Solutions et ressources StorageGRID

StorageGRID solutions and resources

NetApp
December 12, 2025

Sommaire

Solutions et ressources StorageGRID

Procédure d’accès au logiciel d’évaluation StorageGRID

Cette instruction s’adresse aux commerciaux, aux partenaires et aux prospects NetApp qui travaillent avec NetApp.

Créez un compte

1. Créez un compte sur le "Site de support NetApp" à l’aide de votre adresse e-mail professionnelle.
   a. Assurez-vous que vous n’êtes pas connecté avec le nouveau compte créé.
   b. Si vous possédez déjà un compte, assurez-vous que vous n’êtes pas connecté et passez à l’étape suivante.
2. Créez un dossier de support non technique afin d’élever les niveaux d’accès au « prospect ». Pour ce faire, cliquez sur le ""Signalez les problèmes"lien " dans le pied de page du site Web.
3. Sélectionnez « problème d’enregistrement » comme catégorie de commentaires.
4. Dans la section des commentaires, écrivez : « mon adresse e-mail de compte est *votre-adresse e-mail*. J’aimerais obtenir un accès prospect pour télécharger le logiciel d’évaluation StorageGRID. »
   a. Mentionnez le nom de la personne interne de NetApp qui a suggéré l’accès du prospect.

Télécharger StorageGRID

1. Une fois que votre dossier de demande de support a été examiné et approuvé, le support NetApp vous informe par e-mail que votre compte a été autorisé à accéder à vos prospects.
2. Téléchargez le "Logiciel d’évaluation StorageGRID".

Le fichier de licence Eval se trouve dans le fichier zip. Il s’agit de StorageGRID-Webscale-<version>\vsphere\NLF000000.txt une fois décompressé.

Le téléchargement du logiciel est un processus qui implique des mesures de conformité commerciale pour se conformer aux exigences légales. Pour garantir la conformité, les utilisateurs doivent créer un compte et ouvrir un dossier de demande de support avant d’accéder à ce service. Ce processus nous aide à maintenir un contrôle et une documentation appropriés tout en fournissant aux prospects le logiciel prêt à la production dont ils ont besoin.

Nous fournissons la version « prête pour la production » de StorageGRID, qui n’est pas une version open source ou alternative. Il est important de noter que **le support n’est pas fourni** à moins que le prospect ne passe à une licence de production.

Veuillez contacter StorageGRID.Feedback@netapp.com pour tout problème avec les étapes ci-dessus.

Des solutions tierces validées

Solutions tierces validées : présentation

NetApp, en collaboration avec ses partenaires, a validé ces solutions pour StorageGRID. Consultez les informations de cette section pour savoir quelles solutions ont été validées et pour obtenir des instructions supplémentaires, le cas échéant.

Ensemble, nous pouvons accélérer l'innovation, sensibiliser davantage le marché et augmenter les ventes grâce à la création de solutions NetApp testées et de pointe. "Devenir un partenaire Alliance".

Solutions tierces validées StorageGRID 12.0

Les solutions tierces suivantes ont été validées pour une utilisation avec StorageGRID 12.0. + Si la solution que vous recherchez n'est pas répertoriée, veuillez contacter votre représentant de compte NetApp .

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Almuxio
- Apache Kafka
- Point de montage AWS
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- Collibra (qualité minimale des données de Collibra version 2024.02)
- CommVault 11
- Couchbase Enterprise Analytics 2.0
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données
- DétendX
- Disquette de données
- Dremio
- ElasticSearch Snapshot (y compris le Tier figé)
- Emam
- Archive d'objets Fujifilm
- GitHub Enterprise Server

- IBM FileNet
- IBM Storage Protect
- Interica
- Komprise
- Clusters de Big Data Microsoft SQL Server
- Modèle 9
- Modzy
- La promenade au clair de lune Universal
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- Reveille v10 construire 220706 ou plus
- CDM Rubrik
- s3a
- Signiant
- Flocon de neige
- Spectra Logic On-sur-site Glacier
- SmartStore Splunk
- En étoile
- Pour un stockage simplifié
- Trino
- Vernis Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 et versions ultérieures
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric

- Weka v3.10 ou ultérieure

Solutions tierces validées sur StorageGRID avec verrouillage objet

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Fonctionnalité CommVault 11 version 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 et versions ultérieures

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Gitlab
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH
- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Gestionnaires de clés pris en charge sur StorageGRID

Ces solutions ont été testées.

