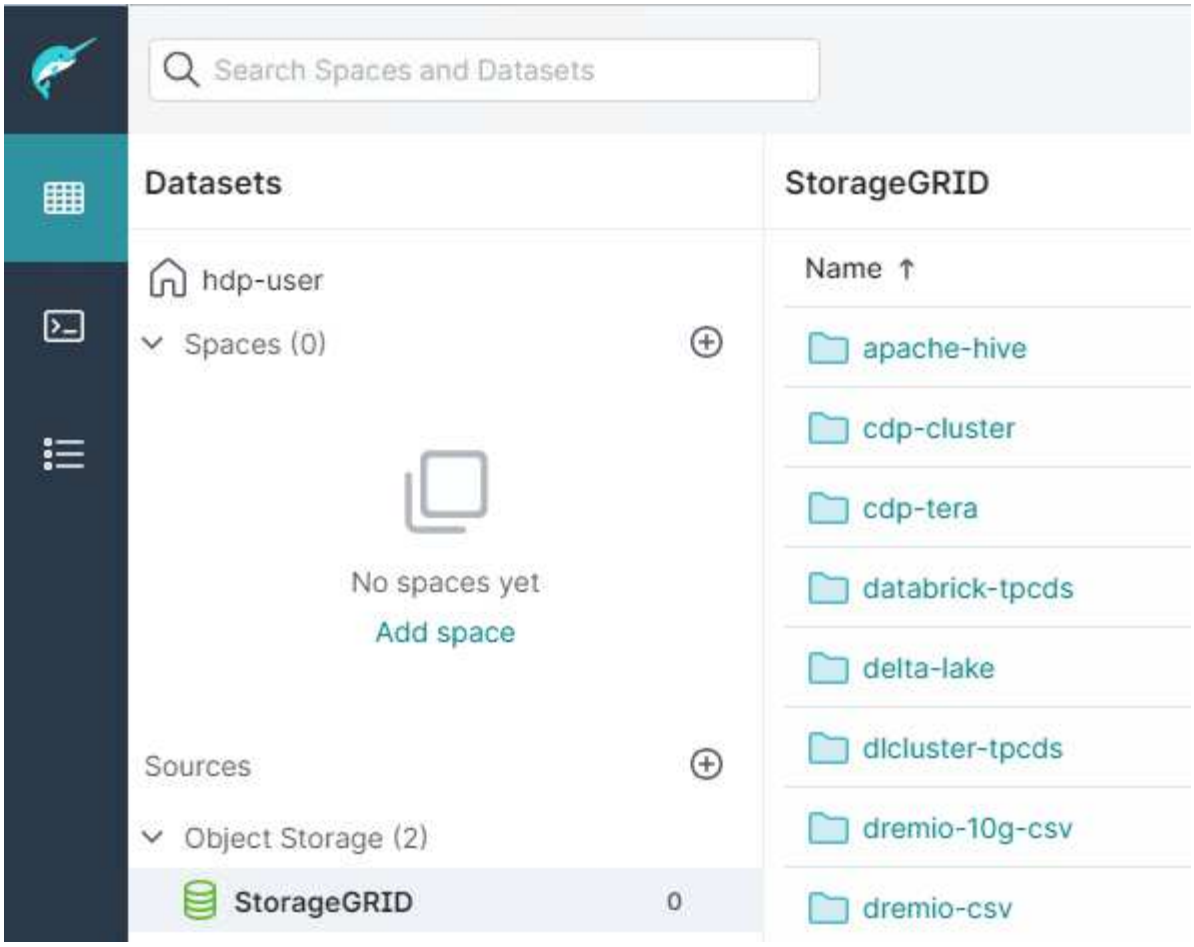
4. Fare clic su "Opzioni avanzate" e selezionare "attiva modalità di compatibilità"
5. In Proprietà di connessione, fare clic su + Aggiungi proprietà e aggiungere queste S3A proprietà.
6. fs.s3a.connection.il valore massimo predefinito è 100. Se i set di dati S3 includono file Parquet di grandi dimensioni 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



NetApp StorageGRID con GitLab

Di Angela Cheng

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

Di Aron Klein

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
```

Testare e dimostrare il blocco di oggetti S3 su StorageGRID

Di Aron Klein

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": "56622399308951294926"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "56622399308951294926"
            },
            "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
```

Esempio di policy di bucket e di gruppo (IAM)

Di seguito sono riportati alcuni criteri e autorizzazioni di esempio in StorageGRID S3.

La struttura di una politica

In StorageGRID, le policy di gruppo sono le stesse delle policy di servizio dell'utente AWS (IAM) S3.

I criteri di gruppo sono necessari in StorageGRID. Un utente con S3 chiavi di accesso ma non assegnato a un gruppo di utenti o assegnato a un gruppo senza un criterio che concede alcune autorizzazioni, non potrà accedere a nessun dato.

I criteri bucket e gruppo condividono la maggior parte degli stessi elementi. Le policy vengono create in formato json e possono essere generate utilizzando "Generatore di policy AWS"

Tutti i criteri definiscono l'effetto, le azioni e le risorse. Anche i criteri bucket definiranno un'entità principale.

Il **effetto** sarà quello di consentire o negare la richiesta.

Il **Principal**

- Valido solo per le politiche bucket.
- L'entità è costituita dagli account/utenti ai quali vengono concesse o negate le autorizzazioni.
- Può essere definito come:
  - Un carattere jolly "*"

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

  - Un ID tenant per tutti gli utenti in un tenant (equivalente all'account AWS)

```
"Principal": { "AWS": "27233906934684427525" }
```

- Un utente (locale o federato dall'interno del tenant in cui risiede il bucket o un altro tenant nella griglia)

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:user/tenant1user1" }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/tenant2user1" }
```

- Un gruppo (locale o federato dall'interno del tenant in cui risiede il bucket o un altro tenant nella griglia).

```
"Principal": { "AWS":
"arn:aws:iam::76233906934699427431:group/DevOps"  }
```

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

La **azione** è l'insieme di operazioni S3 concesse o negate agli utenti.

> Per i criteri di gruppo, l'azione S3:ListBucket Allowed è necessaria per consentire agli utenti di eseguire qualsiasi azione S3.

La **risorsa** è il bucket o i bucket a cui sono stati concessi o negati i principi di eseguire le azioni su. Facoltativamente, può essere presente una condizione * per quando l'azione del criterio è valida.

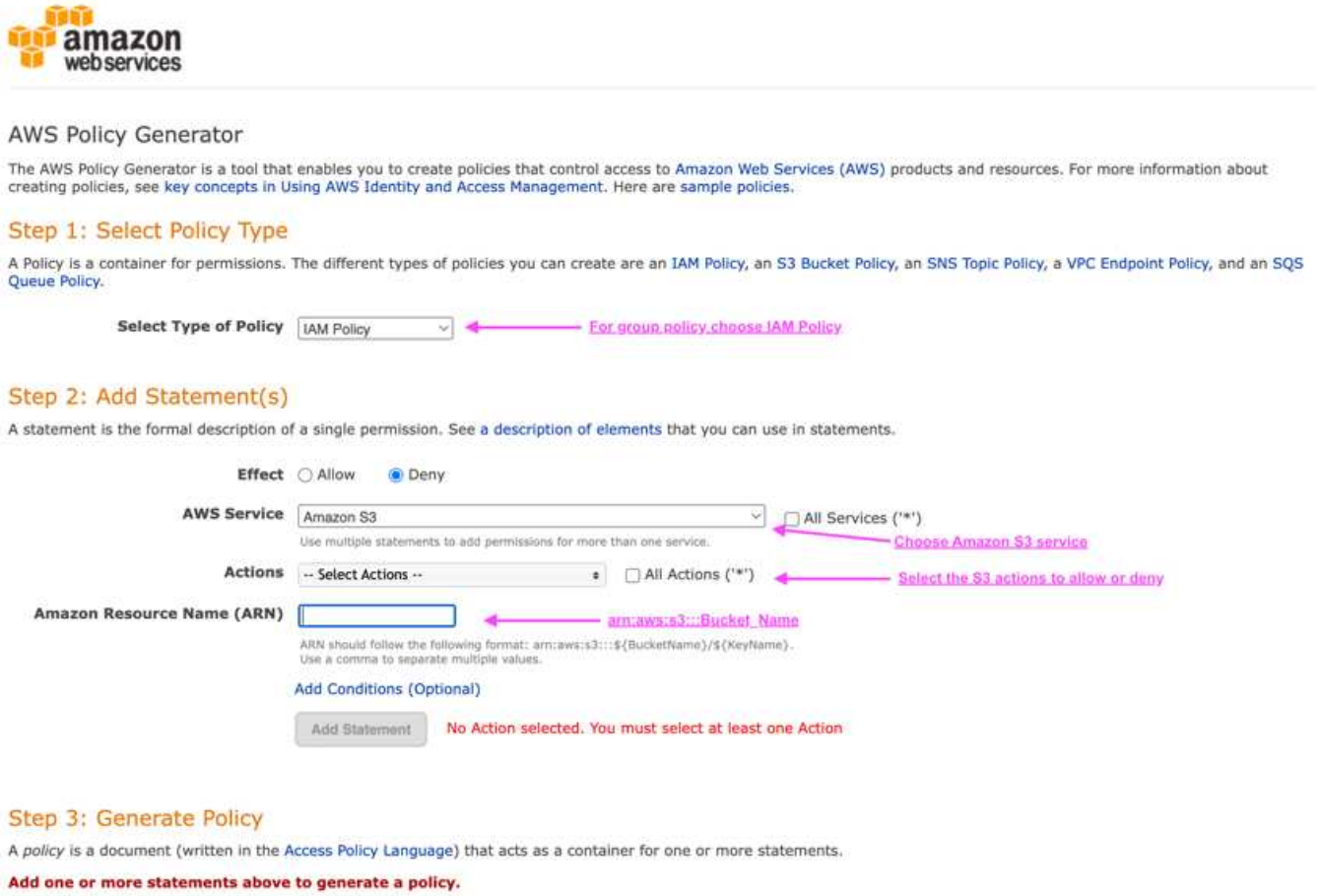
Il formato del criterio JSON sarà il seguente:

```
{
  "Statement": [
    {
      "Sid": "Custom name for this permission",
      "Effect": "Allow or Deny",
      "Principal": {
        "AWS": [
          "arn:aws:iam::tenant_ID::user/User_Name",
          "arn:aws:iam::tenant_ID::federated-user/User_Name",
          "arn:aws:iam::tenant_ID:group/Group_Name",
          "arn:aws:iam::tenant_ID:federated-group/Group_Name",
          "tenant_ID"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:Other_Action"
      ],
      "Resource": [
        "arn:aws:s3:::Example_Bucket",
        "arn:aws:s3:::Example_Bucket/*"
      ],
    }
  ]
}
```

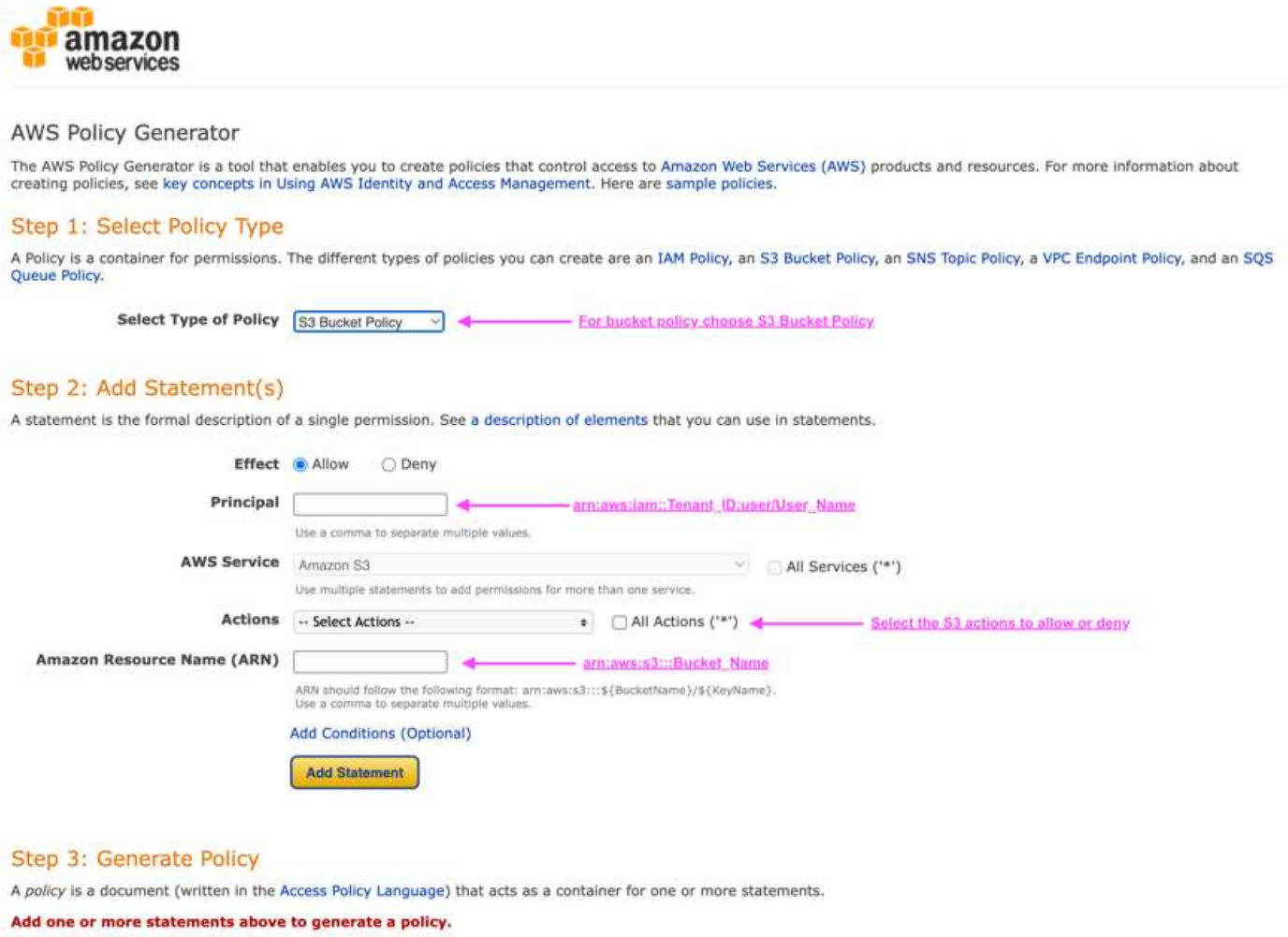
Utilizzo del generatore di policy AWS

AWS Policy generator è un ottimo tool per aiutare a ottenere il codice json con il formato e le informazioni corrette che stai cercando di implementare.

Per generare le autorizzazioni per un criterio di gruppo StorageGRID: * Scegliere il criterio IAM per il tipo di criterio. * Selezionare il pulsante per l'effetto desiderato - Allow (Consenti) o Deny (Nega). È buona norma avviare i criteri con le autorizzazioni di negazione e quindi aggiungere le autorizzazioni di autorizzazione * nel menu a discesa azioni fare clic sulla casella accanto a tutte le S3 azioni che si desidera includere in questa autorizzazione o nella casella "tutte le azioni". * Digitare i percorsi bucket nella casella Amazon Resource Name (ARN). Includere "arn:aws:S3:::" prima del nome bucket. Es. "arn:aws:s3:::example_bucket"

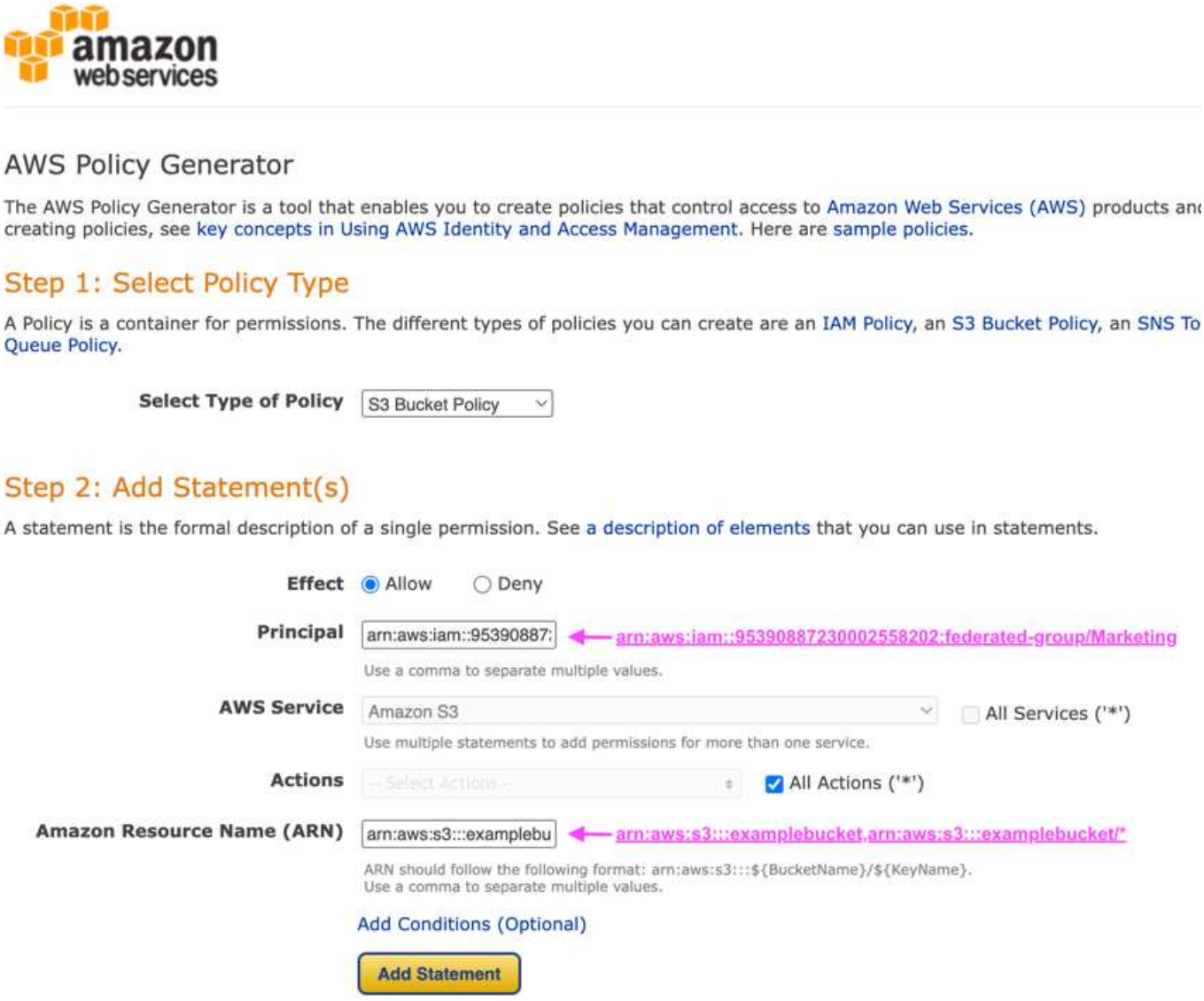


Per generare le autorizzazioni per un criterio bucket: * Scegliere il criterio bucket S3 per il tipo di criterio. * Selezionare il pulsante per l'effetto desiderato - Allow (Consenti) o Deny (Nega). È buona norma avviare i criteri con le autorizzazioni di negazione e quindi aggiungere il tipo Consenti autorizzazioni * nelle informazioni relative all'utente o al gruppo per il principale. * Nell'elenco a discesa azioni, fare clic sulla casella accanto a tutte le S3 azioni che si desidera includere in questa autorizzazione o nella casella "tutte le azioni". * Digitare i percorsi bucket nella casella Amazon Resource Name (ARN). Includere "arn:aws:S3:::" prima del nome bucket. Es. "arn:aws:s3:::example_bucket"



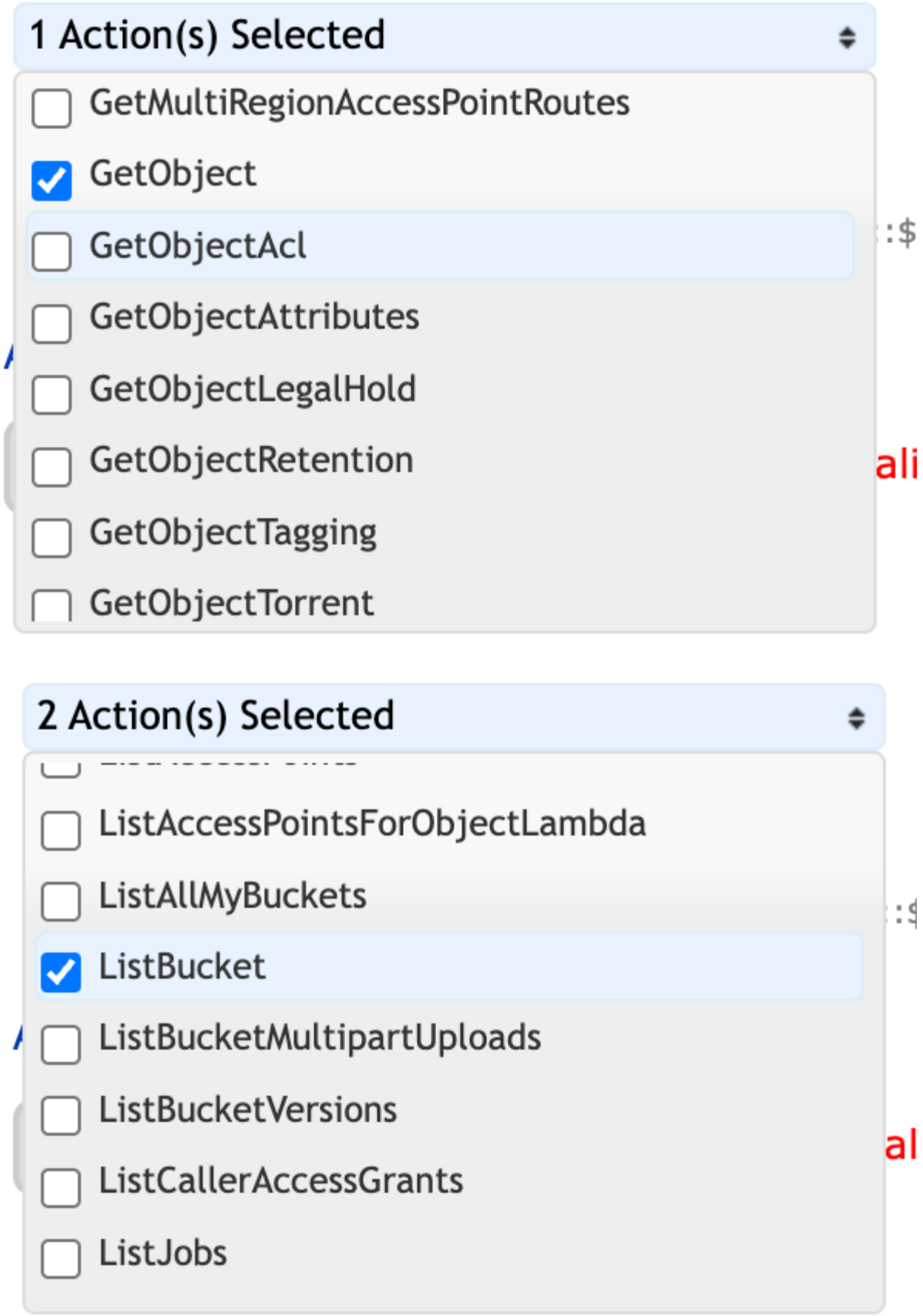
Ad esempio, se si desidera generare un criterio bucket per consentire a tutti gli utenti di eseguire operazioni GetObject su tutti gli oggetti nel bucket, mentre solo gli utenti appartenenti al gruppo "Marketing" nell'account specificato possono accedere completamente.

- Selezionare S3 criterio bucket come tipo di criterio.
- Scegliere l'effetto Consenti
- Inserisci le informazioni del gruppo Marketing - arn:aws:iam::95390887230002558202:Federated-group/Marketing
- Fare clic sulla casella "tutte le azioni"
- Inserisci le informazioni del bucket - arn:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*

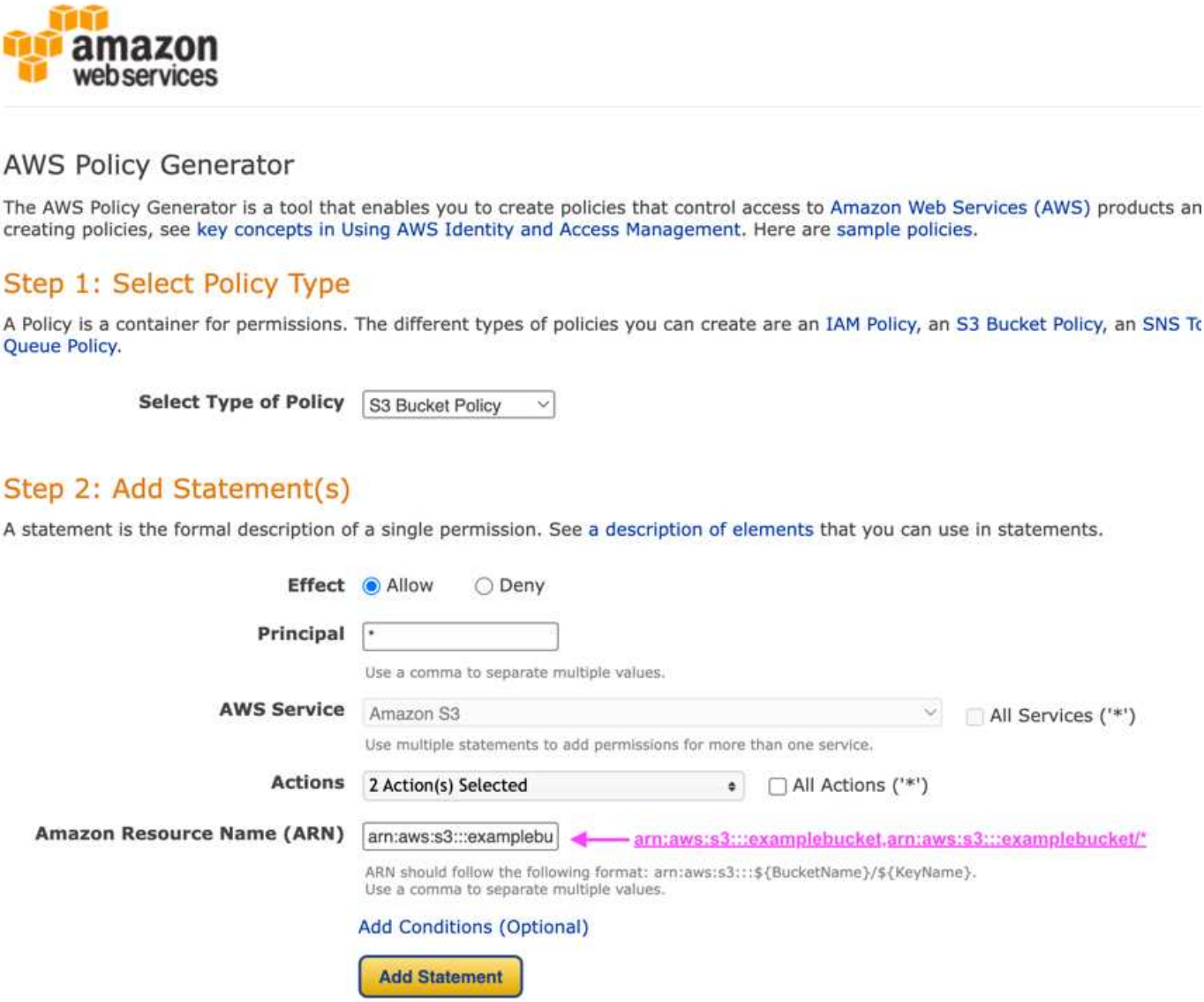


- Fare clic sul pulsante "Aggiungi dichiarazione"

- Scegliere l’effetto Consenti
- Inserisci l’asterisco * per tutti
- Fare clic sulla casella accanto alle azioni GetObject e ListBucket"

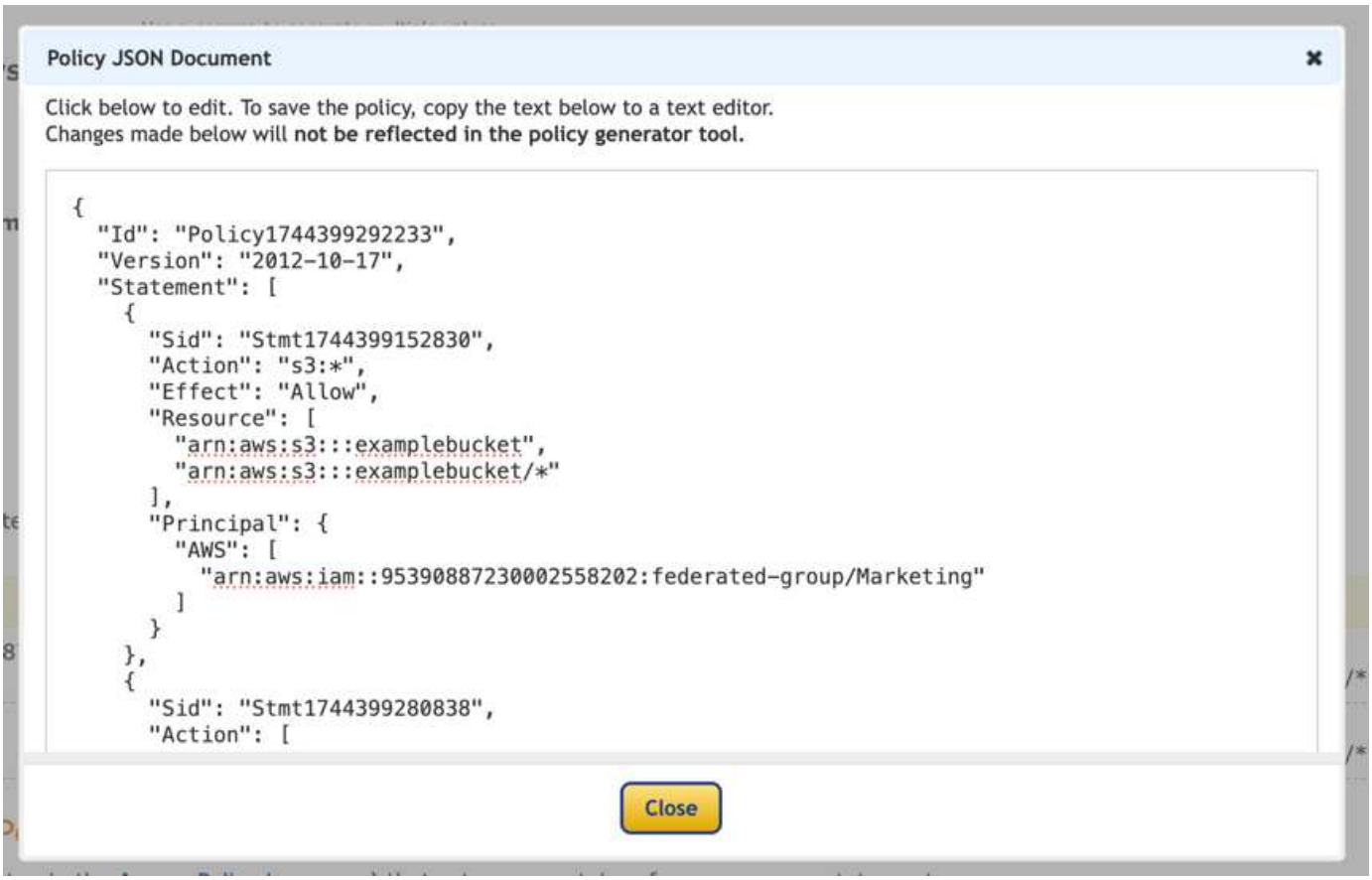


- Inserisci le informazioni del bucket - arn:aws:S3:::example_bucket,arn:aws:S3:::example_bucket/*



- Fare clic sul pulsante "Aggiungi dichiarazione"

- Fare clic sul pulsante "genera criterio" per visualizzare una finestra a comparsa con la policy generata.



- Copiare il testo json completo che dovrebbe avere l'aspetto seguente:

```
{
  "Id": "Policy1744399292233",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1744399152830",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "Stmt1744399280838",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

Questo json può essere utilizzato così com'è, oppure è possibile rimuovere le righe ID e Version sopra la riga "Statement" e personalizzare il Sid per ogni autorizzazione con un titolo più significativo per ogni autorizzazione o anche questi possono essere rimossi.

Ad esempio:

```
{
  "Statement": [
    {
      "Sid": "MarketingAllowFull",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::95390887230002558202:federated-group/Marketing"
        ]
      }
    },
    {
      "Sid": "EveryoneReadOnly",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::example_bucket",
        "arn:aws:s3:::example_bucket/*"
      ],
      "Principal": "*"
    }
  ]
}
```

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:::*"
        }
    ]
}
```

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/*"
            ]
        }
    ]
}
```

Criteri benna

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": "arn:aws:iam::349215141330028336 65:user/user1"
            },
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        },
        {
            "Sid": "Allow user1 read access to bucket bucket1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::349215141330028336 65:user/user1"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket1",
                "arn:aws:s3:::bucket1/*"
            ]
        }
    ]
}
```

limita un bucket a pochi utenti con accesso in sola lettura.

```
{
    "Statement": [
      {
        "Sid": "Deny all S3 actions to employees 002-005",
        "Effect": "deny",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": "*",
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      },
      {
        "Sid": "Allow read-only access for employees 002-005",
        "Effect": "Allow",
        "Principal": {
          "AWS": [
            "arn:aws:iam::465215141330027038 82:user/employee-002",
            "arn:aws:iam::465215141330027038 82:user/employee-003",
            "arn:aws:iam::465215141330027038 82:user/employee-004",
            "arn:aws:iam::465215141330027038 82:user/employee-005"
          ]
        },
        "Action": [
          "s3:GetObject",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion"
        ],
        "Resource": [
          "arn:aws:s3:::databucket1",
          "arn:aws:s3:::databucket1/*"
        ]
      }
    ]
}
```

Limita l'eliminazione degli oggetti con versione in un bucket da parte dell'utente

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"
        ]
      }
    }
  ]
}
```

Report tecnici

Introduzione ai report tecnici di StorageGRID

NetApp StorageGRID è una suite di storage a oggetti software-defined che supporta un'ampia gamma di casi di utilizzo in ambienti multicloud pubblici, privati e ibridi. StorageGRID offre il supporto nativo per l'API Amazon S3 e offre innovazioni leader del settore come la gestione automatica del ciclo di vita per memorizzare, proteggere, proteggere e conservare i dati non strutturati in modo conveniente per lunghi periodi.

StorageGRID fornisce documentazione relativa alle Best practice e ai consigli per diverse funzionalità e integrazioni di StorageGRID.

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.

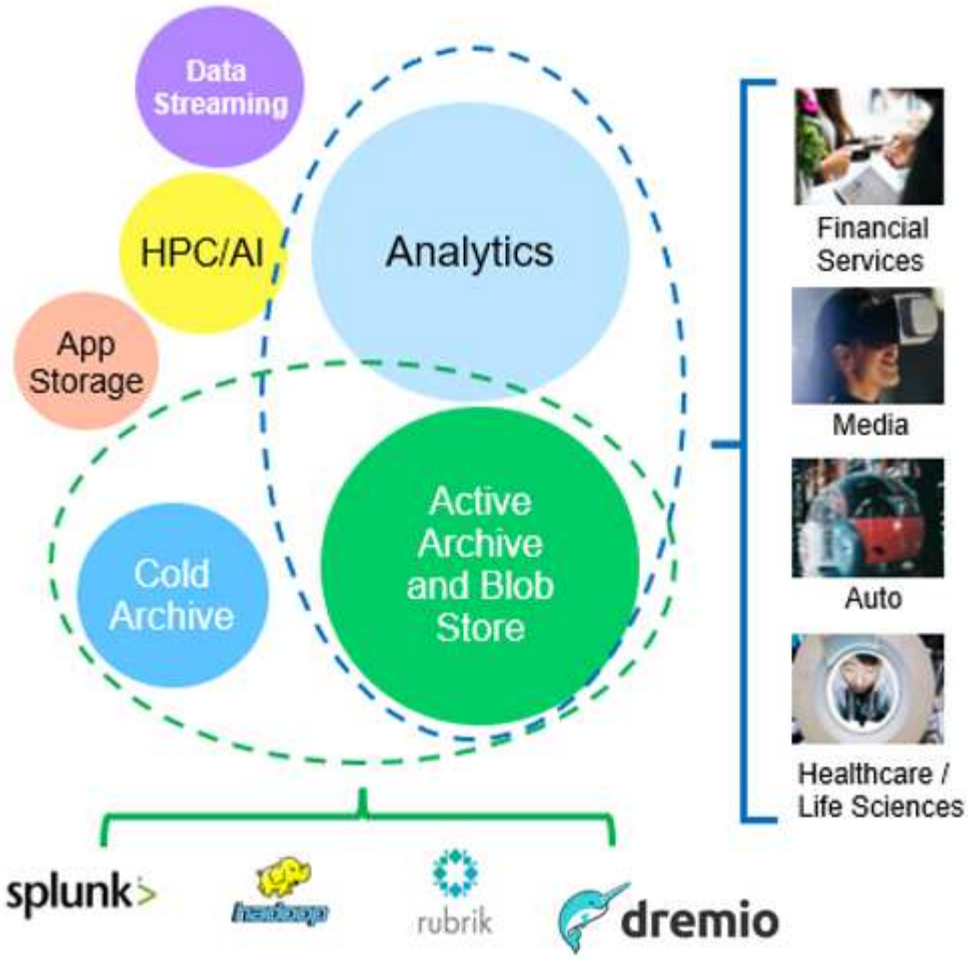
Backup dei dati e ripristino di emergenza: le aziende possono utilizzare StorageGRID S3 come soluzione affidabile e conveniente per il backup dei dati critici e il ripristino in caso di emergenza.

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.

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

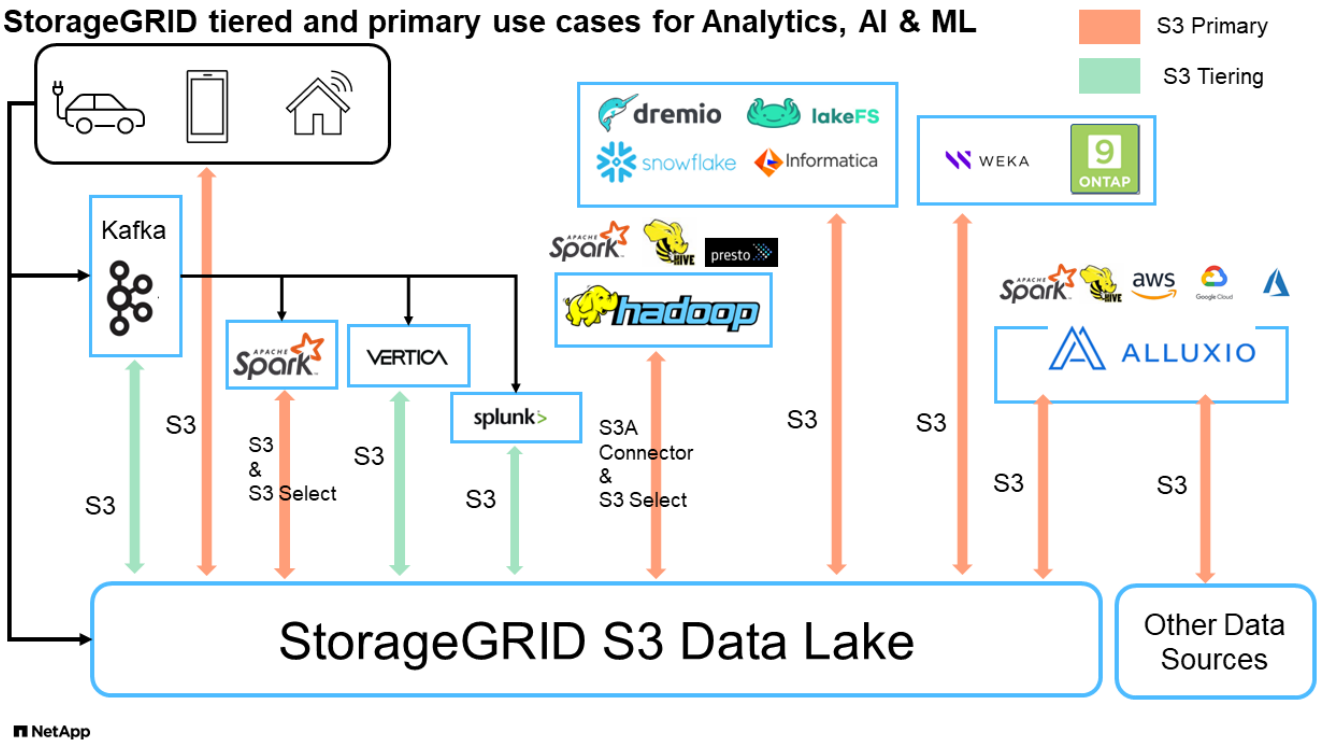


Tra questi, l'analisi dei big data è uno dei casi di utilizzo più importanti e l'andamento del suo utilizzo sta aumentando.

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



Benchmarking di Data warehouse e Lakehouses con storage a oggetti S3: Uno studio comparativo

Questo articolo presenta un benchmark completo di vari ecosistemi di data warehouse e lakehouse che utilizzano NetApp StorageGRID. L'obiettivo è determinare il sistema che funziona meglio con lo storage a oggetti S3. Fare riferimento a questo "Apache Iceberg: La guida definitiva" per ulteriori informazioni sulle architetture datawarehous/lakehouse e sul formato tabella (Parquet e Iceberg).

- Strumento benchmark - TPC-DS - https://www.tpc.org/tpcds/
- Ecosistemi di big data
  - Cluster di macchine virtuali, ciascuno 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 v25,2 (1 coordinatore + 5 esecutori)
  - Trino v438 (1 coordinatore + 5 lavoratori)
  - Starburst v453 (1 coordinatore + 5 lavoratori)
- Storage a oggetti
  - NetApp® StorageGRID^® 11,8 con bilanciamento del carico 3 x SG6060 + 1x SG1000
  - Protezione degli oggetti - 2 copie (il risultato è simile a EC 2+1)
- Dimensioni del database 1000GB
- La cache è stata disabilitata in tutti gli ecosistemi per ogni test di query utilizzando il formato Parquet. Per il formato Iceberg, abbiamo confrontato il numero di richieste GET S3 e il tempo totale di query tra scenari con cache disabilitata e scenari con cache abilitata.

TPC-DS include 99 query SQL complesse progettate per il benchmarking. Abbiamo misurato il tempo totale impiegato per eseguire tutte le 99 query e abbiamo condotto un'analisi dettagliata esaminando il tipo e il numero di richieste S3. I nostri test hanno confrontato l'efficienza di due formati di tabella popolari: Parquet e Iceberg.

Risultato query TPC-DS con formato tabella parquet

Ecosistema	Alveare	Lago Delta	Dremio	Trino	Starburst
TPCDS 99 query minuti totali	1084 [1]	55	36	32	28
S3 richieste di ripartizione	OTTIENI	1.117.184	2.074.610	3.939.690	1.504.212
1.495.039	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, 2500 - 3000 requests/sec	Dimensioni del range: 50% inferiore a 100KB, 16% circa 1MB, 27% 2MB-9MB, 3500 - 4000 richieste/sec
Dimensioni del range: 50% inferiore a 100KB, 16% circa 1MB, 27% 2MB-9MB, 4000 - 5000 richiesta/sec	Elenca oggetti	312.053	24.158	120	509
512	TESTA (oggetto inesistente)	156.027	12.103	96	0
0	TESTA (oggetto esistente)	982.126	922.732	0	0
0	Richieste totali	2.567.390	3.033.603	3.939,906	1.504.721

[1] Impossibile completare la query numero 72

Risultato query TPC-DS con formato tabella Iceberg

Ecosistema	Dremio	Trino	Starburst
TPCDS 99 query + minuti totali (cache disattivata)	22	28	22
TPCDS 99 query + minuti totali [2] (cache abilitata)	16	28	21,5
S3 richieste di ripartizione	GET (OTTIENI) (cache disattivata)	1.985.922	938.639
931.582	GET (OTTIENI) (cache abilitata)	611.347	30.158
3.281	osservazione: Tutta la gamma	Dimensioni di RICEZIONE intervallo: 67% 1MB, 15% 100KB, 10% 500KB, 3500 - 4500 richieste/sec	Dimensioni del range: 42% inferiore a 100KB, 17% circa 1MB, 33% 2MB-9MB, 3500 - 4000 richieste/sec
Dimensioni del range: 43% inferiore a 100KB, 17% circa 1MB, 33% 2MB-9MB, 4000 - 5000 richieste/sec	Elenca oggetti	1465	0
0	TESTA (oggetto inesistente)	1464	0
0	TESTA (oggetto esistente)	3.702	509
509	Richieste totali (cache disattivata)	1.992.553	939.148

[2] le prestazioni Trino/Starburst sono causate da colli di bottiglia causati dalle risorse di elaborazione; l'aggiunta di più RAM al cluster riduce il tempo totale di query.