- Plateforme de sécurité cryptographique Entrust v10.4.5
- Entrust KeyControl 10.2
- Coffre-fort Hashicorp 1.20.2
- Gestionnaire de ciblage Thales CipherTrust 2.20

Solutions tierces validées par StorageGRID 11.9

L'utilisation des solutions tierces suivantes a été validée avec StorageGRID 11.9. + si la solution que vous recherchez n'est pas répertoriée, contactez votre ingénieur commercial NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Almuxio
- Apache Kafka
- Point de montage AWS
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- Collibra (qualité minimale des données de Collibra version 2024.02)
- CommVault 11
- Couchbase Enterprise Analytics 2.0
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données
- DétendX
- Disquette de données
- Dremio
- ElasticSearch Snapshot (y compris le Tier figé)
- Emam
- Archive d'objets Fujifilm
- GitHub Enterprise Server
- IBM FileNet
- IBM Storage Protect
- Interica
- Komprise

- Clusters de Big Data Microsoft SQL Server
- Modèle 9
- Modzy
- La promenade au clair de lune Universal
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- Reveille v10 construire 220706 ou plus
- CDM Rubrik
- s3a
- Signiant
- Flocon de neige
- Spectra Logic On-sur-site Glacier
- SmartStore Splunk
- En étoile
- Pour un stockage simplifié
- Trino
- Vernis Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 et versions ultérieures
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric
- Weka v3.10 ou ultérieure

Solutions tierces validées sur StorageGRID avec verrouillage objet

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Fonctionnalité CommVault 11 version 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 et versions ultérieures

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Gitlab
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH
- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Gestionnaires de clés pris en charge sur StorageGRID

Ces solutions ont été testées.

- Plateforme de sécurité cryptographique Entrust v10.4.5
- Entrust KeyControl 10.2
- Coffre-fort Hashicorp 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
- Gestionnaire de ciblage Thales CipherTrust 2.15
- Gestionnaire de ciblage Thales 2.16
- Gestionnaire de ciblage Thales CipherTrust 2.20

Solutions tierces validées par StorageGRID 11.8

L'utilisation des solutions tierces suivantes a été validée avec StorageGRID 11.8.
Si la solution que vous recherchez n'est pas répertoriée, contactez votre représentant de compte NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Almuxio
- Apache Kafka
- Point de montage AWS
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- Collibra (qualité minimale des données de Collibra version 2024.02)
- CommVault 11
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données
- DétendX
- Disquette de données
- Dremio

- ElasticSearch Snapshot (y compris le Tier figé)
- Emam
- Archive d’objets Fujifilm
- GitHub Enterprise Server
- IBM FileNet
- IBM Storage Protect
- Interica
- Komprise
- Clusters de Big Data Microsoft SQL Server
- Modèle 9
- Modzy
- La promenade au clair de lune Universal
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- Reveille v10 construire 220706 ou plus
- CDM Rubrik
- s3a
- Signiant
- Flocon de neige
- Spectra Logic On-sur-site Glacier
- SmartStore Splunk
- En étoile
- Pour un stockage simplifié
- Trino
- Vernis Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 15,1

- Veritas NetBackup 10.1.1 et versions ultérieures
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric
- Weka v3.10 ou ultérieure

Solutions tierces validées sur StorageGRID avec verrouillage objet

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Fonctionnalité CommVault 11 version 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 15,1
- Veritas NetBackup 10.1.1 et versions ultérieures

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Gitlab
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH
- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Gestionnaires de clés pris en charge sur StorageGRID

Ces solutions ont été testées.

- Entrust KeyControl 10.2
- Coffre-fort Hashicorp 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

Solutions tierces validées par StorageGRID 11.7

L’utilisation des solutions tierces suivantes a été validée avec StorageGRID 11.7. + si la solution que vous recherchez n’est pas répertoriée, contactez votre ingénieur commercial NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Almuxio
- Apache Kafka
- Point de montage AWS
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- Collibra (qualité minimale des données de Collibra version 2024.02)
- CommVault 11
- Portail CTERA 6
- Dalet
- Datobi