Come mostrato nella prima tabella, Hive è significativamente più lento di altri moderni dati ecosistemi lakehouse. Abbiamo osservato che Hive ha inviato un gran numero di richieste list-objects S3, che in genere sono lente su tutte le piattaforme di storage a oggetti, soprattutto quando si gestiscono bucket contenenti molti oggetti. Ciò aumenta notevolmente la durata complessiva della query. Inoltre, i moderni ecosistemi lakehouse possono inviare in parallelo un elevato numero di richieste GET, che vanno da 2.000 a 5.000 richieste al secondo, rispetto alle richieste da 50 a 100 di Hive al secondo. Il file system standard mimicry di Hive e Hadoop S3A contribuisce alla lentezza di Hive nell'interazione con lo 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, oltre a una comprensione dell'interazione delle impostazioni di ogni servizio. Insieme, hanno più di 1.000 impostazioni, molte delle quali sono correlate e non possono essere modificate indipendentemente. Trovare la combinazione ottimale di impostazioni e valori richiede un'enorme quantità di tempo e di lavoro.

Confrontando i risultati di Parquet e Iceberg, notiamo che il formato della tabella è un fattore di prestazioni importante. Il formato della tavola Iceberg è più efficiente del Parquet in termini di numero di S3 richieste, con

un numero di richieste inferiore dal 35% al 50% rispetto al formato Parquet.

Le prestazioni di Dremio, Trino o Starburst sono principalmente determinate dalla potenza di calcolo del cluster. Sebbene tutte e tre utilizzino il connettore S3A per la connessione allo storage a oggetti S3, non richiedono Hadoop e la maggior parte delle impostazioni fs.S3A di Hadoop non sono utilizzate da questi sistemi. Questo semplifica il tuning delle performance, eliminando la necessità di imparare e testare le varie impostazioni di Hadoop S3A.

Da questo risultato del benchmark, possiamo concludere che il sistema di analisi dei big data ottimizzato per carichi di lavoro basati su S3 è un importante fattore di performance. I moderni Lakehouse ottimizzano l'esecuzione delle query, utilizzano in modo efficiente i metadati e forniscono un accesso perfetto ai dati S3, producendo performance migliori rispetto a Hive quando si utilizza lo storage S3.

Fare riferimento a questa "pagina" sezione 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

Di Angela Cheng

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.

TR-4871: Configurare StorageGRID per il backup e recovery con CommVault

Eseguire backup e recovery di dati utilizzando StorageGRID e CommVault

CommVault e NetApp hanno collaborato alla creazione di una soluzione congiunta per la data Protection, che combina il software CommVault complete Backup and Recovery for NetApp con il software NetApp StorageGRID per il cloud storage. CommVault complete Backup and Recovery e NetApp StorageGRID forniscono soluzioni uniche e facili da utilizzare che collaborano per aiutarti a soddisfare le richieste di una rapida crescita dei dati e delle normative in aumento in tutto il mondo.

Molte organizzazioni vogliono migrare lo storage nel cloud, scalare i sistemi e automatizzare la policy per la conservazione dei dati a lungo termine. Lo storage a oggetti basato sul cloud è celebre per la sua resilienza, la sua capacità di scalare e le efficienze operative e legate ai costi, caratteristiche che lo rendono la scelta naturale come destinazione del backup. CommVault e NetApp hanno certificato congiuntamente la propria soluzione combinata nel 2014 e da allora hanno progettato una più profonda integrazione tra le due soluzioni. I clienti di ogni tipo in tutto il mondo hanno adottato la soluzione combinata di backup e recovery CommVault complete e StorageGRID.

Informazioni su CommVault e StorageGRID

Il software CommVault complete Backup and Recovery è una soluzione di gestione integrata dei dati e delle informazioni di livello aziendale, costruita da zero su una singola piattaforma e con una base di codice unificata. Tutte le sue funzioni condividono tecnologie di back-end, apportando gli impareggiabili vantaggi e vantaggi di un approccio completamente integrato alla protezione, alla gestione e all'accesso ai dati. Il software contiene moduli per la protezione, l'archiviazione, l'analisi, la replica e la ricerca dei dati. I moduli condividono una serie comune di servizi back-end e funzionalità avanzate che interagiscono perfettamente tra loro. La soluzione affronta tutti gli aspetti della gestione dei dati nell'azienda, fornendo una scalabilità infinita e un controllo senza precedenti di dati e informazioni.

NetApp StorageGRID come Tier di cloud CommVault è una soluzione di storage a oggetti di cloud ibrido aziendale. Puoi implementarla su più siti, sia su un'appliance costruita ad hoc che come implementazione software-defined. StorageGRID ti consente di stabilire policy di gestione dei dati che determinano il modo in cui i dati vengono archiviati e protetti. StorageGRID raccoglie le informazioni necessarie per sviluppare e applicare le policy. Prende in esame un'ampia gamma di caratteristiche ed esigenze, tra cui performance, durata, disponibilità, posizione geografica, longevità e costi. I dati sono pienamente mantenuti e protetti durante lo spostamento tra posizioni e man mano che invecchiano.

Il motore di policy intelligente di StorageGRID consente di scegliere una delle seguenti opzioni:

- Utilizzare l'erasure coding per eseguire il backup dei dati su diversi siti allo scopo di ottenere resilienza.
- Copia degli oggetti in siti remoti per ridurre al minimo il costo e la latenza della WAN.

Quando StorageGRID archivia un oggetto, lo accedi come un unico oggetto, indipendentemente da dove si trova o dal numero di copie esistenti. Questo comportamento è fondamentale per il disaster recovery, perché con esso, anche se una copia di backup dei dati è danneggiata, StorageGRID è in grado di ripristinare i dati.

Conservare i dati di backup nello storage primario può rivelarsi costoso. Utilizzando NetApp StorageGRID, potrai liberare spazio sullo storage primario migrando i dati di backup inattivi in StorageGRID, senza rinunciare

alle numerose funzionalità di StorageGRID. Il valore dei dati di backup cambia con il passare del tempo, così come il costo legato alla loro memorizzazione. StorageGRID può ridurre al minimo il costo dello storage primario aumentando al contempo la durata dei dati.

Funzionalità principali

Le funzionalità principali della piattaforma software CommVault includono:

- Una soluzione completa di protezione dei dati che supporta tutti i principali sistemi operativi, database e applicazioni su server virtuali e fisici, sistemi NAS, infrastrutture basate sul cloud e dispositivi mobili.
- Gestione semplificata attraverso un'unica console: Puoi visualizzare, gestire e accedere a tutte le funzioni, tutti i dati e le informazioni dell'azienda.
- Diversi metodi di protezione, tra cui backup e archiviazione dei dati, gestione delle snapshot, replica dei dati e indicizzazione dei contenuti per l'e-Discovery.
- Gestione efficiente dello storage mediante la deduplica per il disco e il cloud storage.
- Integrazione con storage array NetApp come AFF, FAS, NetApp HCI ed e-Series e con i sistemi di storage scale-out NetApp SolidFire^®. Integrazione anche con il software NetApp Cloud Volumes ONTAP per automatizzare la creazione di copie Snapshot™ NetApp indicizzate e compatibili con le applicazioni nell'intero portafoglio di storage NetApp.
- Gestione completa dell'infrastruttura virtuale che supporta i principali hypervisor virtuali on-premise e piattaforme hyperscaler di cloud pubblico.
- Funzionalità di sicurezza avanzate per limitare l'accesso ai dati critici, offrire funzionalità di gestione granulari e fornire accesso single-sign-on agli utenti di Active Directory.
- Gestione dei dati basata su criteri che consente di gestire i dati in base alle esigenze aziendali, non in base a una posizione fisica.
- Un'esperienza utente finale all'avanguardia, che consente agli utenti di proteggere, trovare e ripristinare i propri dati.
- Automazione basata su API per utilizzare strumenti di terze parti come vRealize Automation o Service Now per gestire le operazioni di data Protection e recovery.

Per ulteriori informazioni sui carichi di lavoro supportati, visitare il sito Web "Tecnologie supportate da CommVault".

Opzioni di backup

Quando implementi il software di backup e recovery CommVault complete con il cloud storage, hai due opzioni di backup:

- Eseguire il backup su una destinazione disco primaria e una copia ausiliaria su cloud storage.
- Eseguire il backup sul cloud storage come destinazione primaria.

In passato, lo storage a oggetti o cloud era considerato dalle performance troppo basse per essere utilizzato per il backup primario. L'utilizzo di una destinazione disco primaria ha permesso ai clienti di disporre di processi di backup e ripristino più rapidi e di mantenere una copia ausiliaria nel cloud come backup cold. StorageGRID rappresenta la nuova generazione dello storage a oggetti. StorageGRID è in grado di offrire performance elevate, throughput elevato, performance e flessibilità superiori a quelle degli altri vendor di soluzioni storage a oggetti.

Nella seguente tabella sono elencati i vantaggi di ciascuna opzione di backup con StorageGRID:

	Backup primario su disco e copia ausiliaria su StorageGRID	Backup primario su StorageGRID
Performance	Tempo di recovery più rapido, con montaggio live o live recovery: La soluzione migliore per i carichi di lavoro Tier0/Tier1.	Non può essere utilizzato per operazioni di montaggio live o ripristino live. Ideale per le operazioni di ripristino in streaming e per la conservazione a lungo termine.
Architettura di implementazione	Utilizzo di una tecnologia all-flash o di un disco a rotazione come primo landing Tier di backup. StorageGRID viene utilizzato come Tier secondario.	Semplifica l'implementazione utilizzando StorageGRID come destinazione di backup all-inclusive.
Funzioni avanzate (ripristino in tempo reale)	Supportato	Non supportato

Dove trovare ulteriori informazioni

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

- Centro di documentazione di StorageGRID 11,9 + https://docs.netapp.com/us-en/storagegrid-119/
- Documentazione del prodotto NetApp https://docs.netapp.com
- Documentazione CommVault https://documentation.commvault.com/2024/essential/index.html

Panoramica della soluzione testata

La soluzione collaudata combina le soluzioni CommVault e NetApp per realizzare una potente soluzione congiunta.

Setup della soluzione

Durante la configurazione in laboratorio, l'ambiente StorageGRID era composto da quattro appliance NetApp StorageGRID SG5712, un nodo amministrativo primario virtuale e un nodo gateway virtuale. L'appliance SG5712 è l'opzione entry-level, una configurazione di base. La scelta di opzioni dalle performance più elevate come NetApp StorageGRID SG5760 o SG6060 può fornire benefici significativi in termini di performance. Per assistenza sul dimensionamento, consulta il Solution Architect NetApp StorageGRID.

Per la policy di protezione dei dati, StorageGRID utilizza una policy di Lifecycle management integrata (ILM) per gestire e proteggere i dati. Le regole ILM vengono valutate in una politica dall'alto verso il basso. Il criterio ILM viene implementato come illustrato nella tabella seguente:

Regola ILM	Qualificatori	Comportamento di acquisizione
Erasure coding 2+1	Oggetti superiori a 200KB	Bilanciato

Regola ILM	Qualificatori	Comportamento di acquisizione
2 Copia	Tutti gli oggetti	Dual commit

La regola di copia di ILM 2 è la regola predefinita. La regola Erasure Coding 2+1 è stata applicata per questo test a qualsiasi oggetto 200KB o superiore. La regola predefinita è stata applicata agli oggetti di dimensioni inferiori a 200KB. L'applicazione delle regole in questo modo è una Best practice di StorageGRID.

Per informazioni tecniche su questo ambiente di test, leggere la sezione progettazione della soluzione e Best practice nella "Data Protection scale-out NetApp con CommVault" report tecnico.

Specifiche dell'hardware StorageGRID

La tabella seguente descrive l'hardware NetApp StorageGRID utilizzato per questo test. L'appliance StorageGRID SG5712 con connettività di rete 10Gbps è l'opzione entry-level e rappresenta una configurazione di base. In alternativa, SG5712 può essere configurato per il collegamento in rete 25Gbps.

Hardware	Quantità	Disco	Capacità utilizzabile	Rete
Appliance StorageGRID SG5712	4	48 x 4TB GB (HDD SAS near-line)	136TB	10Gbps

La scelta di opzioni di appliance con performance più elevate come le appliance NetApp StorageGRID SG5760, SG6060 o All Flash SGF6112 può fornire benefici significativi in termini di performance. Per assistenza sul dimensionamento, consulta il Solution Architect NetApp StorageGRID.

Requisiti software CommVault e StorageGRID

Le tabelle seguenti elencano i requisiti software per il software CommVault e NetApp StorageGRID installato sul software VMware ai fini del test. Sono stati installati quattro programmi di gestione della trasmissione dati MediaAgent e un server CommServe. Nel test è stata implementata la connettività di rete 10Gbps per l'infrastruttura VMware. La tabella seguente

La tabella seguente elenca i requisiti di sistema totali del software CommVault:

Componente	Quantità	Datastore	Dimensione	Totale	Numero totale di IOPS richiesti
CommServe Server	1	SISTEMA OPERATIVO	500GB	500GB	n/a.
		SQL	500GB	500GB	n/a.
MediaAgent	4	CPU virtuale (vCPU)	16	64	n/a.
		RAM	128GB	512	n/a.

Componente	Quantità	Datastore	Dimensione	Totale	Numero totale di IOPS richiesti
		SISTEMA OPERATIVO	500GB	2TB	n/a.
		Cache indice	2TB	8TB	200+
		DB	2TB	8TB	200-80.000K

Nell'ambiente di test, sono stati implementati un nodo di amministrazione principale virtuale e un nodo di gateway virtuale su VMware su uno storage array NetApp e-Series E2812. Ciascun nodo si trovava su un server separato con i requisiti minimi dell'ambiente di produzione descritti nella tabella seguente:

Nella tabella seguente sono elencati i requisiti per i nodi amministrativi virtuali StorageGRID e i nodi gateway:

Tipo di nodo	Quantità	VCPU	RAM	Storage
Nodo gateway	1	8	24GB	100GB LUN per il sistema operativo
Nodo amministrativo	1	8	24GB	100GB LUN per il sistema operativo 200GB LUN per le tabelle dei nodi Admin 200GB LUN per l'audit log del nodo Admin

Guida al dimensionamento di StorageGRID

Consulta i tuoi specialisti in materia di data Protection NetApp per dimensionamento specifico del tuo ambiente. Gli specialisti della data Protection di NetApp possono utilizzare lo strumento CommVault Total Backup Storage Calculator per stimare i requisiti dell'infrastruttura di backup. Lo strumento richiede l'accesso al portale per i partner CommVault. Se necessario, registrati per accedere.

Input per il dimensionamento di CommVault

È possibile utilizzare le seguenti attività per eseguire il rilevamento per il dimensionamento della soluzione per la data Protection:

- Identifica i carichi di lavoro del sistema o dell'applicazione/database e la capacità front-end corrispondente (in terabyte [TB]) da proteggere.
- Identifica il carico di lavoro VM/file e la capacità front-end (TB) simile che deve essere protetta.
- Identificare i requisiti di conservazione a breve e a lungo termine.

- Identificare il change rate quotidiano in % per i set di dati/carichi di lavoro identificati.
- Identificazione della crescita dei dati prevista nei prossimi 12, 24 e 36 mesi.
- Definisci RTO e RPO per la data Protection/recovery in base alle esigenze di business.

Quando queste informazioni sono disponibili, è possibile eseguire il dimensionamento dell'infrastruttura di backup in modo da suddividere le capacità di storage richieste.

Guida al dimensionamento di StorageGRID

Prima di eseguire il dimensionamento del NetApp StorageGRID, prendi in considerazione questi aspetti del carico di lavoro:

- Capacità utilizzabile
- Modalità WORM
- Dimensione media dell'oggetto
- Requisiti relativi alle performance
- Criterio ILM applicato

La quantità di capacità utilizzabile ha bisogno di per adattarsi alla dimensione del workload di backup su cui si è eseguito il tiering in StorageGRID e al programma di conservazione.

La modalità WORM sarà attivata o meno? Una volta abilitato WORM in CommVault, il blocco degli oggetti verrà configurato su StorageGRID. In questo modo si aumenterà la capacità dello storage a oggetti necessaria. La quantità di capacità richiesta varia in base alla durata di conservazione e al numero di modifiche agli oggetti per ogni backup.

Average object size è un parametro di input che aiuta nel dimensionamento delle performance in un ambiente StorageGRID. Le dimensioni medie degli oggetti utilizzate per un carico di lavoro CommVault dipendono dal tipo di backup.

La tabella seguente elenca le dimensioni medie degli oggetti per tipo di backup e descrive le letture del processo di ripristino dall'archivio di oggetti:

Tipo di backup	Dimensione media oggetto	Ripristinare il comportamento
Eseguire una copia ausiliaria in StorageGRID	32MB	Lettura completa dell'oggetto 32MB
Backup diretto su StorageGRID (deduplica abilitata)	8MB	1MB lettura casuale
Backup diretto su StorageGRID (deduplica disattivata)	32MB	Lettura completa dell'oggetto 32MB

Inoltre, la comprensione dei requisiti prestazionali per backup completi e backup incrementali consente di determinare il dimensionamento dei nodi di storage StorageGRID. I metodi di data Protection della policy ILM (Information Lifecycle management) di StorageGRID determinano la capacità necessaria per memorizzare i backup CommVault e influiscono sul dimensionamento del grid.

La replica ILM di StorageGRID è uno dei due meccanismi utilizzati da StorageGRID per memorizzare i dati

degli oggetti. Quando StorageGRID assegna gli oggetti a una regola ILM che replica i dati, il sistema crea copie esatte dei dati degli oggetti e memorizza le copie nei nodi storage.

Erasure coding è il secondo metodo utilizzato da StorageGRID per memorizzare i dati degli oggetti. Quando StorageGRID assegna gli oggetti a una regola ILM configurata per creare copie con erasure coding, suddivide i dati degli oggetti in frammenti di dati. Calcola quindi ulteriori frammenti di parità e memorizza ogni frammento su un nodo storage diverso. Quando si accede a un oggetto, questo viene riassemblato utilizzando i frammenti memorizzati. Se un frammento di dati o un frammento di parità si danneggia o viene perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei dati e dei frammenti di parità rimanenti.

I due meccanismi richiedono diverse quantità di storage, come dimostrano questi esempi:

- Se si memorizzano due copie replicate, il carico di storage raddoppia.
- Se si archivia una copia con erasure coding 2+1, l'overhead dello storage aumenta di 1,5 volte.

Per la soluzione sottoposta a test, è stata utilizzata un'implementazione StorageGRID entry-level su un singolo sito:

- Nodo amministrativo: Macchina virtuale VMware (VM)
- Bilanciamento del carico: VMware VM
- Nodi storage: 4x SG5712 PB con 4TB dischi
- Nodo amministrativo primario e nodo gateway: Macchine virtuali VMware con i requisiti minimi del carico di lavoro di produzione

StorageGRID supporta anche i sistemi di bilanciamento del carico di terze parti.

Di solito, StorageGRID viene implementato in due o più siti con policy di data Protection che replicano i dati per proteggersi dai guasti a livello di nodo e di sito. Effettuando il backup dei dati su StorageGRID, i dati saranno protetti da copie multiple o dall'erasure coding che separa e riassembla i dati in modo affidabile attraverso un algoritmo.

È possibile utilizzare lo strumento di dimensionamento "Fusion" per dimensionare la griglia.

Scalabilità

È possibile espandere un sistema NetApp StorageGRID aggiungendo storage ai nodi storage, aggiungendo nuovi nodi grid a un sito esistente o aggiungendo un nuovo sito per il data center. È possibile eseguire espansioni senza interrompere il funzionamento del sistema corrente.
StorageGRID scala le performance utilizzando nodi con performance più elevate per i nodi storage o l'appliance fisica che esegue il bilanciamento del carico e i nodi amministrativi o semplicemente aggiungendo nodi aggiuntivi.

Per ulteriori informazioni sull'espansione del sistema StorageGRID, vedere "Guida all'espansione di StorageGRID 11,9".

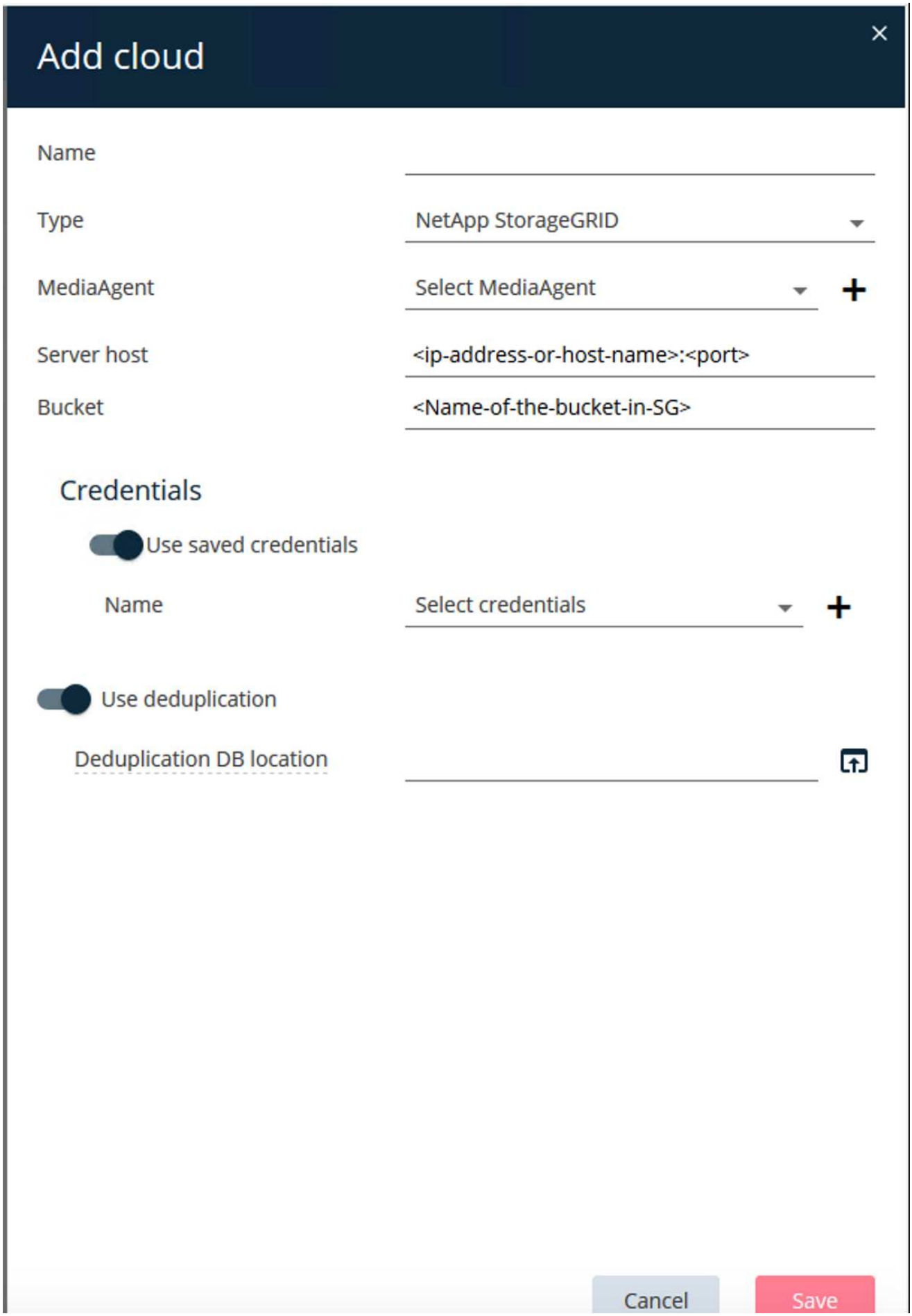
Eseguire un lavoro di protezione dati

Per configurare StorageGRID con CommVault complete Backup and Recovery for NetApp, sono stati eseguiti i seguenti passaggi per aggiungere StorageGRID come libreria cloud all'interno del software CommVault.

Fase 1: Configurare CommVault con StorageGRID

Fasi

1. Effettua l’accesso al CommVault Command Center. Nel pannello di sinistra, fare clic su archiviazione > Cloud > Aggiungi per visualizzare e rispondere alla finestra di dialogo Aggiungi cloud:


Add cloud
Name
Type
NetApp StorageGRID
MediaAgent
Select MediaAgent
Server host
<ip-address-or-host-name>:<port>
Bucket
<Name-of-the-bucket-in-SG>
Credentials
Use saved credentials
Name
Select credentials
Use deduplication
Deduplication DB location
Cancel
Save

2. Per tipo, selezionare NetApp StorageGRID.
3. Per MediaAgent, selezionare tutte le voci associate alla libreria cloud.
4. Per host server, immettere l'indirizzo IP o il nome host dell'endpoint StorageGRID e il numero di porta.

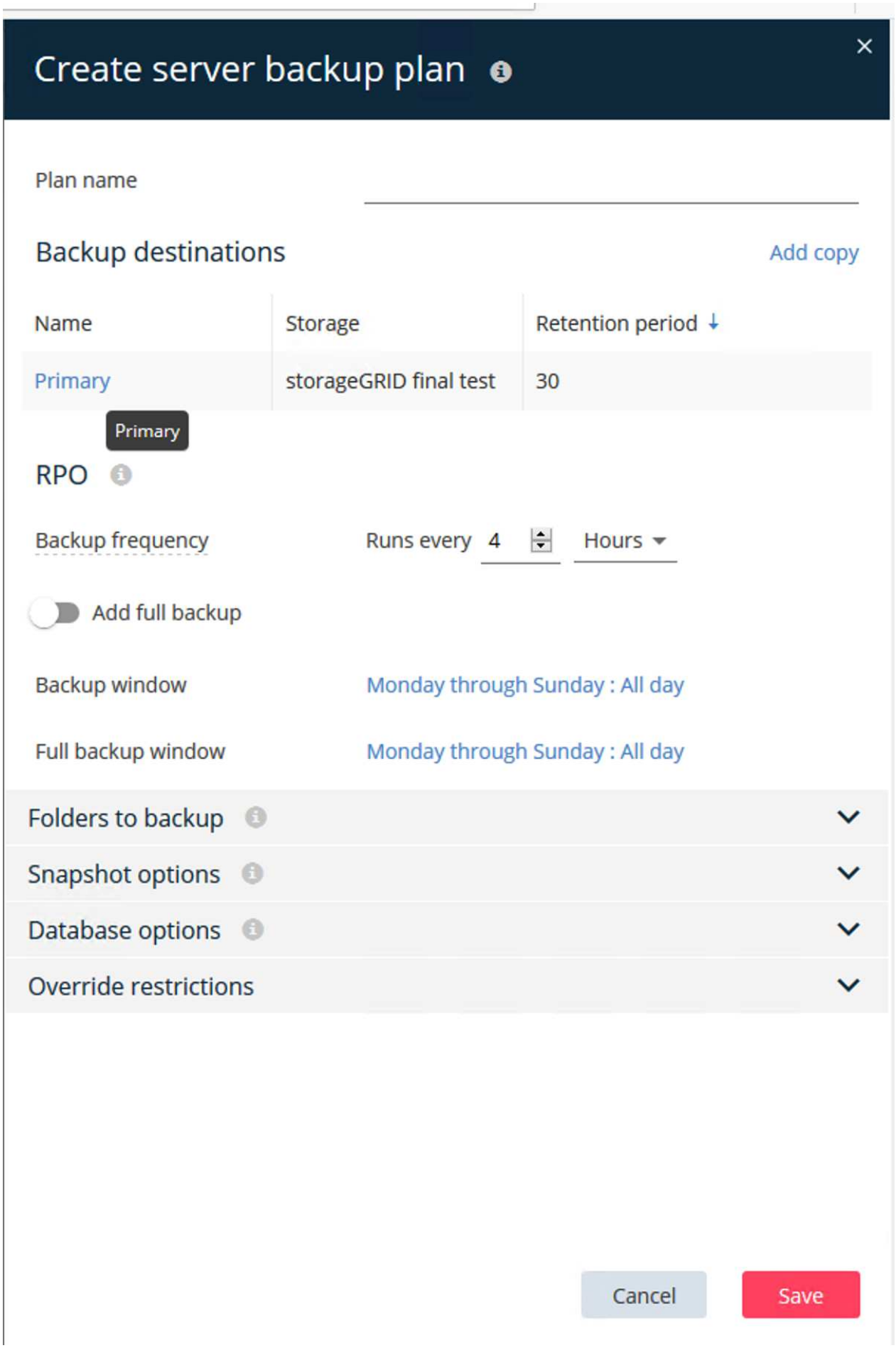
   Seguire le istruzioni riportate nella documentazione di StorageGRID a. "come configurare un endpoint del bilanciamento del carico (porta)". Assicurarsi di disporre di una porta HTTPS con un certificato autofirmato e dell'indirizzo IP o del nome di dominio dell'endpoint StorageGRID.

5. Se si desidera utilizzare la deduplica, attivare questa opzione e specificare il percorso del database di deduplica.
6. Fare clic su Salva.

Fase 2: Creare un piano di backup con StorageGRID come destinazione principale

Fasi

1. Nel pannello di sinistra, selezionare Gestisci > piani per visualizzare e rispondere alla finestra di dialogo Crea piano di backup server.

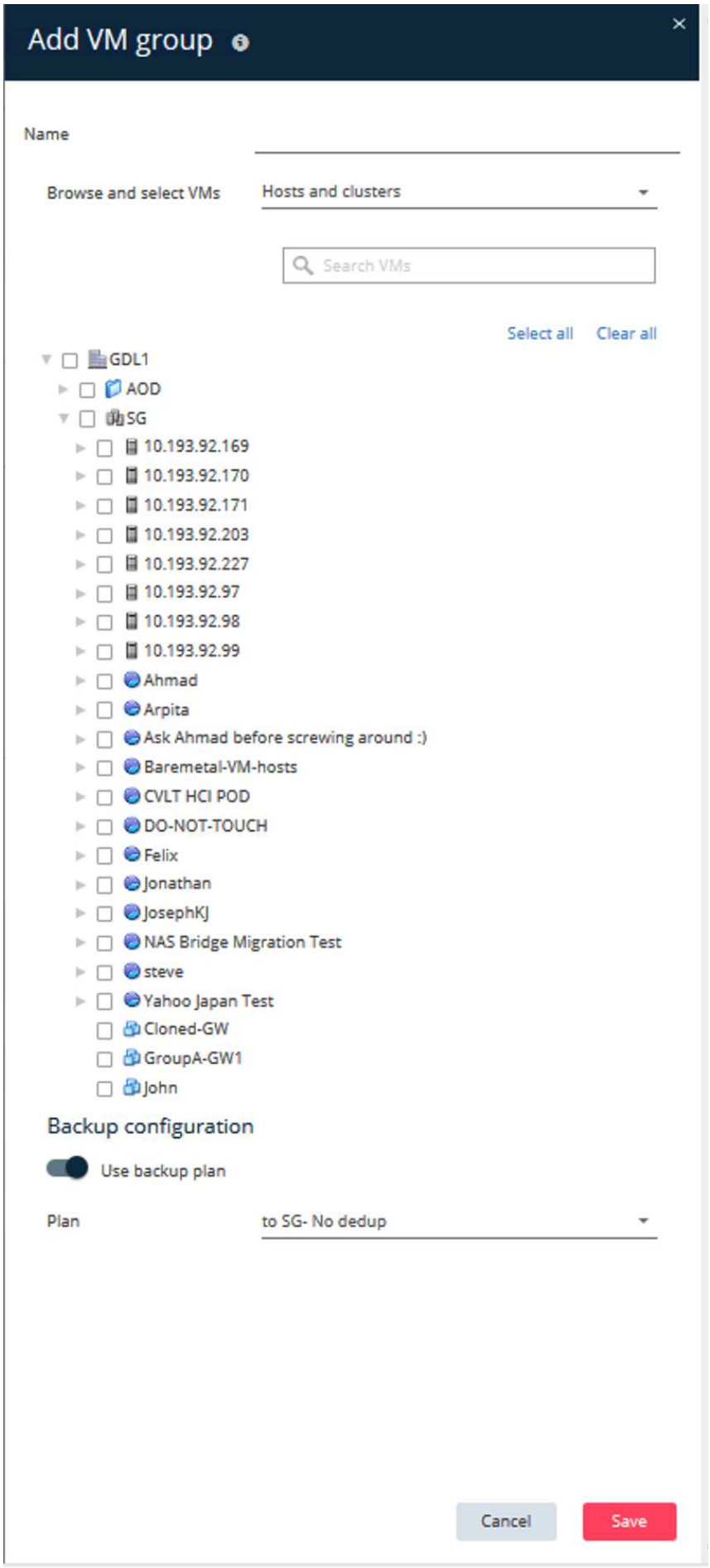

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to backup
Snapshot options
Database options
Override restrictions
Cancel
Save

2. Immettere il nome di un piano.
3. Selezionare la destinazione di backup dello storage di StorageGRID Simple Storage Service (S3) creata in precedenza.
4. Inserisci il periodo di conservazione dei backup e il recovery point objective (RPO) che preferisci.
5. Fare clic su Salva.

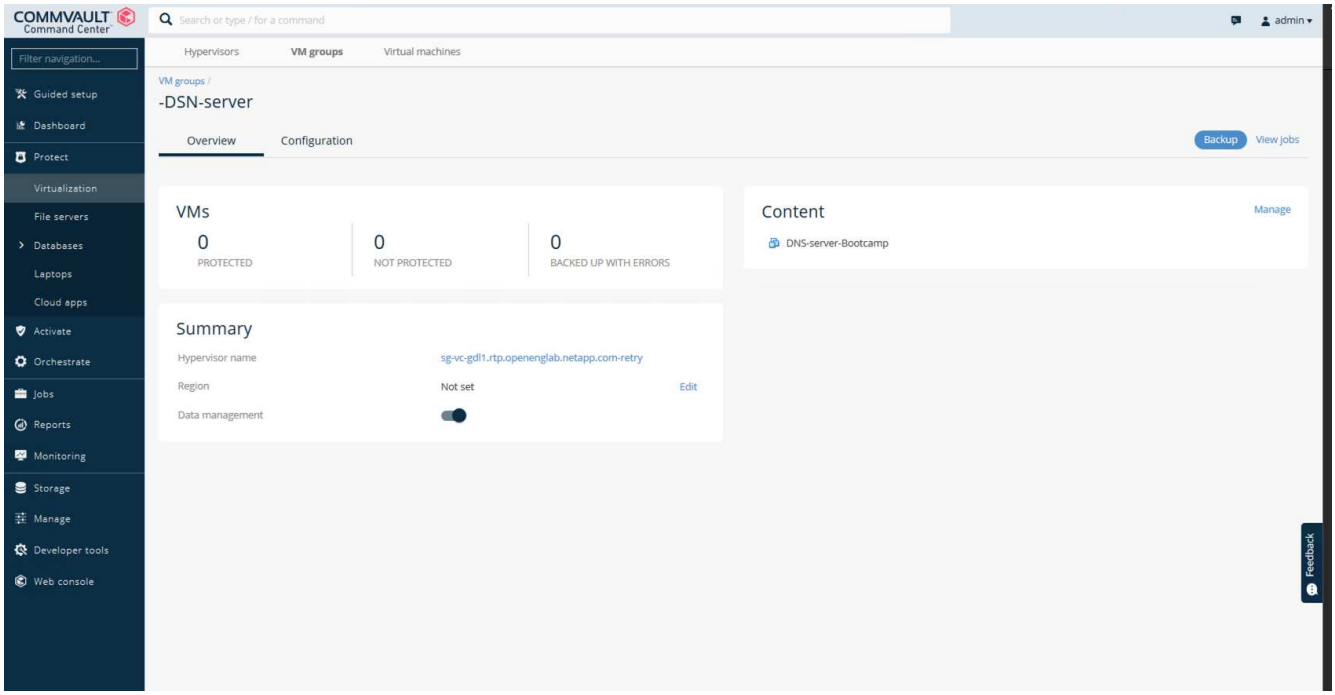
Fase 3: Avviare un processo di backup per proteggere i carichi di lavoro

Fasi

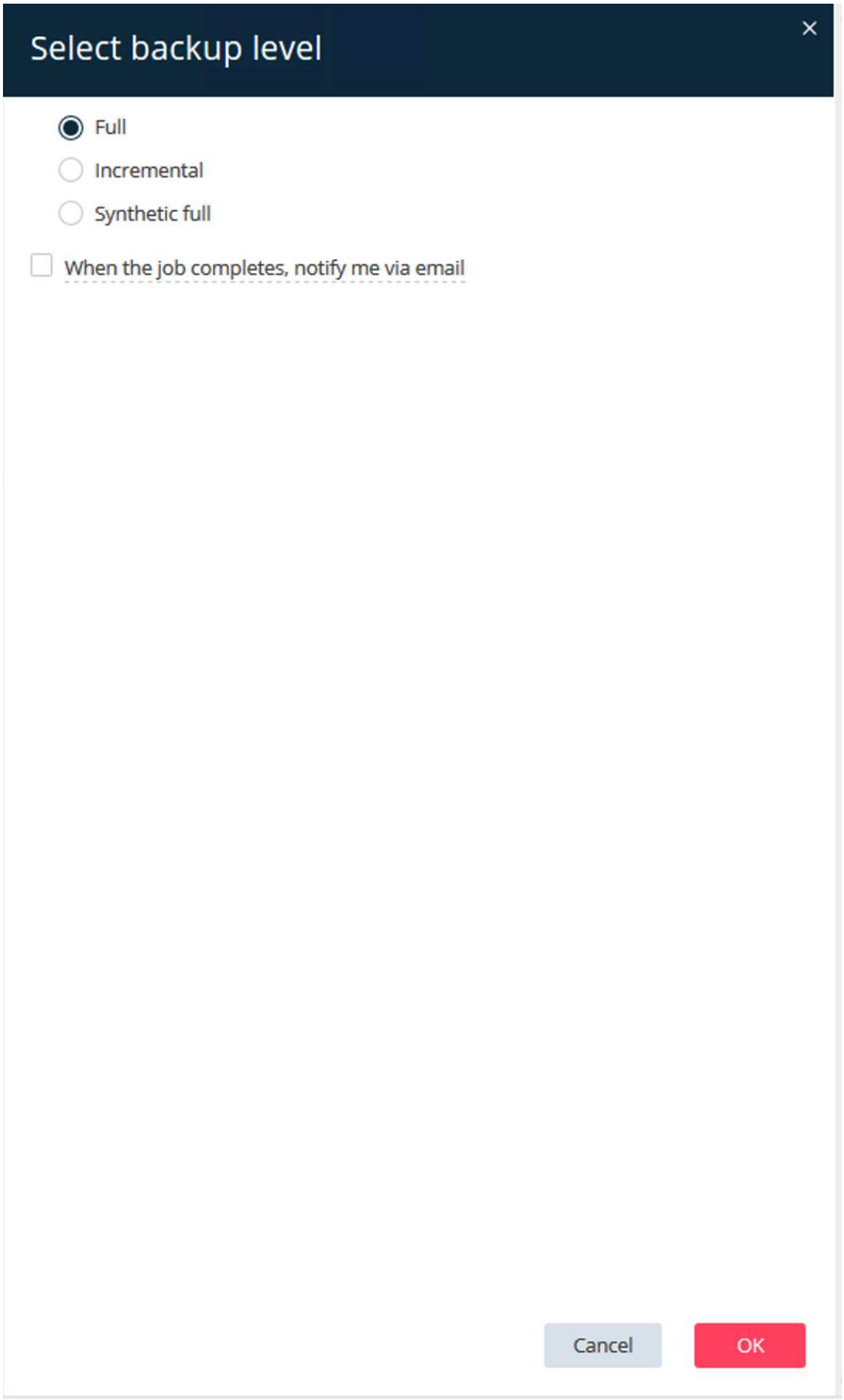
1. Sul CommVault Command Center, selezionare Protect > Virtualization (protezione > virtualizzazione).
2. Aggiunta di un hypervisor VMware vCenter Server.
3. Fare clic sull'hypervisor appena aggiunto.
4. Fare clic su Add VM group (Aggiungi gruppo VM) per rispondere alla finestra di dialogo Add VM Group (Aggiungi gruppo VM) in modo da visualizzare l'ambiente vCenter che si intende proteggere.


Add VM group
Name
Browse and select VMs
Hosts and clusters
Search VMs
Select all
Clear all
GDL1
AOD
SG
10.193.92.169
10.193.92.170
10.193.92.171
10.193.92.203
10.193.92.227
10.193.92.97
10.193.92.98
10.193.92.99
Ahmad
Arpita
Ask Ahmad before screwing around :)
Baremetal-VM-hosts
CVLT HCI POD
DO-NOT-TOUCH
Felix
Jonathan
JosephKJ
NAS Bridge Migration Test
steve
Yahoo Japan Test
Cloned-GW
GroupA-GW1
John
Backup configuration
Use backup plan
Plan
to SG- No dedup
Cancel
Save

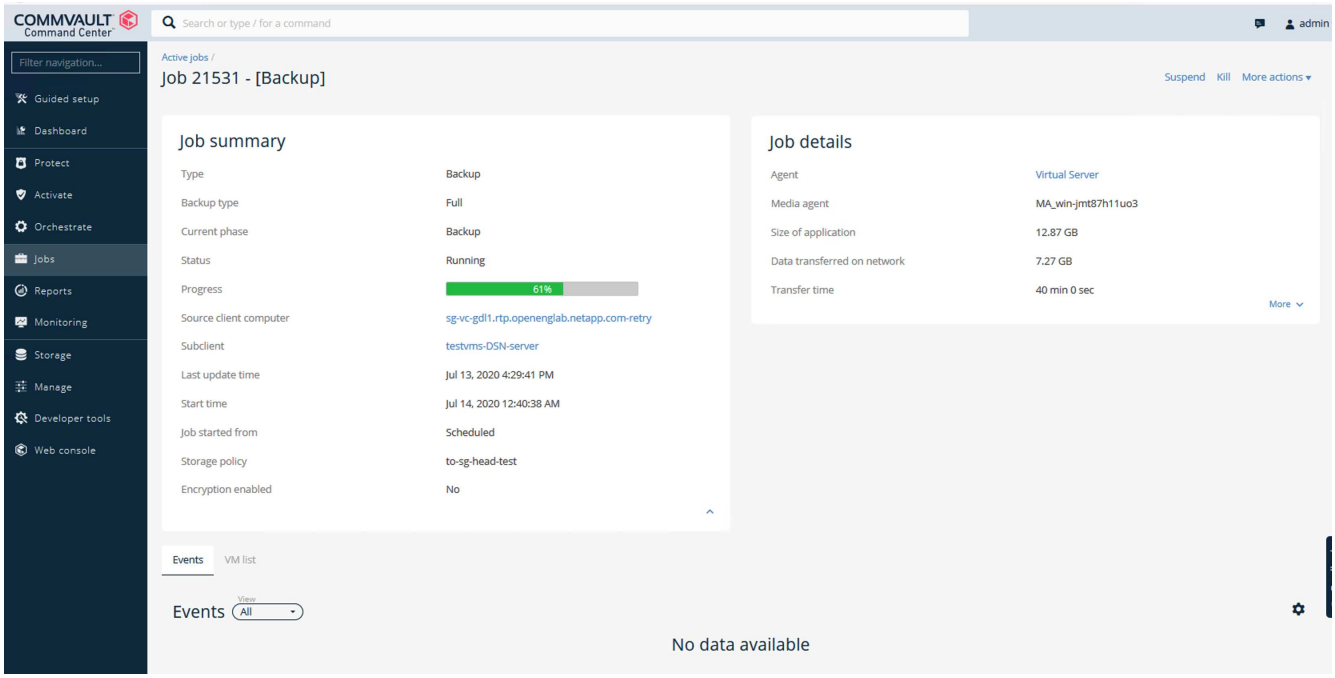
5. Seleziona un datastore, una macchina virtuale o una raccolta di macchine virtuali e inserisci un nome per questo.
6. Selezionare il piano di backup creato nell'attività precedente.
7. Fare clic su Salva per visualizzare il gruppo VM creato.
8. Nell'angolo superiore destro della finestra del gruppo VM, selezionare Backup:



9. Selezionare Full come livello di backup, (facoltativamente) richiedere un'e-mail al termine del backup, quindi fare clic su OK per avviare il processo di backup:


Select backup level
Full
Incremental
Synthetic full
When the job completes, notify me via email
Cancel
OK

10. Passare alla pagina di riepilogo dei lavori per visualizzare le metriche dei lavori:



Esaminare i test delle prestazioni di base

Nell'operazione di copia ausiliaria, quattro CommVault MediaAgent hanno eseguito il backup dei dati su un sistema NetApp AFF A300 e una copia ausiliaria è stata creata su NetApp StorageGRID. Per informazioni dettagliate sull'ambiente di configurazione dei test, leggere la sezione progettazione della soluzione e Best practice nel "Data Protection scale-out NetApp con CommVault" report tecnico.