- Le stockage dynamique des données
- DétendX
- Disquette de données
- Dremio
- ElasticSearch Snapshot (y compris le Tier figé)
- Emam
- Archive d’objets Fujifilm
- GitHub Enterprise Server
- IBM FileNet
- IBM Spectrum Protect plus
- IBM Storage Protect
- Interica
- Komprise
- Clusters de Big Data Microsoft SQL Server
- Modèle 9
- Modzy
- La promenade au clair de lune Universal
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- Reveille v10 construire 220706 ou plus
- CDM Rubrik
- s3a
- Signiant
- Flocon de neige
- Spectra Logic On-sur-site Glacier
- SmartStore Splunk
- Pour un stockage simplifié

- Trino
- Vernis Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 10.1.1 et versions ultérieures
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric
- Weka v3.10 ou ultérieure

Solutions tierces validées sur StorageGRID avec verrouillage objet

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Fonctionnalité CommVault 11 version 26
- IBM FileNet
- IBM Storage Protect
- OpenText Documentum 21.4
- Rubrik
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 et versions ultérieures

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Gitlab
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH

- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Gestionnaires de clés pris en charge sur StorageGRID

Ces solutions ont été testées.

- 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

Des solutions tierces validées pour StorageGRID 11.6

Les solutions tierces suivantes ont été validées pour une utilisation avec StorageGRID 11.6. + si la solution que vous recherchez n'est pas répertoriée, contactez votre ingénieur commercial NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Almuxio
- Apache Kafka
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- CommVault 11
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données
- DétendX
- Disquette de données
- Dremio
- Emam

- Archive d’objets Fujifilm
- GitHub Enterprise Server
- IBM FileNet
- IBM Spectrum Protect plus
- Interica
- Komprise
- Clusters de Big Data Microsoft SQL Server
- Modèle 9
- Modzy
- La promenade au clair de lune Universal
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- PixitMedia ngenea
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- Reveille v10 construire 220706 ou plus
- CDM Rubrik
- s3a
- Signiant
- Flocon de neige
- Spectra Logic On-sur-site Glacier
- SmartStore Splunk
- Pour un stockage simplifié
- Trino
- Vernis Enterprise 6.0.4
- Veeam 12
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine

- Virtalica StorageFabric
- Weka v3.10 ou ultérieure

Solutions tierces validées sur StorageGRID avec verrouillage objet

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Fonctionnalité CommVault 11 version 26
- IBM FileNet
- OpenText Documentum 21.4
- Veeam 12
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1 et versions ultérieures

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Gitlab
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH
- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Des solutions tierces validées pour StorageGRID 11.5

Les solutions tierces suivantes ont été validées pour une utilisation avec StorageGRID 11.5. + si la solution que vous recherchez n’est pas répertoriée, contactez votre ingénieur commercial NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Almuxio
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- CommVault 11
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données
- DétendX
- Interica
- Komprise
- La promenade au clair de lune Universal
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Documentum 21.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- CDM Rubrik
- s3a
- Signiant
- SmartStore Splunk
- Trino
- Vernis Enterprise 6.0.4
- Veeam 11
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12

- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine
- Virtalica StorageFabric

Solutions tierces validées sur StorageGRID avec verrouillage objet

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- OpenText Documentum 21.4
- Veeam 11

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Gitlab
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH
- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Des solutions tierces validées pour StorageGRID 11.4

Les solutions tierces suivantes ont été validées pour une utilisation avec StorageGRID 11.4. + si la solution que vous recherchez n’est pas répertoriée, contactez votre ingénieur commercial NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- CommVault 11
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données
- DétendX
- Interica
- Komprise
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText InfoArchive 16 EP7
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- CDM Rubrik
- Signiant
- SmartStore Splunk
- Vernis Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- Vidispine

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d'archivage
- Communications d'axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d'objets Fujifilm
- Archive GE Centricity Enterprise
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH
- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Des solutions tierces validées pour StorageGRID 11.3

Les solutions tierces suivantes ont été validées pour une utilisation avec StorageGRID 11.3. + si la solution que vous recherchez n'est pas répertoriée, contactez votre ingénieur commercial NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- CommVault 11
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données

- DétendX
- Interica
- Komprise
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- Passerelle d’archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- SmartStore Splunk
- Vernis Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vidispine

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH

- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Des solutions tierces validées pour StorageGRID 11.2

Les solutions tierces suivantes ont été validées pour une utilisation avec StorageGRID 11.2. + si la solution que vous recherchez n'est pas répertoriée, contactez votre ingénieur commercial NetApp.