I test sono stati eseguiti con 100 VM e 1000 VM, entrambi con una combinazione di 50/50 VM Windows e CentOS. La tabella seguente mostra i risultati dei nostri test di base sulle prestazioni:

Operazione	Velocità di backup	Ripristina velocità
Copia AUX	2 TB/ora	1,27 TB/ora
Diretto da e verso l'oggetto (deduplica attivata)	2,2 TB/ora	1,22 TB/ora

Per testare le performance di vecchiaia, sono stati eliminati 2,5 milioni di oggetti. Come mostrato nelle Figure 2 e 3, l'esecuzione di eliminazione è stata completata in meno di 3 ore e ha liberato più di 80TB GB di spazio. La seriografia di eliminazione è iniziata alle 10:30:00 AM.

Figura 1: Eliminazione di 2,5 milioni (80TB) oggetti in meno di 3 ore.

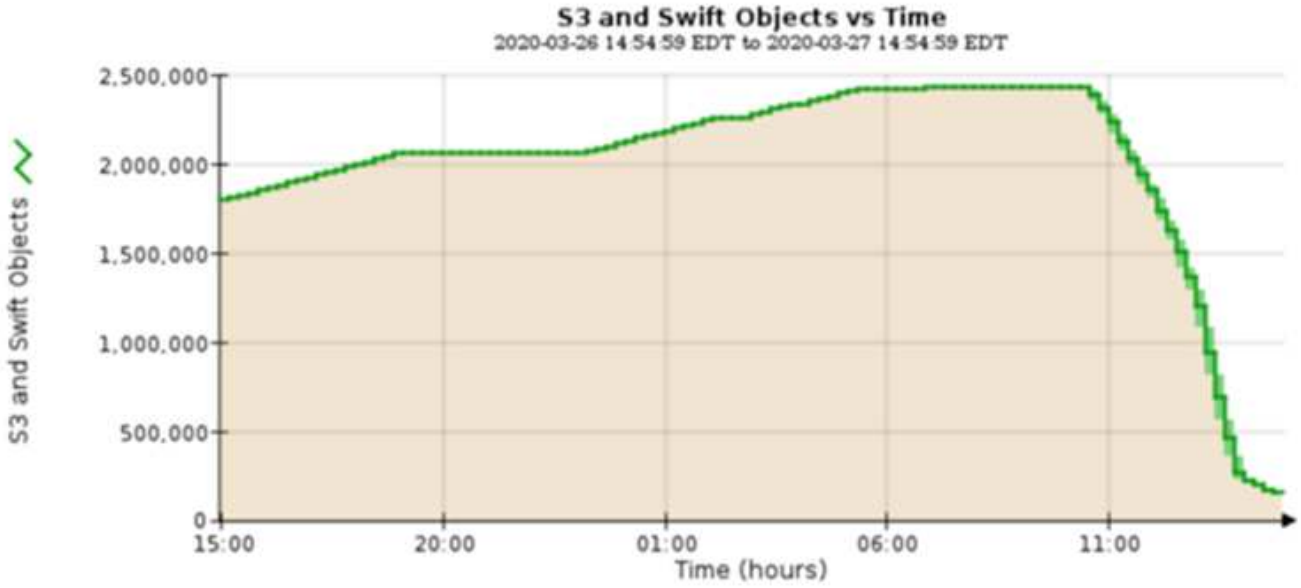
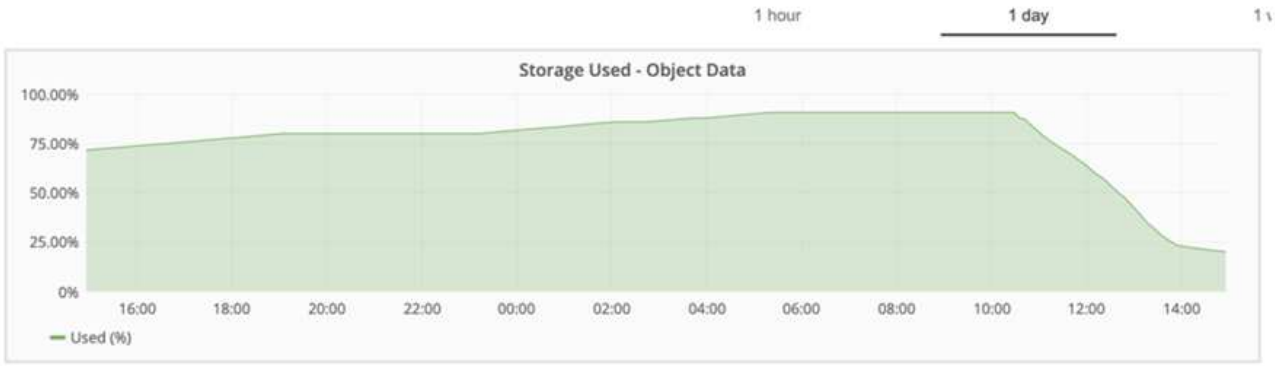


Figura 2: Liberare 80TB TB di storage in meno di 3 ore.



Suggerimento del livello di coerenza della benna

NetApp StorageGRID consente all'utente finale di selezionare il livello di coerenza per le operazioni eseguite sugli oggetti nei bucket Simple Storage Service (S3).

CommVault MediaAgent è il data mover di un ambiente CommVault. Nella maggior parte dei casi, i MediaAgent sono configurati per scrivere localmente in un sito StorageGRID primario. Per questo motivo, si consiglia un elevato livello di coerenza all'interno di un sito primario locale. Utilizza le seguenti linee guida quando imposti il livello di coerenza sui bucket CommVault creati in StorageGRID.

Se si dispone di una versione di CommVault precedente alla 11.0.0 - Service Pack 16, valutare la possibilità di aggiornare CommVault alla versione più recente. Se questa opzione non è disponibile, attenersi alle linee guida per la versione in uso.

- Versioni di CommVault precedenti alla 11.0.0 - Service Pack 16.* nelle versioni precedenti alla 11.0.0 - Service Pack 16, CommVault esegue S3 TESTE e OTTIENE le operazioni su oggetti inesistenti come parte del processo di ripristino e pruning. Impostare il livello di coerenza del bucket su un sito sicuro per ottenere un livello di coerenza ottimale per i backup CommVault su StorageGRID.
- CommVault versioni 11.0.0 - Service Pack 16 e successive.* nelle versioni 11.0.0 - Service Pack 16 e successive, il numero di operazioni HEAD S3 e GET eseguite su oggetti inesistenti viene ridotto al minimo.

Impostare il livello di coerenza del bucket predefinito su Read-after-new-write per garantire un elevato livello di coerenza nell'ambiente CommVault e StorageGRID.

TR-4626: Bilanciatori del carico

Utilizza sistemi di bilanciamento del carico di terze parti con StorageGRID

Scopri il ruolo di bilanciatori del carico globale e di terze parti in sistemi storage a oggetti come StorageGRID.

Indicazioni generali per l'implementazione di NetApp® StorageGRID® con sistemi di bilanciamento del carico di terze parti.

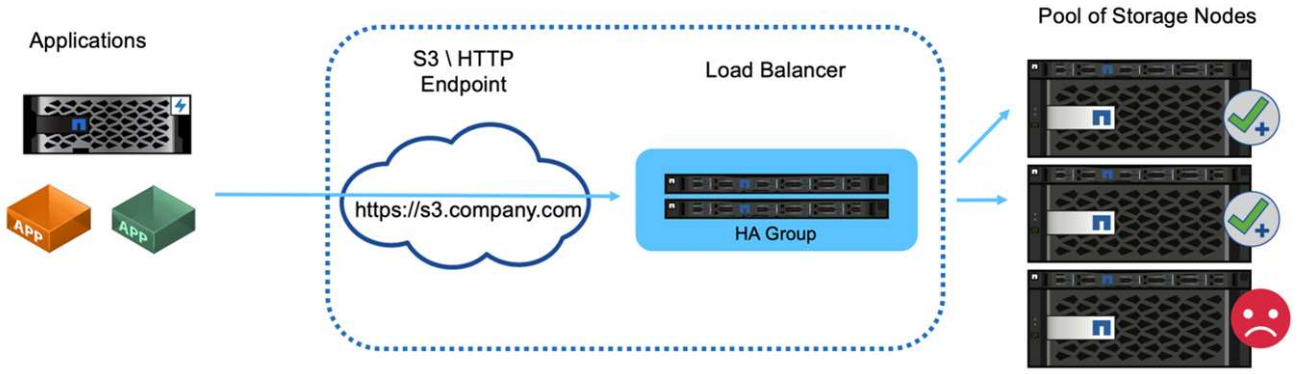
Lo storage a oggetti è sinonimo del termine cloud storage e, come ti aspetti, le applicazioni che sfruttano il cloud storage indirizzano tale storage attraverso un URL. Dietro questo semplice URL, StorageGRID può scalare capacità, performance e durata in un singolo sito o in siti distribuiti geograficamente. Il componente che rende possibile questa semplicità è il bilanciamento del carico.

Lo scopo di questo documento è informare i clienti StorageGRID sulle opzioni del bilanciamento del carico e fornire una guida generale per la configurazione dei bilanciatori del carico di terze parti.

Nozioni di base sul bilanciamento del carico

I bilanciatori del carico sono un componente essenziale di un sistema storage a oggetti di livello Enterprise come StorageGRID. StorageGRID è composto da più nodi storage, ciascuno dei quali può presentare l'intero spazio dei nomi di Simple Storage Service (S3) per una determinata istanza di StorageGRID. I bilanciatori del carico creano un endpoint altamente disponibile dietro cui è possibile posizionare i nodi StorageGRID. StorageGRID è un'esclusiva tra i sistemi di storage a oggetti compatibili con S3, in quanto offre un proprio bilanciamento del carico, ma supporta anche bilanciatori del carico di terze parti o General-purpose come F5, Citrix Netscaler, ha Proxy, NGINX e così via.

Nella figura seguente viene utilizzato l'URL di esempio/nome di dominio completo (FQDN) "s3.company.com". Il bilanciamento del carico crea un IP virtuale (VIP) che viene risolto all'FQDN tramite DNS, quindi indirizza le richieste dalle applicazioni a un pool di nodi StorageGRID. Il bilanciamento del carico esegue un controllo dello stato di salute su ogni nodo e stabilisce solo connessioni a nodi sani.



La figura mostra il bilanciamento del carico fornito da StorageGRID, ma il concetto è lo stesso per i bilanciatori del carico di terze parti. Le applicazioni stabiliscono una sessione HTTP utilizzando il VIP sul bilanciamento del carico e il traffico passa attraverso il bilanciamento del carico fino ai nodi di storage. Per impostazione predefinita, tutto il traffico, dall'applicazione al bilanciamento del carico e dal bilanciamento del carico al nodo storage è crittografato tramite HTTPS. HTTP è un'opzione supportata.

Bilanciatori del carico locali e globali

Esistono due tipi di bilanciatori del carico:

- **Gestione del traffico locale (LTM)**. Distribuisce le connessioni su un pool di nodi in un singolo sito.
- **Bilanciamento del carico di servizio globale (GSLB)**. Distribuisce le connessioni su siti multipli, bilanciando efficacemente il carico LTM. Pensate a un GSLB come a un server DNS intelligente. Quando un client richiede un URL endpoint StorageGRID, il GSLB lo risolve al VIP di un LTM in base alla disponibilità o ad altri fattori (ad esempio, quale sito può fornire una latenza inferiore all'applicazione). Mentre un LTM è sempre richiesto, un GSLB è opzionale a seconda del numero di siti StorageGRID e dei requisiti dell'applicazione.

Bilanciamento del carico del nodo gateway StorageGRID rispetto a quello di terze parti

StorageGRID è un'esclusiva tra i vendor di storage a oggetti compatibili con S3, in quanto offre un bilanciatore del carico nativo disponibile come appliance, VM o container costruiti ad hoc. Il bilanciamento del carico fornito da StorageGRID è anche detto nodo gateway.

Per i clienti che non dispongono già di un sistema di bilanciamento del carico, ad esempio F5, Citrix e così via, l'implementazione di un sistema di bilanciamento del carico di terze parti può rivelarsi molto complessa. Il bilanciamento del carico StorageGRID semplifica notevolmente le operazioni di bilanciamento del carico.

Il Gateway Node è un bilanciatore del carico di livello Enterprise, altamente disponibile e dalle performance elevate. I clienti possono scegliere di implementare il nodo gateway, il sistema di bilanciamento del carico di terze parti o anche entrambi nello stesso grid. Il nodo gateway è un gestore del traffico locale rispetto a un GSLB.

Il bilanciamento del carico StorageGRID offre i seguenti vantaggi:

- **Semplicità**. Configurazione automatica di pool di risorse, controlli dello stato di salute, applicazione di patch e manutenzione, il tutto gestito da StorageGRID.
- **Prestazioni**. Il sistema di bilanciamento del carico StorageGRID è dedicato a StorageGRID e non è in competizione con altre applicazioni per la larghezza di banda.
- **Costo**. Le versioni di macchina virtuale (VM) e container sono fornite senza costi aggiuntivi.
- **Classificazioni del traffico**. La funzionalità Advanced Traffic Classification consente di applicare regole QoS specifiche di StorageGRID insieme all'analisi dei workload.
- **Caratteristiche specifiche future di StorageGRID**. StorageGRID continuerà a ottimizzare e aggiungere funzioni innovative al bilanciatore di carico nelle prossime release.

Per informazioni dettagliate sulla distribuzione del nodo gateway StorageGRID, vedere "Documentazione StorageGRID".

Dove trovare ulteriori informazioni

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

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Considerazioni sulla progettazione del bilanciamento del carico StorageGRID F5 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/

- Loadbalancer.org—Load bilanciamento NetApp StorageGRID https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp - NetApp StorageGRID di bilanciamento del carico https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Informazioni su come implementare i certificati SSL per HTTPS in StorageGRID

Comprendere l'importanza e i passaggi per implementare i certificati SSL in StorageGRID.

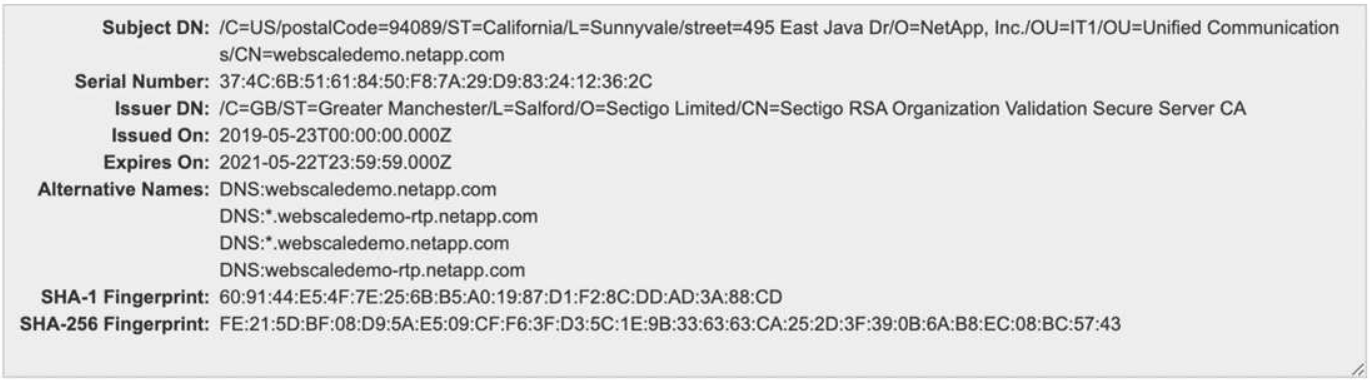
Se si utilizza HTTPS, è necessario disporre di un certificato SSL (Secure Sockets Layer). Il protocollo SSL identifica i client e gli endpoint, convalidandoli come attendibili. SSL fornisce anche la crittografia del traffico. Il certificato SSL deve essere attendibile dai client. A tal fine, il certificato SSL può provenire da un'autorità di certificazione (CA) globalmente attendibile, ad esempio DigiCert, una CA privata in esecuzione nell'infrastruttura o un certificato autofirmato generato dall'host.

L'utilizzo di un certificato CA globale attendibile è il metodo preferito poiché non sono necessarie ulteriori azioni sul lato client. Il certificato viene caricato nel bilanciamento del carico o StorageGRID e i client si fidano e si connettono all'endpoint.

L'utilizzo di una CA privata richiede l'aggiunta al client di tutti i certificati subordinati e della directory principale. Il processo per considerare attendibile un certificato CA privato può variare in base al sistema operativo e alle applicazioni del client. Ad esempio, in ONTAP per FabricPool, è necessario caricare ciascun certificato nella catena individualmente (certificato di origine, certificato di subordinazione, certificato di endpoint) nel cluster ONTAP.

L'utilizzo di un certificato autofirmato richiede al client di considerare attendibile il certificato fornito senza alcuna CA per verificarne l'autenticità. Alcune applicazioni potrebbero non accettare certificati autofirmati e non essere in grado di ignorare la verifica.

Il posizionamento del certificato SSL nel percorso StorageGRID di bilanciamento del carico del client dipende da dove è necessaria la terminazione SSL. È possibile configurare un bilanciamento del carico come endpoint di terminazione per il client, quindi eseguire nuovamente la crittografia o la crittografia a caldo con un nuovo certificato SSL per il bilanciamento del carico alla connessione StorageGRID. In alternativa, è possibile passare attraverso il traffico e lasciare che StorageGRID sia l'endpoint di terminazione SSL. Se il bilanciamento del carico è l'endpoint di terminazione SSL, il certificato viene installato sul bilanciamento del carico e contiene il nome del soggetto per il nome/URL DNS e qualsiasi nome URL/DNS alternativo per il quale un client è configurato per connettersi alla destinazione StorageGRID tramite il bilanciamento del carico, inclusi i nomi dei caratteri jolly. Se il bilanciamento del carico è configurato per il pass-through, il certificato SSL deve essere installato in StorageGRID. Anche in questo caso, il certificato deve contenere il nome del soggetto per il nome/URL DNS e tutti i nomi URL/DNS alternativi per i quali un client è configurato per connettersi alla destinazione StorageGRID tramite il sistema di bilanciamento del carico, inclusi i nomi di caratteri jolly. Non è necessario includere nel certificato i nomi dei singoli nodi di archiviazione, ma solo gli URL degli endpoint.



Configurare il bilanciamento del carico di terze parti attendibile in StorageGRID

Scopri come configurare il bilanciamento del carico di terze parti attendibile in StorageGRID.

Se si utilizzano uno o più bilanciatori di carico Layer 7 esterni e un bucket S3 o policy di gruppo basati su IP, StorageGRID deve determinare l'indirizzo IP reale del mittente. Ciò avviene guardando l'intestazione X-Forwarding-for (XFF), che viene inserita nella richiesta dal bilanciatore di carico. Poiché l'intestazione XFF può essere facilmente sottoposta a spoofing nelle richieste inviate direttamente ai nodi di archiviazione, StorageGRID deve confermare che ogni richiesta è stata instradata da un bilanciatore di carico di livello 7 attendibile. Se StorageGRID non è in grado di considerare attendibile l'origine della richiesta, ignorerà l'intestazione XFF. È disponibile un'API di gestione griglia che consente di configurare un elenco di bilanciatori del carico di livello 7 esterni attendibili. Questa nuova API è privata ed è soggetta a modifiche nelle versioni future di StorageGRID. Per le informazioni più aggiornate, vedere l'articolo della Knowledge base, "Come configurare StorageGRID per il funzionamento con sistemi di bilanciamento del carico Layer 7 di terze parti".

Informazioni sui bilanciatori del carico dei gestori del traffico locali

Esplora le linee guida per i bilanciatori del carico del gestore del traffico locale e determina la configurazione ottimale.

Quanto segue viene presentato come guida generale per la configurazione dei sistemi di bilanciamento del carico di terze parti. Collabora con l'amministratore del sistema di bilanciamento del carico per determinare la configurazione ottimale per il tuo ambiente.

Creare un gruppo di risorse di nodi di archiviazione

Raggruppare i nodi di storage StorageGRID in un pool di risorse o in un gruppo di servizi (la terminologia potrebbe differire con specifici bilanciatori del carico). I nodi storage StorageGRID presentano l'API S3 sulle seguenti porte:

- S3 HTTPS: 18082
- S3 HTTP: 18084

La maggior parte dei clienti sceglie di presentare le API sul server virtuale tramite le porte HTTPS e HTTP standard (443 e 80).

> Ogni sito StorageGRID richiede un'impostazione predefinita di tre nodi storage, due dei quali devono essere integri.

Controllo dello stato di salute

I sistemi di bilanciamento del carico di terze parti richiedono un metodo per determinare lo stato di salute di ogni nodo e la sua idoneità a ricevere il traffico. NetApp consiglia di utilizzare il metodo HTTP `OPTIONS` per eseguire il controllo dello stato di salute. Il bilanciamento del carico invia richieste HTTP `OPTIONS` a ogni singolo nodo di storage e prevede una `200` risposta di stato.

Se un nodo di archiviazione non fornisce una `200` risposta, tale nodo non è in grado di eseguire il servizio delle richieste di archiviazione. I requisiti dell'applicazione e dell'azienda devono determinare il timeout per questi controlli e l'azione intrapresa dal bilanciamento del carico.

Ad esempio, se tre dei quattro nodi storage del data center 1 non sono attivi, è possibile indirizzare tutto il traffico al data center 2.

L'intervallo di polling consigliato è una volta al secondo, contrassegnando il nodo offline dopo tre controlli non riusciti.

Esempio di controllo dello stato di salute di S3

Nell'esempio seguente, inviamo `OPTIONS` e controlliamo `200 OK`. Lo utilizziamo `OPTIONS` perché Amazon S3) non supporta richieste non autorizzate.

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

Controlli dello stato di salute basati su file o contenuti

In generale, NetApp non consiglia controlli dello stato di salute basati su file. In genere, un file di piccole dimensioni —`healthcheck.htm`, ad esempio, viene creato in un bucket con un criterio di sola lettura. Questo file viene quindi recuperato e valutato dal bilanciamento del carico. Questo approccio presenta diversi svantaggi:

- **Dipendente da un unico conto.** Se l'account proprietario del file è disattivato, il controllo di integrità non riesce e non vengono elaborate richieste di archiviazione.
- **Regole per la protezione dei dati.** Lo schema di protezione dei dati predefinito è un approccio a due copie. In questo scenario, se i due nodi storage che ospitano il file di controllo dello stato di salute non sono disponibili, il controllo dello stato di salute non riesce e le richieste di storage non vengono inviate ai nodi storage sani, rendendo la griglia offline.
- **Registro di controllo bloat.** Il bilanciamento del carico recupera il file da ogni nodo storage ogni X minuti, creando molte voci di registro di controllo.
- **Uso intensivo delle risorse.** Il recupero del file di controllo dello stato da ogni nodo ogni pochi secondi consuma le risorse della rete e della griglia.

Se è necessario un controllo dello stato di salute basato sul contenuto, utilizzare un tenant dedicato con un bucket S3 dedicato.

Persistenza della sessione

La persistenza della sessione, o stickiness, si riferisce al tempo in cui una data sessione HTTP può persistere. Per impostazione predefinita, le sessioni vengono interrotte dai nodi storage dopo 10 minuti. Una persistenza più lunga può portare a performance migliori, perché le applicazioni non devono ristabilire le sessioni per ogni azione; tuttavia, mantenendo queste sessioni aperte si consumano le risorse. Se ritieni che il tuo carico di lavoro trarrà beneficio, puoi ridurre la persistenza della sessione su un bilanciamento del carico di terze parti.

Indirizzamento virtuale in stile host

Lo stile in hosting virtuale è ora il metodo predefinito per AWS S3 e, sebbene StorageGRID e molte applicazioni supportino ancora lo stile del percorso, è consigliabile implementare il supporto in stile in hosting virtuale. Le richieste in stile host virtuale hanno il bucket come parte del nome host.

Per supportare lo stile host virtuale, procedere come segue:

- Supporta ricerche DNS con caratteri jolly: *.s3.company.com
- Utilizzare un certificato SSL con nomi alt del soggetto per supportare i caratteri jolly: *.s3.company.com alcuni clienti hanno espresso preoccupazioni per la sicurezza riguardo all'uso dei certificati jolly. StorageGRID continua a supportare l'accesso in stile percorso, così come le applicazioni chiave come FabricPool. Detto questo, alcune chiamate API S3 non riescono o si comportano in modo errato senza supporto di hosting virtuale.

Terminazione SSL

La terminazione SSL dei sistemi di bilanciamento del carico di terze parti offre vantaggi in termini di sicurezza. Se il bilanciamento del carico è compromesso, la griglia viene suddivisa in comparti.

Sono disponibili tre configurazioni supportate:

- **Pass-through SSL.** Il certificato SSL viene installato su StorageGRID come certificato server personalizzato.
- **Terminazione SSL e nuova crittografia (consigliata).** Ciò potrebbe essere utile se si sta già eseguendo la gestione dei certificati SSL sul sistema di bilanciamento del carico piuttosto che installare il certificato SSL su StorageGRID. Questa configurazione offre un ulteriore vantaggio in termini di sicurezza nel limitare la superficie di attacco al bilanciatore del carico.
- **Terminazione SSL con HTTP.** In questa configurazione, SSL viene terminato sul bilanciamento del carico di terze parti e la comunicazione dal bilanciamento del carico a StorageGRID non è crittografata per

sfruttare il off-load SSL (con librerie SSL incorporate nei processori moderni questo è di limitato beneficio).

Configurazione pass-through

Se si preferisce configurare il bilanciamento del carico per il pass-through, è necessario installare il certificato su StorageGRID. Andare al **Configurazione › certificati server › certificato server endpoint del servizio API di archiviazione oggetti**.

Visibilità IP del client di origine

StorageGRID 11,4 ha introdotto il concetto di un sistema di bilanciamento del carico di terze parti affidabile. Per inoltrare l'IP dell'applicazione client a StorageGRID, è necessario configurare questa funzione. Per ulteriori informazioni, vedere "Come configurare StorageGRID per il funzionamento con sistemi di bilanciamento del carico Layer 7 di terze parti."

Per abilitare l'intestazione XFF per la visualizzazione dell'IP dell'applicazione client, attenersi alla seguente procedura:

Fasi

1. Registrare l'IP del client nel registro di controllo.
2. Utilizzare `aws:SourceIp` criteri di gruppo o bucket S3.

Strategie di bilanciamento del carico

La maggior parte delle soluzioni di bilanciamento del carico offre molteplici strategie per il bilanciamento del carico. Le seguenti sono strategie comuni:

- **Rotondi.** Un adattamento universale ma soffre di pochi nodi e grandi trasferimenti che ostruiscono i singoli nodi.
- **Connessione minima.** Ideale per workload di oggetti piccoli e misti, con una distribuzione equa delle connessioni a tutti i nodi.

La scelta dell'algoritmo diventa meno importante con un numero crescente di nodi storage tra cui scegliere.

Percorso dei dati

Tutti i flussi di dati attraverso i bilanciatori del carico del gestore del traffico locale. StorageGRID non supporta il routing diretto del server (DSR).

Verifica della distribuzione dei collegamenti

Per verificare che il metodo in uso distribuisca il carico in modo uniforme tra i nodi storage, controllare le sessioni stabilite su ciascun nodo in un determinato sito:

- **Metodo UI.** Andare al **supporto › metriche › Panoramica S3 › sessioni HTTP LDR**
- **API metriche.** Uso `storagegrid_http_sessions_incoming_currently_established`

Scopri i pochi casi di utilizzo per le configurazioni StorageGRID

Scopri alcuni casi di utilizzo per le configurazioni StorageGRID implementate dai clienti e da NetApp IT.

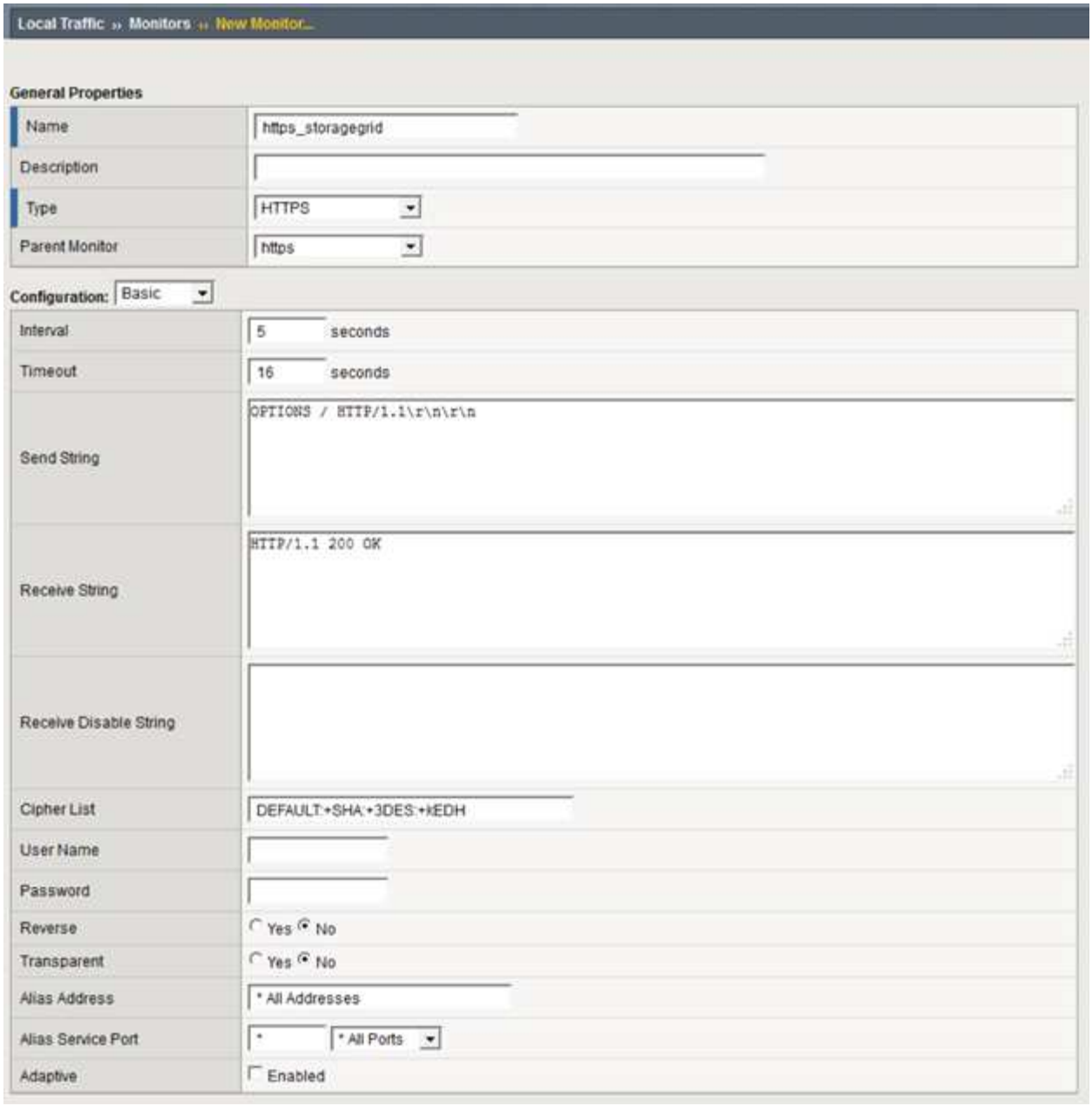
I seguenti esempi illustrano le configurazioni implementate dai clienti StorageGRID, incluso NetApp IT.

F5 BIG-IP, il monitor di controllo dello stato del gestore del traffico locale per bucket S3

Per configurare il monitor di controllo dello stato del gestore del traffico locale BIG-IP F5, attenersi alla seguente procedura:

Fasi

1. Creare un nuovo monitor.
   a. Nel campo tipo, immettere `HTTPS`.
   b. Configurare l'intervallo e il timeout come desiderato.
   c. Nel campo Invia stringa, immettere `OPTIONS / HTTP/1.1\r\n\r\n`. \r\n sono ritorni a capo; versioni diverse del software BIG-IP richiedono zero, uno o due set di sequenze \r\n. Per ulteriori informazioni, vedere https://support.f5.com/csp/article/K10655.
   d. Nel campo Receive String (stringa di ricezione), immettere: `HTTP/1.1 200 OK`.



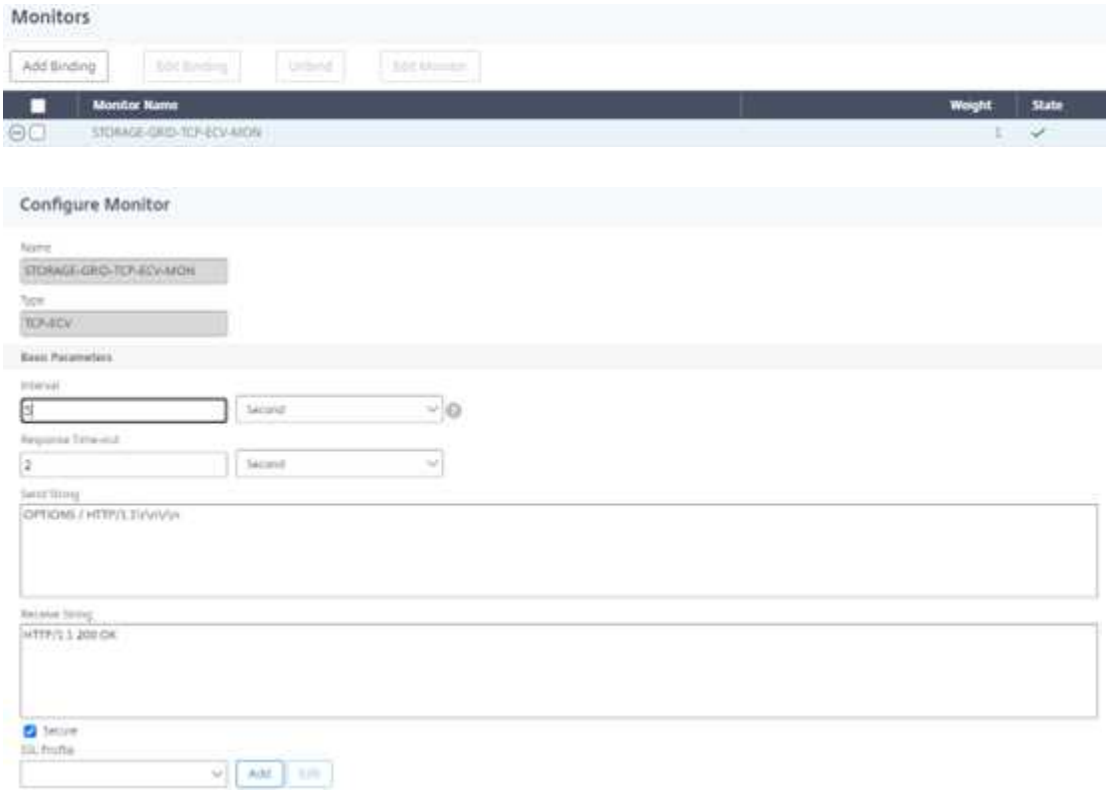
2. In Create Pool (Crea pool) creare un pool per ciascuna porta richiesta.
   a. Assegnare il monitor dello stato creato nel passaggio precedente.
   b. Selezionare un metodo di bilanciamento del carico.
   c. Selezionare la porta di servizio: 18082 (S3).
   d. Aggiungere nodi.

Citrix NetScaler

Citrix NetScaler crea un server virtuale per l'endpoint di storage e fa riferimento ai nodi storage StorageGRID come server applicazioni, che vengono quindi raggruppati in servizi.

Utilizzare il monitor di controllo dello stato HTTPS-ECV per creare un monitor personalizzato per eseguire il controllo dello stato consigliato utilizzando le OPZIONI richiesta e ricezione `200`. HTTP-ECV è configurato con una stringa di invio e convalida una stringa di ricezione.

Per ulteriori informazioni, consultare la documentazione Citrix, "Configurazione di esempio per il monitor di controllo dello stato HTTP-ECV".



Loadbalancer.org

Loadbalancer.org ha eseguito i propri test di integrazione con StorageGRID e dispone di una guida completa alla configurazione: https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp ha condotto i propri test di integrazione con StorageGRID e dispone di una guida alla configurazione completa: https://kemptechnologies.com/solutions/netapp/.

HAProxy

Configurare HAProxy per utilizzare la richiesta di OPZIONI e controllare una risposta di stato 200 per il controllo dello stato in hproxy.cfg. È possibile modificare la porta di binding nella parte anteriore in una porta diversa, ad esempio 443.

Di seguito è riportato un esempio di terminazione SSL su HAProxy:

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

Di seguito è riportato un esempio di pass-through SSL:

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

Per esempi completi di configurazioni per StorageGRID, vedere "Esempi di configurazione HAProxy" su GitHub.

Convalidare la connessione SSL in StorageGRID

Informazioni su come convalidare la connessione SSL in StorageGRID.

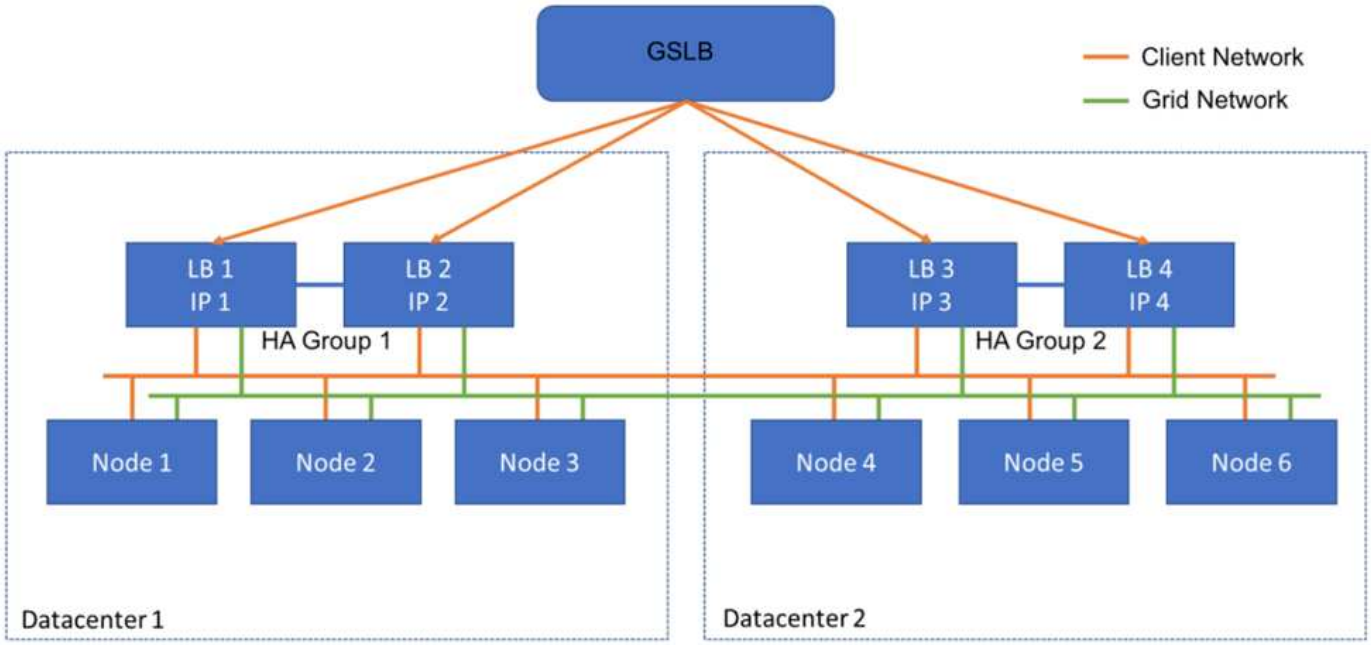
Una volta configurato il bilanciamento del carico, è necessario convalidare la connessione utilizzando strumenti come OpenSSL e l'interfaccia CLI di AWS. Altre applicazioni, come il browser S3, potrebbero ignorare errori di configurazione SSL.

Comprendere i requisiti globali di bilanciamento del carico per StorageGRID

Esplorate le considerazioni e i requisiti di progettazione per il bilanciamento del carico globale in StorageGRID.

Il bilanciamento del carico globale richiede l'integrazione con DNS per fornire routing intelligente su più siti StorageGRID. Questa funzione si trova al di fuori del dominio StorageGRID e deve essere fornita da una soluzione di terze parti come i prodotti di bilanciamento del carico discussi in precedenza e/o una soluzione di controllo del traffico DNS come Infoblox. Il bilanciamento del carico di livello superiore fornisce un routing

intelligente al sito di destinazione più vicino nello spazio dei nomi, nonché il rilevamento e il reindirizzamento dei black-out al sito successivo nello spazio dei nomi. Una tipica implementazione GSLB è costituita dal GSLB di livello superiore con pool di siti contenenti bilanciatori del carico locale-sito. I bilanciatori del carico del sito contengono pool di nodi di storage del sito locale. Ciò può includere una combinazione di bilanciatori del carico di terze parti per le funzioni GSLB e StorageGRID che fornisce il bilanciamento del carico locale del sito, o una combinazione di terze parti, o molte delle terze parti discusse in precedenza possono fornire bilanciamento del carico sia GSLB che locale del sito.



TR-4645: Funzionalità di sicurezza

Proteggi dati e metadati StorageGRID in un archivio di oggetti

Scopri le funzionalità di sicurezza integrate della soluzione di storage a oggetti StorageGRID.

Questa è una panoramica delle numerose funzionalità di protezione di NetApp® StorageGRID®, che includono l'accesso ai dati, gli oggetti e i metadati, l'accesso amministrativo e la protezione della piattaforma. È stato aggiornato per includere le funzioni più recenti rilasciate con StorageGRID 11,9.

La sicurezza è parte integrante della soluzione di storage a oggetti NetApp StorageGRID. La sicurezza è particolarmente importante, in quanto molti tipi di dati rich content adatti allo storage a oggetti sono anche sensibili, soggetti a normative e conformità. Con la continua evoluzione delle funzionalità di StorageGRID, il software rende disponibili molte funzionalità di sicurezza preziose per proteggere il livello di sicurezza di un'organizzazione e aiutare l'organizzazione a soddisfare le Best practice del settore.

In questo documento viene fornita una panoramica delle numerose funzioni di protezione di StorageGRID 11,9, suddivise in cinque categorie:

- Funzioni di sicurezza per l'accesso ai dati
- Funzionalità di sicurezza di oggetti e metadati
- Funzioni di protezione di amministrazione
- Funzioni di sicurezza della piattaforma

- Integrazione del cloud

Questo documento è destinato a essere una scheda tecnica di protezione, non descrive in dettaglio come configurare il sistema in modo che supporti le funzioni di protezione enumerate all'interno delle quali non sono configurate per impostazione predefinita. La "Guida alla tempra StorageGRID" è disponibile nella pagina ufficiale "Documentazione StorageGRID" .

Oltre alle funzionalità descritte in questo rapporto, StorageGRID segue la "Criteri di notifica e risposta alle vulnerabilità di protezione dei prodotti NetApp". Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

NetApp StorageGRID offre funzionalità di sicurezza avanzate per casi di utilizzo dello storage a oggetti aziendale molto esigenti.

Dove trovare ulteriori informazioni

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

- NetApp StorageGRID: Valutazione della conformità SEC 17a-4(f), FINRA 4511(c) e CFTC 1,31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Pagina della documentazione di StorageGRID 11,9 https://docs.netapp.com/us-en/storagegrid-119/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Termini e acronimi

In questa sezione vengono fornite le definizioni della terminologia utilizzata nel documento.