Solutions tierces validées sur StorageGRID

Ces solutions ont été testées en collaboration avec les partenaires respectifs.

- Actifio
- Bridgesdor
- Cantemo
- Collaboration de contenu Citrix
- CommVault 11
- Portail CTERA 6
- Dalet
- Datobi
- Le stockage dynamique des données
- DétendX
- Interica
- Komprise
- BIEN
- Nasuni
- OpenText Documentum 16.4
- OpenText Media Management 16.5 avec CyanGate Cloud
- Panzura
- Passerelle d'archivage de points 2.0
- Point Storage Manager 6.4
- Primestream
- StorNext de Quantum 5.4.0.1
- Rubrik CDM 5.0.1 p1-1342
- Signiant
- SmartStore Splunk
- Vernis Enterprise 6.0.4

- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vidispine

Solutions tierces prises en charge sur StorageGRID

Ces solutions ont été testées.

- Logiciel d’archivage
- Communications d’axe
- Congruity360
- DataFrameworks
- Plate-forme DIVA EcoDigital
- Encoding.com
- Archive d’objets Fujifilm
- Archive GE Centricity Enterprise
- Acuo Hyland
- IBM Aspera
- Systèmes Milestone
- RSSI
- Moteur REACH
- SilverTrak
- SoftNAS
- QSTAR
- Velasea

Guides des fonctionnalités des produits

Objectif de point de récupération de zéro avec StorageGRID, Un guide complet de réplication multisite

Ce rapport technique fournit un guide complet sur la mise en œuvre des stratégies de réplication StorageGRID pour atteindre un objectif de point de récupération (RPO) de zéro en cas de défaillance d'un site. Le document détaille différentes options de déploiement pour StorageGRID, notamment la réplication synchrone multisite et la réplication asynchrone multi-grille. Il explique comment les politiques de gestion du cycle de vie des informations (ILM) de StorageGRID peuvent être configurées pour garantir la durabilité et la disponibilité des données sur plusieurs sites. En outre, le rapport aborde les considérations relatives aux performances, les scénarios de défaillance et les processus de récupération afin de maintenir la continuité des opérations des clients. L'objectif de ce document est de fournir des informations permettant de garantir que les données restent accessibles et cohérentes, même en cas de panne complète du site, en tirant parti des techniques de réplication synchrone et asynchrone.

Présentation de StorageGRID

NetApp StorageGRID est un système de stockage objet qui prend en charge l'API Amazon simple Storage Service (Amazon S3) standard.

StorageGRID fournit un espace de noms unique à plusieurs emplacements avec des niveaux de service variables basés sur des règles de gestion du cycle de vie des informations (ILM). Grâce à ces politiques de cycle de vie, vous pouvez optimiser l'emplacement de vos données tout au long de leur cycle de vie.

StorageGRID permet une durabilité et une disponibilité configurables de vos données dans des solutions locales et réparties géographiquement. Que vos données soient sur site ou dans un cloud public, les flux de travail cloud hybrides intégrés permettent à votre entreprise de tirer parti de services cloud tels qu'Amazon Simple Notification Service (Amazon SNS), Google Cloud, Microsoft Azure Blob, Amazon S3 Glacier, Elasticsearch, etc.

StorageGRID Scale

Un déploiement minimal de StorageGRID se compose d'un nœud d'administration et de 3 nœuds de stockage sur un seul site. Une seule grille peut comporter jusqu'à 220 nœuds. StorageGRID peut être déployé sur un seul site ou étendu à 16 sites.

Le nœud Admin contient l'interface de gestion, un point central pour les métriques et la journalisation, et maintient la configuration des composants StorageGRID . Le nœud Admin contient également un équilibreur de charge intégré pour l'accès à l'API S3.

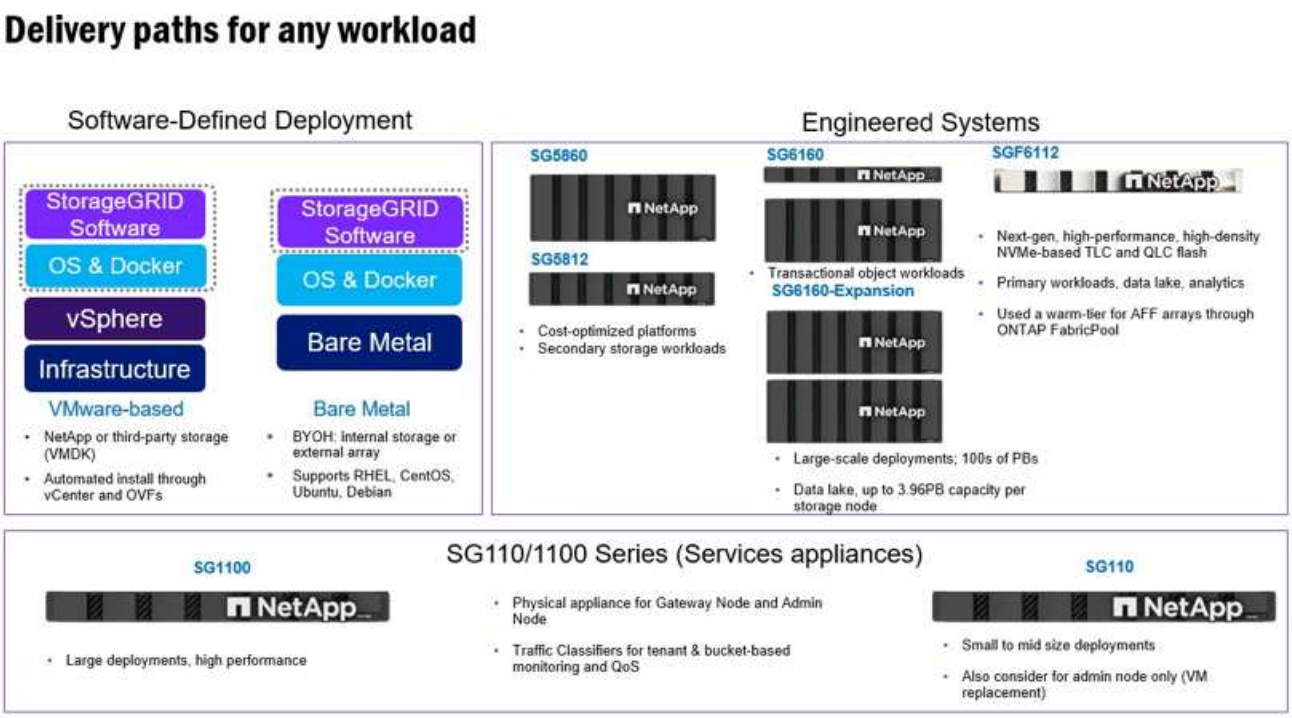
StorageGRID peut être déployé uniquement en tant que logiciel, en tant qu'appliances de machines virtuelles VMware ou en tant qu'appliances spécialement conçues.

Un nœud de stockage peut être déployé comme suit :

- Un nœud de métadonnées uniquement maximisant le nombre d'objets

- Un nœud de stockage d'objets uniquement maximisant l'espace objet
- Un nœud combiné de métadonnées et de stockage d'objets ajoutant à la fois le nombre d'objets et l'espace d'objets

Chaque nœud de stockage peut évoluer vers une capacité de plusieurs pétaoctets pour le stockage d'objets, permettant un espace de noms unique dans les centaines de pétaoctets. StorageGRID fournit également un équilibreur de charge intégré pour les opérations API S3 appelé nœud de passerelle.



StorageGRID se compose d'un ensemble de nœuds placés dans une topologie de site. Un site dans StorageGRID peut être un emplacement physique unique ou résider dans un emplacement physique partagé comme d'autres sites de la grille en tant que construction logique. Un site StorageGRID ne doit pas s'étendre sur plusieurs emplacements physiques. Un site représente une infrastructure de réseau local (LAN) partagée et un domaine de défaillance.

StorageGRID et domaines de défaillance

StorageGRID comprend plusieurs couches de domaines de défaillance à prendre en compte pour décider de l'architecture de votre solution, du mode de stockage des données et de l'emplacement de stockage des données afin de limiter les risques de défaillance.