Termine o acronimo	Definizione
S3	Simple Storage Service.
Client	Applicazione in grado di interfacciarsi con StorageGRID tramite il protocollo S3 per l'accesso ai dati o il protocollo HTTP per la gestione.
Amministratore tenant	L'amministratore dell'account tenant StorageGRID
Utente tenant	Un utente all'interno di un account tenant StorageGRID
TLS	Transport Layer Security
ILM	Gestione del ciclo di vita delle informazioni
LAN	Local Area Network (rete locale)
Amministratore di grid	L'amministratore del sistema StorageGRID
Griglia	Il sistema StorageGRID
Bucket	Un contenitore per gli oggetti memorizzati in S3
LDAP	Lightweight Directory Access Protocol
SEC.	Securities and Exchange Commission; regola i membri di Exchange, i broker o i dealer

Termine o acronimo	Definizione
FINRA	Autorità di regolamentazione del settore finanziario; difende i requisiti di formato e media della norma SEC 17a-4(f)
CFTC	Commodity Futures Trading Commission; regola il commodity futures trading
NIST	Istituto Nazionale di Standard e tecnologia

Funzioni di sicurezza per l’accesso ai dati

Scopri le funzionalità di sicurezza dell’accesso ai dati di StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
TLS (Transport Layer Security) configurabile	TLS stabilisce un protocollo di handshake per la comunicazione tra un client e un nodo di gateway StorageGRID, un nodo storage o un endpoint del bilanciamento del carico. StorageGRID supporta le seguenti suite di crittografia per TLS: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 Supporto di TLS v1,2 e 1,3. SSLv3, TLS v1,1 e versioni precedenti non sono più supportati.	Consente a un client e a StorageGRID di identificarsi e autenticarsi reciprocamente e comunicare con riservatezza e integrità dei dati. Garantisce l'uso di una versione TLS recente. Le crittografie sono ora configurabili nelle impostazioni di configurazione/protezione	—

Funzione	Funzione	Impatto	Conformità normativa
Certificato server configurabile (endpoint bilanciamento del carico)	Gli amministratori di grid possono configurare gli endpoint di Load Balancer in modo da generare o utilizzare un certificato server.	Consente l'utilizzo di certificati digitali firmati dalla propria autorità di certificazione (CA) standard per autenticare le operazioni API degli oggetti tra la griglia e il client per ogni endpoint di bilanciamento del carico.	—
Certificato server configurabile (endpoint API)	Gli amministratori della griglia possono configurare centralmente tutti gli endpoint delle API StorageGRID in modo che utilizzino un certificato server firmato dalla CA attendibile dell'organizzazione.	Consente l'utilizzo di certificati digitali firmati dalla CA standard e attendibile per autenticare le operazioni API degli oggetti tra un client e la griglia.	—

Funzione	Funzione	Impatto	Conformità normativa
Multi-tenancy	StorageGRID supporta tenant multipli per grid e ogni tenant ha il proprio namespace. Un tenant offre un protocollo S3:1; per impostazione predefinita, l'accesso a bucket/container e oggetti è limitato agli utenti all'interno dell'account. I tenant possono avere un utente (ad esempio, un'implementazione aziendale, in cui ogni utente ha un proprio account) o più utenti (ad esempio, un'implementazione di un provider di servizi, in cui ogni account è un'azienda e un cliente del provider di servizi). Gli utenti possono essere locali o federati; gli utenti federati sono definiti da Active Directory o LDAP (Lightweight Directory Access Protocol). StorageGRID fornisce una dashboard per tenant, in cui gli utenti accedono utilizzando le credenziali dell'account locale o federato. Gli utenti possono accedere ai report visualizzati sull'utilizzo del tenant rispetto alla quota assegnata dall'amministratore del grid, incluse le informazioni sull'utilizzo nei dati e negli oggetti archiviati dai bucket. Gli utenti con autorizzazioni amministrative possono eseguire attività di amministrazione del sistema a livello di tenant, come la gestione di utenti, gruppi e chiavi di accesso.	Consente agli amministratori di StorageGRID di ospitare i dati da più tenant isolando al contempo l'accesso al tenant e di stabilire l'identità dell'utente federando gli utenti con un provider di identità esterno, come Active Directory o LDAP.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Mancata pubblicazione delle credenziali di accesso	Ogni operazione S3 viene identificata e registrata con un account tenant, un utente e una chiave di accesso univoci.	Consente agli amministratori Grid di stabilire quali azioni API vengono eseguite da ciascun utente.	—

Funzione	Funzione	Impatto	Conformità normativa
Accesso anonimo disattivato	Per impostazione predefinita, l'accesso anonimo è disattivato per gli account S3. Un richiedente deve disporre di una credenziale di accesso valida per un utente valido nell'account tenant per accedere a bucket, contenitori o oggetti all'interno dell'account. L'accesso anonimo a bucket o oggetti S3 può essere abilitato con un criterio IAM esplicito.	Consente agli amministratori Grid di disabilitare o controllare l'accesso anonimo a bucket/container e oggetti.	—
WORM di conformità	Progettato per soddisfare i requisiti della norma SEC 17a-4(f) e convalidato da Cohasset. I clienti possono garantire la conformità a livello della benna. La ritenzione può essere estesa ma mai ridotta. Le regole di Information Lifecycle management (ILM) applicano livelli minimi di protezione dei dati.	Consente ai tenant con requisiti di data retention normativi per consentire protezione WORM su oggetti memorizzati e metadati di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
WORM	Gli amministratori di grid possono abilitare IL WORM a livello di griglia attivando l'opzione Disattiva modifica client, che impedisce ai client di sovrascrivere o eliminare oggetti o metadati di oggetti in tutti gli account tenant. Gli amministratori dei tenant S3 possono inoltre abilitare il WORM in base al tenant, bucket o prefisso dell'oggetto specificando il criterio IAM, che include l'autorizzazione personalizzata S3: PutOverwriteObject per la sovrascrittura di oggetti e metadati.	Permette agli amministratori di Grid e agli amministratori dei tenant di controllare la protezione WORM su oggetti archiviati e metadati di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Gestione della chiave di crittografia del server host KMS	Gli amministratori di grid possono configurare uno o più server KMS (External Key Management Server) in Grid Manager in modo da fornire chiavi di crittografia ai servizi StorageGRID e alle appliance di storage. Ogni server host KMS o cluster di server host KMS utilizza il Key Management Interoperability Protocol (KMIP) per fornire una chiave di crittografia ai nodi di appliance nel sito StorageGRID associato.	Crittografia dei dati a riposo attivata. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il server host KMS.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Failover automatico	StorageGRID offre ridondanza integrata e failover automatizzato. L'accesso ad account, bucket e oggetti tenant può continuare anche in caso di guasti multipli, da dischi o nodi a interi siti. StorageGRID è consapevole delle risorse e reindirizza automaticamente le richieste ai nodi disponibili e alle posizioni dei dati. I siti StorageGRID possono persino funzionare in modalità island; se un'interruzione della WAN disconnette un sito dal resto del sistema, le letture e le scritture possono continuare con le risorse locali e la replica riprende automaticamente quando la WAN viene ripristinata.	Consente agli amministratori Grid di gestire i tempi di attività, gli SLA e altri obblighi contrattuali e di implementare i piani di business continuity.	—
Funzionalità di protezione dell'accesso ai dati specifiche per S3	Firma AWS versione 2 e versione 4	La firma delle richieste API fornisce l'autenticazione per le operazioni API S3. Amazon supporta due versioni di Signature versione 2 e 4. Il processo di firma verifica l'identità del richiedente, protegge i dati in transito e protegge da potenziali attacchi di riproduzione.	Si allinea al suggerimento AWS per la versione Signature 4 e consente la compatibilità con le versioni precedenti delle applicazioni con la versione Signature 2.

Funzione	Funzione	Impatto	Conformità normativa
—	Blocco oggetti S3	La funzionalità blocco oggetti S3 in StorageGRID è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon S3.	Consente ai tenant di creare bucket con blocco oggetti S3 abilitato per la conformità alle normative che richiedono la conservazione di determinati oggetti per un periodo di tempo fisso o indefinitamente.
Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)	Archiviazione protetta di credenziali S3	Le chiavi di accesso S3 sono memorizzate in un formato protetto da una funzione di hashing di password (SHA-2).	Consente l'archiviazione protetta delle chiavi di accesso mediante una combinazione di lunghezza della chiave (un numero generato casualmente da 10^{31}) e un algoritmo di hash delle password.
—	S3 tasti di accesso con limite di tempo	Quando si crea una chiave di accesso S3 per un utente, i clienti possono impostare una data e un'ora di scadenza sulla chiave di accesso.	Offre agli amministratori Grid la possibilità di fornire chiavi di accesso S3 temporanee.
—	Più chiavi di accesso per account utente	StorageGRID consente di creare più chiavi di accesso e contemporaneamente di attivarle per un account utente. Poiché ogni azione API viene registrata con un account utente tenant e una chiave di accesso, la non ripubblicazione viene mantenuta nonostante siano attive più chiavi.	Consente ai client di ruotare le chiavi di accesso senza interruzioni e consente a ciascun client di disporre della propria chiave, scoraggiando la condivisione delle chiavi tra i client.

Funzione	Funzione	Impatto	Conformità normativa
—	S3 criterio di accesso IAM	StorageGRID supporta policy IAM S3, consentendo agli amministratori Grid di specificare un controllo granulare degli accessi per tenant, bucket o prefisso oggetto. StorageGRID supporta inoltre le variabili e le condizioni dei criteri IAM, consentendo criteri di controllo degli accessi più dinamici.	Consente agli amministratori di Grid di specificare il controllo dell'accesso per gruppi di utenti per l'intero tenant; inoltre, permette agli utenti tenant di specificare il controllo dell'accesso per i propri bucket e oggetti.
—	Crittografia lato server con chiavi gestite da StorageGRID (SSE)	StorageGRID supporta SSE, consentendo una protezione multitenant dei dati a riposo con chiavi di crittografia gestite da StorageGRID.	Consente ai tenant di crittografare gli oggetti. La chiave di crittografia è necessaria per scrivere e recuperare questi oggetti.
Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)	Crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)	StorageGRID supporta SSE-C, abilitando la protezione multitenant dei dati a riposo con chiavi di crittografia gestite dal client. Sebbene StorageGRID gestisca tutte le operazioni di crittografia e decrittografia degli oggetti, con SSE-C, il client deve gestire autonomamente le chiavi di crittografia.	Consente ai client di crittografare gli oggetti con le chiavi controllate dall'utente. La chiave di crittografia è necessaria per scrivere e recuperare questi oggetti.

Sicurezza di oggetti e metadati

Esplora le funzionalità di sicurezza degli oggetti e dei metadati in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Crittografia degli oggetti lato server AES (Advanced Encryption Standard)	StorageGRID fornisce la crittografia degli oggetti sul lato server basata su AES 128 e AES 256. Gli amministratori della griglia possono abilitare la crittografia come impostazione predefinita globale. StorageGRID supporta inoltre l'intestazione di crittografia S3 x-amz-lato server per consentire l'attivazione o la disattivazione della crittografia in base all'oggetto. Se abilitato, gli oggetti vengono crittografati quando vengono archiviati o in transito tra i nodi della griglia.	Aiuta a proteggere lo storage e la trasmissione degli oggetti, indipendentemente dall'hardware per lo storage sottostante.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Gestione delle chiavi integrata	Quando la crittografia è attivata, ogni oggetto viene crittografato con una chiave simmetrica univoca generata in modo casuale, memorizzata all'interno di StorageGRID senza accesso esterno.	Consente la crittografia degli oggetti senza richiedere una gestione esterna delle chiavi.	
Dischi di crittografia conformi a Federal Information Processing Standard (FIPS) 140-2-2	Le appliance SG5812, SG5860, SG6160 e SGF6024 StorageGRID offrono l'opzione di dischi di crittografia conformi FIPS 140-2-2. Le chiavi di crittografia dei dischi possono essere facoltativamente gestite da un server KMIP esterno.	Abilita lo storage sicuro di dati, metadati e oggetti di sistema. Fornisce inoltre una crittografia degli oggetti basata su software StorageGRID, che protegge storage e trasmissione di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Scansione di integrità in background e autoriparazione	StorageGRID utilizza un meccanismo di interblocco costituito da hash, checksum e controlli di ridondanza ciclici (CRC) a livello di oggetto e sottooggetto per proteggere da incoerenza, manomissioni o modifiche dei dati, sia quando gli oggetti sono in storage che in transito. StorageGRID rileva automaticamente gli oggetti corrotti e manomessi e li sostituisce, mettendo in quarantena i dati modificati e avvisando l'amministratore.	Permette agli amministratori di grid di soddisfare SLA, normative e altri obblighi in termini di conservazione dei dati. Aiuta i clienti a rilevare ransomware o virus che tentano di crittografare, manomettere o modificare i dati.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Conservazione e posizionamento degli oggetti basati su policy	StorageGRID consente agli amministratori di grid di configurare regole ILM che specificano conservazione, posizionamento, protezione, transizione e scadenza degli oggetti. Gli amministratori del grid possono configurare StorageGRID per filtrare gli oggetti in base ai propri metadati e applicare regole a vari livelli di granularità, tra cui Grid-wide, tenant, bucket, key prefix, coppie di valori chiave e metadati definiti dall'utente. StorageGRID contribuisce a garantire che gli oggetti vengano memorizzati in base alle regole ILM durante il loro ciclo di vita, a meno che non vengano esplicitamente eliminati dal client.	Aiuta ad applicare il posizionamento, la protezione e la conservazione dei dati. Aiuta i clienti a raggiungere gli SLA relativi a durata, disponibilità e performance.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Scansione dei metadati in background	StorageGRID esegue periodicamente la scansione dei metadati degli oggetti in background per applicare modifiche al posizionamento o alla protezione dei dati degli oggetti come specificato da ILM.	Aiuta a rilevare gli oggetti danneggiati.	
Uniformità regolabile	I tenant possono selezionare livelli di coerenza a livello del bucket per garantire che siano disponibili risorse come la connettività multisito.	Offre l'opzione per eseguire il commit delle scritture sulla griglia solo quando è disponibile un numero richiesto di siti o risorse.	

Funzioni di protezione di amministrazione

Scoprite le funzioni di protezione dell'amministrazione in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Certificato server (Grid Management Interface)	Gli amministratori di rete possono configurare Grid Management Interface in modo che utilizzi un certificato server firmato dalla CA attendibile dell'organizzazione.	Consente l'utilizzo di certificati digitali firmati dalla CA standard e attendibile per autenticare l'accesso all'interfaccia utente di gestione e all'API tra un client di gestione e la griglia.	—
Autenticazione utente amministrativo	Gli utenti amministrativi vengono autenticati utilizzando il nome utente e la password. Gli utenti e i gruppi amministrativi possono essere locali o federati, importati da Active Directory o LDAP del cliente. Le password degli account locali sono memorizzate in un formato protetto da bcrypt; le password della riga di comando sono memorizzate in un formato protetto da SHA-2.	Autentica l'accesso amministrativo alla UI di gestione e alle API.	—
Supporto SAML	StorageGRID supporta il single sign-on (SSO) utilizzando lo standard SAML 2,0 (Security Assertion Markup Language 2,0). Quando SSO è attivato, tutti gli utenti devono essere autenticati da un provider di identità esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.	Offre livelli aggiuntivi di sicurezza per gli amministratori di tenant e grid come SSO e Multifactor Authentication (MFA).	NIST SP800-63
Controllo granulare delle autorizzazioni	Gli amministratori Grid possono assegnare autorizzazioni ai ruoli e assegnare ruoli a gruppi di utenti amministrativi, in base alle attività a cui i client amministrativi possono eseguire utilizzando sia l'interfaccia utente di gestione che le API.	Consente agli amministratori Grid di gestire il controllo degli accessi per gli utenti e i gruppi amministrativi.	—

Funzione	Funzione	Impatto	Conformità normativa
Registrazione di controllo distribuita	StorageGRID fornisce un'infrastruttura integrata di registrazione degli audit distribuita, scalabile fino a centinaia di nodi in un massimo di 16 siti. I nodi software StorageGRID generano messaggi di audit, che vengono trasmessi attraverso un sistema di inoltro di audit ridondante e infine acquisiti in uno o più repository di audit log. I messaggi di audit acquisiscono eventi a livello di granularità degli oggetti, come operazioni API S3 avviate dal client, eventi del ciclo di vita degli oggetti da ILM, controlli dello stato di salute degli oggetti in background e modifiche della configurazione effettuate dall'interfaccia utente di gestione o dalle API. È possibile esportare gli audit log dai nodi amministrativi tramite CIFS o NFS, consentendo il mining dei messaggi di audit da parte di tool come Splunk ed ELK. Esistono quattro tipi di messaggi di controllo: • Messaggi di audit del sistema • Messaggi di audit dello storage a oggetti • Messaggi di controllo del protocollo HTTP • Gestione dei messaggi di controllo	Fornisce agli amministratori Grid un servizio di controllo collaudato e scalabile e consente loro di estrarre i dati di controllo per vari obiettivi. Tali obiettivi includono la risoluzione dei problemi, il controllo delle prestazioni dello SLA, le operazioni API di accesso ai dati dei client e le modifiche alla configurazione di gestione.	—

Funzione	Funzione	Impatto	Conformità normativa
Audit del sistema	I messaggi di controllo del sistema acquisiscono gli eventi correlati al sistema, come gli stati dei nodi della griglia, il rilevamento degli oggetti corrotti, gli oggetti sottoposti a commit in tutte le posizioni specificate per la regola ILM e l'avanzamento delle attività di manutenzione a livello di sistema (attività griglia).	Aiuta i clienti a risolvere i problemi del sistema e fornisce la prova che gli oggetti vengono memorizzati in base al loro SLA. Gli SLA sono implementati dalle regole ILM di StorageGRID e protetti dall'integrità.	—
Verifica dello storage a oggetti	I messaggi di audit dello storage a oggetti acquisiscono la transazione di API a oggetti e gli eventi relativi al ciclo di vita. Questi eventi includono storage e recupero di oggetti, trasferimenti da grid-node a grid-node e verifiche.	Aiuta i clienti a controllare lo stato di avanzamento dei dati nel sistema e se gli SLA, specificati come StorageGRID ILM, vengono erogati.	—
Controllo del protocollo HTTP	I messaggi di controllo del protocollo HTTP acquisiscono le interazioni del protocollo HTTP correlate alle applicazioni client e ai nodi StorageGRID. Inoltre, i clienti possono acquisire intestazioni specifiche delle richieste HTTP (ad esempio, X-Forwarding-for e metadati utente [x-amz-meta-*]) nella verifica.	Aiuta i clienti a controllare le operazioni API di accesso ai dati tra client e StorageGRID e a tracciare un'azione per un account utente e una chiave di accesso individuali. I clienti possono anche registrare i metadati degli utenti nelle verifiche e utilizzare strumenti di log mining come Splunk o ELK, per cercare i metadati degli oggetti.	—
Audit di gestione	I messaggi di controllo di gestione registrano le richieste degli utenti amministrativi all'interfaccia utente di gestione (Grid Management Interface) o alle API. Ogni richiesta che non è UNA richiesta GET o HEAD all'API registra una risposta con il nome utente, l'IP e il tipo di richiesta all'API.	Aiuta gli amministratori Grid a stabilire un record delle modifiche alla configurazione del sistema apportate dall'utente da quale IP di origine e quale IP di destinazione in quale momento.	—

Funzione	Funzione	Impatto	Conformità normativa
Supporto TLS 1,3 per l'interfaccia utente di gestione e l'accesso API	TLS stabilisce un protocollo handshake per la comunicazione tra un client admin e un nodo admin StorageGRID.	Consente a un client amministrativo e a StorageGRID di identificarsi e autenticarsi reciprocamente e comunicare con riservatezza e integrità dei dati.	—
SNMPv3 per il monitoraggio StorageGRID	SNMPv3 garantisce la sicurezza offrendo autenticazione avanzata e crittografia dei dati per la privacy. Con v3, le unità dei dati del protocollo vengono crittografate utilizzando CBC-DES per il protocollo di crittografia. L'autenticazione dell'utente di chi ha inviato l'unità dati del protocollo è fornita dal protocollo di autenticazione HMAC-SHA o HMAC-MD5. SNMPv2 e v1 sono ancora supportati.	Aiuta gli amministratori di rete a monitorare il sistema StorageGRID abilitando un agente SNMP sul nodo Admin.	—
Certificati client per l'esportazione delle metriche Prometheus	Gli amministratori di rete possono caricare o generare certificati client che possono essere utilizzati per fornire un accesso sicuro e autenticato al database StorageGRID Prometheus.	Gli amministratori di rete possono utilizzare i certificati client per monitorare StorageGRID esternamente utilizzando applicazioni come Grafana.	—

Funzioni di sicurezza della piattaforma

Informazioni sulle funzionalità di sicurezza della piattaforma in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Infrastruttura a chiave pubblica (PKI) interna, certificati dei nodi e TLS	StorageGRID utilizza un'infrastruttura PKI interna e certificati di nodo per autenticare e crittografare la comunicazione internodale. La comunicazione internodale è protetta da TLS.	Contribuisce a proteggere il traffico del sistema su LAN o WAN, soprattutto in un'implementazione multisito.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Firewall nodo	StorageGRID configura automaticamente le tabelle IP e le regole di firewall per controllare il traffico di rete in entrata e in uscita, oltre a chiudere le porte non utilizzate.	Consente di proteggere il sistema StorageGRID, i dati e i metadati dal traffico di rete non richiesto.	—
Protezione avanzata dei sistemi operativi	Il sistema operativo di base delle appliance fisiche e dei nodi virtuali StorageGRID è rafforzato; vengono rimossi i pacchetti software non correlati.	Contribuisce a ridurre al minimo le potenziali superfici di attacco.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Aggiornamenti periodici della piattaforma e del software	StorageGRID fornisce versioni software regolari che includono il sistema operativo, i file binari delle applicazioni e gli aggiornamenti software.	Aiuta a mantenere il sistema StorageGRID aggiornato con i software e i file binari delle applicazioni correnti.	—
Accesso root disabilitato su Secure Shell (SSH)	Il login root su SSH è disabilitato su tutti i nodi StorageGRID. L'accesso SSH utilizza l'autenticazione del certificato.	Aiuta i clienti a proteggersi da potenziali violazioni remote delle password del login root.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Sincronizzazione automatica dell'ora	StorageGRID sincronizza automaticamente gli orologi di sistema di ciascun nodo con più server NTP (Time Network Protocol) esterni. Sono necessari almeno quattro server NTP di strato 3 o successivo.	Garantisce lo stesso riferimento temporale in tutti i nodi.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Separare le reti per il traffico grid interno, amministrativo e client	I nodi software e le appliance hardware StorageGRID supportano più interfacce di rete virtuali e fisiche, in modo che i clienti possano separare il traffico di client, amministrazione e rete interna su reti diverse.	Consenti agli amministratori Grid di separare il traffico di rete interno ed esterno e di distribuire il traffico sulle reti con SLA diversi.	—
Interfacce VLAN (Virtual LAN) multiple	StorageGRID supporta la configurazione delle interfacce VLAN sul client StorageGRID e sulle reti grid.	Consenti agli amministratori Grid di partizionare e isolare il traffico delle applicazioni per garantire sicurezza, flessibilità e prestazioni.	

Funzione	Funzione	Impatto	Conformità normativa
Rete client non attendibile	L'interfaccia di rete client non attendibile accetta connessioni in entrata solo su porte che sono state esplicitamente configurate come endpoint di bilanciamento del carico.	Garantisce la protezione delle interfacce esposte a reti non attendibili.	—
Firewall configurabile	Gestire le porte aperte e chiuse per le reti Admin, Grid e client.	Consentire agli amministratori di rete di controllare l'accesso alle porte e di gestire l'accesso alle porte dei dispositivi approvati.	
Comportamento SSH avanzato	Nuovi certificati host SSH e chiavi host vengono generati quando si aggiorna un nodo a StorageGRID 11,5.	Migliora la protezione da attacchi "uomo in mezzo".	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Crittografia dei nodi	Come parte della nuova funzione di crittografia del server host KMS, viene aggiunta una nuova impostazione di crittografia dei nodi al programma di installazione dell'appliance StorageGRID.	Questa impostazione deve essere attivata durante la fase di configurazione hardware dell'installazione dell'appliance.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Integrazione del cloud

Scopri come StorageGRID si integra con i servizi cloud.

Funzione	Funzione	Impatto
Scansione antivirus basata su notifiche	I servizi della piattaforma StorageGRID supportano le notifiche degli eventi. Le notifiche degli eventi possono essere utilizzate con servizi di cloud computing esterni per attivare i flussi di lavoro di scansione antivirus sui dati.	Consente agli amministratori dei tenant di attivare la scansione dei dati tramite virus utilizzando servizi di cloud computing esterni.

TR-4921: Difesa dal ransomware

Proteggere gli oggetti StorageGRID S3 dal ransomware

Scopri di più sugli attacchi ransomware e su come proteggere i dati grazie alle Best practice di sicurezza di StorageGRID.

Gli attacchi ransomware sono in aumento. Questo documento fornisce alcuni consigli su come proteggere i dati degli oggetti su StorageGRID.

Il ransomware di oggi è il pericolo sempre presente nel data center. Il ransomware è progettato per crittografare i dati e renderli inutilizzabili dagli utenti e dalle applicazioni che li fanno affidamento. La protezione inizia con le solite difese di reti rafforzate e solide pratiche di sicurezza per gli utenti, e dobbiamo seguire le procedure di sicurezza per l'accesso ai dati.

Il ransomware è una delle maggiori minacce alla sicurezza odierne. Il team NetApp StorageGRID collabora con i nostri clienti per stare al passo con queste minacce. Con l'uso del blocco degli oggetti e del controllo delle versioni, è possibile proteggere da modifiche indesiderate e ripristinare da attacchi dannosi. La sicurezza dei dati è un'impresa multi-layer che considera lo storage a oggetti solo una parte del data center.

Best practice di StorageGRID

Per StorageGRID, le Best practice sulla sicurezza devono includere l'utilizzo di HTTPS con certificati firmati sia per la gestione che per l'accesso agli oggetti. Crea account utente dedicati per applicazioni e singoli utenti e non utilizza gli account root tenant per l'accesso alle applicazioni o ai dati utente. In altre parole, seguire il principio del privilegio minimo. Utilizzare i gruppi di protezione con criteri IAM (Identity and Access Management) definiti per gestire i diritti degli utenti e accedere agli account specifici per le applicazioni e gli utenti. Con queste misure in atto, devi comunque assicurarti che i tuoi dati siano protetti. Nel caso di Simple Storage Service (S3), quando gli oggetti vengono modificati per crittografarli, viene eseguita la sovrascrittura dell'oggetto originale.

Metodi di difesa

Il meccanismo di protezione dal ransomware primario nell'API S3 consiste nell'implementare il blocco degli oggetti. Non tutte le applicazioni sono compatibili con il blocco degli oggetti, pertanto sono disponibili altre due opzioni per proteggere gli oggetti descritti in questo report: La replica in un altro bucket con la versione abilitata e la versione con i criteri IAM.

Dove trovare ulteriori informazioni

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

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Difesa dal ransomware tramite il blocco degli oggetti

Scopri come il blocco degli oggetti in StorageGRID fornisce un modello WORM per impedire la cancellazione o la sovrascrittura dei dati e come soddisfa i requisiti normativi.

Il blocco degli oggetti fornisce un modello WORM per impedire che gli oggetti vengano eliminati o sovrascritti. L'implementazione di StorageGRID del blocco degli oggetti è "Valutazione Cohasset" per aiutare a soddisfare i requisiti normativi, supportando la conservazione a fini giudiziari, la modalità di conformità e la modalità di governance per la conservazione degli oggetti e le policy di conservazione predefinite dei bucket. È necessario abilitare il blocco degli oggetti come parte della creazione e del controllo delle versioni del bucket. Una versione specifica di un oggetto è bloccata e, se non viene definito alcun ID di versione, la conservazione viene posizionata sulla versione corrente dell'oggetto. Se la versione corrente ha la conservazione configurata e si tenta di eliminare, modificare o sovrascrivere l'oggetto, viene creata una nuova versione con un marcatore

di eliminazione o la nuova revisione dell'oggetto come versione corrente, e la versione bloccata viene mantenuta come una versione non corrente. Per le applicazioni non ancora compatibili, è comunque possibile utilizzare la configurazione di blocco degli oggetti e di conservazione predefinita inserita nel bucket. Una volta definita la configurazione, viene applicata una conservazione degli oggetti a ogni nuovo oggetto inserito nel bucket. Questa operazione funziona finché l'applicazione è configurata per non eliminare o sovrascrivere gli oggetti prima che sia trascorso il tempo di conservazione.

Di seguito sono riportati alcuni esempi di utilizzo dell'API di blocco degli oggetti:

Blocco oggetto conservazione legale è un semplice stato on/off applicato a un oggetto.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

L'impostazione dello stato di conservazione a fini giudiziari non restituisce alcun valore se l'operazione è riuscita, pertanto può essere verificata con un'operazione GET.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

Per disattivare la sospensione legale, applicare lo stato OFF.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

L'impostazione della conservazione dell'oggetto viene eseguita con un Retain until timestamp.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

Anche in questo caso, non viene restituito alcun valore in caso di esito positivo, pertanto è possibile verificare lo stato di conservazione in modo simile con una chiamata Get.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

L'inserimento di una conservazione predefinita in un bucket abilitato per il blocco degli oggetti utilizza un periodo di conservazione in giorni e anni.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

Come per la maggior parte di queste operazioni, non viene restituita alcuna risposta in caso di esito positivo, quindi è possibile eseguire un'operazione di RECUPERO per la verifica della configurazione.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

Successivamente, è possibile inserire un oggetto nel bucket con la configurazione di conservazione applicata.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

L'operazione PUT restituisce una risposta.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

Nell'oggetto Retention, la durata di conservazione impostata nel bucket nell'esempio precedente viene

convertita in un timestamp di conservazione sull'oggetto.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

Difesa da ransomware tramite bucket replicati con versione

Scopri come replicare gli oggetti in un bucket secondario utilizzando StorageGRID CloudMirror.

Non tutte le applicazioni e i carichi di lavoro saranno compatibili con il blocco degli oggetti. Un'altra opzione è replicare gli oggetti in un bucket secondario nella stessa griglia (preferibilmente un tenant diverso con accesso limitato) o in qualsiasi altro endpoint S3 con il servizio della piattaforma StorageGRID, CloudMirror.

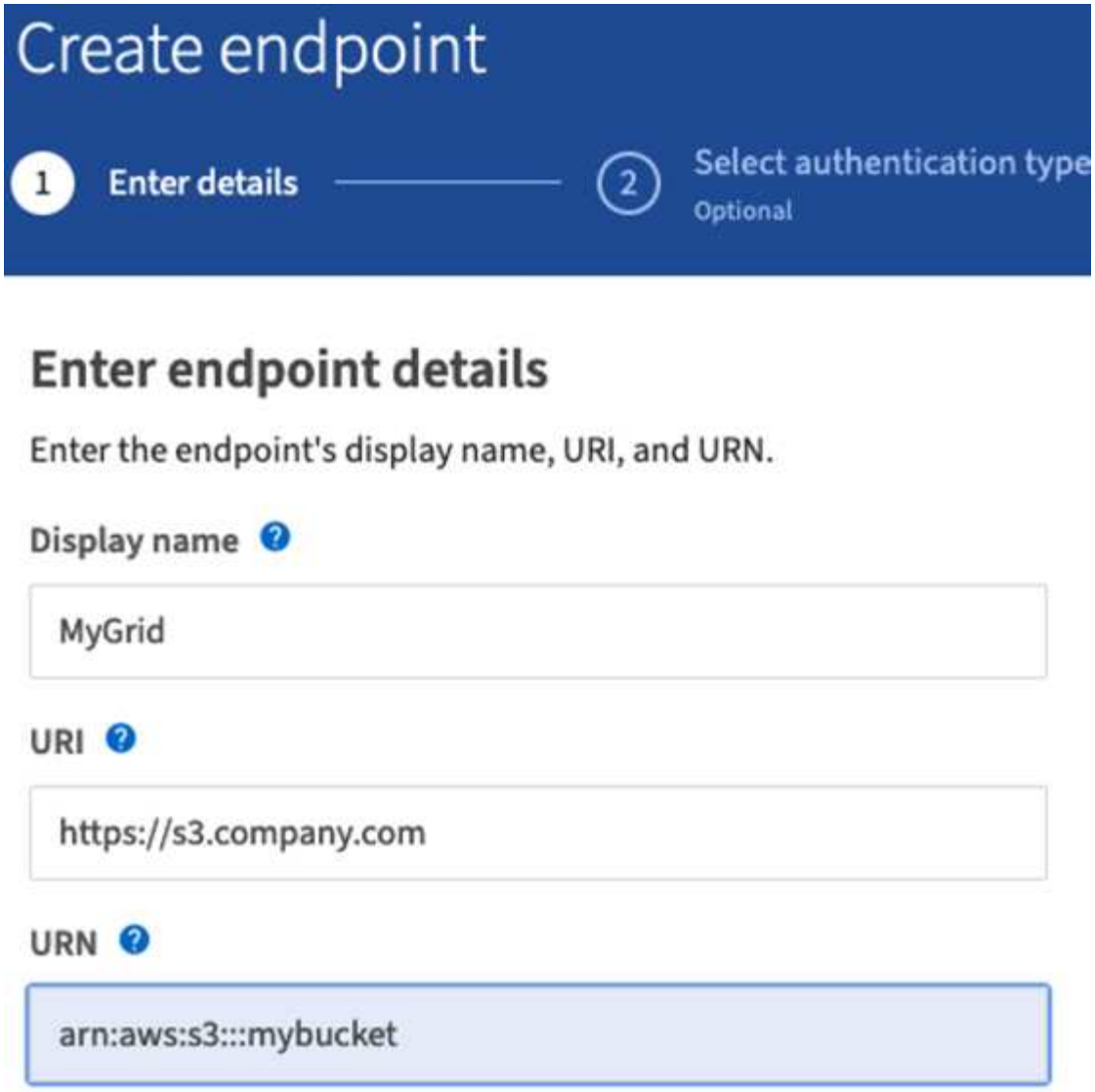
StorageGRID CloudMirror è un componente di StorageGRID che può essere configurato per replicare gli oggetti di un bucket in una destinazione definita quando vengono acquisiti nel bucket di origine e non replicano le eliminazioni. Poiché CloudMirror è un componente integrato di StorageGRID, non può essere disattivato o manipolato da un attacco basato su API S3. È possibile configurare questo bucket replicato con la versione abilitata. In questo scenario, è necessario eseguire una pulizia automatica delle vecchie versioni del bucket replicato, che possono essere eliminate in modo sicuro. A tale scopo, è possibile utilizzare il motore dei criteri ILM di StorageGRID. Creare regole per gestire il posizionamento degli oggetti in base al tempo non corrente per diversi giorni sufficienti ad identificarli e recuperarli da un attacco.

Un aspetto negativo di questo approccio è il fatto che consuma più storage disponendo di una seconda copia completa del bucket e di più versioni degli oggetti conservati per un po' di tempo. Inoltre, gli oggetti intenzionalmente eliminati dal bucket primario devono essere rimossi manualmente dal bucket replicato. Esistono altre opzioni di replica esterne al prodotto, come NetApp CloudSync, che possono replicare le eliminazioni per una soluzione simile. Un altro aspetto negativo per il bucket secondario che è abilitato per il controllo delle versioni e non per il blocco degli oggetti è la presenza di una serie di account privilegiati che potrebbero essere utilizzati per causare danni alla posizione secondaria. Il vantaggio è che dovrebbe essere un account univoco per quel bucket di endpoint o tenant e la compromissione probabilmente non include l'accesso agli account nella sede principale o viceversa.

Una volta creati i bucket di origine e destinazione e configurata la destinazione con la versione, è possibile configurare e abilitare la replica, come segue:

Fasi

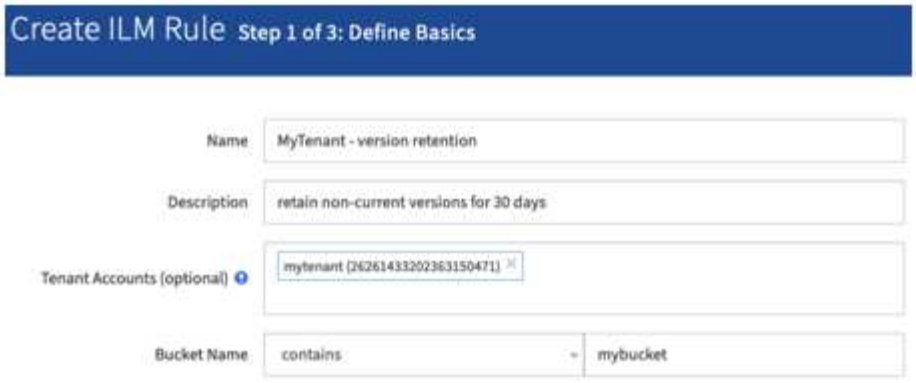
1. Per configurare CloudMirror, creare un endpoint dei servizi di piattaforma per la destinazione S3.

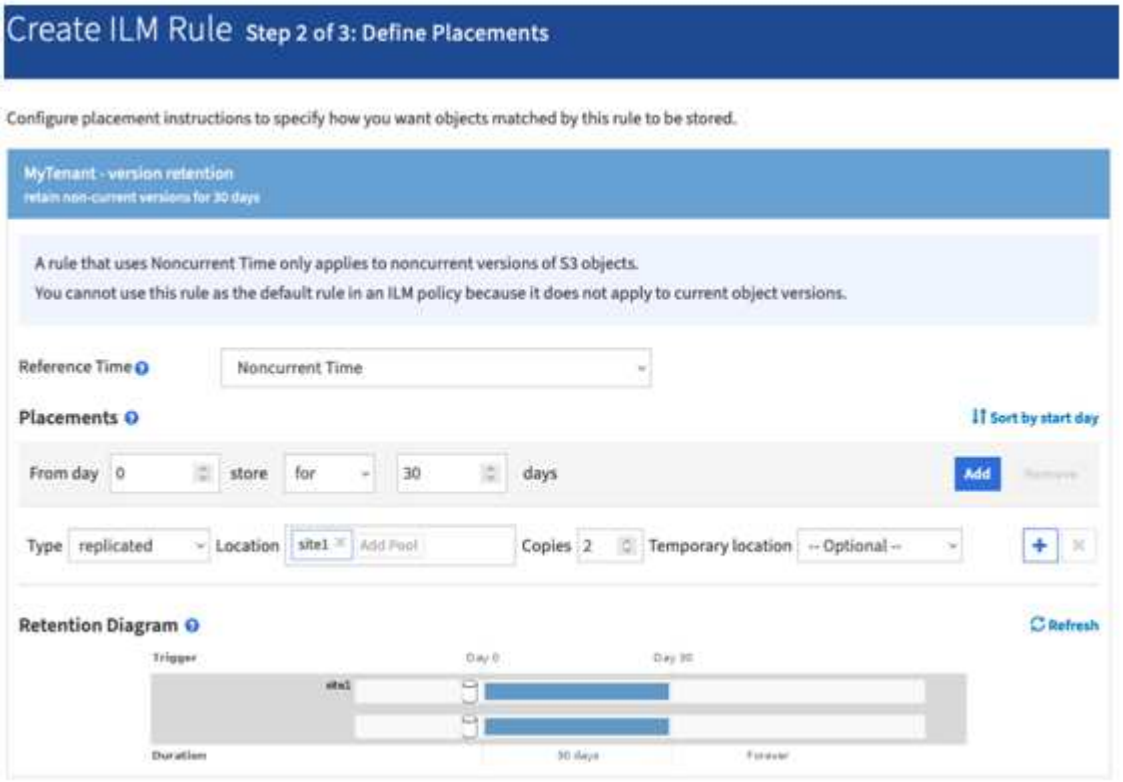


2. Nel bucket di origine, configurare la replica per utilizzare l'endpoint configurato.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. Creare regole ILM per gestire il posizionamento dello storage e la gestione della durata dello storage della versione. In questo esempio, vengono configurate le versioni non correnti degli oggetti da memorizzare.





Ci sono due copie nel sito 1 per 30 giorni. È inoltre possibile configurare le regole per la versione corrente degli oggetti in base all'utilizzo del tempo di acquisizione come tempo di riferimento nella regola ILM in modo che corrispondano alla durata di archiviazione del bucket di origine. Il posizionamento dello storage per le versioni a oggetti può essere sottoposto a erasure coding o replicato.

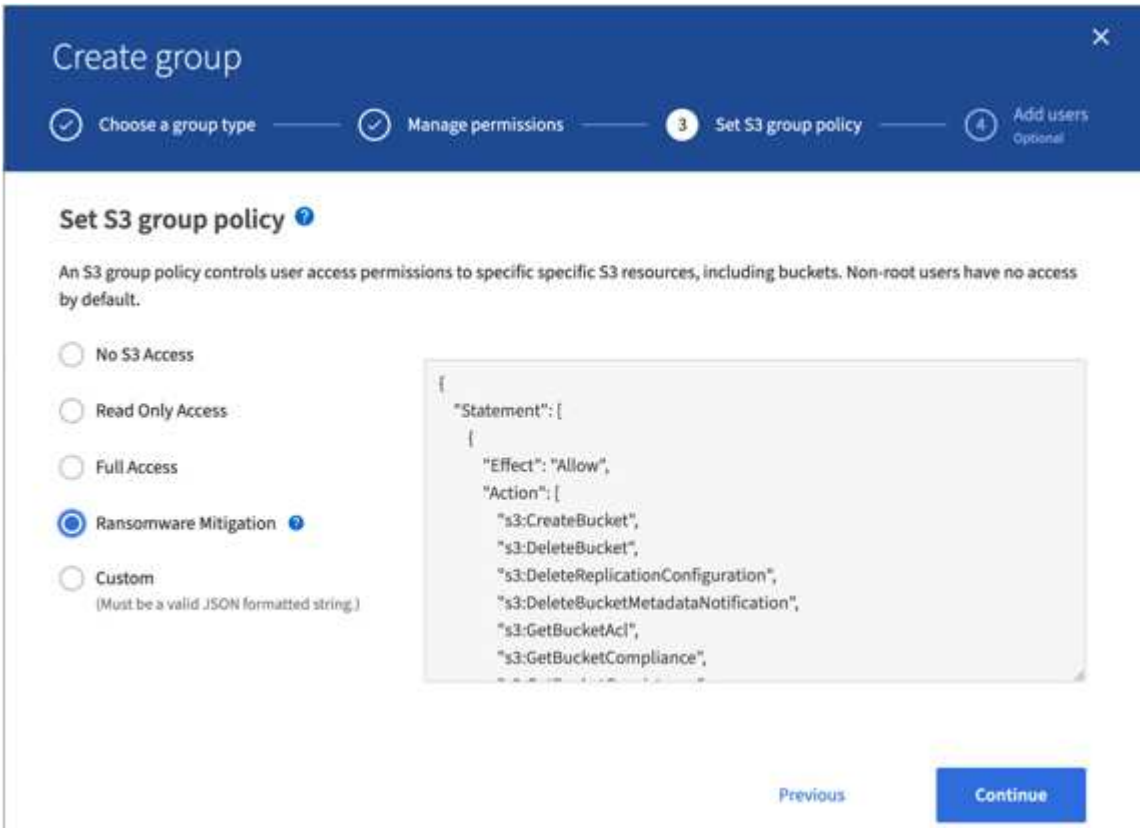
Difesa dal ransomware tramite versione con policy IAM di protezione

Scopri come proteggere i tuoi dati abilitando il controllo delle versioni nel bucket e implementando criteri IAM nei gruppi di sicurezza degli utenti in StorageGRID.

Un metodo per proteggere i dati senza utilizzare il blocco degli oggetti o la replica consiste nell'abilitare la versione nel bucket e implementare le policy IAM sui gruppi di sicurezza degli utenti per limitare la capacità degli utenti di gestire versioni degli oggetti. In caso di attacco, vengono create nuove versioni errate dei dati come la versione corrente e la versione non corrente più recente è quella sicura. Gli account compromessi per ottenere l'accesso ai dati non hanno accesso per eliminare o modificare in altro modo la versione non corrente

proteggendoli per operazioni di ripristino successive. Proprio come lo scenario precedente, le regole ILM gestiscono la conservazione delle versioni non correnti con una durata a scelta. L'aspetto negativo è che esiste ancora la possibilità di disporre di account privilegiati per un attacco di un attore non valido, ma tutti gli account del servizio applicazioni e gli utenti devono essere configurati con un accesso più restrittivo. I criteri di gruppo restrittivi devono consentire esplicitamente a ogni azione di cui si desidera che gli utenti o l'applicazione siano in grado di eseguire e negare esplicitamente le azioni di cui non si desidera che siano in grado di eseguire tali azioni. NetApp sconsiglia l'utilizzo di un'opzione con caratteri jolly, poiché in futuro potrebbe essere introdotta una nuova azione e si desidera controllare se è consentita o negata. Per questa soluzione, l'elenco di negazione deve includere DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration e PutBucketVersioning per proteggere la configurazione delle versioni del bucket e delle versioni dell'oggetto da modifiche dell'utente o del programma.

In StorageGRID 11,7 è stata introdotta una nuova opzione di policy di gruppo S3 "mitigazione del ransomware" per rendere più semplice l'implementazione di questa soluzione. Quando si crea un gruppo di utenti nel tenant, dopo aver selezionato le autorizzazioni del gruppo, è possibile visualizzare questo nuovo criterio opzionale.



Di seguito viene riportato il contenuto dei criteri di gruppo che includono la maggior parte delle operazioni disponibili esplicitamente consentite e il minimo richiesto negato.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
```

```
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
```

```
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

TR-4765: StorageGRID monitor

Introduzione al monitoraggio StorageGRID

Scopri come monitorare il tuo sistema StorageGRID utilizzando applicazioni esterne, come Splunk.

Un efficace monitoraggio dello storage basato su oggetti NetApp StorageGRID permette agli amministratori di rispondere rapidamente ai problemi urgenti e di aggiungere risorse in modo proattivo per gestire carichi di lavoro in crescita. Questo report fornisce una guida generale su come monitorare le metriche chiave e come sfruttare le applicazioni di monitoraggio esterne. Lo scopo è di integrare la guida al monitoraggio e alla risoluzione dei problemi esistente.

Un'implementazione NetApp StorageGRID è costituita generalmente da diversi siti e nodi che operano per creare un sistema di storage a oggetti distribuito e tollerante agli errori. In un sistema storage distribuito e resiliente come StorageGRID, è normale che sussistano condizioni di errore mentre il grid continua a funzionare normalmente. La sfida per l'amministratore è capire la soglia alla quale le condizioni di errore (come i nodi inattivi) presentano un problema che deve essere immediatamente affrontato rispetto alle informazioni che devono essere analizzate. Analizzando i dati presenti in StorageGRID, potrai comprendere il tuo carico di lavoro e prendere decisioni informate, come ad esempio quando aggiungere altre risorse.

StorageGRID fornisce un'eccellente documentazione che approfondisce l'argomento del monitoraggio. Questo report presuppone che l'utente abbia acquisito dimestichezza con StorageGRID e che abbia esaminato la relativa documentazione. Invece di ripetere queste informazioni, in questa guida si fa riferimento alla documentazione del prodotto. La documentazione dei prodotti StorageGRID è disponibile online e in formato

PDF.

L'obiettivo di questo documento è integrare la documentazione di prodotto e discutere delle modalità di monitoraggio del sistema StorageGRID utilizzando applicazioni esterne come Splunk.

Origini dei dati

Per monitorare con successo NetApp StorageGRID, è importante sapere dove raccogliere dati sullo stato e sul funzionamento del sistema StorageGRID.

- **Interfaccia utente Web e dashboard.** Il gestore di griglie StorageGRID presenta una vista di livello superiore delle informazioni che l'amministratore deve visualizzare in una presentazione logica. Gli amministratori possono inoltre approfondire le informazioni sul livello di servizio per la risoluzione dei problemi e la raccolta di log.
- **Registri di controllo.** StorageGRID mantiene registri di audit granulari delle azioni dei tenant come PUT, GET ed DELETE. È anche possibile tracciare il ciclo di vita di un oggetto, dall'acquisizione all'applicazione di regole di gestione dei dati.
- **API metriche.** Alla base dell'interfaccia GMI di StorageGRID vi sono API aperte, in quanto l'interfaccia utente è basata su API. Questo approccio consente di estrarre i dati utilizzando strumenti esterni di analisi e monitoring.

Dove trovare ulteriori informazioni

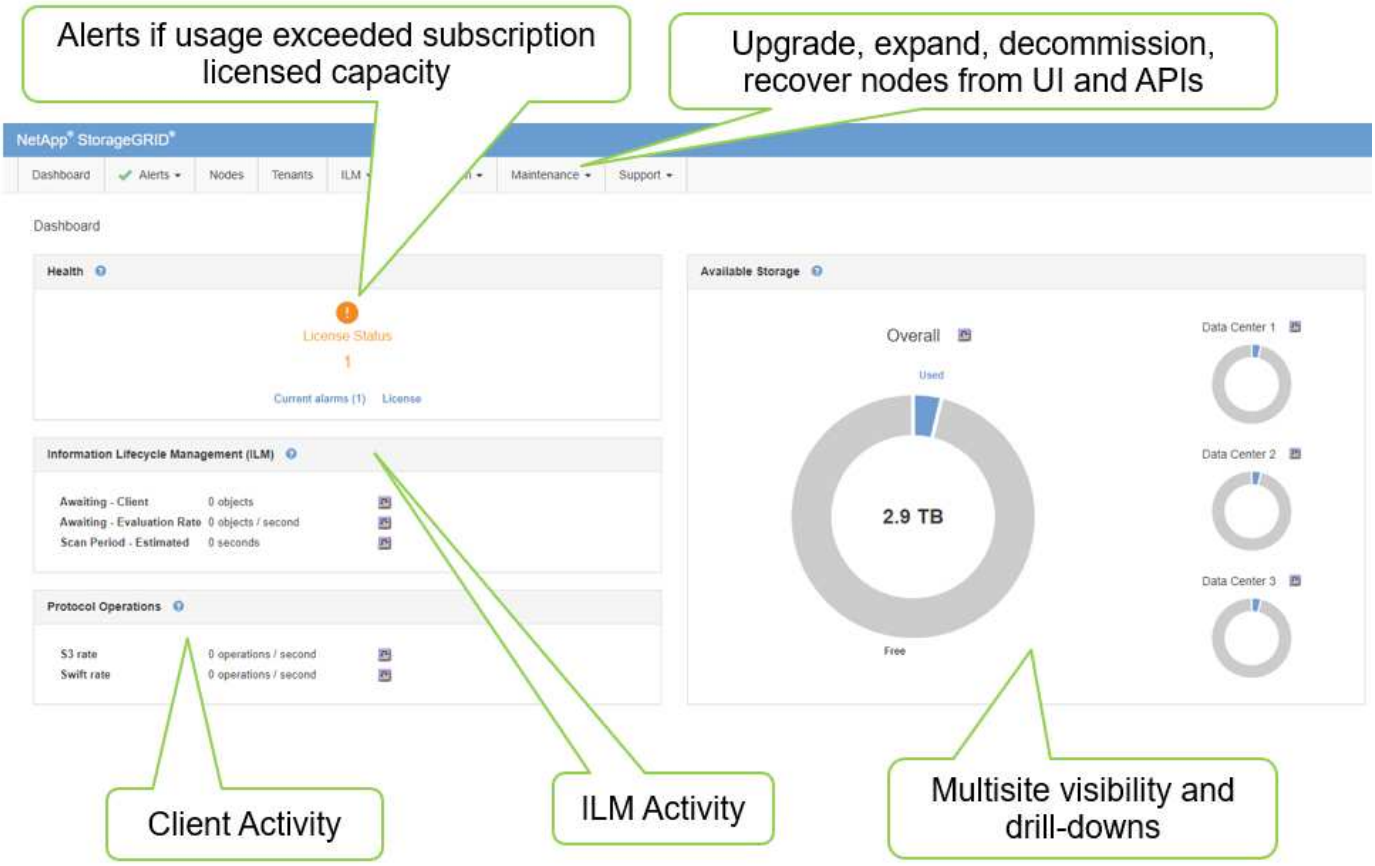
Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/
- App NetApp StorageGRID per Splunk https://splunkbase.splunk.com/app/3898/#/details

Utilizzare il dashboard GMI per monitorare StorageGRID

La dashboard dell'interfaccia GMI (Grid Management Interface) di StorageGRID fornisce una vista centralizzata dell'infrastruttura StorageGRID, consentendo di controllare lo stato, le prestazioni e la capacità dell'intero grid.

Utilizzare il dashboard GMI per esaminare ciascun componente principale della griglia.



Informazioni che è necessario monitorare regolarmente

In una versione precedente di questo report tecnico sono elencate le metriche da controllare periodicamente rispetto alle tendenze. Tali informazioni sono ora incluse nella "Guida al monitoraggio e alla risoluzione di problemi".

Monitoraggio dei costi

Una versione precedente di questo report tecnico elenca le aree in cui monitorare metriche importanti, come Object Storage Space, Metadata Space, Network Resources e così via. Tali informazioni sono ora incluse nella "Guida al monitoraggio e alla risoluzione di problemi".

Utilizzare gli avvisi per monitorare StorageGRID

Informazioni su come utilizzare il sistema di avvisi in StorageGRID per monitorare i problemi, gestire avvisi personalizzati ed estendere le notifiche di avviso tramite SNMP o e-mail.

Gli avvisi forniscono informazioni critiche che consentono di monitorare i vari eventi e condizioni all'interno del sistema StorageGRID.

Il sistema di avvisi è progettato per essere lo strumento principale per il monitoraggio di eventuali problemi che potrebbero verificarsi nel sistema StorageGRID. Il sistema di avvisi è incentrato su problemi pratici nel sistema e offre un'interfaccia semplice da utilizzare.

Forniamo una varietà di regole di avviso predefinite che mirano a monitorare e risolvere i problemi del sistema. È possibile gestire ulteriormente gli avvisi creando avvisi personalizzati, modificando o disabilitando gli avvisi

predefiniti e tacitando le notifiche degli avvisi.

È possibile estendere gli avvisi anche tramite notifiche SNMP o e-mail.

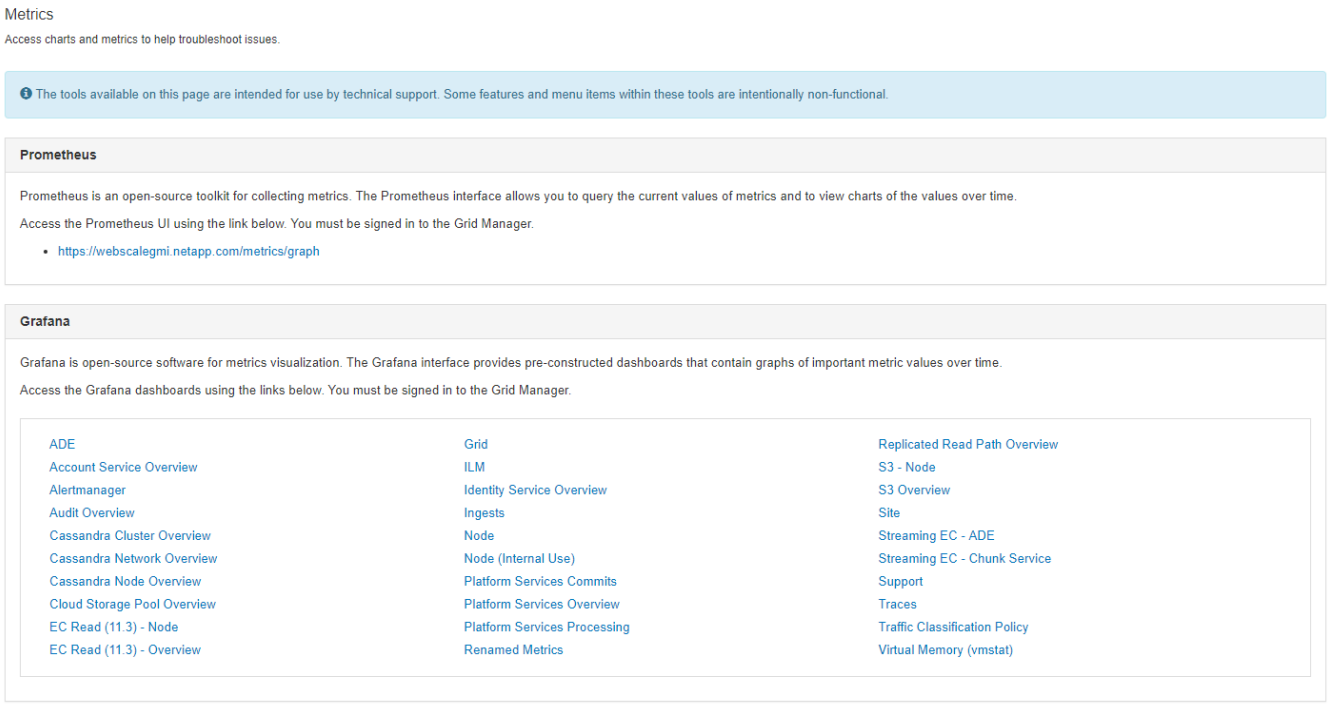
Per ulteriori informazioni sugli avvisi, vedere la "documentazione del prodotto" disponibile online e in formato PDF.

Monitoraggio avanzato in StorageGRID

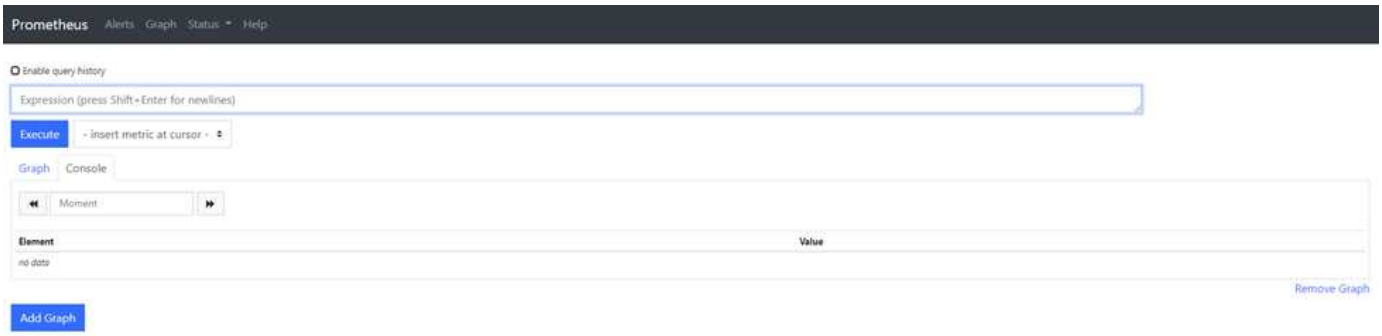
Scopri come accedere ed esportare le metriche per risolvere i problemi.

Visualizzare l'API delle metriche tramite una query Prometheus

Prometheus è un software open-source per la raccolta delle metriche. Per accedere al Prometheus integrato di StorageGRID tramite l'GMI, vai al **Support › Metrics**.



In alternativa, è possibile accedere direttamente al collegamento.

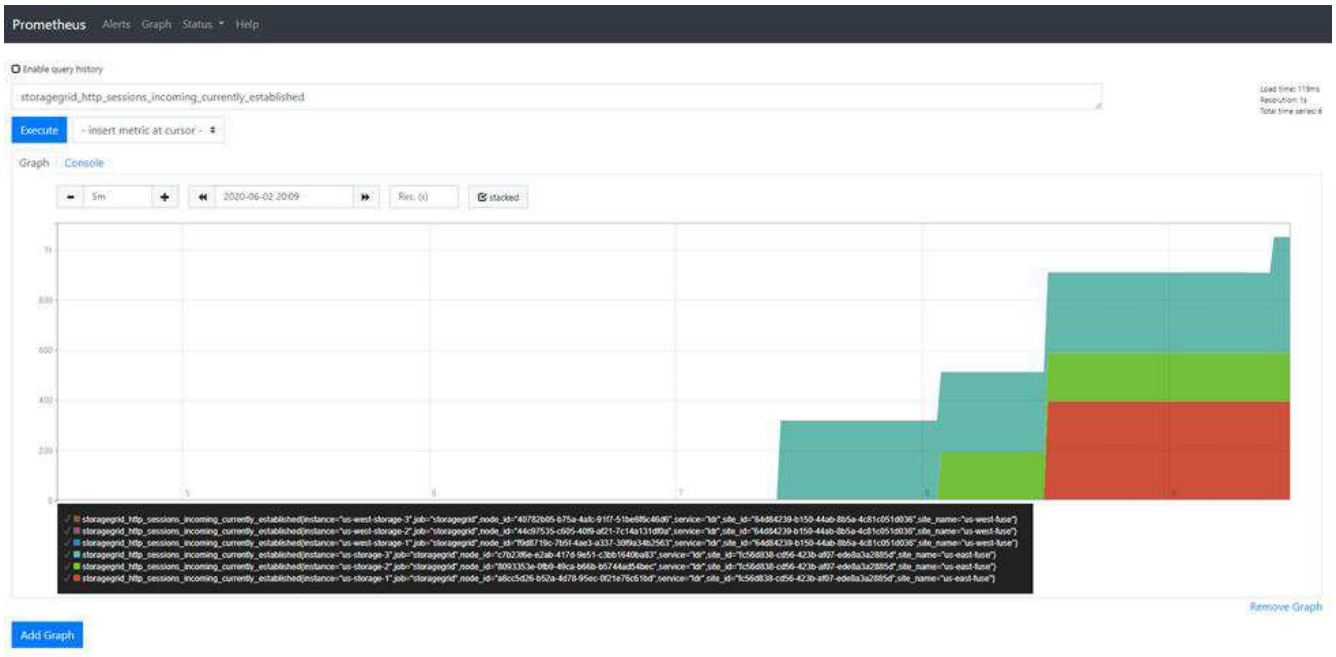


Con questa visualizzazione, è possibile accedere all'interfaccia Prometheus. Da lì, puoi cercare nelle metriche disponibili e persino sperimentare le query.

Per eseguire una query URL Prometheus, attenersi alla seguente procedura:

Fasi

1. Iniziare a digitare nella casella di testo della query. Durante la digitazione, vengono elencate le metriche. Per i nostri scopi, sono importanti solo le metriche che iniziano con StorageGRID e nodo.
2. Per visualizzare il numero di sessioni HTTP per ogni nodo, digitare `storagegrid_http` e selezionare `storagegrid_http_sessions_incoming_currently_established`. Fare clic su Esegui e visualizzare le informazioni in formato grafico o console.



Le query e i grafici creati tramite questo URL non persistono. Le query complesse consumano risorse sul nodo amministrativo. NetApp consiglia di utilizzare questa vista per esplorare le metriche disponibili.

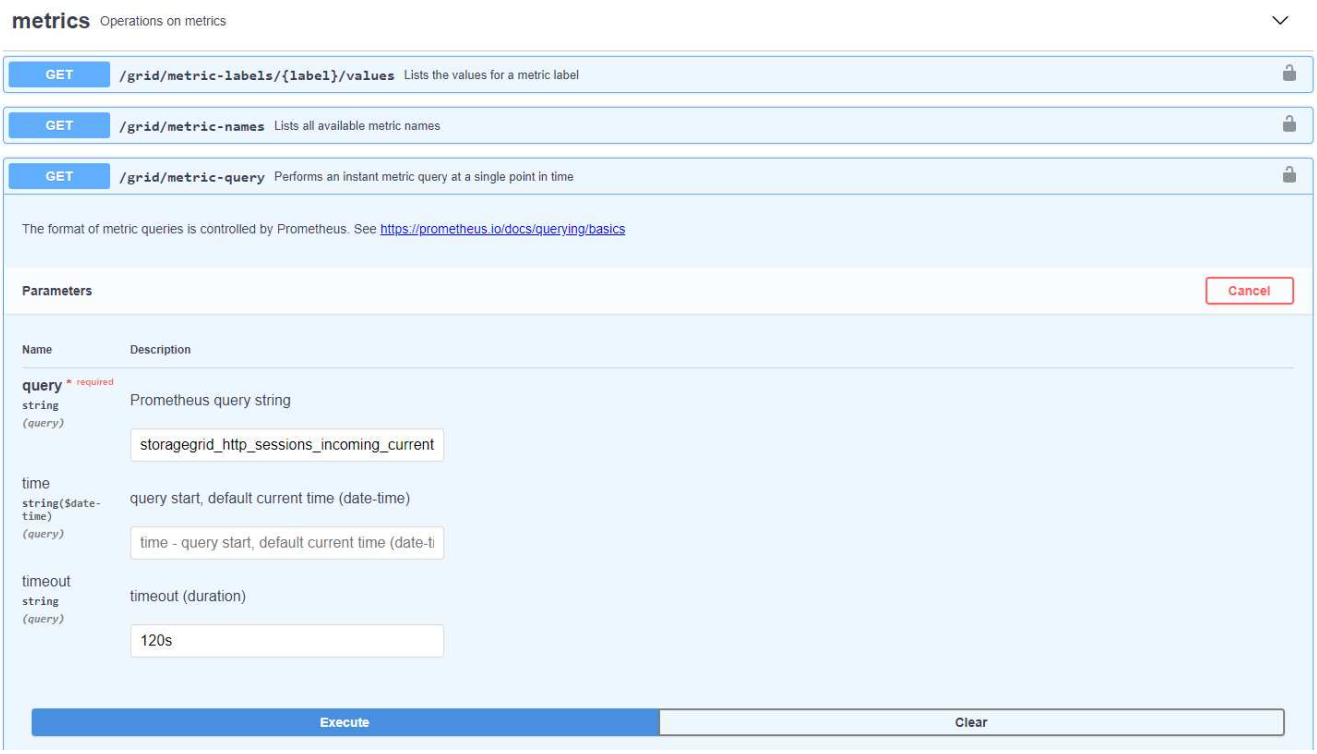
Si sconsiglia di interfacciarsi direttamente con la nostra istanza Prometheus perché questo richiede l'apertura di porte aggiuntive. L'accesso alle metriche tramite la nostra API è il metodo consigliato e sicuro.

Esporta metriche tramite API

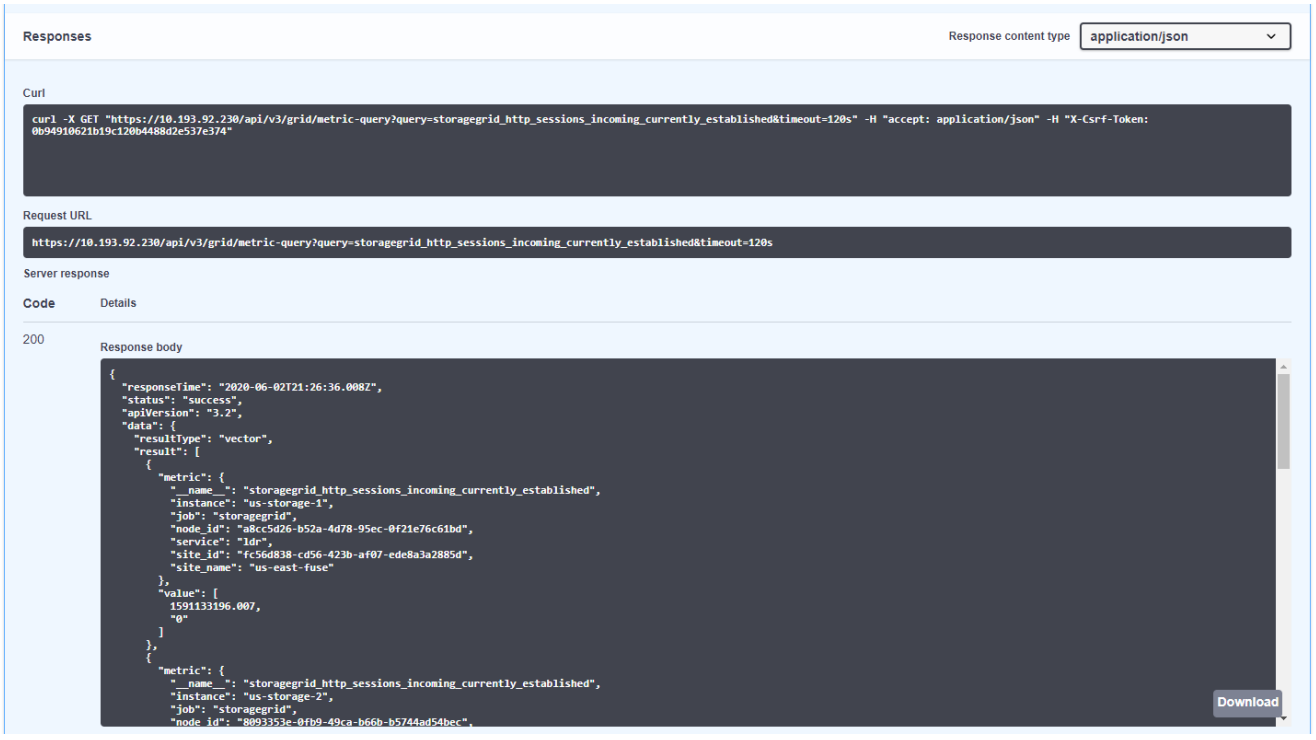
Puoi anche accedere agli stessi dati tramite l'API di gestione StorageGRID.

Per esportare le metriche tramite l'API, attenersi alla seguente procedura:

1. Nell'interfaccia GMI, selezionare **Guida › documentazione API**.
2. Scorrere fino a Metrics (metriche) e selezionare GET /grid/METRIC-query (OTTIENI /griglia/query metrica).



La risposta include le stesse informazioni che è possibile ottenere tramite una query URL Prometheus. È possibile visualizzare nuovamente il numero di sessioni HTTP attualmente stabilite su ciascun nodo di storage. È anche possibile scaricare la risposta in formato JSON per la leggibilità. La figura seguente mostra risposte di query Prometheus di esempio.



Il vantaggio dell'utilizzo dell'API è che consente di eseguire query autenticate

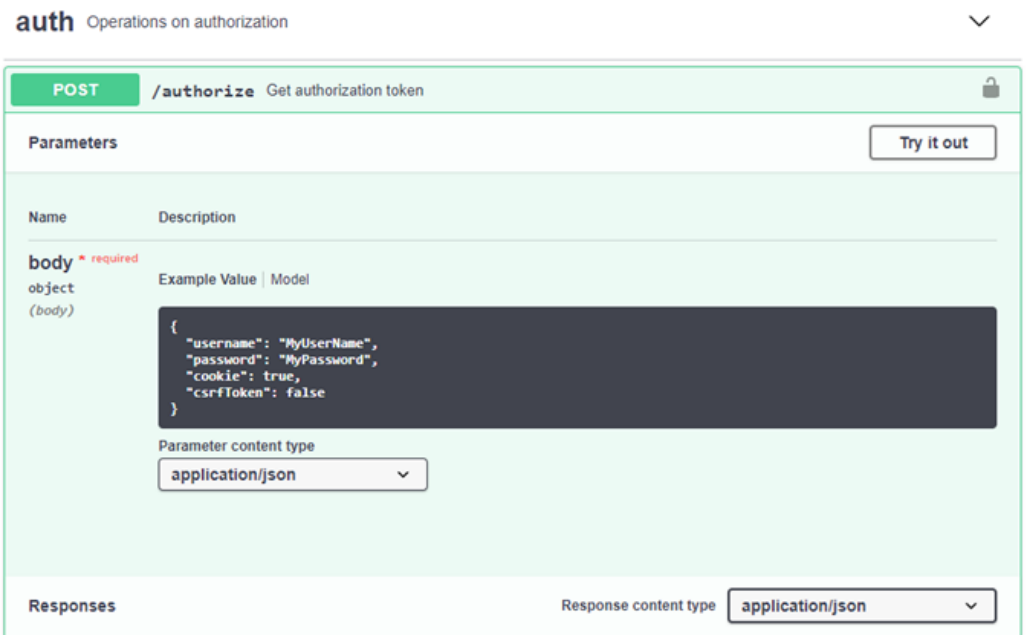
Accedi alle metriche utilizzando Curl in StorageGRID

Scopri come accedere alle metriche tramite l'interfaccia CLI utilizzando Curl.

Per eseguire questa operazione, è necessario prima ottenere un token di autorizzazione. Per richiedere un token, attenersi alla seguente procedura:

Fasi

1. Nell'interfaccia GMI, selezionare **Guida › documentazione API**.
2. Scorrere verso il basso fino a Auth per trovare le operazioni su autorizzazione. La seguente schermata mostra i parametri per il metodo POST.



3. Fare clic su prova e modificare il corpo con il nome utente e la password GMI.
4. Fare clic su Esegui.
5. Copiare il comando curl fornito nella sezione curl e incollarlo in una finestra terminale. Il comando è simile al seguente:

```
curl -X POST "https:// <Primary_Admin_IP>/api/v3/authorize" -H "accept:
application/json" -H "Content-Type: application/json" -H "X-Csrf-Token:
dc30b080e1ca9bc05ddb81104381d8c8" -d "{ \"username\": \"MyUsername\",
\"password\": \"MyPassword\", \"cookie\": true, \"csrfToken\": false}"
-k
```

> Se la password GMI contiene caratteri speciali, utilizzare \ per uscire da caratteri speciali. Ad esempio, sostituire ! con \!

6. Dopo aver eseguito il comando curl precedente, l'output fornisce un token di autorizzazione come l'esempio seguente:

```
{"responseTime":"2020-06-
03T00:12:17.031Z","status":"success","apiVersion":"3.2","data":"8a1e528d
-18a7-4283-9a5e-b2e6d731e0b2"}
```

Ora è possibile utilizzare la stringa del token di autorizzazione per accedere alle metriche tramite curl. Il processo di accesso alle metriche è simile a quello descritto nella sezione "Monitoraggio avanzato in StorageGRID". Tuttavia, a scopo dimostrativo, viene mostrato un esempio con GET /grid/metric-labels/{label}/values selezionato nella categoria Metrics.

7. Ad esempio, il seguente comando curl con il token di autorizzazione precedente elenca i nomi dei siti in StorageGRID.

```
curl -X GET "https://10.193.92.230/api/v3/grid/metric-
labels/site_name/values" -H "accept: application/json" -H
"Authorization: Bearer 8a1e528d-18a7-4283-9a5e-b2e6d731e0b2"
```

Il comando curl genera il seguente output:

```
{"responseTime":"2020-06-
03T00:17:00.844Z","status":"success","apiVersion":"3.2","data":["us-
east-fuse","us-west-fuse"]}
```

Visualizza le metriche utilizzando la dashboard Grafana di StorageGRID

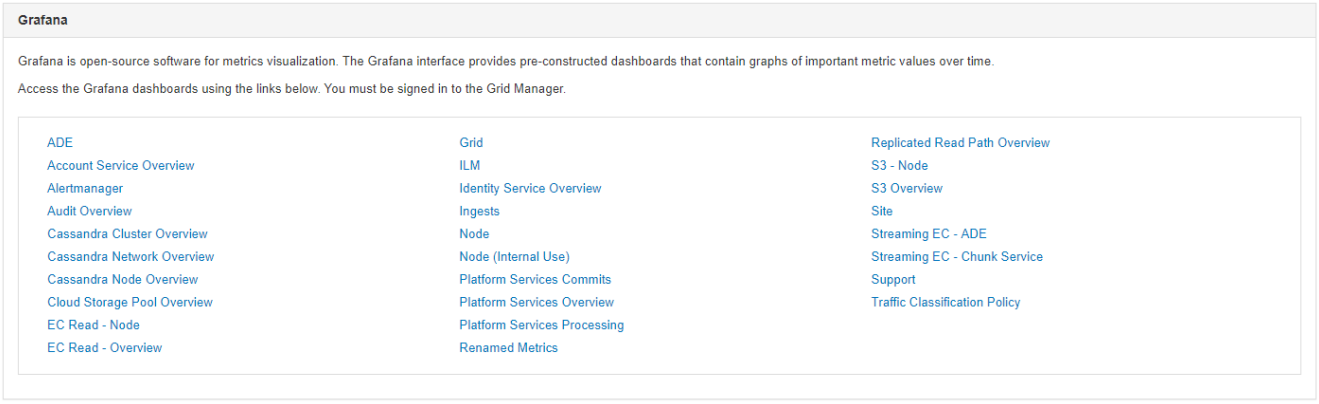
Scopri come utilizzare l'interfaccia Grafana per visualizzare e monitorare i tuoi dati StorageGRID.

Grafana è un software open-source per la visualizzazione delle metriche. Per impostazione predefinita, sono disponibili dashboard predefiniti che forniscono informazioni utili e potenti sul sistema StorageGRID in uso.

Questi dashboard predefiniti sono utili non solo per il monitoraggio ma anche per la risoluzione di un problema. Alcune sono destinate all'uso da parte del supporto tecnico. Ad esempio, per visualizzare le metriche di un nodo storage, segui questa procedura.

Fasi

1. Nell'interfaccia GMI, **Support › Metrics** (supporto[metriche]).
2. Nella sezione Grafana, selezionare il dashboard Node (nodo).



3. In Grafana, impostare gli host sul nodo su cui si desidera visualizzare le metriche. In questo caso, viene selezionato un nodo storage. Vengono fornite ulteriori informazioni rispetto alle seguenti schermate acquisite.

Utilizzare i criteri di classificazione del traffico in StorageGRID

Scoprite come impostare e configurare criteri di classificazione del traffico per gestire e ottimizzare il traffico di rete in StorageGRID.

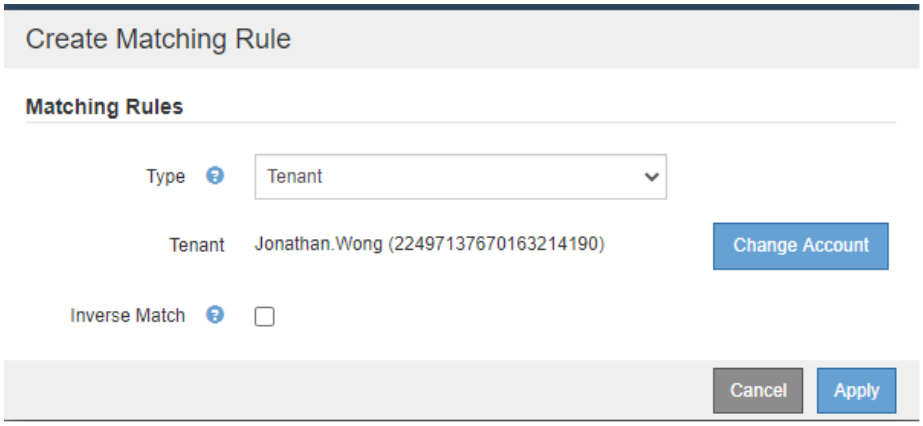
I criteri di classificazione del traffico forniscono un metodo per monitorare e/o limitare il traffico in base a specifici endpoint di tenant, bucket, subnet IP o bilanciamento del carico. La connettività di rete e la larghezza di banda sono parametri particolarmente importanti per StorageGRID.

Per configurare un criterio di classificazione del traffico, attenersi alla seguente procedura:

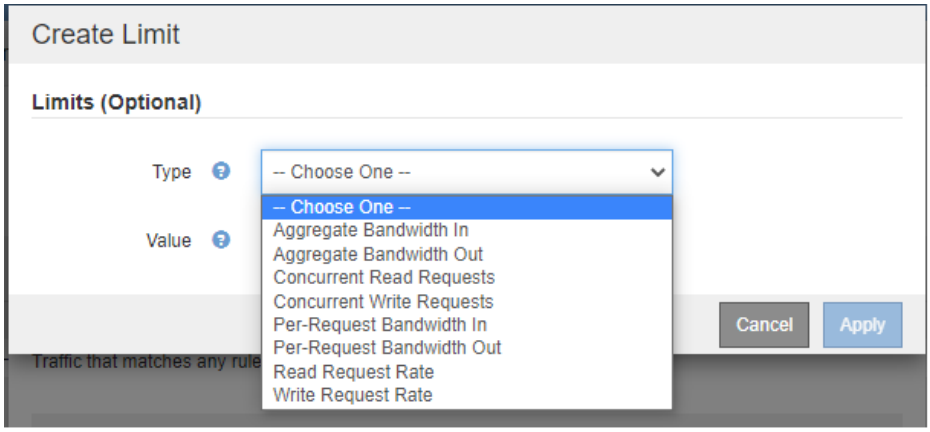
Fasi

1. Sull'interfaccia GMI, accedere al **Configurazione › Impostazioni del sistema › classificazione del traffico**.
2. Fare clic su Crea +

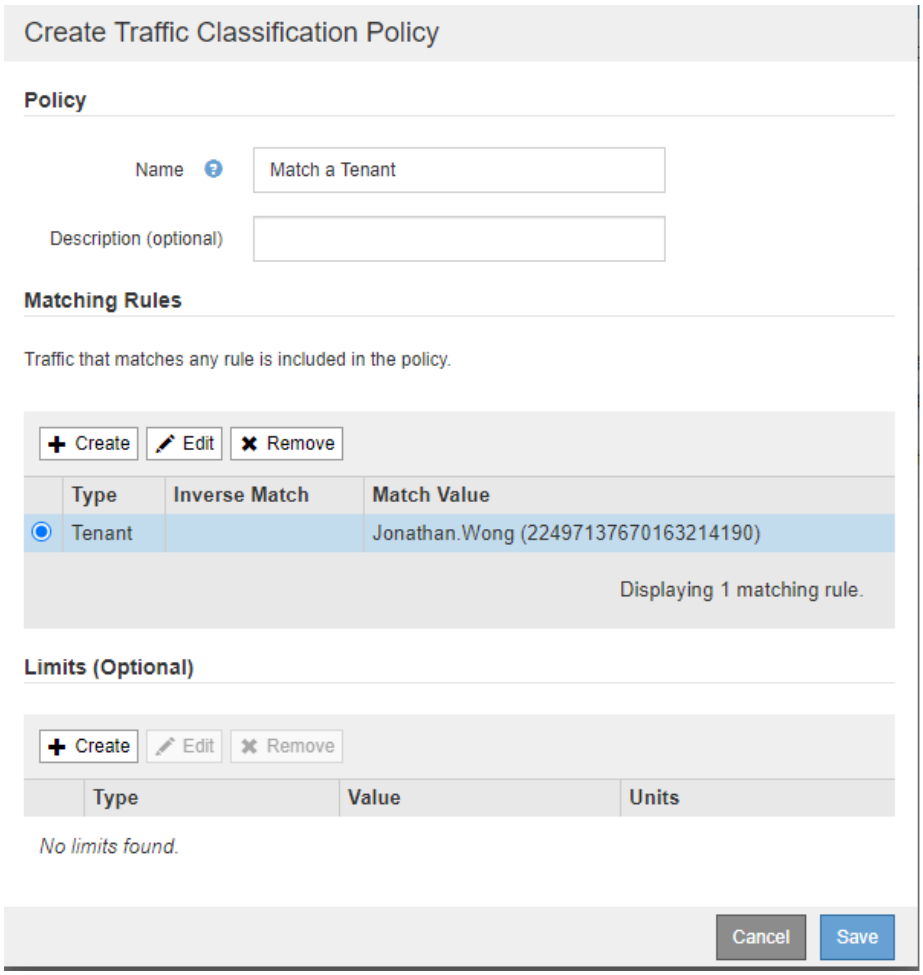
3. Immettere un nome e una descrizione per la politica.
4. Creare una regola corrispondente.



5. Impostare un limite (opzionale).



6. Salvare la policy



Per visualizzare le metriche associate al criterio di classificazione del traffico, selezionare il criterio e fare clic su metriche. Viene generata una dashboard Grafana che visualizza informazioni come il traffico delle richieste di bilanciamento del carico e la durata media delle richieste.

Utilizzare i registri di controllo per monitorare StorageGRID

Scopri come utilizzare l'audit log di StorageGRID per approfondimenti dettagliati sulle attività di tenant e grid e come sfruttare strumenti come Splunk per l'analisi dei log.

L'audit log di StorageGRID consente di raccogliere informazioni dettagliate sul tenant e sull'attività della griglia. L'audit log può essere esposto per analisi tramite NFS. Per istruzioni dettagliate su come esportare il registro di controllo, consultare la Guida dell'amministratore.

Dopo l'esportazione della audit, puoi utilizzare strumenti di analisi dei log come Splunk o Logstash + Elasticsearch per comprendere l'attività dei tenant o creare report dettagliati su fatturazione e charge back.

I dettagli sui messaggi di controllo sono inclusi nella documentazione di StorageGRID. Vedere "Messaggi di audit".

USA l'app StorageGRID per Splunk

Scopri l'app NetApp StorageGRID per Splunk, che consente di monitorare e analizzare il tuo ambiente StorageGRID all'interno della piattaforma Splunk.

Splunk è una piattaforma software che importa e indicizza i dati delle macchine per fornire potenti funzionalità di ricerca e analisi. L'app NetApp StorageGRID è un add-on per Splunk che importa e arricchisce i dati sfruttati da StorageGRID.

Le istruzioni su come installare, aggiornare e configurare il componente aggiuntivo StorageGRID sono disponibili qui: https://splunkbase.splunk.com/app/3895/#/details

TR-4882: Installazione di una griglia bare metal StorageGRID

Introduzione all'installazione di StorageGRID

Scopri come installare StorageGRID su host bare metal.

TR-4882 fornisce una pratica serie di istruzioni passo-passo che produce un'installazione funzionante di NetApp StorageGRID. L'installazione potrebbe essere su server bare metal o su macchine virtuali (VM) in esecuzione su Red Hat Enterprise Linux (RHEL). L'approccio consiste nell'eseguire un'installazione "chiavi in mano" di sei servizi racchiusi in container StorageGRID su tre macchine fisiche (o virtuali), seguendo un layout e una configurazione dello storage suggeriti. Per alcuni clienti potrebbe essere più semplice comprendere il processo di implementazione, seguire l'esempio riportato in questo report tecnico.

Per una comprensione più approfondita di StorageGRID e del processo di installazione, vedere https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html [Installazione, aggiornamento e aggiornamento rapido StorageGRID] nella documentazione del prodotto.

Prima di iniziare l'implementazione, esaminiamo i requisiti di calcolo, storage e rete per il software NetApp StorageGRID. StorageGRID viene eseguito come servizio containerizzato all'interno di Podman o Docker. In questo modello, alcuni requisiti fanno riferimento al sistema operativo host (il sistema operativo che ospita Docker, che esegue il software StorageGRID). Inoltre, alcune risorse vengono allocate direttamente nei container Docker eseguiti all'interno di ciascun host. In questa distribuzione, al fine di ottimizzare l'utilizzo dell'hardware, vengono distribuiti due servizi per host fisico. Per ulteriori informazioni, passare alla sezione successiva, "Prerequisiti per l'installazione di StorageGRID".

I passaggi descritti in questo TR comportano un'installazione StorageGRID funzionante su sei host bare metal. Ora si dispone di una griglia di lavoro e di una rete client, utili nella maggior parte degli scenari di test.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo report tecnico, consultare le seguenti risorse della documentazione:

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Prerequisiti per l'installazione di StorageGRID

Scopri i requisiti di calcolo, storage, rete, docker e nodo per implementare StorageGRID.

Requisiti di calcolo

La tabella riportata di seguito elenca i requisiti minimi delle risorse supportate per ogni tipo di nodo StorageGRID. Queste sono le risorse minime richieste per i nodi StorageGRID.

Tipo di nodo	Core di CPU	RAM
Amministratore	8	24GB
Storage	8	24GB
Gateway	8	24GB

Inoltre, per garantire il corretto funzionamento di ciascun host fisico di Docker deve essere allocato un minimo di 16GB GB di RAM. Ad esempio, per ospitare insieme due dei servizi descritti nella tabella in un unico host fisico di Docker, occorre eseguire il seguente calcolo:

24 + 24 + 16 = 64GB GB di RAM e 8 + 8 = 16 core

Poiché molti server moderni superano questi requisiti, combiniamo sei servizi (container StorageGRID) su tre server fisici.

Requisiti di rete

I tre tipi di traffico StorageGRID includono:

- **Traffico griglia (obbligatorio).** Il traffico StorageGRID interno che viaggia tra tutti i nodi della griglia.
- **Traffico amministrativo (opzionale).** Il traffico utilizzato per l'amministrazione e la manutenzione del sistema.
- **Traffico client (opzionale).** Il traffico che viaggia tra le applicazioni client esterne e il grid, incluse tutte le richieste di storage a oggetti dai client S3 e Swift.

È possibile configurare fino a tre reti da utilizzare con il sistema StorageGRID. Ogni tipo di rete deve trovarsi su una subnet separata senza sovrapposizioni. Se tutti i nodi si trovano nella stessa subnet, non è necessario un indirizzo gateway.

Per questa valutazione, verrà eseguita la distribuzione su due reti, che contengono la rete e il traffico client. È

possibile aggiungere successivamente una rete di amministrazione per supportare questa funzione aggiuntiva.

È molto importante mappare le reti in modo coerente alle interfacce in tutti gli host. Ad esempio, se su ogni nodo sono presenti due interfacce, ens192 e ens224, tutte devono essere mappate alla stessa rete o VLAN su tutti gli host. In questa installazione, il programma di installazione esegue il mapping di questi dati nei contenitori Docker come eth0@IF2 e eth2@IF3 (poiché il loopback è IF1 all'interno del contenitore), pertanto un modello coerente è molto importante.

Nota sul networking di Docker

StorageGRID utilizza il networking in modo diverso da alcune implementazioni di container Docker. Non utilizza il networking fornito da Docker (o Kubernetes o Swarm). Al contrario, in realtà StorageGRID utilizza il container come --net=none, in modo che Docker non esegua alcuna operazione di rete. Dopo che il contenitore è stato generato dal servizio StorageGRID, viene creato un nuovo dispositivo macvlan dall'interfaccia definita nel file di configurazione del nodo. Tale dispositivo dispone di un nuovo indirizzo MAC e funge da dispositivo di rete separato in grado di ricevere pacchetti dall'interfaccia fisica. Il dispositivo macvlan viene quindi spostato nello spazio dei nomi dei contenitori e rinominato in uno dei eth0, eth1 o eth2 all'interno del contenitore. A questo punto, il dispositivo di rete non è più visibile nel sistema operativo host. Nel nostro esempio, il dispositivo di rete Grid è eth0 all'interno dei container Docker e la rete Client è eth2. Se avessimo una rete di amministrazione, il dispositivo sarebbe eth1 nel container.

> Il nuovo indirizzo MAC del dispositivo di rete del contenitore potrebbe richiedere l'attivazione della modalità promiscua in alcuni ambienti di rete e virtuali. Questa modalità consente al dispositivo fisico di ricevere e inviare pacchetti per gli indirizzi MAC che differiscono dagli indirizzi MAC fisici noti. se si esegue in VMware vSphere, è necessario accettare la modalità promiscua, le modifiche degli indirizzi MAC e le trasmissioni falsificate nei gruppi di porte che serviranno il traffico StorageGRID quando si esegue RHEL. Ubuntu o Debian funziona senza questi cambiamenti nella maggior parte delle circostanze.

Requisiti di storage

I nodi richiedono ciascuno dispositivi di dischi locali o basati su SAN delle dimensioni indicate nella tabella seguente.

> I numeri contenuti nella tabella sono relativi a ciascun tipo di servizio StorageGRID, non all'intero grid o a ciascun host fisico. In base alle scelte di distribuzione, verranno calcolati i numeri per ciascun host fisico in , più avanti in "Layout e requisiti dell'host fisico"questo documento. i percorsi o i file system contrassegnati con un asterisco verranno creati nel contenitore StorageGRID stesso dall'installatore. L'amministratore non richiede alcuna configurazione manuale o creazione di file system, ma gli host hanno bisogno di dispositivi a blocchi per soddisfare questi requisiti. In altre parole, il dispositivo a blocchi dovrebbe apparire utilizzando il comando `lsblk` ma non essere formattato o montato all'interno del sistema operativo host.

Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensione minima di LUN	File system manuale richiesto	Voce di configurazione nodo consigliata
Tutto	Spazio di sistema del nodo amministrativo `/var/local` (SSD utile qui)	Uno per ogni nodo amministrativo	90GB	No	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`

Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensione minima di LUN	File system manuale richiesto	Voce di configurazione nodo consigliata
Tutti i nodi	Pool di storage Docker all'indirizzo `/var/lib/docker for container pool`	Uno per ciascun host (fisico o VM)	100GB per contenitore	Sì – etx4	NA – formatta e monta come file system host (non mappato nel contenitore)
Amministratore	Audit log del nodo amministrativo (dati del sistema nel container dell'amministratore) `/var/local/audit/export`	Uno per ogni nodo amministrativo	200GB	No	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
Amministratore	Tabelle nodo amministrativo (dati di sistema nel contenitore amministrativo) `/var/local/mysql_ibdata`	Uno per ogni nodo amministrativo	200GB	No	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
Nodi di storage	Storage a oggetti (dispositivi a blocchi `/var/local/rangedb0`) (SSD utili qui) `/var/local/rangedb1` `/var/local/rangedb2`	Tre per ciascun contenitore di stoccaggio	4000GB	No	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

In questo esempio, le dimensioni dei dischi mostrate nella seguente tabella sono necessarie per tipo di contenitore. I requisiti per host fisico sono descritti nella , più avanti in "Layout e requisiti dell'host fisico"questo documento.

Dimensioni dei dischi per tipo di container

Container di amministrazione

Nome	Dimensioni (GiB)
Docker-Store	100 (per contenitore)
ADM-OS	90
ADM-Audit	200
ADM-MySQL	200

Contenitore di stoccaggio

Nome	Dimensioni (GiB)
Docker-Store	100 (per contenitore)
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

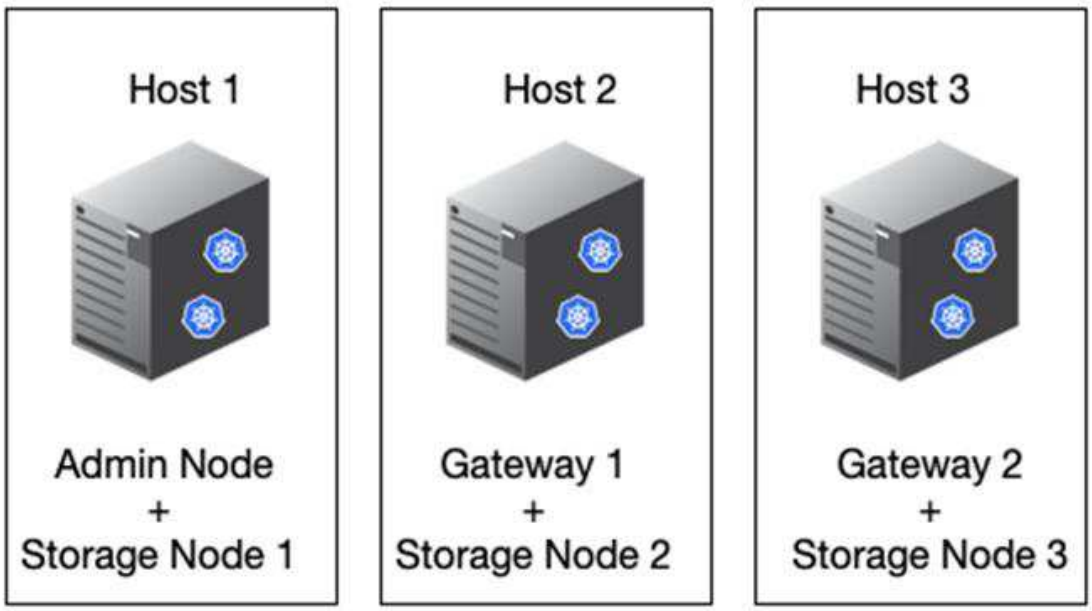
Contenitore gateway

Nome	Dimensioni (GiB)
Docker-Store	100 (per contenitore)
/var/local	90

Layout e requisiti dell'host fisico

Combinando i requisiti di elaborazione e di rete illustrati nella tabella precedente, è possibile ottenere un set di hardware di base necessario per questa installazione di tre server fisici (o virtuali) con 16 core, 64GB di RAM e due interfacce di rete. Se si desidera un throughput più elevato, è possibile collegare due o più interfacce sulla griglia o sulla rete client e utilizzare un'interfaccia con codifica VLAN come bond0,520 nel file di configurazione del nodo. In presenza di carichi di lavoro più intensi, è preferibile una maggiore quantità di memoria per l'host e i container.

Come illustrato nella seguente figura, questi server ospitano sei container Docker, due per host. La RAM viene calcolata fornendo 24GB GB per contenitore e 16GB GB per il sistema operativo host stesso.



La RAM totale richiesta per host fisico (o VM) è 24 x 2 GB + 16 GB = 64GB GB. Nelle tabelle che seguono sono elencati i requisiti di archiviazione su disco per gli host 1, 2 e 3.

Host 1	**Dimensioni (GiB)**
Docker Store	`/var/lib/docker` (File system)
200 (100 x 2)	**Contenitore amministratore**
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
Contenitore di stoccaggio	SN-OS `/var/local` (dispositivo)
90	Rangedb-0 (dispositivo)
4096	Rangedb-1 (dispositivo)
4096	Rangedb-2 (dispositivo)

Host 2	**Dimensioni (GiB)**
Docker Store	`/var/lib/docker` (Condiviso)
200 (100 x 2)	**Contenitore gateway**
GW-OS */`var/local`	100
Contenitore di stoccaggio	*/`var/local`
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Host 3	**Dimensioni (GiB)**
Docker Store	`/var/lib/docker` (Condiviso)
200 (100 x 2)	**Contenitore gateway**
*/`var/local`	100
Contenitore di stoccaggio	*/`var/local`
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Docker Store è stato calcolato consentendo 100GB per /var/local (per contenitore) x due contenitori = 200GB.

Preparazione dei nodi

Per preparare l'installazione iniziale di StorageGRID, installare prima RHEL versione 9,2 e abilitare SSH. Impostare le interfacce di rete, NTP (Network Time Protocol), DNS e il nome host in base alle Best practice. È necessaria almeno un'interfaccia di rete abilitata sulla rete di rete e un'altra per la rete client. Se si utilizza un'interfaccia con codifica VLAN, configurarla come descritto negli esempi seguenti. In caso contrario, sarà sufficiente una semplice configurazione standard dell'interfaccia di rete.

Se è necessario utilizzare un tag VLAN sull'interfaccia di rete della griglia, la configurazione dovrebbe avere due file nel `/etc/sysconfig/network-scripts/` seguente formato:

```
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0
# This is the parent physical device
TYPE=Ethernet
BOOTPROTO=none
DEVICE=enp67s0
ONBOOT=yes
# cat /etc/sysconfig/network-scripts/ifcfg-enp67s0.520
# The actual device that will be used by the storage node file
DEVICE=enp67s0.520
BOOTPROTO=none
NAME=enp67s0.520
IPADDR=10.10.200.31
PREFIX=24
VLAN=yes
ONBOOT=yes
```

Questo esempio presuppone che il dispositivo di rete fisico per la rete di rete sia enp67s0. Potrebbe anche essere un dispositivo Unito come bond0. Sia che si utilizzi il bonding o un'interfaccia di rete standard, è necessario utilizzare l'interfaccia con codifica VLAN nel file di configurazione del nodo se la porta di rete non dispone di una VLAN predefinita o se la VLAN predefinita non è associata alla rete di rete. Il contenitore StorageGRID stesso non annulla l'etichetta dei frame Ethernet, quindi deve essere gestito dal sistema operativo padre.

Configurazione dello storage opzionale con iSCSI

Se non si utilizza storage iSCSI, è necessario assicurarsi che host1, Host2 e host3 contengano dispositivi a blocchi di dimensioni sufficienti per soddisfare i relativi requisiti. Consultare la sezione "Dimensioni dei dischi per tipo di container" per i requisiti di storage di host1, Host2 e host3.

Per configurare lo storage con iSCSI, attenersi alla seguente procedura:

Fasi

1. Se si utilizza storage iSCSI esterno, ad esempio il software di gestione dei dati NetApp e-Series o NetApp ONTAP®, installare i seguenti pacchetti:

```
sudo yum install iscsi-initiator-utils
sudo yum install device-mapper-multipath
```

2. Individuare l'ID iniziatore su ciascun host.

```
# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2006-04.com.example.node1
```

3. Utilizzando il nome dell'iniziatore del passaggio 2, mappare i LUN del dispositivo di archiviazione (del numero e delle dimensioni indicati nella tabella) a ciascun nodo di archiviazione "Requisiti di storage" .
4. Scopri i LUN appena creati `iscsiadm` ed effettua l'accesso.

```
# iscsiadm -m discovery -t st -p target-ip-address
# iscsiadm -m node -T iqn.2006-04.com.example:3260 -l
Logging in to [iface: default, target: iqn.2006-04.com.example:3260,
portal: 10.64.24.179,3260] (multiple)
Login to [iface: default, target: iqn.2006-04.com.example:3260, portal:
10.64.24.179,3260] successful.
```

Per ulteriori informazioni, consultate il "Creazione di un iniziatore iSCSI" portale clienti Red Hat.

5. Per visualizzare i dispositivi multipath e i WWID LUN associati, eseguire il seguente comando:

```
# multipath -ll
```

Se non si utilizza iSCSI con dispositivi multipercorso, è sufficiente montare il dispositivo con un nome di percorso univoco che mantiene le modifiche e il riavvio del dispositivo allo stesso modo.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
```

Se i dispositivi vengono rimossi o aggiunti, la semplice utilizzo dei `/dev/sdx` nomi dei dispositivi potrebbe causare problemi in seguito. se si utilizzano dispositivi multipath, modificare il `/etc/multipath.conf` file per utilizzare gli alias come segue.

Questi dispositivi potrebbero essere o meno presenti su tutti i nodi, a seconda del layout.

```
multipaths {
multipath {
wwid 36d039ea00005f06a000003c45fa8f3dc
alias Docker-Store
}
multipath {
wwid 36d039ea00006891b000004025fa8f597
alias Adm-Audit
}
multipath {
wwid 36d039ea00005f06a000003c65fa8f3f0
alias Adm-MySQL
}
multipath {
wwid 36d039ea00006891b000004015fa8f58c
alias Adm-OS
}
multipath {
wwid 36d039ea00005f06a000003c55fa8f3e4
alias SN-OS
}
multipath {
wwid 36d039ea00006891b000004035fa8f5a2
alias SN-Db00
}
multipath {
wwid 36d039ea00005f06a000003c75fa8f3fc
alias SN-Db01
}
multipath {
    wwid 36d039ea00006891b000004045fa8f5af
alias SN-Db02
}
multipath {
wwid 36d039ea00005f06a000003c85fa8f40a
alias GW-OS
}
}
```

Prima di installare Docker nel sistema operativo host, formattare e montare il LUN o il backup del disco `/var/lib/docker`. Le altre LUN sono definite nel file di configurazione del nodo e utilizzate direttamente dai container StorageGRID. In altre parole, non vengono visualizzati nel sistema operativo host; vengono visualizzati nei contenitori stessi e i file system vengono gestiti dall'installatore.

Se si utilizza un LUN con backup iSCSI, inserire nel file fstab qualcosa di simile alla seguente riga. Come notato, gli altri LUN non devono essere montati nel sistema operativo host ma devono essere visualizzati come

dispositivi a blocchi disponibili.

```
/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
defaults 0 0
```

Preparazione dell'installazione di Docker

Per prepararsi all'installazione di Docker, attenersi alla seguente procedura:

Fasi

1. Crea un file system sul volume di storage Docker su tutti e tre gli host.

   ```
   # sudo mkfs.ext4 /dev/sd?
   ```

   Se si utilizzano dispositivi iSCSI con multipath, utilizzare `/dev/mapper/Docker-Store`.

2. Creare il punto di montaggio del volume di storage Docker:

   ```
   # sudo mkdir -p /var/lib/docker
   ```

3. Aggiungere una voce simile per la periferica-volume-archiviazione-docker a `/etc/fstab`.

   ```
   /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0 /var/lib/docker ext4
   defaults 0 0
   ```

   L'opzione seguente `_netdev` è consigliata solo se si utilizza un dispositivo iSCSI. Se si utilizza un dispositivo di blocco locale `_netdev` non è necessario ed `defaults` è consigliato.

   ```
   /dev/mapper/Docker-Store /var/lib/docker ext4 _netdev 0 0
   ```

4. Montare il nuovo file system e visualizzare l'utilizzo del disco.

   ```
   # sudo mount /var/lib/docker
   [root@host1]# df -h | grep docker
   /dev/sdb 200G 33M 200G 1% /var/lib/docker
   ```

5. Disattivare lo swap e disattivarlo per motivi di prestazioni.

   ```
   $ sudo swapoff --all
   ```

6. Per mantenere le impostazioni, rimuovete tutte le voci di swap da /etc/fstab come:

```
/dev/mapper/rhel-swap swap defaults 0 0
```

La mancata disattivazione completa dello swap può ridurre notevolmente le performance.

7. Eseguire un riavvio di prova del nodo per verificare che il `/var/lib/docker` volume sia persistente e che tutti i dispositivi disco ritornino.

Installa Docker per StorageGRID

Scopri come installare Docker per StorageGRID.

Per installare Docker, attenersi alla procedura illustrata di seguito:

Fasi

1. Configurazione del repo yum per Docker.

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo \
https://download.docker.com/linux/rhel/docker-ce.repo
```

2. Installare i pacchetti necessari.

```
sudo yum install docker-ce docker-ce-cli containerd.io
```

3. Avviate Docker.

```
sudo systemctl start docker
```

4. Testa Docker.

```
sudo docker run hello-world
```

5. Assicurati che Docker venga eseguito all'avvio del sistema.

```
sudo systemctl enable docker
```

Preparare i file di configurazione dei nodi per StorageGRID

Scopri come preparare i file di configurazione dei nodi per StorageGRID.

Ad un livello alto, il processo di configurazione dei nodi include i seguenti passaggi:

Fasi

1. Creare la `/etc/storagegrid/nodes` directory su tutti gli host.

```
sudo [root@host1 ~]# mkdir -p /etc/storagegrid/nodes
```

2. Creare i file necessari per ciascun host fisico in modo che corrispondano al layout del tipo di container/nodo. In questo esempio, sono stati creati due file per host fisico su ciascun computer host.

> Il nome del file definisce il nome del nodo effettivo per l'installazione. Ad esempio, `dc1-adm1.conf` diventa un nodo denominato `dc1-adm1`.

— Host1:
`dc1-adm1.conf`
`dc1-sn1.conf`

— Host2:
`dc1-gw1.conf`
`dc1-sn2.conf`

— Host3:
`dc1-gw2.conf`
`dc1-sn3.conf`

Preparazione dei file di configurazione del nodo

I seguenti esempi utilizzano il `/dev/disk/by-path` formato. È possibile verificare i percorsi corretti eseguendo i seguenti comandi:

```
[root@host1 ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 90G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 89G 0 part
├─rhel-root 253:0 0 50G 0 lvm /
├─rhel-swap 253:1 0 9G 0 lvm
└─rhel-home 253:2 0 30G 0 lvm /home
sdb 8:16 0 200G 0 disk /var/lib/docker
sdc 8:32 0 90G 0 disk
sdd 8:48 0 200G 0 disk
sde 8:64 0 200G 0 disk
sdf 8:80 0 4T 0 disk
sdg 8:96 0 4T 0 disk
sdh 8:112 0 4T 0 disk
sdi 8:128 0 90G 0 disk
sr0 11:0 1 1024M 0 rom
```

E questi comandi:

```
[root@host1 ~]# ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:02:01.0-ata-1.0 ->
../../sr0
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:4:0 ->
../../sde
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:5:0 ->
../../sdf
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:6:0 ->
../../sdg
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:8:0 ->
../../sdh
lrwxrwxrwx 1 root root 9 Dec 21 16:42 pci-0000:03:00.0-scsi-0:0:9:0 ->
../../sdi
```

Esempio per il nodo Admin primario

Nome file di esempio:

```
/etc/storagegrid/nodes/dc1-adm1.conf
```

Contenuto del file di esempio:

> I percorsi del disco possono seguire gli esempi riportati di seguito o utilizzare la `/dev/mapper/alias` denominazione dello stile. Non utilizzare i nomi dei dispositivi di blocco, ad esempio `/dev/sdb` perché possono cambiare al riavvio e causare gravi danni alla griglia.

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
MAXIMUM_RAM = 24g
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:2:0
BLOCK_DEVICE_AUDIT_LOGS = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:3:0
BLOCK_DEVICE_TABLES = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:4:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.43
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_IP = 10.193.205.43
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Esempio di un nodo storage

Nome file di esempio:

```
/etc/storagegrid/nodes/dc1-sn1.conf
```

Contenuto del file di esempio:

```
NODE_TYPE = VM_Storage_Node
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.174.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:9:0
BLOCK_DEVICE_RANGEDB_00 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:5:0
BLOCK_DEVICE_RANGEDB_01 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:6:0
BLOCK_DEVICE_RANGEDB_02 = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:8:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.44
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
```

Esempio per nodo gateway

Nome file di esempio:

```
/etc/storagegrid/nodes/dc1-gw1.conf
```

Contenuto del file di esempio:

```
NODE_TYPE = VM_API_Gateway
MAXIMUM_RAM = 24g
ADMIN_IP = 10.193.204.43
BLOCK_DEVICE_VAR_LOCAL = /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:1:0
GRID_NETWORK_TARGET = ens192
CLIENT_NETWORK_TARGET = ens224
GRID_NETWORK_IP = 10.193.204.47
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.193.204.1
CLIENT_NETWORK_IP = 10.193.205.47
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.193.205.1
```

Installare dipendenze e pacchetti StorageGRID

Scopri come installare le dipendenze e i pacchetti StorageGRID.

Per installare le dipendenze e i pacchetti di StorageGRID, eseguire i seguenti comandi:

```
[root@host1 rpms]# yum install -y python-netaddr
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -ivh StorageGRID-Webscale-Service-*.rpm
```

Convalidare i file di configurazione di StorageGRID

Scopri come convalidare il contenuto dei file di configurazione per StorageGRID.

Dopo aver creato i file di configurazione in `/etc/storagegrid/nodes` per ciascuno dei nodi StorageGRID, è necessario convalidare il contenuto di tali file.

Per convalidare il contenuto dei file di configurazione, eseguire il seguente comando su ciascun host:

```
sudo storagegrid node validate all
```

Se i file sono corretti, l'output mostra SUPERATO per ogni file di configurazione:

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Se i file di configurazione non sono corretti, i problemi vengono visualizzati come AVVISI ed ERRORI. Se vengono rilevati errori di configurazione, è necessario correggerli prima di procedere con l'installazione.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Avviare il servizio host StorageGRID

Informazioni su come avviare il servizio host StorageGRID.

Per avviare i nodi StorageGRID e assicurarsi che vengano riavviati dopo il riavvio dell'host, è necessario attivare e avviare il servizio host StorageGRID.

Per avviare il servizio host StorageGRID, attenersi alla procedura riportata di seguito.

Fasi

1. Eseguire i seguenti comandi su ciascun host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

   Il processo di avvio potrebbe richiedere del tempo durante l'esecuzione iniziale.

2. Eseguire il seguente comando per assicurarsi che l'implementazione stia procedendo:

```
sudo storagegrid node status node-name
```

3. Per qualsiasi nodo che restituisce uno stato di `Not-Running` o `Stopped`, eseguire il comando seguente:

```
sudo storagegrid node start node-name
```

   Ad esempio, dato il seguente output si avvierebbe il `dc1-adm1` nodo:

```
[user@host1]# sudo storagegrid node status
Name Config-State Run-State
dc1-adm1 Configured Not-Running
dc1-sn1 Configured Running
```

4. Se in precedenza è stato attivato e avviato il servizio host StorageGRID (o se non si è certi che il servizio sia stato attivato e avviato), eseguire anche il seguente comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurare il gestore di rete in StorageGRID

Informazioni su come configurare il gestore di griglie in StorageGRID sul nodo amministrativo primario.

Completare l'installazione configurando il sistema StorageGRID dall'interfaccia utente di Grid Manager sul

nodo amministrativo primario.

Passaggi di alto livello

La configurazione della griglia e il completamento dell'installazione prevedono le seguenti operazioni:

Fasi

1. Accedere a Grid Manager
2. "Specificare le informazioni sulla licenza StorageGRID"
3. "Aggiungere siti a StorageGRID"
4. "Specificare le subnet della rete griglia"
5. "Approvare i nodi griglia in sospeso"
6. "Specificare le informazioni sul server NTP"
7. "Specificare le informazioni sul server del sistema dei nomi di dominio"
8. "Specificare le password di sistema di StorageGRID"
9. "Esaminare la configurazione e completare l'installazione"

Accedere a Grid Manager

Utilizzare Gestione griglia per definire tutte le informazioni necessarie per configurare il sistema StorageGRID.

Prima di iniziare, il nodo amministrativo primario deve essere distribuito e aver completato la sequenza di avvio iniziale.

Per utilizzare Grid Manager per definire le informazioni, attenersi alla seguente procedura.

Fasi

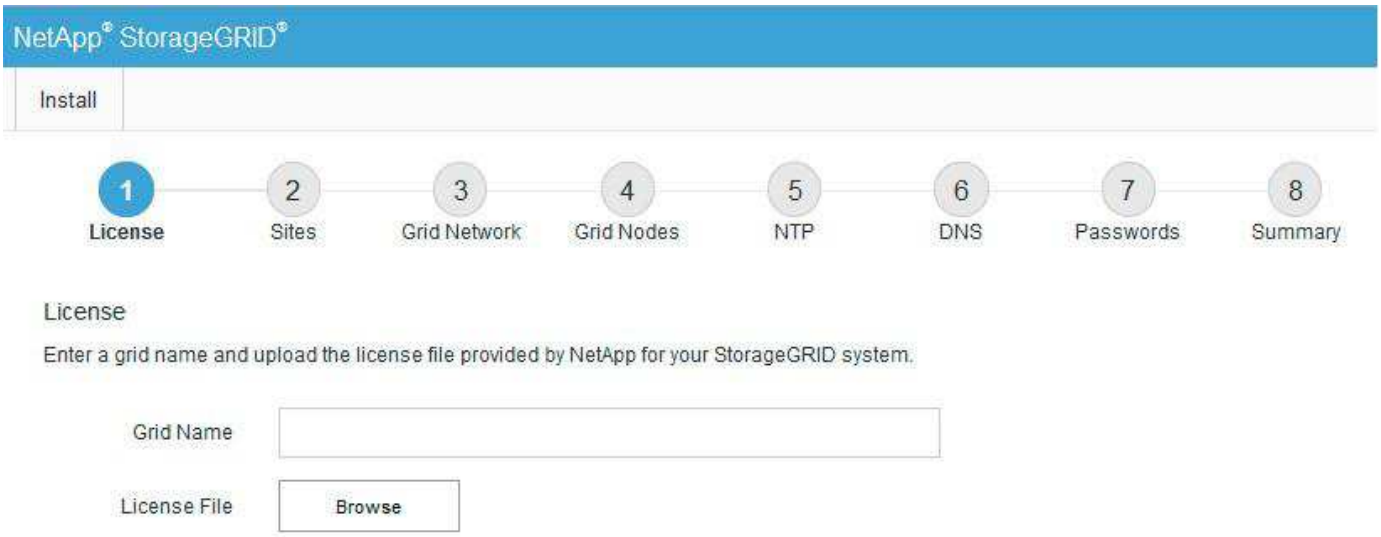
1. Accedere a Grid Manager al seguente indirizzo:

   ```
   https://primary_admin_node_grid_ip
   ```

   In alternativa, è possibile accedere a Grid Manager sulla porta 8443.

   ```
   https://primary_admin_node_ip:8443
   ```

2. Fare clic su Installa un sistema StorageGRID. Viene visualizzata la pagina utilizzata per configurare una griglia StorageGRID.



Aggiungere i dettagli della licenza StorageGRID

Informazioni su come caricare il file di licenza StorageGRID.

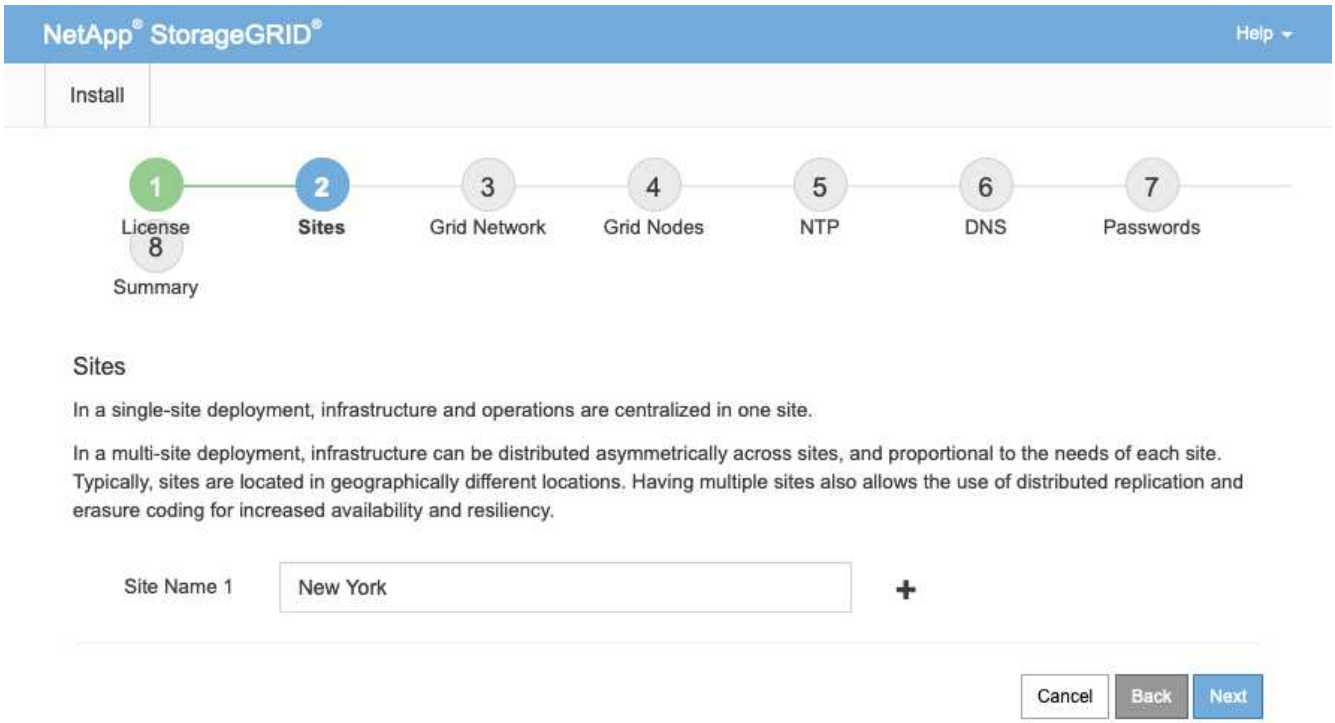
Specificare il nome del sistema StorageGRID e caricare il file di licenza fornito da NetApp.

Per specificare le informazioni sulla licenza StorageGRID, attenersi alla seguente procedura:

Fasi

1. Nella pagina licenza, nel campo Nome griglia, immettere un nome per il sistema StorageGRID. Dopo l'installazione, il nome viene visualizzato come livello superiore nella struttura della topologia della griglia.
2. Fare clic su Sfoglia, individuare il file di licenza NetApp (`NLF-*unique-id*.txt`e fare clic su Apri. Il file di licenza viene validato e vengono visualizzati il numero di serie e la capacità dello storage concesso in licenza.

> L'archivio di installazione di StorageGRID include una licenza gratuita che non fornisce alcun diritto di supporto per il prodotto. È possibile eseguire l'aggiornamento a una licenza che offra supporto dopo l'installazione.



3. Fare clic su Avanti.

Aggiungere siti a StorageGRID

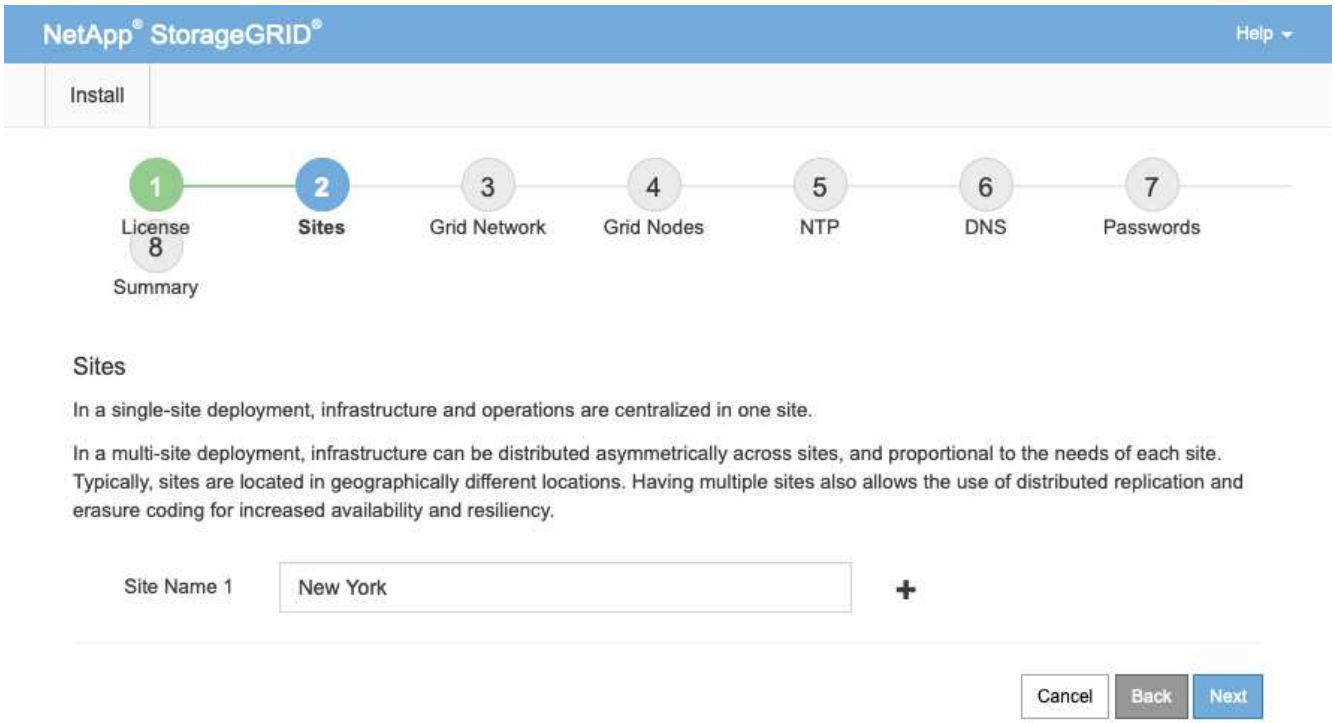
Scopri come aggiungere siti a StorageGRID per aumentare l'affidabilità e la capacità dello storage.

Quando si installa StorageGRID, è necessario creare almeno un sito. È possibile creare siti aggiuntivi per aumentare l'affidabilità e la capacità di storage del sistema StorageGRID.

Per aggiungere siti, attenersi alla seguente procedura:

Fasi

1. Nella pagina Siti, immettere il nome del sito.
2. Per aggiungere altri siti, fare clic sul segno più accanto all'ultima voce del sito e immettere il nome nella nuova casella di testo Nome sito. Aggiungi tutti i siti aggiuntivi necessari per la topologia della griglia. È possibile aggiungere fino a 16 siti.



3. Fare clic su Avanti.

Specificare le subnet di rete della griglia per StorageGRID

Informazioni su come configurare le subnet di rete per StorageGRID.

È necessario specificare le subnet utilizzate sulla rete a griglia.

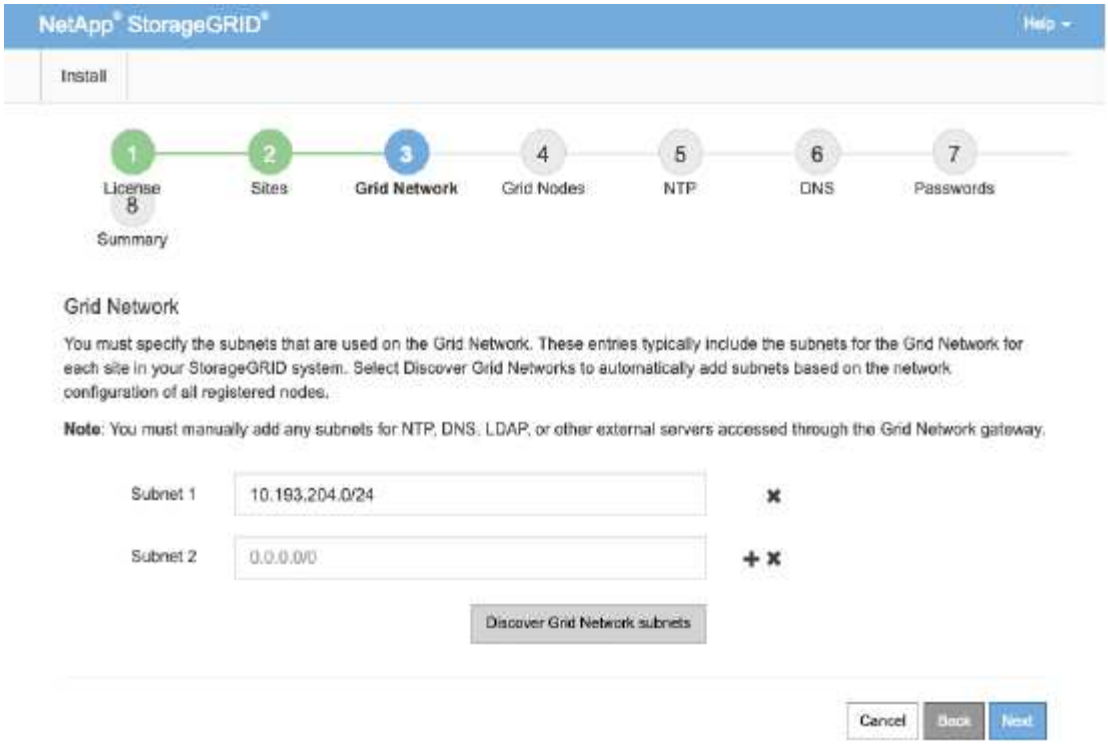
Le voci della subnet includono le subnet per la rete di rete per ogni sito del sistema StorageGRID, oltre alle subnet che devono essere raggiungibili attraverso la rete di rete (ad esempio, le subnet che ospitano i server NTP).

Se si dispone di più sottoreti di rete, è necessario il gateway di rete. Tutte le subnet della griglia specificate devono essere raggiungibili tramite questo gateway.

Per specificare le sottoreti della rete a griglia, attenersi alla seguente procedura:

Fasi

1. Nella casella di testo Subnet 1, specificare l'indirizzo di rete CIDR per almeno una rete a griglia.
2. Fare clic sul segno più accanto all'ultima voce per aggiungere una voce di rete aggiuntiva. Se è già stato distribuito almeno un nodo, fare clic su rileva subnet Grid Networks per compilare automaticamente l'elenco delle subnet della rete griglia con le subnet segnalate dai nodi della griglia registrati con Grid Manager.



3. Fare clic su Avanti.

Approva nodi griglia per StorageGRID

Scopri come esaminare e approvare tutti i nodi grid in sospeso che si uniscono al sistema StorageGRID.

È necessario approvare ciascun nodo griglia prima di unirsi al sistema StorageGRID.

> Prima di iniziare, tutti i nodi grid di appliance virtuali e StorageGRID devono essere implementati.

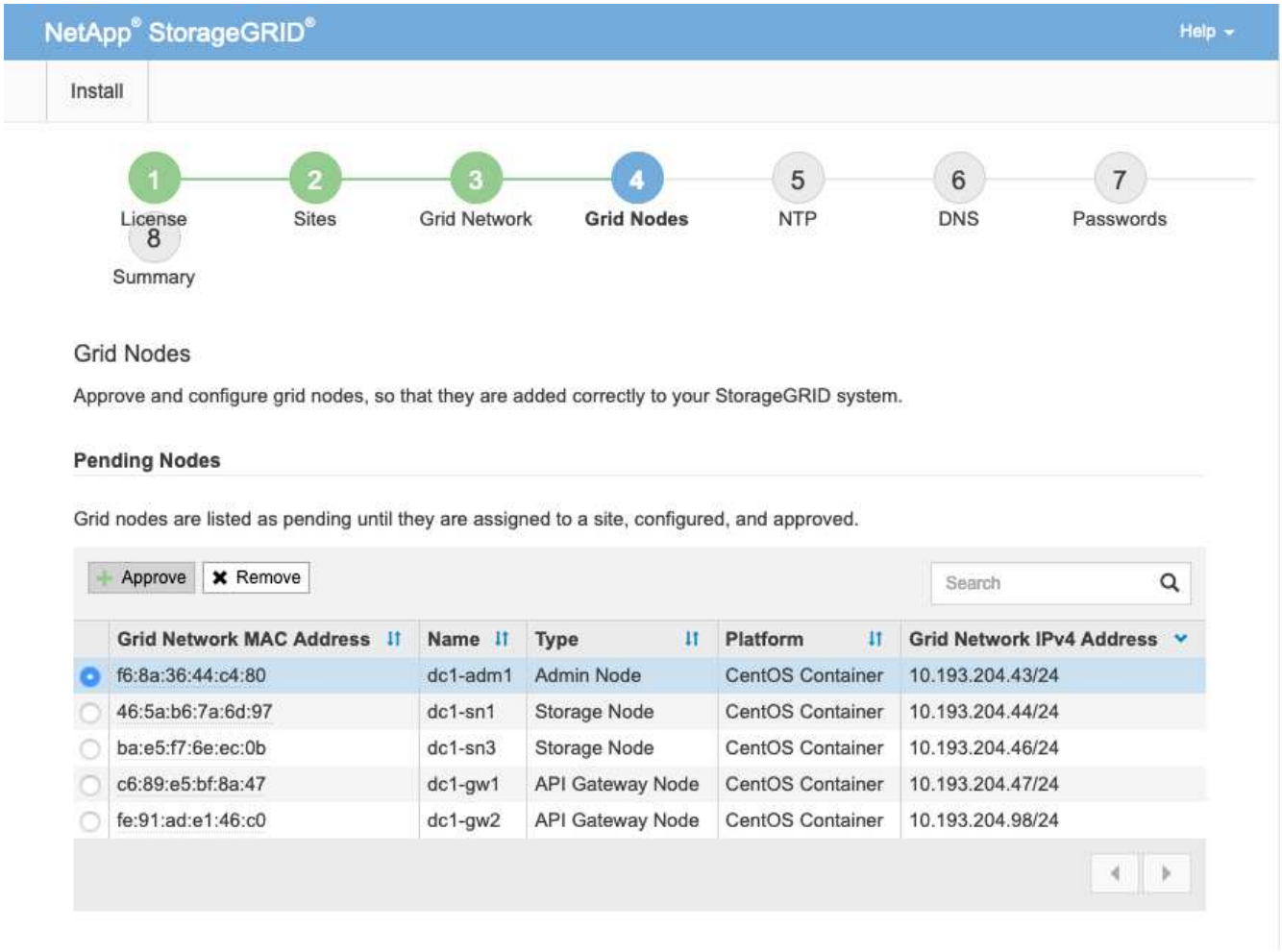
Per approvare i nodi griglia in sospeso, completare i seguenti passaggi:

Fasi

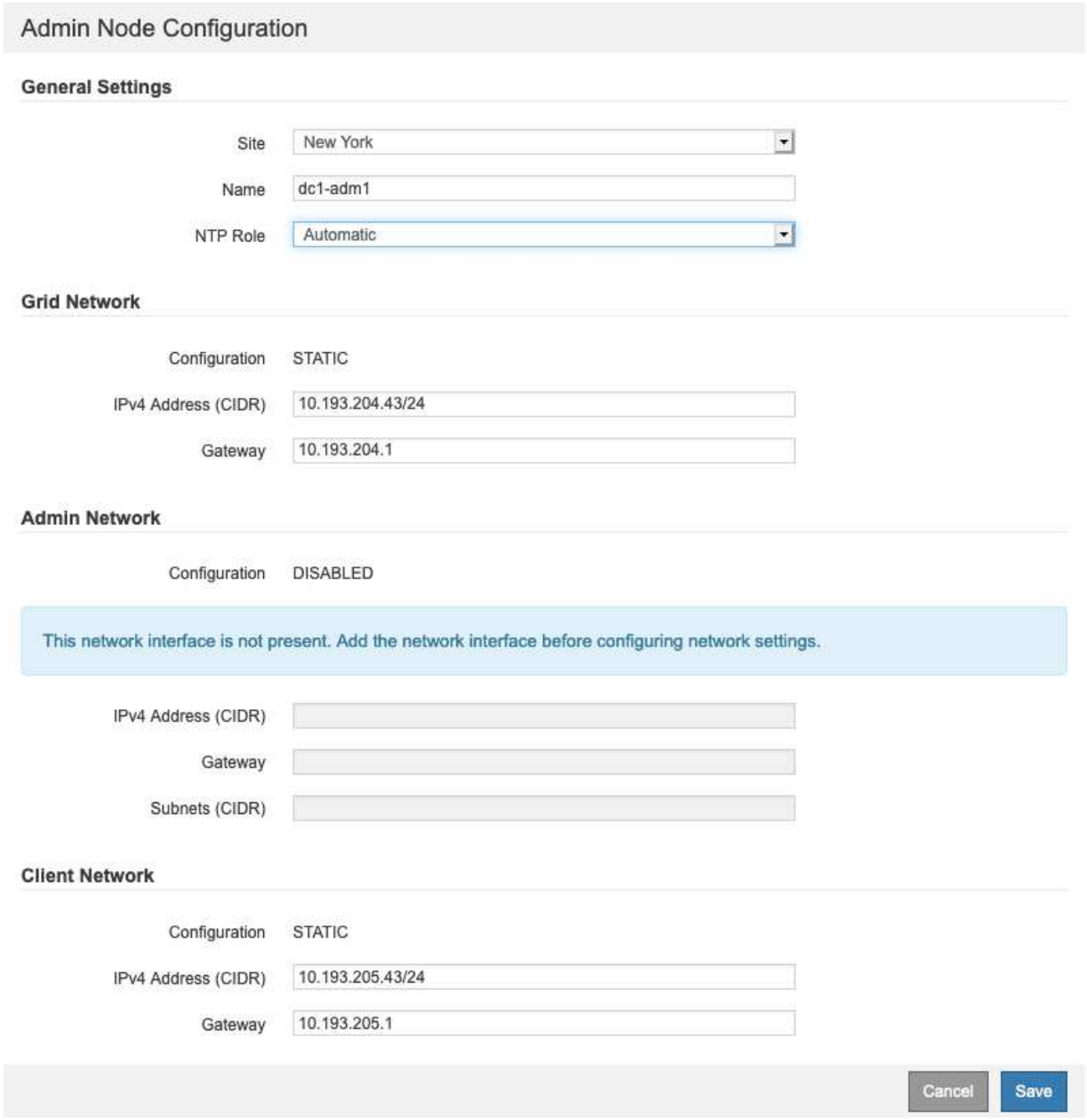
1. Esaminare l'elenco dei nodi in sospeso e verificare che visualizzi tutti i nodi della griglia distribuiti.

   > Se manca un nodo Grid, confermare che è stato implementato correttamente.

2. Fare clic sul pulsante di opzione accanto a un nodo in sospeso che si desidera approvare.



3. Fare clic su approva.
4. In Impostazioni generali, modificare le impostazioni per le seguenti proprietà, se necessario.



— **Sito**: Il nome del sistema del sito per questo nodo della griglia.

— **Nome**: Il nome host che verrà assegnato al nodo e il nome che verrà visualizzato in Grid Manager. Per impostazione predefinita, il nome è quello specificato durante la distribuzione dei nodi, ma è possibile modificarlo in base alle esigenze.

— **ruolo NTP**: Il ruolo NTP del nodo grid. Le opzioni disponibili sono Automatic (automatico), Primary (primario) e Client (Client). Selezionando l'opzione automatico, il ruolo primario viene assegnato ai nodi di amministrazione, ai nodi di archiviazione con i servizi ADC (Administrative Domain Controller), ai nodi gateway e a tutti i nodi di griglia che dispongono di indirizzi IP non statici. A tutti gli altri nodi della griglia viene assegnato il ruolo del client.