- Niveau de la grille : Une grille composée de plusieurs sites peut présenter des pannes de site ou une isolation et le ou les sites accessibles peuvent continuer à fonctionner comme la grille.
- Au niveau du site : les défaillances au sein d'un site peuvent avoir un impact sur les opérations de ce site, mais elles n'auront pas d'impact sur le reste de la grille.
- Niveau nœud : Une défaillance de nœud n'a aucun impact sur le fonctionnement du site.
- Niveau du disque : une défaillance de disque n'a aucun impact sur le fonctionnement du nœud.

Données d’objet et métadonnées

Avec le stockage objet, l’unité de stockage est un objet, et non un fichier ou un bloc. Contrairement à la hiérarchie de type arborescence d’un système de fichiers ou stockage en blocs, le stockage objet organise les données dans une disposition plate et non structurée. Le stockage objet dissocie l’emplacement physique des données de la méthode de stockage et de récupération utilisée.

Chaque objet d’un système de stockage basé sur les objets comporte deux parties : les données d’objet et les métadonnées d’objet.

- Les données objet représentent les données sous-jacentes réelles, par exemple une photographie, un film ou un dossier médical.
- Les métadonnées d’objet constituent toutes les informations qui décrivent un objet.

StorageGRID utilise les métadonnées d’objet pour suivre l’emplacement de tous les objets de la grille, et pour gérer le cycle de vie de chaque objet au fil du temps.

Les métadonnées de l’objet incluent les informations suivantes :

- Métadonnées système, y compris un ID unique pour chaque objet, le nom de l’objet, le nom du compartiment S3, le nom ou l’ID du compte locataire, la taille logique de l’objet, la date et l’heure de la première création de l’objet et la date et l’heure de la dernière modification de l’objet.
- L’emplacement de stockage actuel de la copie répliquée ou du fragment à codage d’effacement de chaque objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l’objet.
- Pour les objets S3, toutes les paires clé-valeur de balise d’objet associées à l’objet
- Pour les objets segmentés et les objets multiparties, les identifiants de segment et les tailles de données.

Les métadonnées de l’objet sont personnalisables et extensibles, ce qui rend la possibilité d’utiliser les applications. Pour plus d’informations sur la manière et l’emplacement du stockage des métadonnées d’objet par StorageGRID, consultez "Gérer le stockage des métadonnées d’objet" .

Le système de gestion du cycle de vie des informations (ILM) de StorageGRID orchestre le placement, la durée et le comportement d’ingestion de toutes les données d’objet de votre système StorageGRID. Les règles ILM déterminent la façon dont StorageGRID stocke les objets au fil du temps à l’aide de répliques d’objets ou du codage d’effacement de l’objet sur plusieurs nœuds et sites. Ce système ILM est responsable de la cohérence des données en mode objet au sein d’une grille.

Le code d’effacement

StorageGRID offre la possibilité d’effacer les données de code au niveau du nœud et au niveau du lecteur. Avec les appliances StorageGRID, nous effaçons le code des données stockées sur chaque nœud sur tous les lecteurs du nœud, offrant ainsi une protection locale contre les pannes de disque multiples entraînant une perte ou des interruptions de données. Les reconstructions après des pannes de disque sont locales sur le nœud et ne nécessitent pas de réplication de données sur le réseau.

De plus, les appliances StorageGRID utilisent des schémas de codage d’effacement pour stocker les données d’objet sur les nœuds d’un site ou réparties sur 3 sites ou plus dans le système StorageGRID via les règles ILM de StorageGRID protégeant contre les pannes de nœud.

Le codage d’effacement offre une structure de stockage résistante aux pannes de nœuds et de sites, avec une surcharge moindre que la réplication. Tous les schémas de codage d’effacement StorageGRID sont déployables sur un seul site à condition que le nombre minimal de nœuds requis pour stocker les blocs de

données soit atteint. Cela signifie que pour un schéma EC de 4+2, il faut un minimum de 6 nœuds disponibles pour recevoir les données.

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%

Cohérence des métadonnées

Dans StorageGRID, les métadonnées sont généralement stockées avec trois réplicas par site pour assurer la cohérence et la disponibilité. Cette redondance permet de préserver l'intégrité et l'accessibilité des données, même en cas de défaillance.

La cohérence par défaut est définie au niveau de la grille. Les utilisateurs peuvent modifier la cohérence à tout moment au niveau du compartiment.

Les options de cohérence des compartiments disponibles dans StorageGRID sont les suivantes :

- **Tous** : fournit le plus haut niveau de cohérence. Tous les nœuds de la grille reçoivent les données immédiatement, faute de quoi la demande échoue.
- **Fort-mondial** :
  - **Legacy Strong Global** : Garantit la cohérence de lecture après écriture pour toutes les requêtes client sur tous les sites.
    - Il s'agit du comportement par défaut pour tous les systèmes mis à niveau de la version 11.9 ou antérieure vers la version 12.0 sans modification manuelle du nouveau Quorum Strong Global.
  - **Quorum Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites. Offre une cohérence pour plusieurs nœuds ou même une panne de site si le quorum de réplication des métadonnées est réalisable.
    - Il s'agit du comportement par défaut pour tous les systèmes nouvellement installés sous la version 12.0 ou supérieure.
    - La cohérence QUORUM est définie comme un quorum de répliques de métadonnées de nœud de stockage, où chaque site dispose de 3 répliques de métadonnées. Il peut être calculé comme suit :

1+((N*3)/2) où N est le nombre total de sites

  - Par exemple, un minimum de 5 répliques doivent être réalisées à partir d'une grille de 3 sites avec un maximum de 3 répliques au sein d'un site.

- **Strong-site** : garantit la cohérence lecture après écriture pour toutes les demandes client au sein d'un site.
- **Read-After-New-write**(par défaut) : fournit une cohérence en lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Cohérence des données en mode objet

Tandis que les métadonnées sont automatiquement répliquées dans et entre les sites, les décisions concernant le placement du stockage des données d'objet vous tiennent. Les données d'objet peuvent être stockées en répliques au sein d'un ou plusieurs sites, avec code d'effacement au sein d'un ou entre plusieurs sites, ou encore une combinaison de répliques et de systèmes de stockage avec code d'effacement. Les règles ILM peuvent s'appliquer à tous les objets ou être filtrées pour ne s'appliquer qu'à certains objets, compartiments ou locataires. Les règles ILM définissent le mode de stockage des objets, les réplicas et/ou le code d'effacement, la durée de stockage des objets à ces emplacements si le nombre de répliques ou le schéma de code d'effacement doit changer, ou si les emplacements doivent changer au fil du temps.

Chaque règle ILM sera configurée avec l'un des trois comportements d'ingestion pour la protection des objets : double allocation, équilibre ou stricte.

L'option de double validation effectuera immédiatement deux copies sur deux nœuds de stockage différents de la grille et renverra la requête au client comme ayant réussi. La sélection des nœuds sera effectuée sur le site de la requête, mais pourra, dans certains cas, utiliser des nœuds d'un autre site. L'objet est ajouté à la file d'attente ILM pour être évalué et placé conformément aux règles ILM.

L'option équilibrée évalue immédiatement l'objet par rapport à la politique ILM et le place de manière synchrone avant de renvoyer la requête au client pour confirmer sa réussite. Si la règle ILM ne peut être respectée immédiatement en raison d'une panne ou d'un espace de stockage insuffisant pour répondre aux exigences de placement, alors une double validation sera utilisée à la place. Une fois le problème résolu, ILM placera automatiquement l'objet selon la règle définie.

L'option stricte évalue immédiatement l'objet par rapport à la politique ILM et le place de manière synchrone avant de renvoyer la requête au client pour confirmer sa réussite. Si la règle ILM ne peut être respectée immédiatement en raison d'une panne ou d'un espace de stockage insuffisant pour répondre aux exigences de placement, la requête échouera et le client devra réessayer.

Équilibrage de la charge

StorageGRID peut être déployé avec accès client via les nœuds de passerelle intégrés, un équilibreur de charge externe tiers 3rd, un round Robin DNS ou directement sur un nœud de stockage. Plusieurs nœuds de passerelle peuvent être déployés dans un site et configurés dans des groupes à haute disponibilité. Ils bénéficient ainsi d'un basculement et d'un retour arrière automatisés en cas de panne d'un nœud de passerelle. Vous pouvez combiner des méthodes d'équilibrage de charge dans une solution afin de fournir un point d'accès unique pour tous les sites d'une solution.

Les nœuds passerelles répartiront la charge entre les nœuds de stockage du site où ils résident par défaut. StorageGRID peut être configuré pour permettre aux nœuds de passerelle d'équilibrer la charge en utilisant

des nœuds provenant de plusieurs sites. Cette configuration ajouterait la latence entre ces sites à la latence de réponse aux requêtes du client. Cette configuration ne doit être mise en place que si la latence totale est acceptable pour les clients.