Assicurarsi che almeno due nodi di ciascun sito possano accedere ad almeno quattro origini NTP esterne. Se solo un nodo di un sito può raggiungere le origini NTP, si verificheranno problemi di tempistica se tale nodo non funziona. Inoltre, la designazione di due nodi per sito come origini NTP primarie garantisce tempi precisi se un sito viene isolato dal resto della rete.

— **Servizio ADC (solo nodi di archiviazione)**: Selezionare automatico per consentire al sistema di determinare se il nodo richiede il servizio ADC. Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi grid. Almeno tre nodi di archiviazione in ogni sito devono includere il servizio ADC. Non è possibile aggiungere il servizio ADC a un nodo dopo averlo implementato.

5. In rete griglia, modificare le impostazioni per le seguenti proprietà, se necessario:

   — **IPv4 address (CIDR)**: L'indirizzo di rete CIDR per l'interfaccia di rete di rete (eth0 all'interno del contenitore). Ad esempio, `192.168.1.234/24`.

   — **Gateway**: Il gateway di rete. Ad esempio, `192.168.0.1`.

   Se sono presenti più sottoreti di rete, è necessario il gateway.

   Se si seleziona DHCP per la configurazione della rete di rete e si modifica il valore in questo punto, il nuovo valore viene configurato come indirizzo statico sul nodo. Verificare che l'indirizzo IP risultante non sia incluso in un pool di indirizzi DHCP.

6. Per configurare la rete di amministrazione per il nodo della griglia, aggiungere o aggiornare le impostazioni nella sezione Admin Network (rete di amministrazione), se necessario.

   Inserire le subnet di destinazione dei percorsi fuori dall'interfaccia nella casella di testo subnet (CIDR). Se sono presenti più sottoreti amministrative, è necessario il gateway amministratore.

   Se si seleziona DHCP per la configurazione della rete amministrativa e si modifica il valore in questo campo, il nuovo valore viene configurato come indirizzo statico sul nodo. Verificare che l'indirizzo IP risultante non sia incluso in un pool di indirizzi DHCP.

   Dispositivi: Per un dispositivo StorageGRID, se la rete di amministrazione non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione del dispositivo StorageGRID, non è possibile configurarla in questa finestra di dialogo Gestione griglia. È invece necessario attenersi alla seguente procedura:

   a. Riavviare il dispositivo: In Appliance Installer, selezionare **Advanced › Reboot** (Avanzate[Riavvia]). Il riavvio può richiedere alcuni minuti.
   b. Selezionare **Configura rete › Configurazione collegamento** e abilitare le reti appropriate.
   c. Selezionare **Configura rete › Configurazione IP** e configurare le reti abilitate.
   d. Tornare alla Home page e fare clic su Start Installation (Avvia installazione).
   e. In Grid Manager: Se il nodo è elencato nella tabella dei nodi approvati, reimpostare il nodo.
   f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
   g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
   h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP. Per ulteriori informazioni, consultare le istruzioni

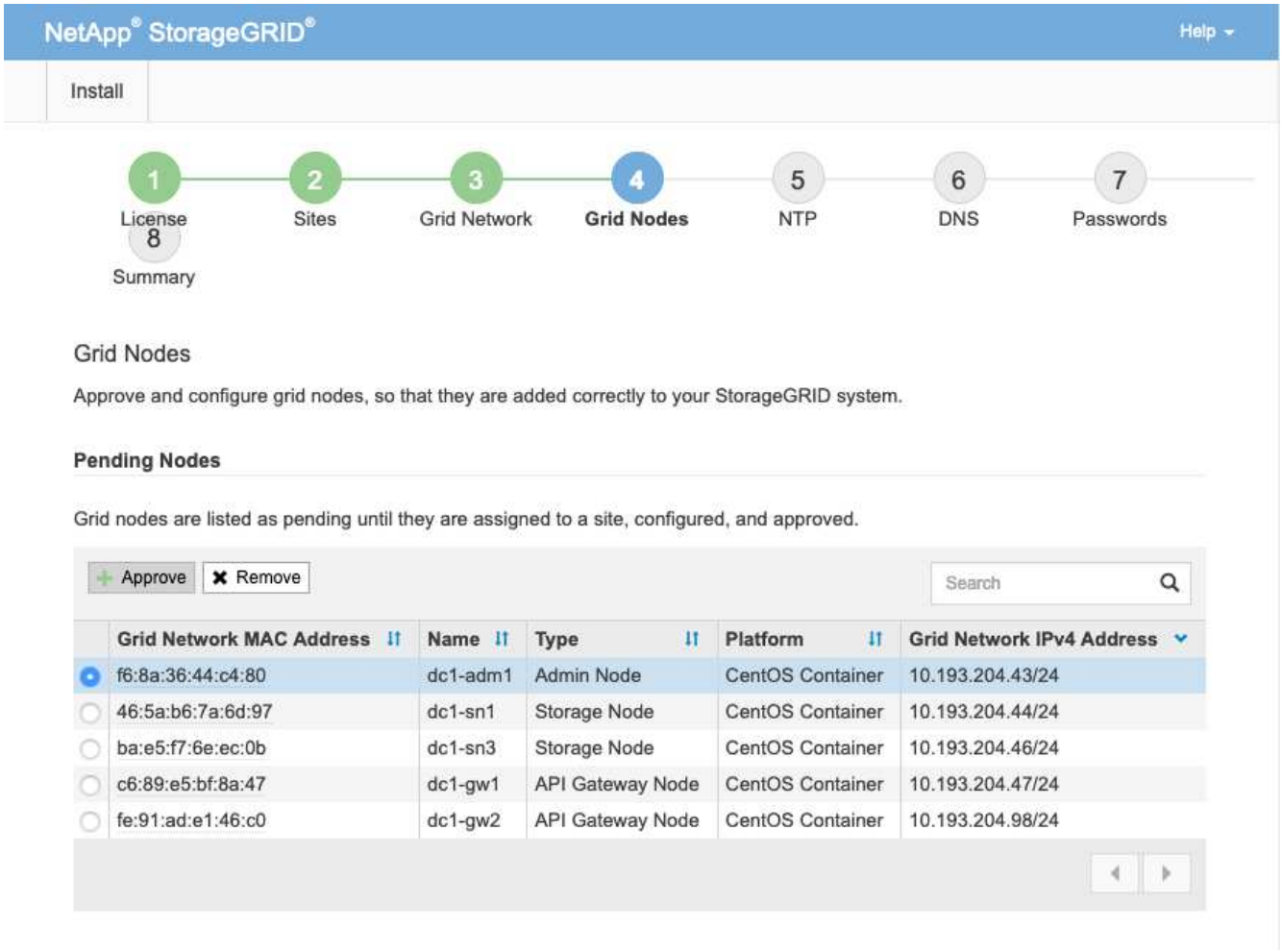
di installazione e manutenzione relative al modello di appliance in uso.

7. Se si desidera configurare la rete client per il nodo Grid, aggiungere o aggiornare le impostazioni nella sezione rete client secondo necessità. Se la rete client è configurata, il gateway è necessario e diventa il gateway predefinito per il nodo dopo l'installazione.

   Dispositivi: Per un dispositivo StorageGRID, se la rete client non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione del dispositivo StorageGRID, non è possibile configurarla in questa finestra di dialogo Gestore griglia. È invece necessario attenersi alla seguente procedura:

   a. Riavviare il dispositivo: In Appliance Installer, selezionare **Advanced › Reboot** (Avanzate[Riavvia]). Il riavvio può richiedere alcuni minuti.
   b. Selezionare **Configura rete › Configurazione collegamento** e abilitare le reti appropriate.
   c. Selezionare **Configura rete › Configurazione IP** e configurare le reti abilitate.
   d. Tornare alla Home page e fare clic su Start Installation (Avvia installazione).
   e. In Grid Manager: Se il nodo è elencato nella tabella dei nodi approvati, reimpostare il nodo.
   f. Rimuovere il nodo dalla tabella Pending Nodes (nodi in sospeso).
   g. Attendere che il nodo riappaia nell'elenco Pending Nodes (nodi in sospeso).
   h. Confermare che è possibile configurare le reti appropriate. Devono essere già popolate con le informazioni fornite nella pagina di configurazione IP. Per ulteriori informazioni, consultare le istruzioni di installazione e manutenzione dell'apparecchio.

8. Fare clic su Salva. La voce del nodo della griglia viene spostata nell'elenco dei nodi approvati.



9. Ripetere i passaggi 1-8 per ogni nodo griglia in sospeso che si desidera approvare.

   È necessario approvare tutti i nodi desiderati nella griglia. Tuttavia, è possibile tornare a questa pagina in qualsiasi momento prima di fare clic su Installa nella pagina Riepilogo. Per modificare le proprietà di un nodo griglia approvato, fare clic sul relativo pulsante di opzione, quindi fare clic su Modifica.

10. Dopo aver approvato i nodi della griglia, fare clic su Avanti.

Specificare i dettagli del server NTP per StorageGRID

Informazioni su come specificare le informazioni di configurazione NTP per il sistema StorageGRID in modo che le operazioni eseguite su server separati possano essere mantenute sincronizzate.

Per evitare problemi di deriva temporale, è necessario specificare quattro riferimenti server NTP esterni dello strato 3 o superiore.

> Quando si specifica l'origine NTP esterna per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time nelle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'uso in ambienti complessi come StorageGRID.

I server NTP esterni vengono utilizzati dai nodi ai quali sono stati precedentemente assegnati i ruoli NTP

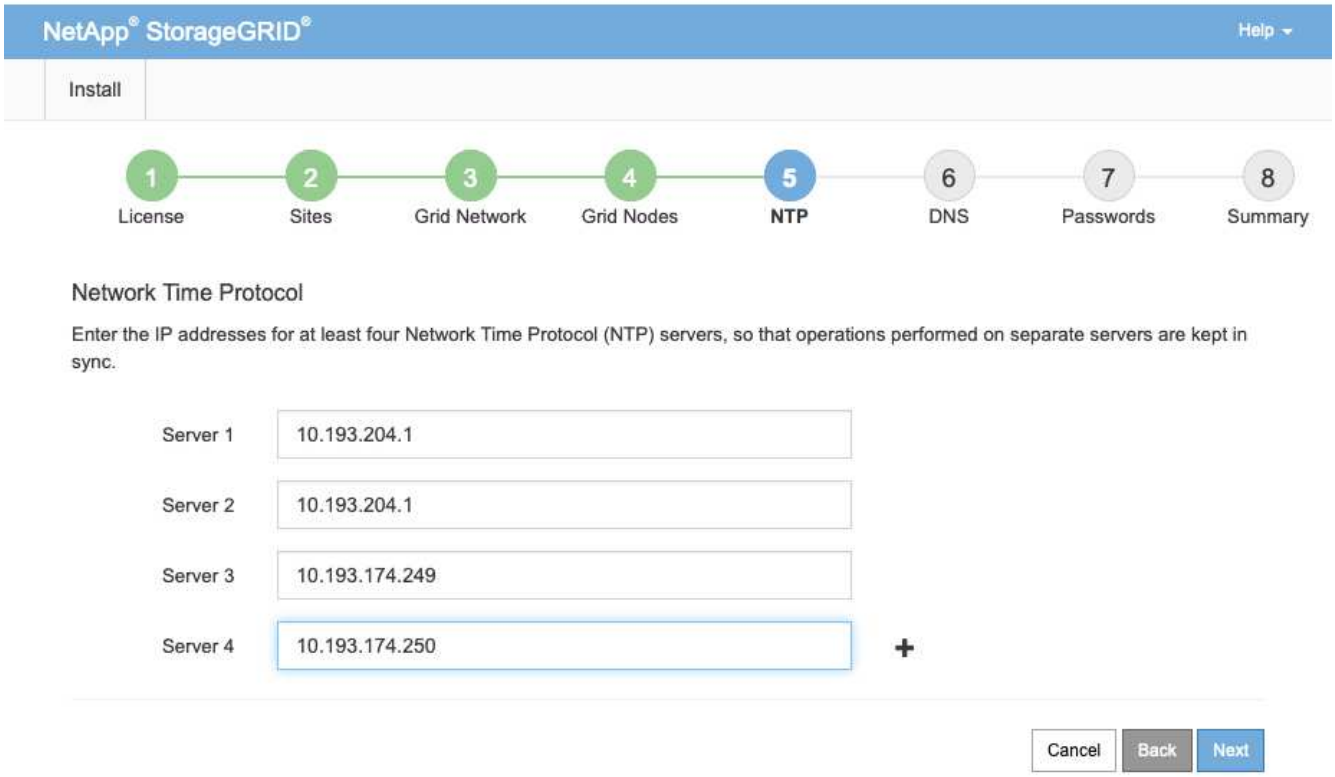
primari.

> La rete client non è abilitata abbastanza presto nel processo di installazione per essere l'unica fonte di server NTP. Assicurarsi che almeno un server NTP possa essere raggiunto sulla rete di rete o sulla rete amministrativa.

Per specificare le informazioni sul server NTP, attenersi alla seguente procedura:

Fasi

1. Nelle caselle di testo Server 1 to Server 4 (Server 1 - Server 2), specificare gli indirizzi IP per almeno quattro server NTP.
2. Se necessario, fare clic sul segno più accanto all'ultima voce per aggiungere altre voci al server.



3. Fare clic su Avanti.

Specificare i dettagli del server DNS per StorageGRID

Informazioni su come configurare il server DNS per StorageGRID.

È necessario specificare le informazioni DNS per il sistema StorageGRID in modo da poter accedere ai server esterni utilizzando nomi host invece di indirizzi IP.

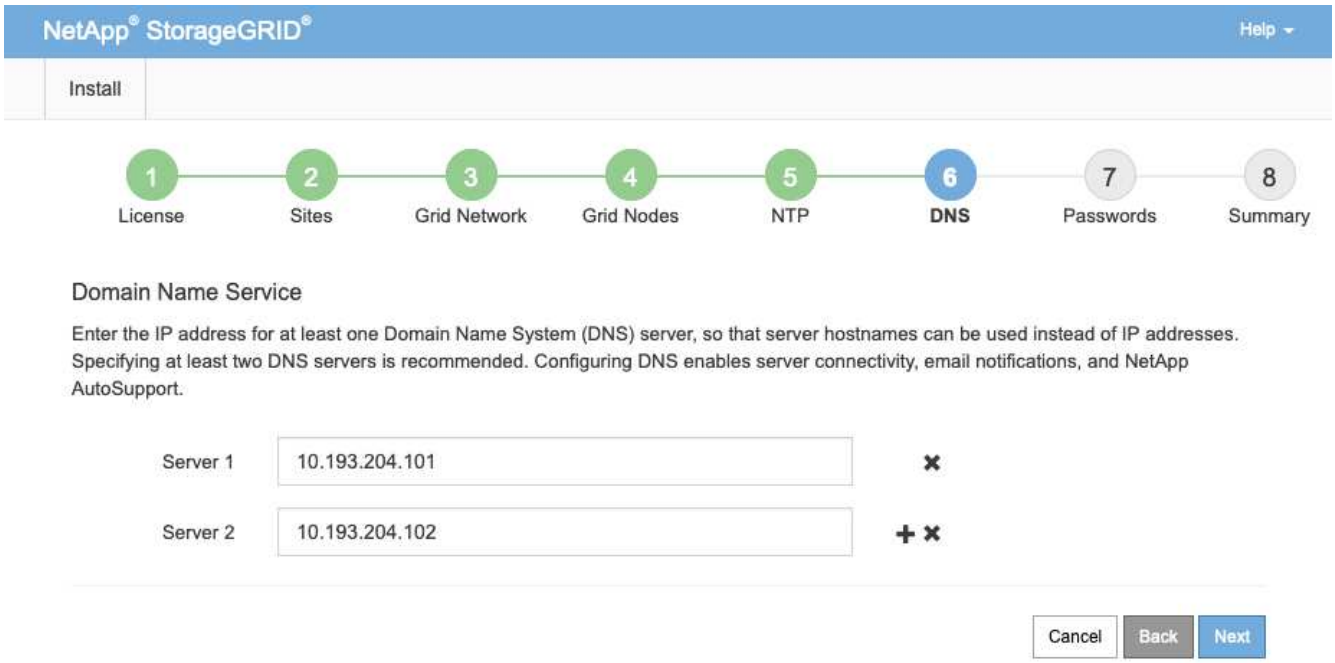
La specifica delle informazioni sul server DNS consente di utilizzare nomi host FQDN (Fully Qualified Domain Name) anziché indirizzi IP per le notifiche e-mail e i messaggi NetApp AutoSupport®. NetApp consiglia di specificare almeno due server DNS.

> Selezionare i server DNS ai quali ciascun sito può accedere localmente in caso di rete.

Per specificare le informazioni sul server DNS, attenersi alla procedura illustrata di seguito:

Fasi

1. Nella casella di testo Server 1, specificare l'indirizzo IP di un server DNS.
2. Se necessario, fare clic sul segno più accanto all'ultima voce per aggiungere altri server.



3. Fare clic su Avanti.

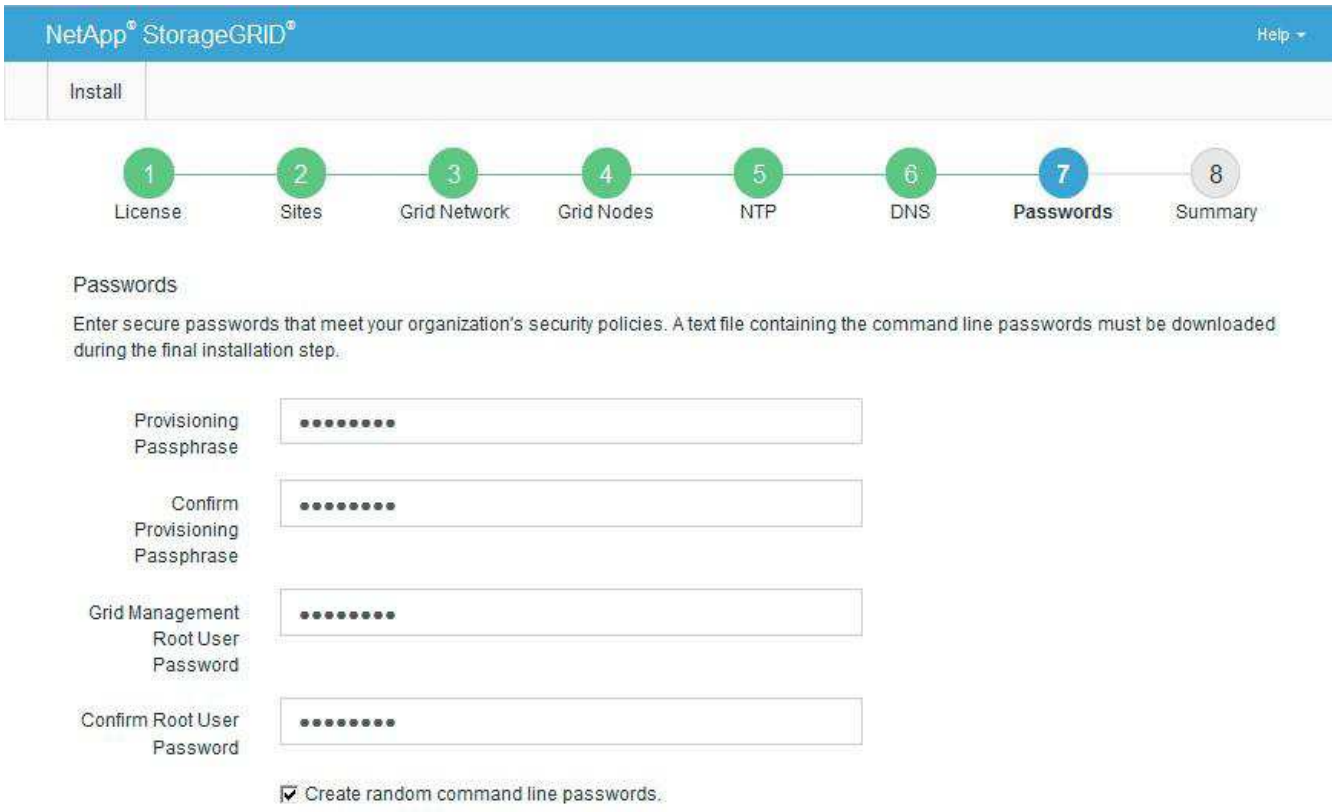
Specificare le password di sistema per StorageGRID

Scoprite come proteggere il vostro sistema StorageGRID impostando la passphrase di provisioning e la password utente root di gestione delle griglie.

Per immettere le password da utilizzare per proteggere il sistema StorageGRID, attenersi alla seguente procedura:

Fasi

1. In Provisioning Passphrase, immettere la passphrase di provisioning necessaria per apportare modifiche alla topologia della griglia del sistema StorageGRID. Registrare la password in un luogo sicuro.
2. In Confirm Provisioning Passphrase (Conferma passphrase di provisioning), immettere nuovamente la passphrase di provisioning.
3. In Grid Management Root User Password (Password utente principale di Grid Management), immettere la password da utilizzare per accedere a Grid Manager come utente root.
4. In Confirm Root User Password (Conferma password utente root), immettere nuovamente la password di Grid Manager.



5. Se si sta installando una griglia per scopi dimostrativi o dimostrativi, deselezionare l'opzione Crea password della riga di comando casuale.

   Per le implementazioni in produzione, le password casuali devono essere sempre utilizzate per motivi di sicurezza. Deselezionare l'opzione Create Random Command Line Passwords (Crea password casuali della riga di comando) solo per le griglie demo se si desidera utilizzare password predefinite per accedere ai nodi della griglia dalla riga di comando utilizzando l'account root o admin.

   > Quando si fa clic su Installa nella pagina Riepilogo, viene richiesto di scaricare il file del pacchetto di ripristino (`sgws-recovery-packageid-revision.zip`. È necessario scaricare questo file per completare l'installazione. Le password di accesso al sistema vengono memorizzate nel `Passwords.txt` file contenuto nel pacchetto di ripristino.

6. Fare clic su Avanti.

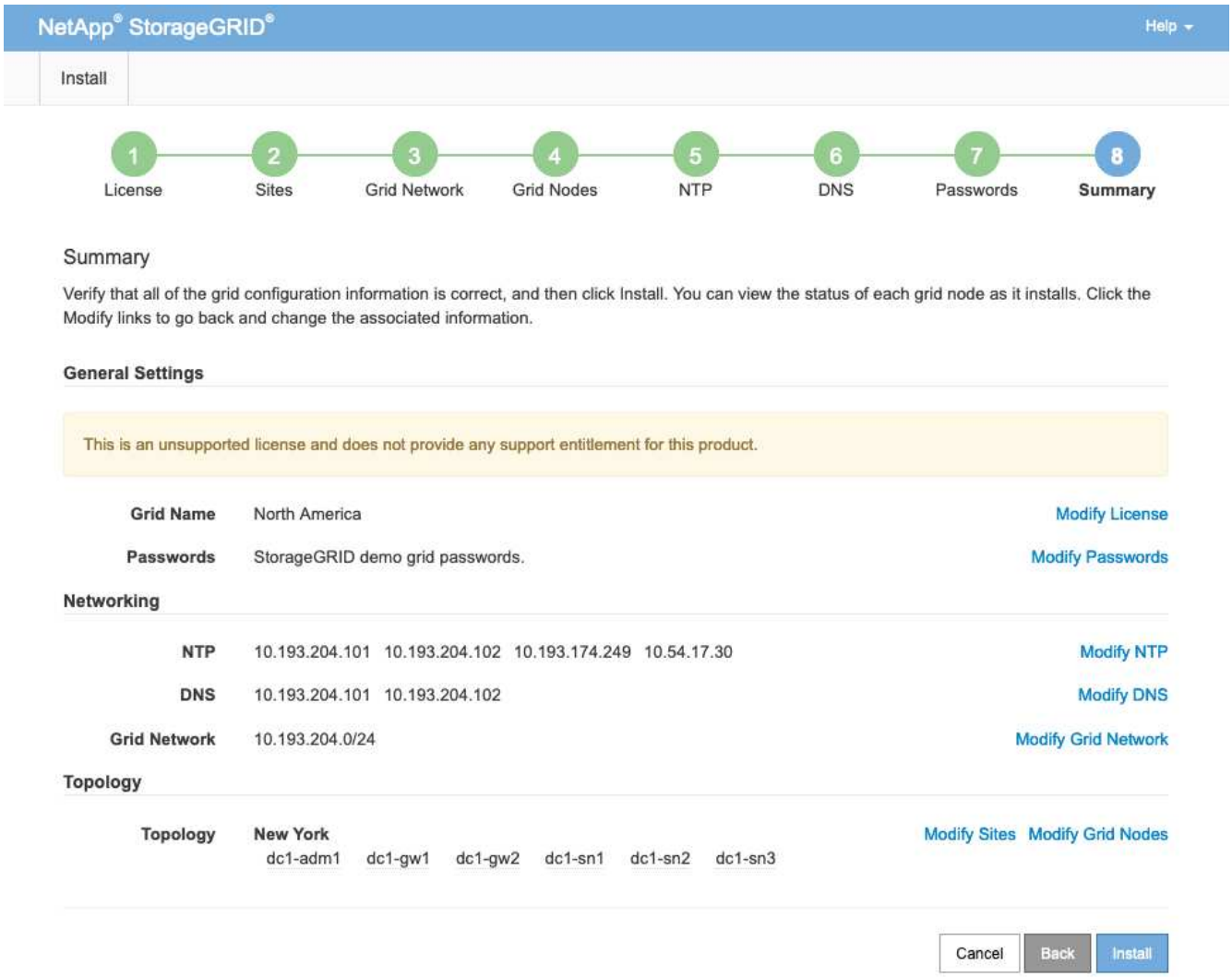
Rivedere la configurazione e completare l'installazione di StorageGRID

Scopri come convalidare le informazioni di configurazione della griglia e completare il processo di installazione di StorageGRID.

Per assicurarsi che l'installazione venga completata correttamente, esaminare attentamente le informazioni di configurazione immesse. Seguire questa procedura.

Fasi

1. Visualizzare la pagina Riepilogo.



2. Verificare che tutte le informazioni di configurazione della griglia siano corrette. Utilizzare i link Modify (Modifica) nella pagina Summary (Riepilogo) per tornare indietro e correggere eventuali errori.
3. Fare clic su Installa.

> Se un nodo è configurato per l'utilizzo della rete client, il gateway predefinito per quel nodo passa dalla rete griglia alla rete client quando si fa clic su Installa. Se si perde la connettività, assicurarsi di accedere al nodo amministrativo primario tramite una subnet accessibile. Per ulteriori informazioni, vedere "Installazione e provisioning della rete".

4. Fare clic su Scarica pacchetto di ripristino.

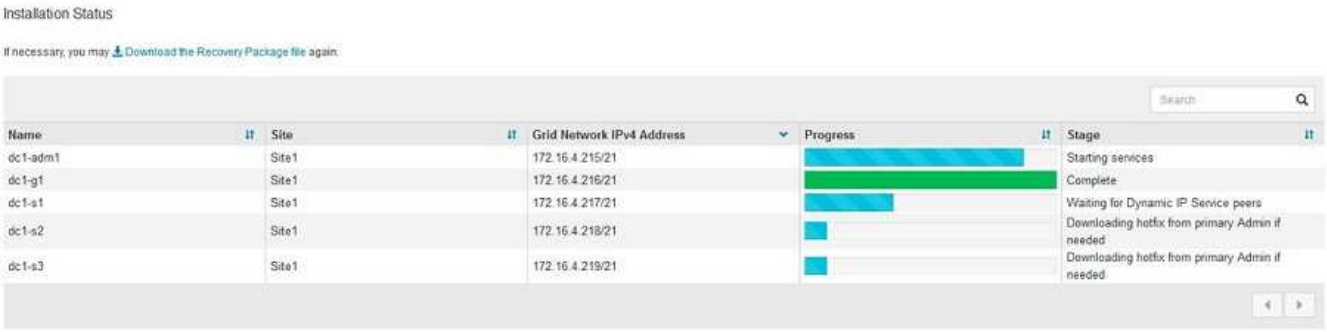
   Quando l'installazione procede fino al punto in cui è definita la topologia della griglia, viene richiesto di scaricare il file del pacchetto di ripristino (`.zip`) e di confermare che è possibile accedere al contenuto di questo file. È necessario scaricare il file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di errore di uno o più nodi della griglia.

   Verificare che sia possibile estrarre il contenuto del `.zip` file e salvarlo in due posizioni sicure, sicure e separate.

> Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

5. Selezionare l'opzione ho scaricato e verificato il file del pacchetto di ripristino, quindi fare clic su Avanti.

Se l'installazione è ancora in corso, viene visualizzata la pagina Stato installazione. Questa pagina indica lo stato di avanzamento dell'installazione per ciascun nodo della griglia.



Quando viene raggiunta la fase completa per tutti i nodi della griglia, si apre la pagina di accesso per Grid Manager.

6. Accedere a Grid Manager come utente root con la password specificata durante l'installazione.

Aggiorna i nodi bare-metal in StorageGRID

Scopri il processo di upgrade per i nodi bare-metal in StorageGRID.

Il processo di upgrade per i nodi bare-metal è diverso rispetto ad appliance o nodi VMware. Prima di eseguire un aggiornamento di un nodo bare-metal, è necessario aggiornare i file RPM su tutti gli host prima di eseguire l'aggiornamento tramite la GUI.

```
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Images-*.rpm
[root@host1 rpms]# rpm -Uvh StorageGRID-Webscale-Service-*.rpm
```

A questo punto è possibile procedere all'aggiornamento del software tramite la GUI.

TR-4907: Configurare StorageGRID con veritas Enterprise Vault

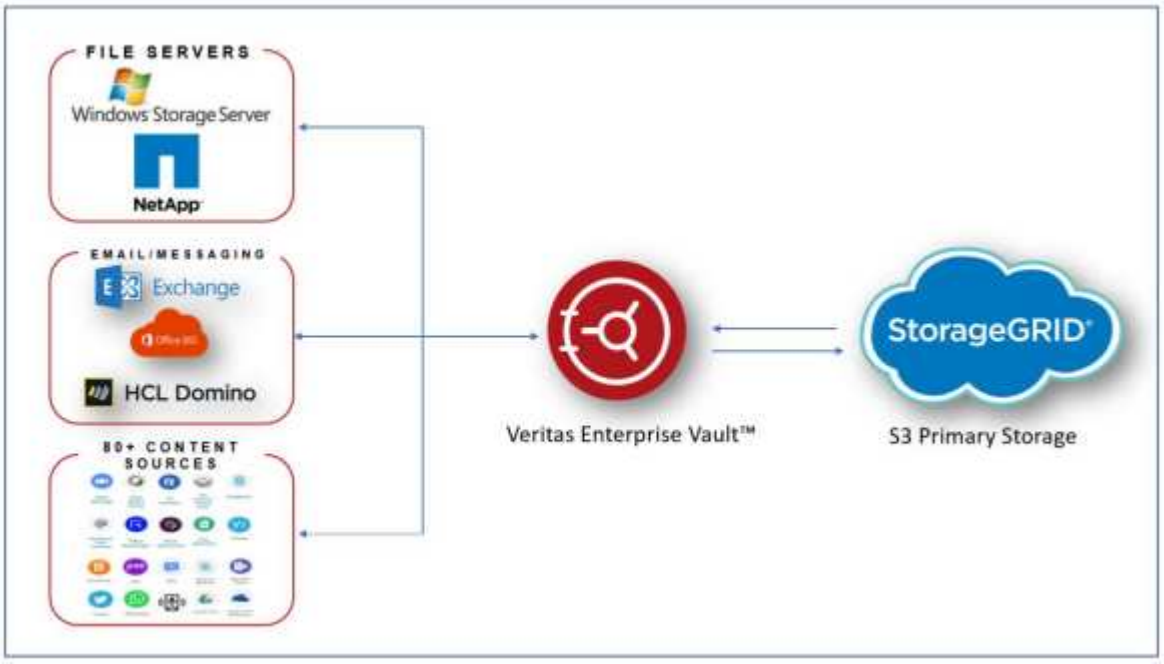
Introduzione alla configurazione di StorageGRID per il failover del sito

Scopri come veritas Enterprise Vault utilizza StorageGRID come destinazione di storage primario per il disaster recovery.

Questa guida alla configurazione fornisce i passaggi per configurare NetApp® StorageGRID® come destinazione di storage primario con veritas Enterprise Vault. Viene inoltre descritto come configurare StorageGRID per il failover del sito in uno scenario di disaster recovery (DR).

Architettura di riferimento

StorageGRID offre una destinazione di backup cloud on-premise compatibile con S3 per veritas Enterprise Vault. La figura seguente illustra l'architettura di veritas Enterprise Vault e StorageGRID.



Dove trovare ulteriori informazioni

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

- Centro di documentazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Abilitazione NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Configurare StorageGRID e veritas Enterprise Vault

Scopri come implementare le configurazioni di base per StorageGRID 11,5 o versioni successive e veritas Enterprise Vault 14,1 o versioni successive.

Questa guida alla configurazione si basa su StorageGRID 11,5 e Enterprise Vault 14,1. Per lo storage in modalità write once, Read many (WORM) utilizzando blocco degli oggetti S3, StorageGRID 11,6 ed Enterprise Vault 14.2.2. Per informazioni più dettagliate su queste linee guida, visitare la "Documentazione StorageGRID" pagina o contattare un esperto StorageGRID.

Prerequisiti per configurare StorageGRID e veritas Enterprise Vault

- Prima di configurare StorageGRID con veritas Enterprise Vault, verificare i seguenti prerequisiti:

> Per lo storage WORM (blocco oggetti) è richiesto StorageGRID 11,6 o superiore.

- È installato veritas Enterprise Vault 14,1 o versione successiva.

> Per lo storage WORM (blocco degli oggetti), è richiesto Enterprise Vault versione 14.2.2 o superiore.

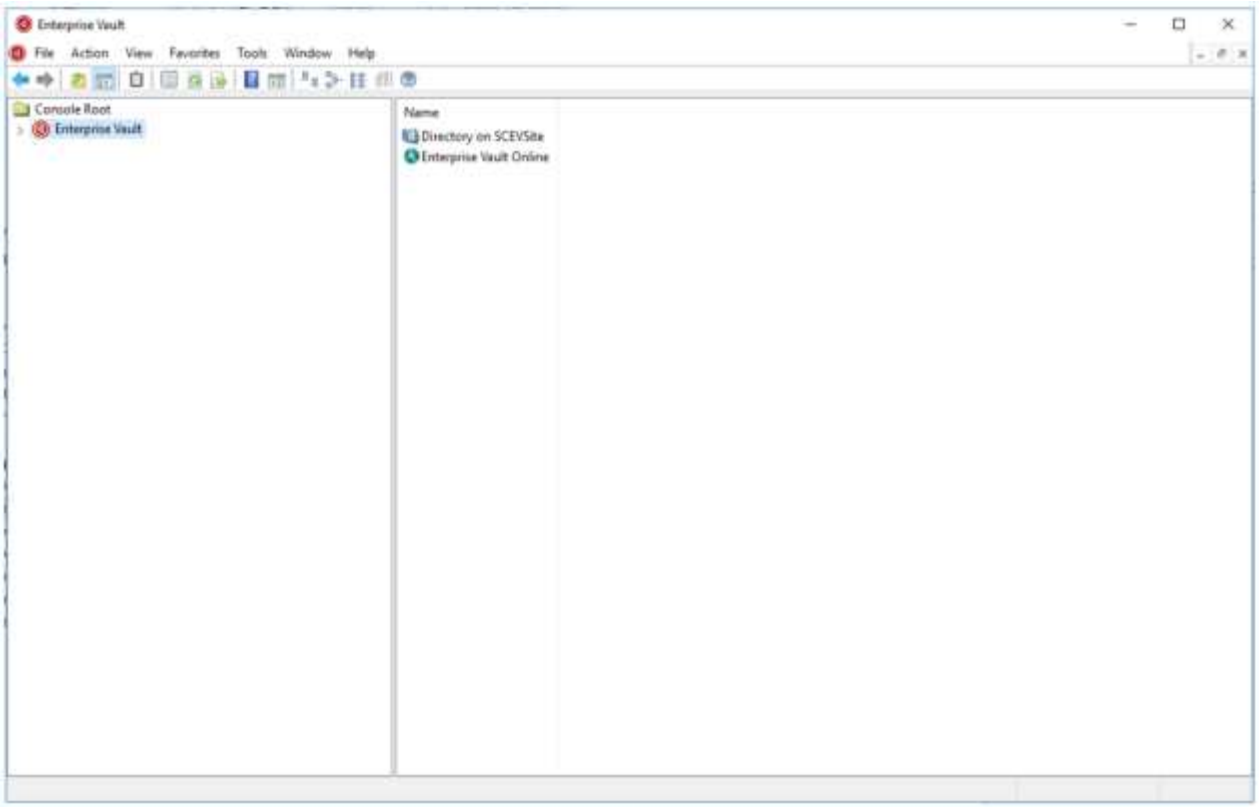
- Sono stati creati gruppi di archivi del vault e un archivio del vault. Per ulteriori informazioni, vedere veritas Enterprise Vault Administration Guide.
- Sono stati creati tenant StorageGRID, chiave di accesso, chiave segreta e bucket.
- È stato creato un endpoint di bilanciamento del carico StorageGRID (HTTP o HTTPS).
- Se si utilizza un certificato autofirmato, aggiungere il certificato CA autofirmato StorageGRID ai server di Enterprise Vault. Per ulteriori informazioni, vedere questo "Articolo della veritas Knowledge base".
- Aggiornare e applicare il file di configurazione del vault Enterprise più recente per abilitare le soluzioni di storage supportate, come NetApp StorageGRID. Per ulteriori informazioni, vedere questo "Articolo della veritas Knowledge base".

Configurare StorageGRID con veritas Enterprise Vault

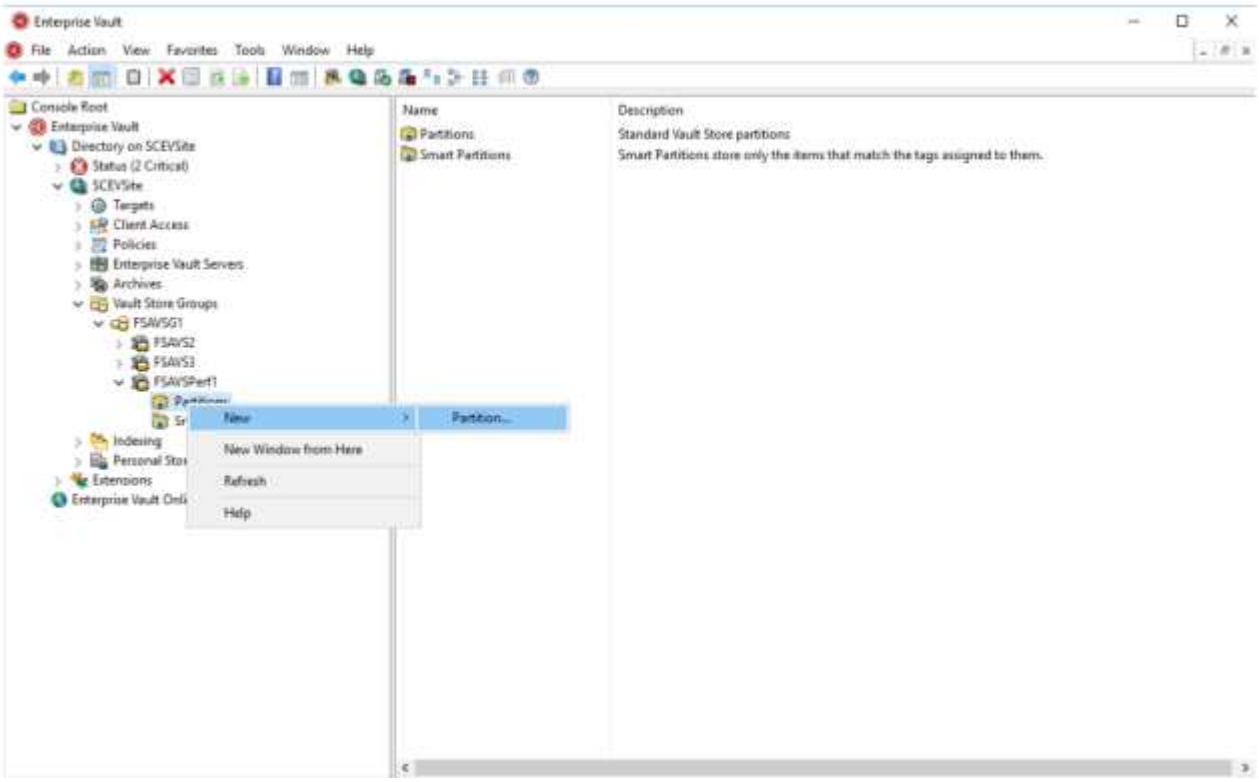
Per configurare StorageGRID con veritas Enterprise Vault, attenersi alla seguente procedura:

Fasi

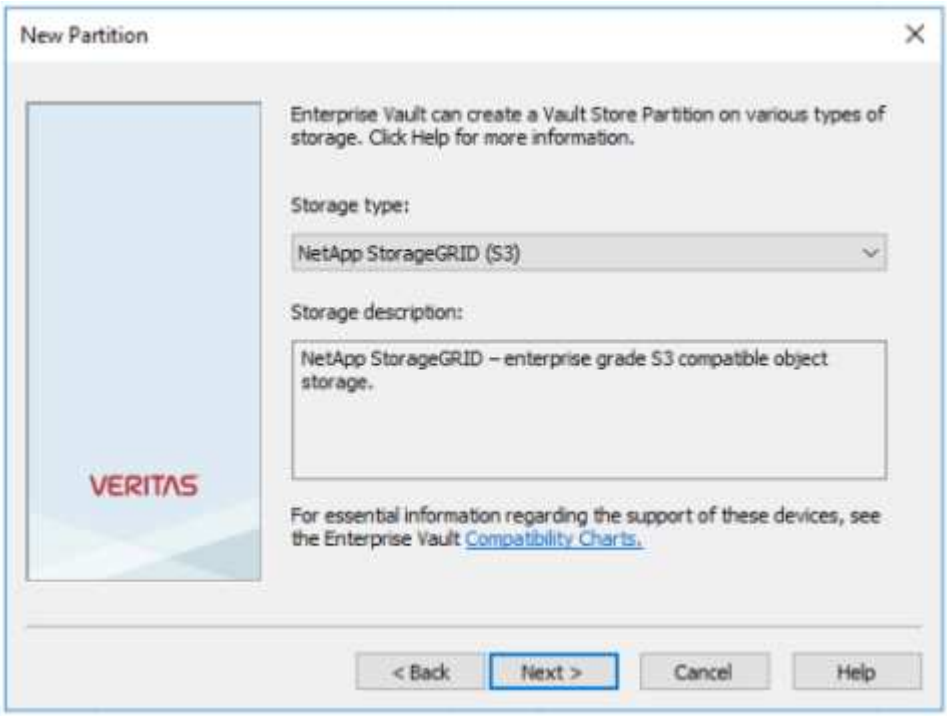
1. Avviare la console di amministrazione di Enterprise Vault.



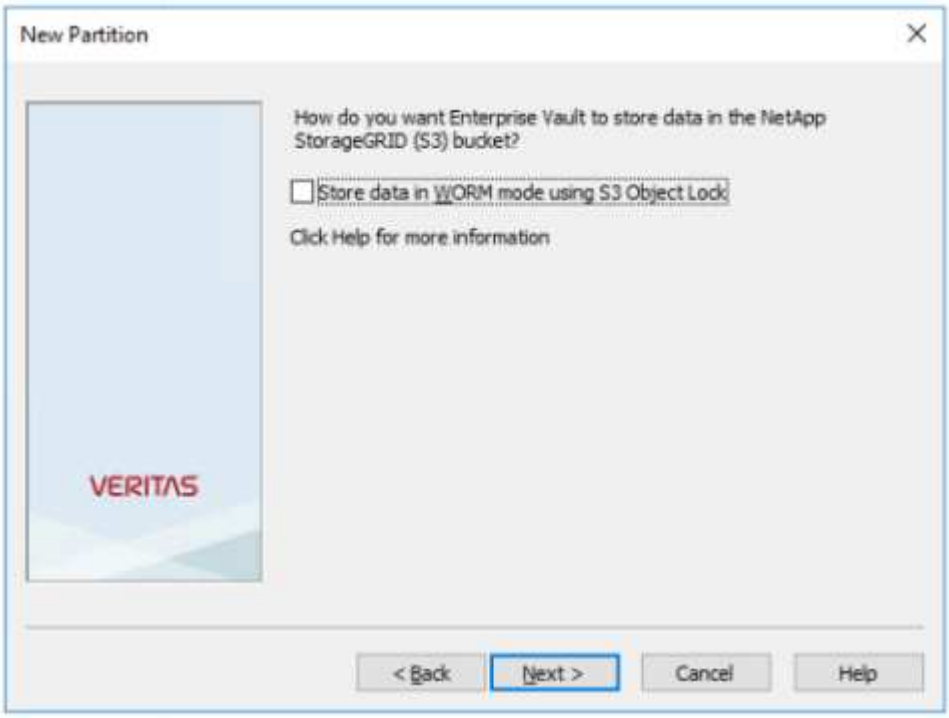
2. Creare una nuova partizione dell'archivio dei vault nell'archivio appropriato. Espandere la cartella Vault Store Groups e quindi l'archivio del vault appropriato. Fare clic con il pulsante destro del mouse su partizione e selezionare **Nuova › partizione**.



3. Seguire la procedura guidata creazione nuova partizione. Dal menu a discesa tipo di archiviazione, selezionare NetApp StorageGRID (S3). Fare clic su Avanti.

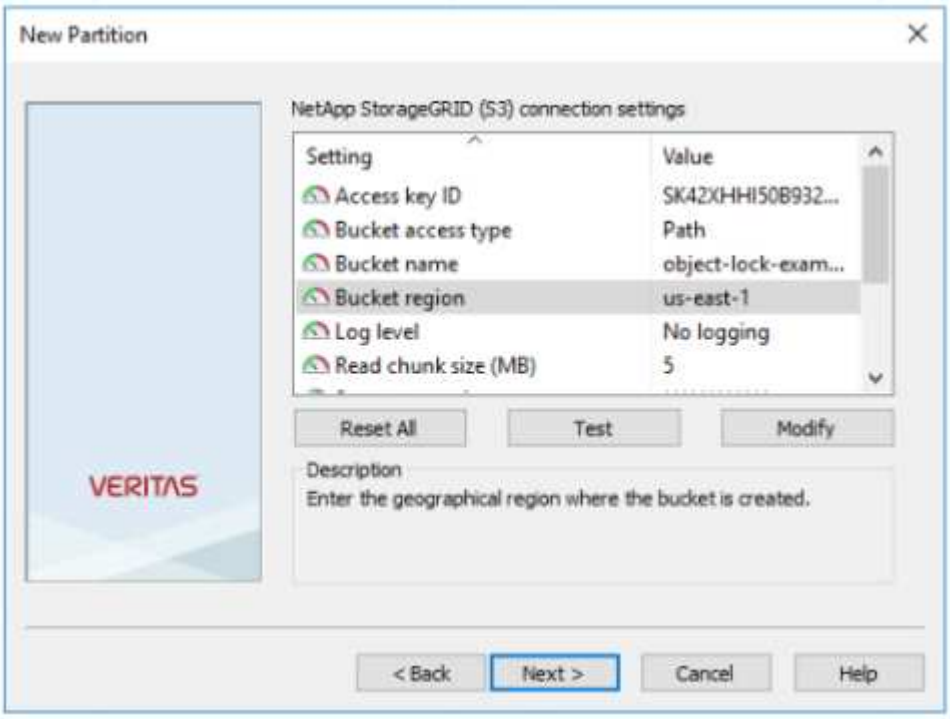


4. Lasciare deselezionata l'opzione Memorizza dati in modalità WORM utilizzando blocco oggetti S3. Fare clic su Avanti.

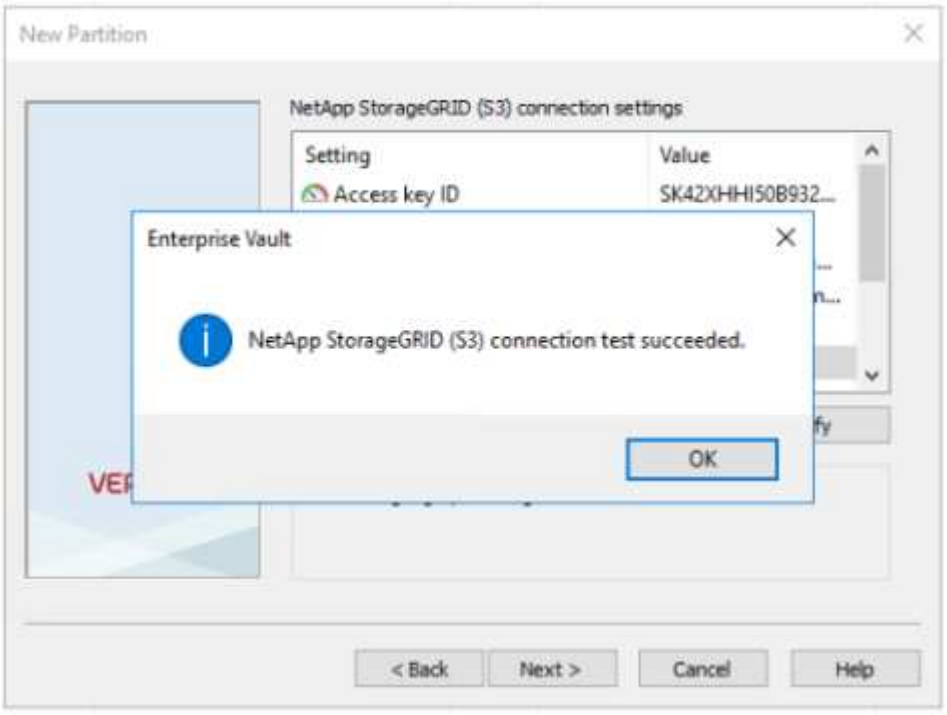


5. Nella pagina delle impostazioni di connessione, fornire le seguenti informazioni:
   - ID chiave di accesso
   - Chiave di accesso segreta
   - Nome host del servizio: Assicurarsi di includere la porta LBE (Load Balancer Endpoint) configurata in StorageGRID (ad esempio https://<hostname>:<LBE_port>)

- Nome bucket: Nome del bucket di destinazione creato in precedenza. veritas Enterprise Vault non crea il bucket.
- Area bucket: `us-east-1` È il valore predefinito.

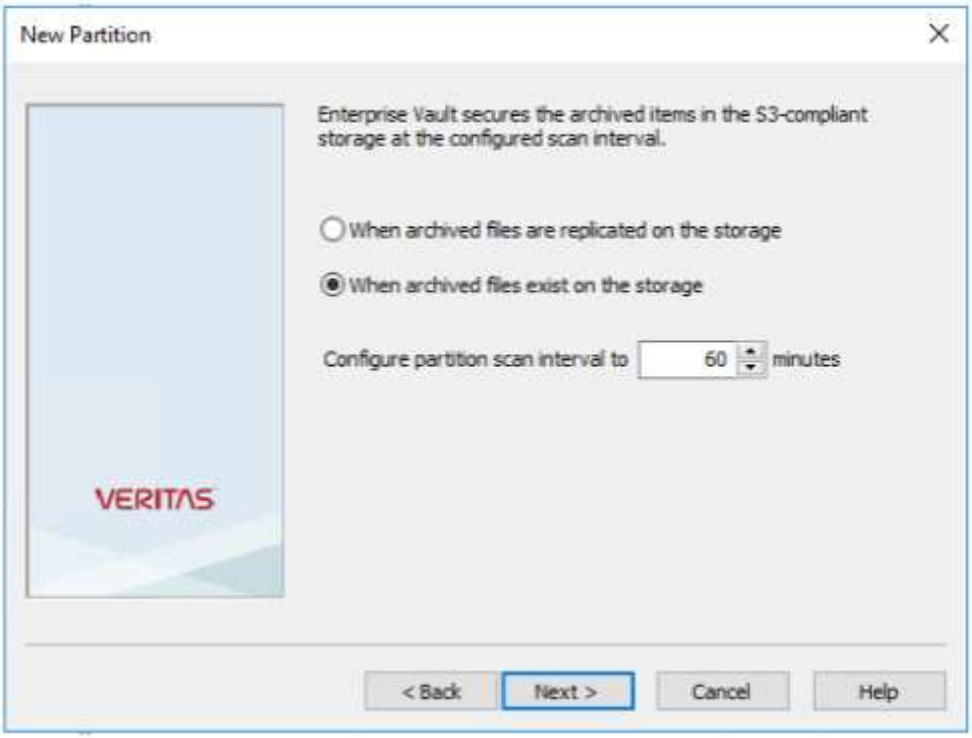


6. Per verificare il collegamento al bucket StorageGRID, fare clic su Test. Verificare che il test di connessione sia stato eseguito correttamente. Fare clic su OK, quindi su Next (Avanti).

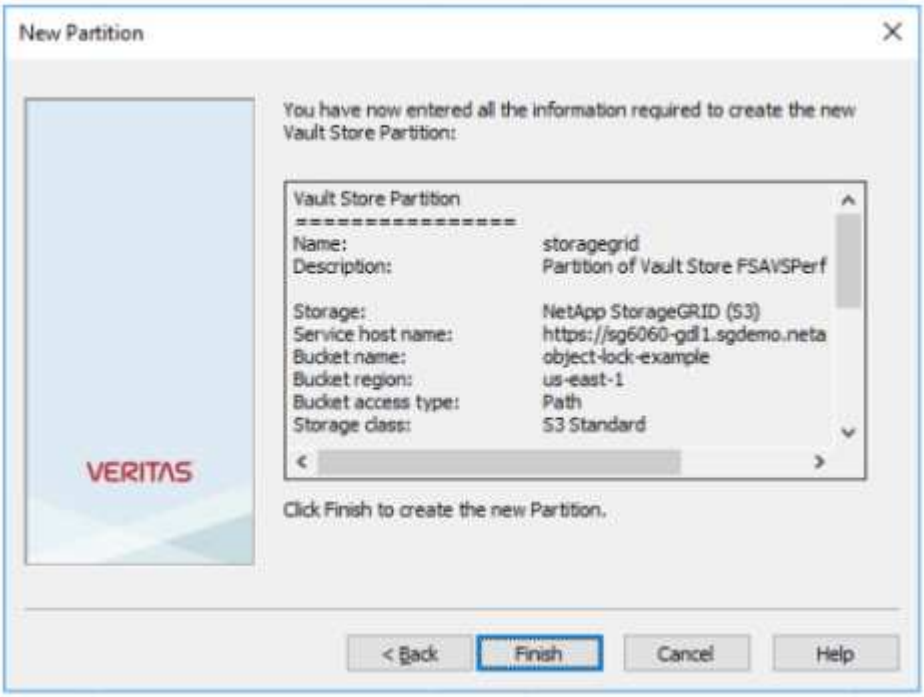


7. StorageGRID non supporta il parametro di replica S3. Per proteggere gli oggetti, StorageGRID utilizza le regole ILM (Information Lifecycle Management) per specificare schemi di protezione dei dati: Copie multiple o erasure coding. Selezionare l'opzione quando esistono file archiviati nell'archiviazione e fare clic

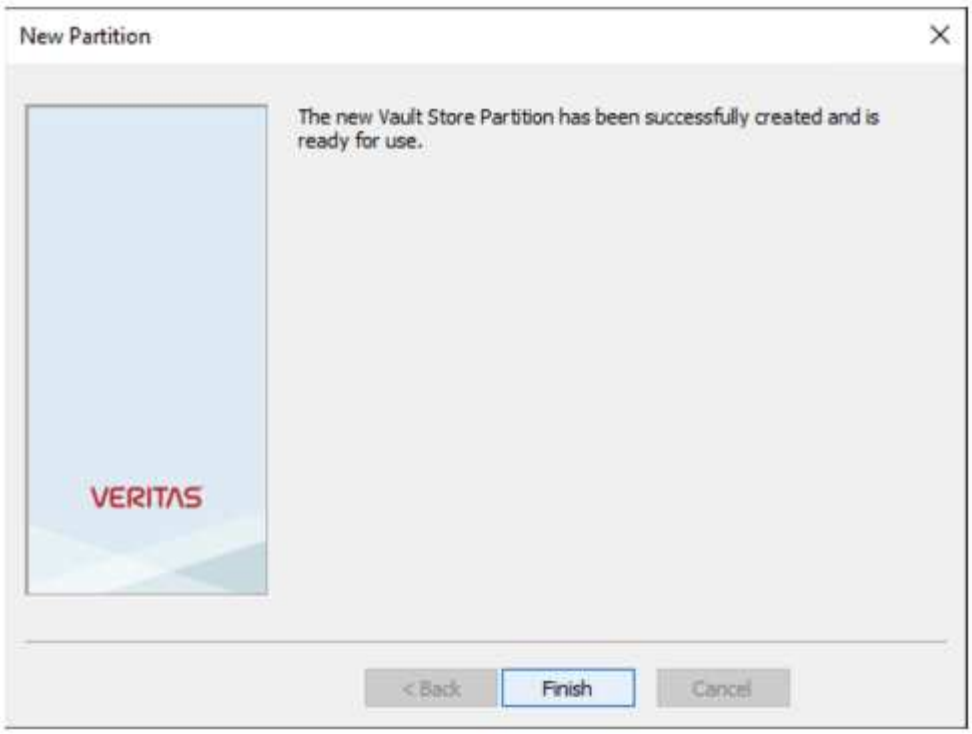
su Avanti.



8. Verificare le informazioni nella pagina di riepilogo e fare clic su fine.



9. Una volta creata la nuova partizione dell'archivio vault, è possibile archiviare, ripristinare e cercare i dati in Enterprise Vault con StorageGRID come storage primario.



Configurare il blocco degli oggetti StorageGRID S3 per lo storage WORM

Scopri come configurare StorageGRID per lo storage WORM utilizzando blocco oggetti S3.

Prerequisiti per configurare StorageGRID per lo storage WORM

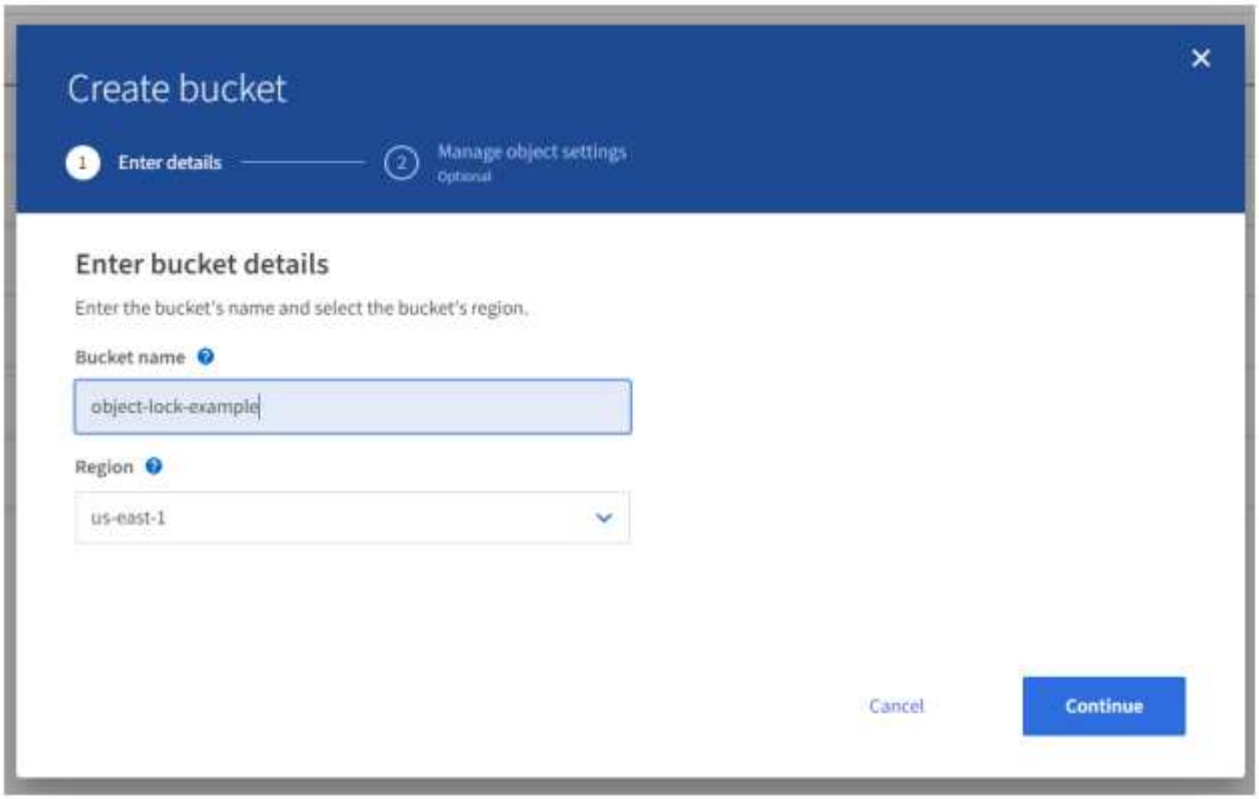
Per lo storage WORM, StorageGRID utilizza il blocco degli oggetti S3 per mantenere gli oggetti per la conformità. Ciò richiede StorageGRID 11,6 o superiore, in cui è stata introdotta la conservazione predefinita del bucket blocco oggetti S3. Enterprise Vault richiede anche la versione 14.2.2 o superiore.

Configurare la conservazione predefinita del bucket di blocco oggetti StorageGRID S3

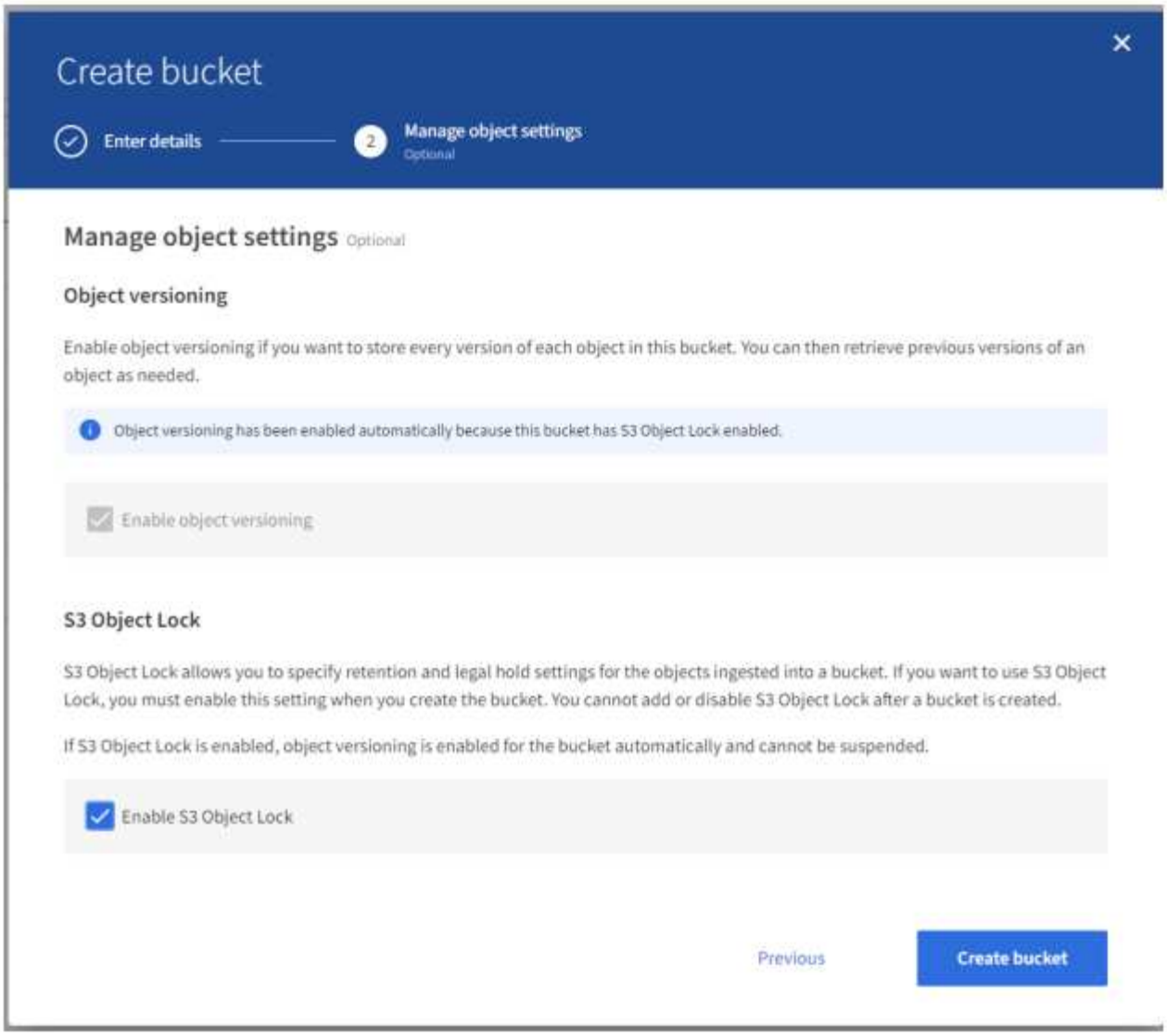
Per configurare la conservazione predefinita del bucket di blocco degli oggetti StorageGRID S3, attenersi alla seguente procedura:

Fasi

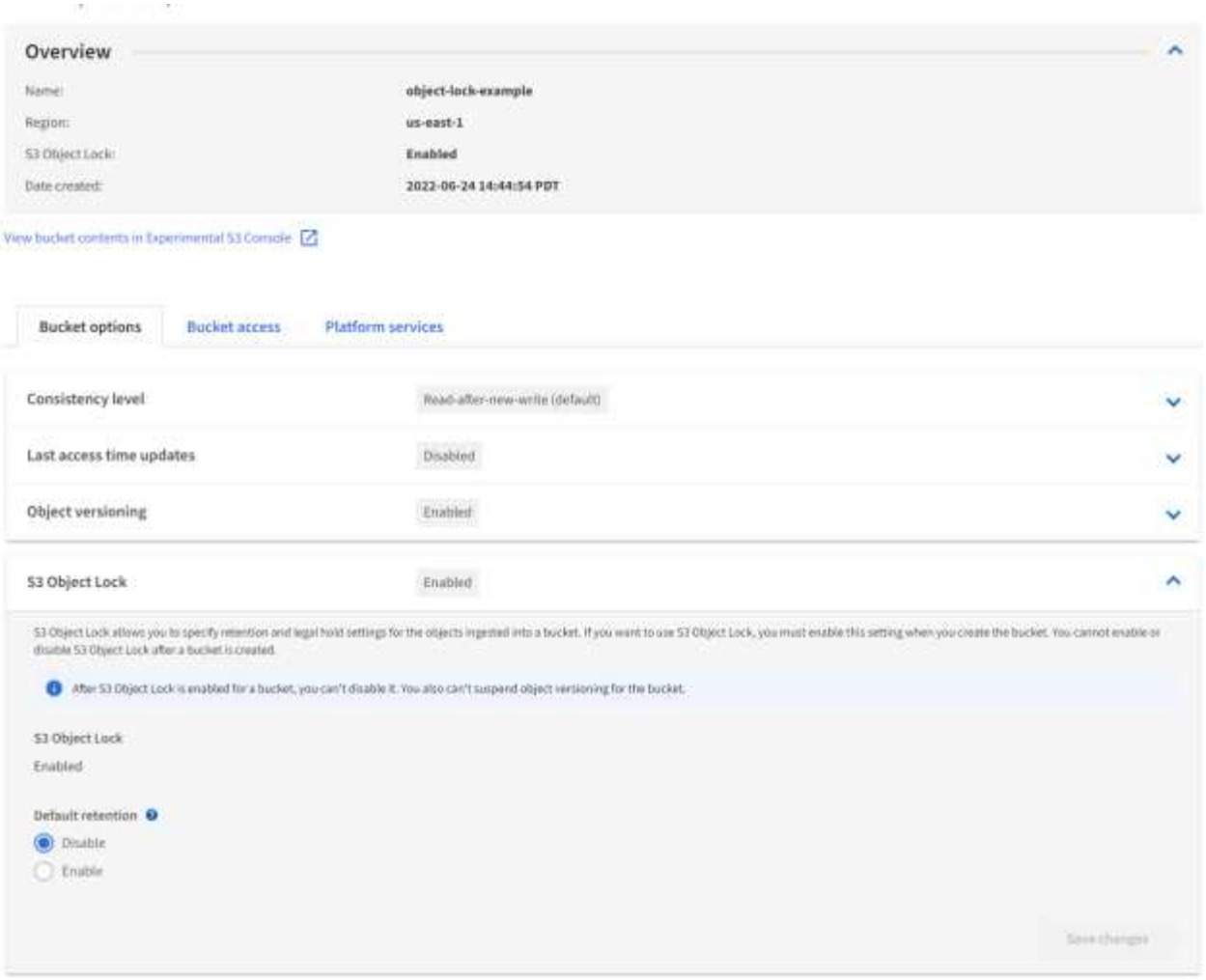
1. In Gestione tenant StorageGRID, creare un bucket e fare clic su continua



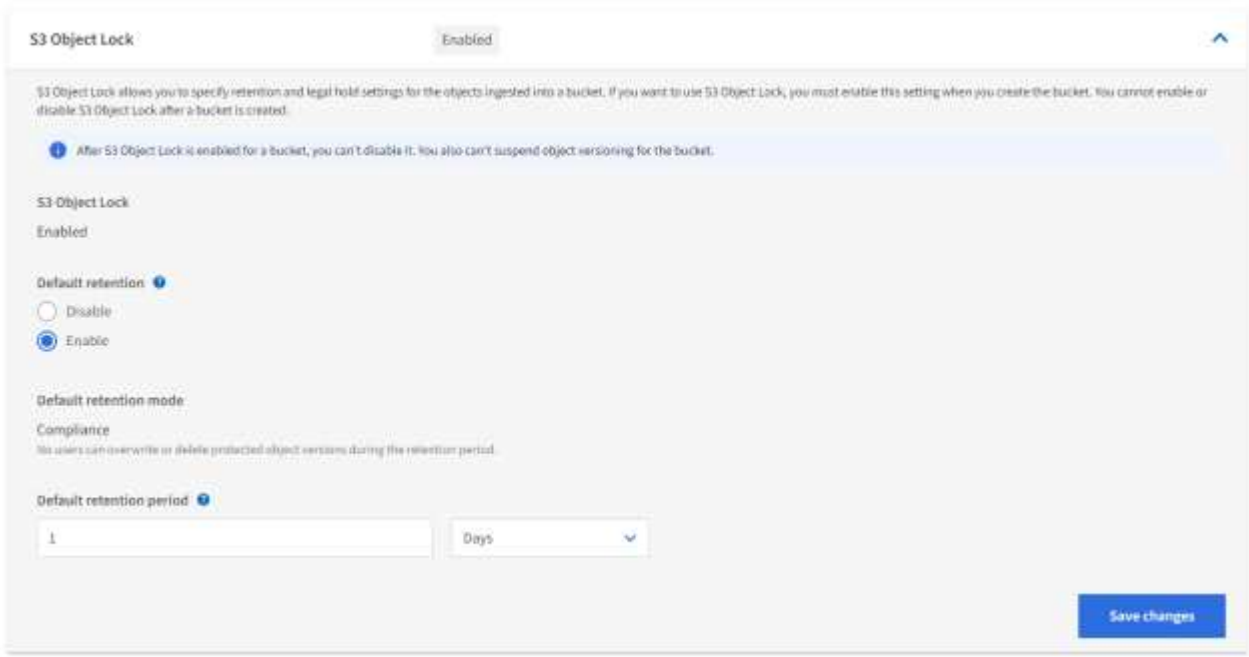
2. Selezionare l’opzione attiva blocco oggetti S3 e fare clic su Crea bucket.



3. Una volta creata la benna, selezionarla per visualizzare le opzioni della benna. Espandere l'opzione a discesa blocco oggetti S3.



4. In conservazione predefinita, selezionare attiva e impostare un periodo di conservazione predefinito di 1 giorno. Fare clic su Salva modifiche.



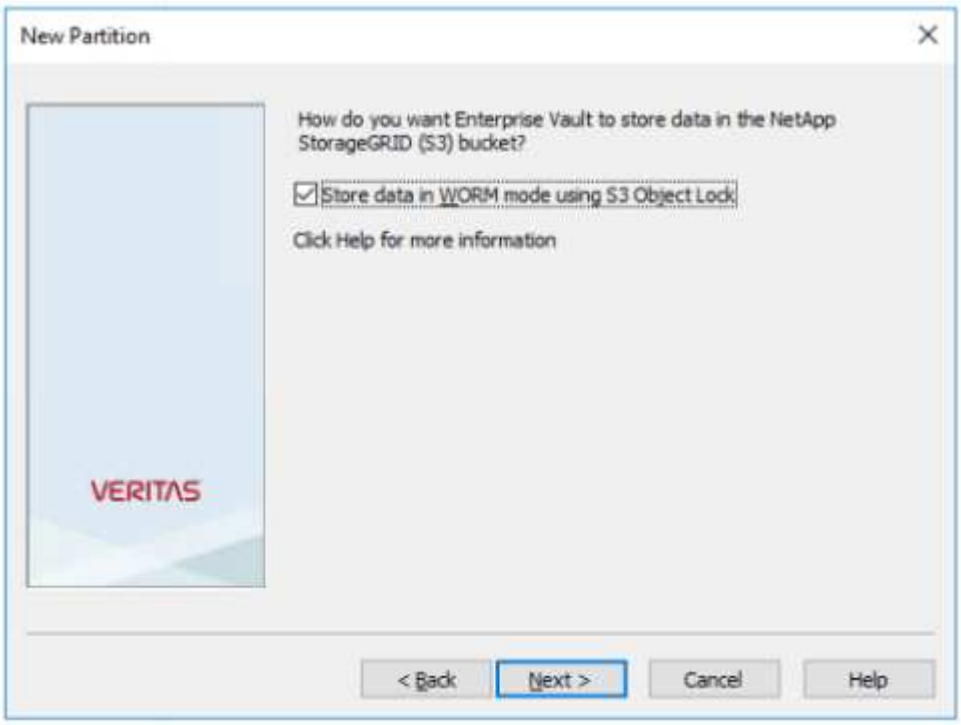
Il bucket è ora pronto per essere utilizzato da Enterprise Vault per memorizzare dati WORM.

Configurare Enterprise Vault

Per configurare Enterprise Vault, completare i seguenti passaggi:

Fasi

1. Ripetere i passaggi 1-3 della "Configurazione di base" sezione, ma questa volta selezionare l'opzione Memorizza dati in modalità WORM utilizzando blocco oggetti S3. Fare clic su Avanti.



2. Quando si immettono le impostazioni di connessione del bucket S3, assicurarsi di immettere il nome di un bucket S3 in cui è attivata la conservazione predefinita del blocco degli oggetti S3.
3. Verificare la connessione per verificare le impostazioni.

Configurare il failover del sito StorageGRID per il disaster recovery

Scoprite come configurare il failover del sito StorageGRID in uno scenario di disaster recovery.

È una prassi comune che l'implementazione di un'architettura StorageGRID sia multisito. I siti possono essere Active-Active o Active-passive per il disaster recovery. In uno scenario di disaster recovery, assicurati che veritas Enterprise Vault mantenga la connessione al proprio storage primario (StorageGRID) e continui ad acquisire e recuperare i dati durante un guasto del sito. In questa sezione vengono fornite istruzioni di configurazione di alto livello per una distribuzione attiva-passiva a due siti. Per informazioni dettagliate su queste linee guida, visitare "Documentazione StorageGRID" la pagina o contattare un esperto StorageGRID.

Prerequisiti per configurare StorageGRID con veritas Enterprise Vault

Prima di configurare il failover del sito StorageGRID, verificare i seguenti prerequisiti:

- È prevista una distribuzione di StorageGRID in due siti, ad esempio site1 e site2.
- È stato creato un nodo admin che esegue il servizio di bilanciamento del carico o un nodo gateway, in ciascun sito, per il bilanciamento del carico.
- È stato creato un endpoint di bilanciamento del carico StorageGRID.

Configurare il failover del sito StorageGRID

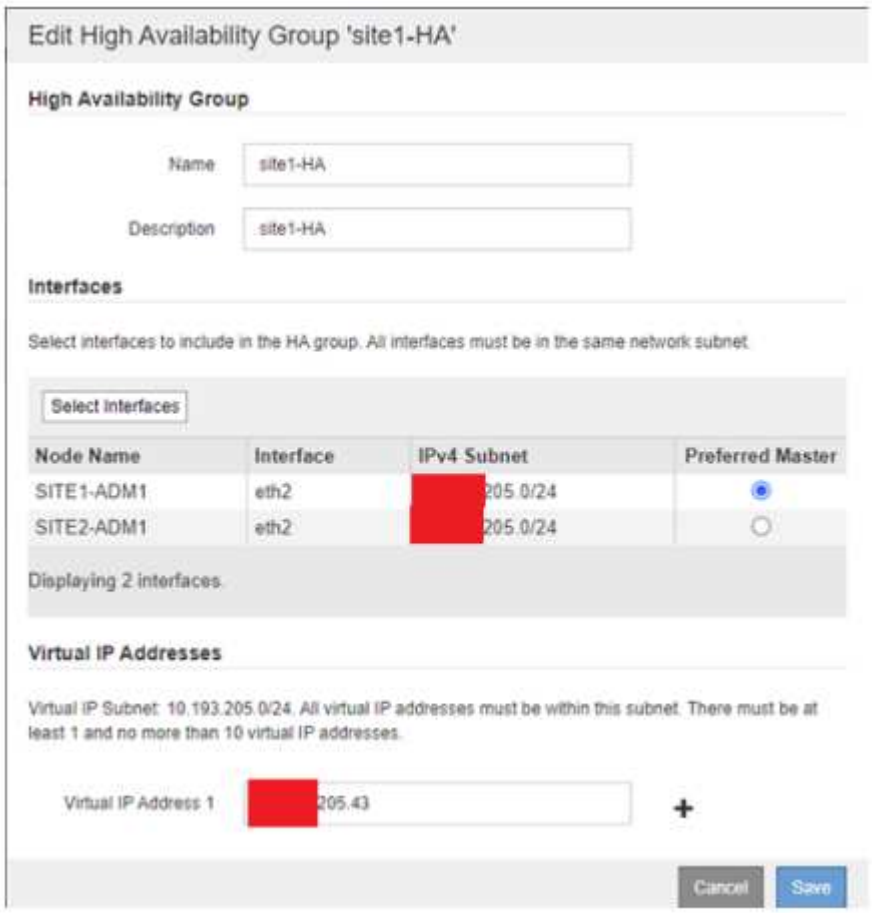
Per configurare il failover del sito StorageGRID, attenersi alla seguente procedura:

Fasi

1. Per garantire la connettività a StorageGRID in caso di guasti nel sito, configurare un gruppo ad alta disponibilità (ha). Dall'interfaccia GMI (StorageGRID Grid Manager Interface), fare clic su Configurazione, gruppi ad alta disponibilità e + Crea.

   [vertias/veritas-create-un-gruppo-ad-alta disponibilità]

2. Inserire le informazioni richieste. Fare clic su Select Interfaces (Seleziona interfacce) e includere le interfacce di rete di site1 e site2 in cui site1 (il sito primario) è il master preferito. Assegnare un indirizzo IP virtuale all'interno della stessa subnet. Fare clic su Salva.

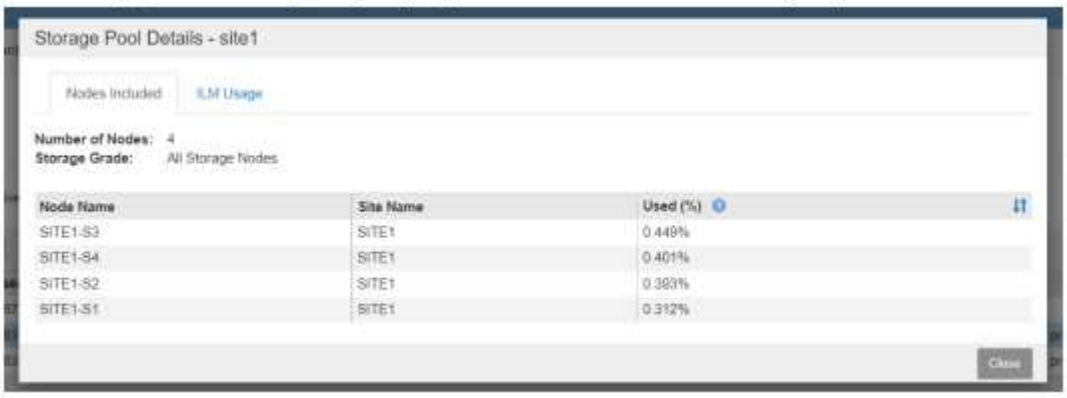


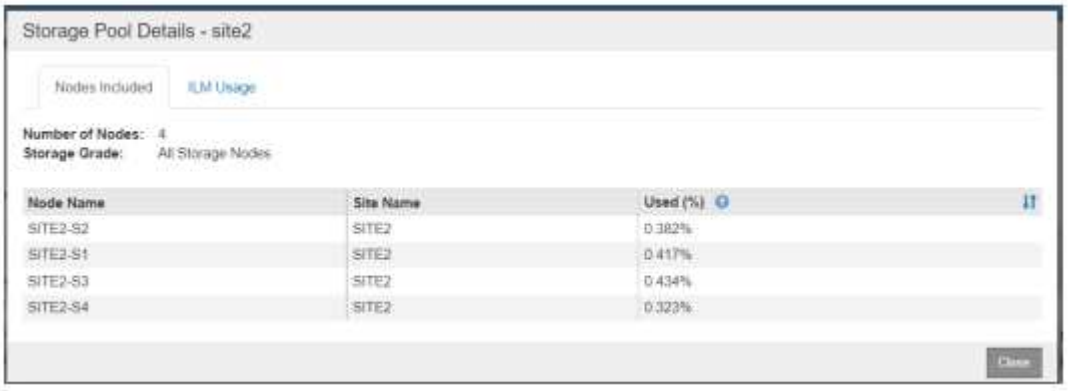
3. Questo indirizzo IP virtuale (VIP) deve essere associato al nome host S3 utilizzato durante la configurazione della partizione di veritas Enterprise Vault. L'indirizzo VIP risolve il traffico a site1 e, durante un errore site1, l'indirizzo VIP reindirizza il traffico a site2 in modo trasparente.
4. Verifica che i dati siano replicati su site1 e site2. In questo modo, se site1 fallisce, i dati dell'oggetto sono

ancora disponibili da site2. Questa operazione viene eseguita configurando per la prima volta i pool di storage.

Da StorageGRID GMI, fare clic su ILM, Storage Pools, quindi su + Crea. Seguire la procedura guidata per creare due pool di storage: Uno per site1 e uno per site2.

I pool di storage sono raggruppamenti logici di nodi utilizzati per definire il posizionamento degli oggetti





5. Da StorageGRID GMI, fare clic su ILM, regole, quindi su + Crea. Seguire la procedura guidata per creare una regola ILM specificando una copia da archiviare per sito con un comportamento di acquisizione bilanciato.

6. Aggiungere la regola ILM in un criterio ILM e attivare il criterio.

Questa configurazione produce i seguenti risultati:

- Un IP endpoint virtuale S3 in cui site1 è l'endpoint primario e site2 è l'endpoint secondario. Se site1

fallisce, il VIP passa a site2.

- Quando i dati archiviati vengono inviati da veritas Enterprise Vault, StorageGRID garantisce che una copia venga archiviata in site1 e un'altra copia di DR in site2. Se site1 si guasta, Enterprise Vault continua ad acquisire e recuperare da site2 TB.

> Entrambe queste configurazioni sono trasparenti per veritas Enterprise Vault. L'endpoint S3, il nome del bucket, le chiavi di accesso e così via sono gli stessi. Non è necessario riconfigurare le impostazioni di connessione S3 nella partizione veritas Enterprise Vault.

Procedura per accedere al software di valutazione StorageGRID

Queste istruzioni sono destinate alla vendita di NetApp, ai partner e ai prospect impegnati in NetApp.

Registrati per un account

1. Registrati per ottenere un account su "Sito di supporto NetApp" utilizzando il tuo indirizzo e-mail aziendale.
   a. Assicurati di non aver effettuato l'accesso con l'account appena creato.
   b. Se si dispone già di un account, assicurarsi di non aver effettuato l'accesso e procedere con il passaggio successivo.
2. Creare un caso di supporto non tecnico per elevare i livelli di accesso al "potenziale cliente". A tale scopo, fare clic sul ""Segnala un problema"collegamento " nel piè di pagina del sito Web.
3. Selezionare "problema di registrazione" come categoria di feedback.
4. Nella sezione dei commenti, scrivi: "Il mio indirizzo e-mail del cliente è *il vostro-indirizzo-e-mail*. Vorrei ottenere l'accesso al potenziale cliente per scaricare il software di valutazione StorageGRID."
   a. Citare il nome della persona interna di NetApp che ha suggerito la richiesta di accesso al prospect.

Scarica StorageGRID

1. Dopo aver esaminato e approvato il tuo caso di supporto, il supporto NetApp ti informerà via e-mail che al tuo account è stato concesso l'accesso ai prospect.
2. Scaricare "Software di valutazione StorageGRID".

Il file di licenza di valutazione si trova all'interno del file zip. Si tratta di StorageGRID-webscale-<version>\vsphere\NLF000000.txt una volta decompresso.

Il download del software è un processo che prevede misure di conformità commerciale per rispettare i requisiti legali. Per garantire la conformità, gli utenti devono creare un account e aprire un caso di supporto prima di poter accedere. Questo processo ci aiuta a mantenere il controllo e la documentazione corretti, fornendo ai potenziali clienti il software pronto per la produzione di cui hanno bisogno.

Forniamo la versione "pronta per la produzione" di StorageGRID, che non è una versione open-source o alternativa. È importante notare che **il supporto non viene fornito** a meno che il potenziale cliente non effettui l'aggiornamento a una licenza di produzione.

Contattare StorageGRID.Feedback@netapp.com per eventuali problemi con i passaggi precedenti.

Blog di NetApp StorageGRID

Puoi trovare alcuni fantastici blog su NetApp StorageGRID qui:

- Febbraio 16 2024: "Presentazione di StorageGRID 11,8: Sicurezza, semplicità ed esperienza utente migliorate"
- Febbraio 16 2024: "Presentazione di StorageGRID 11,8"
- Febbraio 2 2024: "Presentazione della descrizione della soluzione StorageGRID + LakeFS"
- 12 2023 dicembre: "Analisi dei big data su StorageGRID: Dremio esegue 23 volte più velocemente di Apache Hive"
- 7 2023 novembre: "Ghiacciaio on-premise di Spectra Logic con StorageGRID"
- 17 2023 ottobre: "Transizione da Hadoop: Modernizzazione dell'analisi dei dati con Dremio e StorageGRID"
- 1 2023 settembre: "Utilizzo di Cloud Insights per monitorare e raccogliere i registri utilizzando Fluent bit"
- 30 2023 agosto: "Il punto di montaggio per Amazon S3 file System è ora GA"
- 16 2023 maggio: "Introduzione di StorageGRID 11,7 e della nuova appliance di storage a oggetti all-flash SGF6112"
- 16 2023 maggio: "Novità della famiglia di storage a oggetti StorageGRID"
- Marzo 30 2023: "Punto di montaggio per Amazon S3 Alpha release con StorageGRID"
- Marzo 30 2023: "USA BlueXP per proteggere Epic EHR con una policy di backup conforme a 3:2:1"
- Marzo 14 2023: "Come eseguire il backup dei database EHR di Epic Systems con un comando in un'architettura compatibile con 3:2:1"
- Febbraio 14 2023: "Cosa hanno in comune cioccolato, sci, orologi e mainframe?"
- Gennaio 18 2023: "Blocco degli oggetti StorageGRID S3 validato per veritas NetBackup"
- Gennaio 16 2023: "StorageGRID rinnova la certificazione di conformità NF203 e ISO/IEC 25051"
- 6 2022 dicembre: "StorageGRID ottiene la certificazione di conformità KPMG"
- 23 2022 novembre: "Ai spiegabile con MLOPS basati su NetApp e Modzy"
- 7 2022 novembre: "Supporto di StorageGRID e ONTAP S3: Differenze, analogie e integrazione"
- 5 2022 ottobre: "NetApp Cloud Insights aggiunge dashboard della galleria StorageGRID"
- 5 2022 ottobre: "Defrost dei dati su StorageGRID per Snowflake"
- 26 2022 settembre: "NetApp StorageGRID per service provider"
- 19 2022 settembre: "Supporto di protezione DataLock e ransomware per StorageGRID"
- 1 2022 settembre: "Prendi queste metriche e Graph it"
- 23 2022 agosto: "Costruisci il tuo data Lake su StorageGRID"
- 17 2022 agosto: "Tutto inizia con il blocco degli oggetti… Creazione di un ecosistema di storage S3 per le applicazioni di backup critiche"
- 16 2022 agosto: "Integrazione di StorageGRID con lo stack ELK open-source per migliorare l'esperienza del cliente"
- 5 2022 agosto: "NetApp StorageGRID ottiene la certificazione Common Criteria Security"
- 26 2022 luglio: "Consulta l'elenco in continua crescita di soluzioni validate dei partner per StorageGRID"

- 9 2022 giugno: "USA il connettore S3A di Cloudera Hadoop con StorageGRID"
- 26 2022 maggio: "StorageGRID: Memorizzazione e gestione dei dati di replica e backup on-premise"
- 24 2022 maggio: "Modernizza i carichi di lavoro di analisi con NetApp e Alluxio"
- 10 2022 maggio: "Il laboratorio on-demand è il tuo miglior tool di vendita per StorageGRID"

Documentazione di NetApp StorageGRID

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

- "Appliance StorageGRID"
- "StorageGRID 11,9"
- "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