Un RTO nul peut être garanti grâce à une combinaison d'équilibrage de charge local et global. Garantir un accès client ininterrompu nécessite un équilibrage de charge des requêtes client. Une solution StorageGRID peut contenir de nombreux nœuds de passerelle et des groupes à haute disponibilité sur chaque site. Pour garantir un accès ininterrompu aux clients sur n'importe quel site, même en cas de panne de site, vous devez configurer une solution d'équilibrage de charge externe en combinaison avec les nœuds StorageGRID Gateway. Configurez des groupes de haute disponibilité pour les nœuds Gateway qui gèrent la charge au sein de chaque site et utilisez l'équilibreur de charge externe pour répartir la charge entre les groupes de haute disponibilité. L'équilibreur de charge externe doit être configuré pour effectuer un contrôle d'intégrité afin de garantir que les requêtes ne soient envoyées qu'aux sites opérationnels. Pour plus d'informations sur l'équilibrage de charge avec StorageGRID, veuillez consulter la documentation. "Rapport technique sur l'équilibreur de charge StorageGRID".

Exigences pour un RPO nul avec StorageGRID

Pour atteindre un objectif de point de récupération de zéro dans un système de stockage objet, il est essentiel qu'au moment de la défaillance :

- Les métadonnées et le contenu des objets sont synchronisés et sont considérés comme cohérents
- Le contenu de l'objet reste accessible malgré la défaillance.

Pour un déploiement multisite, Quorum Strong Global est le modèle de cohérence privilégié pour garantir la synchronisation des métadonnées sur tous les sites, ce qui le rend essentiel pour répondre à l'exigence de RPO zéro.

Les objets du système de stockage sont stockés selon les règles de gestion du cycle de vie de l'information (ILM), qui dictent comment et où les données sont stockées tout au long de leur cycle de vie. Pour la réplication synchrone, on peut choisir entre l'exécution stricte et l'exécution équilibrée.

- L'exécution stricte de ces règles ILM est nécessaire pour RPO nul, car elle garantit que les objets sont placés aux emplacements définis sans délai ni retour arrière, afin d'assurer la disponibilité et la cohérence des données.
- Le comportement d'ingestion de l'équilibre ILM de StorageGRID offre un équilibre entre haute disponibilité et résilience, permettant aux utilisateurs de continuer à ingérer des données, même en cas de défaillance d'un site.

Déploiements synchrones sur plusieurs sites

Solutions multisites : StorageGRID vous permet de répliquer des objets sur plusieurs sites au sein de la grille de manière synchrone. En configurant des règles de gestion du cycle de vie des informations (ILM) avec un comportement équilibré ou strict, les objets sont placés immédiatement aux emplacements spécifiés. La configuration du niveau de cohérence du bucket sur Quorum Strong Global garantira également la réplication synchrone des métadonnées. StorageGRID utilise un espace de noms global unique, stockant les emplacements de placement des objets sous forme de métadonnées, de sorte que chaque nœud sait où se trouvent toutes les copies ou les éléments codés par effacement. Si un objet ne peut pas être récupéré à partir du site où la demande a été effectuée, il sera automatiquement récupéré à partir d'un site distant sans nécessiter de procédures de basculement.

Une fois la défaillance résolue, aucune opération de restauration manuelle n'est nécessaire. Les performances de réplication dépendent du site avec le débit réseau le plus faible, la latence la plus élevée et les performances les plus faibles. Les performances d'un site dépendent du nombre de nœuds, du nombre de

cœurs et de la vitesse du processeur, de la mémoire, de la quantité de disques et des types de disques.

Solutions multi-grilles : StorageGRID peut répliquer des locataires, des utilisateurs et des compartiments entre plusieurs systèmes StorageGRID à l'aide de la réplication multigrille (CGR). CGR peut étendre des données sélectionnées à plus de 16 sites, augmenter la capacité utilisable de votre magasin d'objets et fournir une reprise après sinistre. La réplication des compartiments avec CGR inclut des objets, des versions d'objets et des métadonnées, et peut être bidirectionnelle ou unidirectionnelle. L'objectif de point de récupération dépend de la performance de chaque système StorageGRID et des connexions réseau qui les relient.

Résumé:

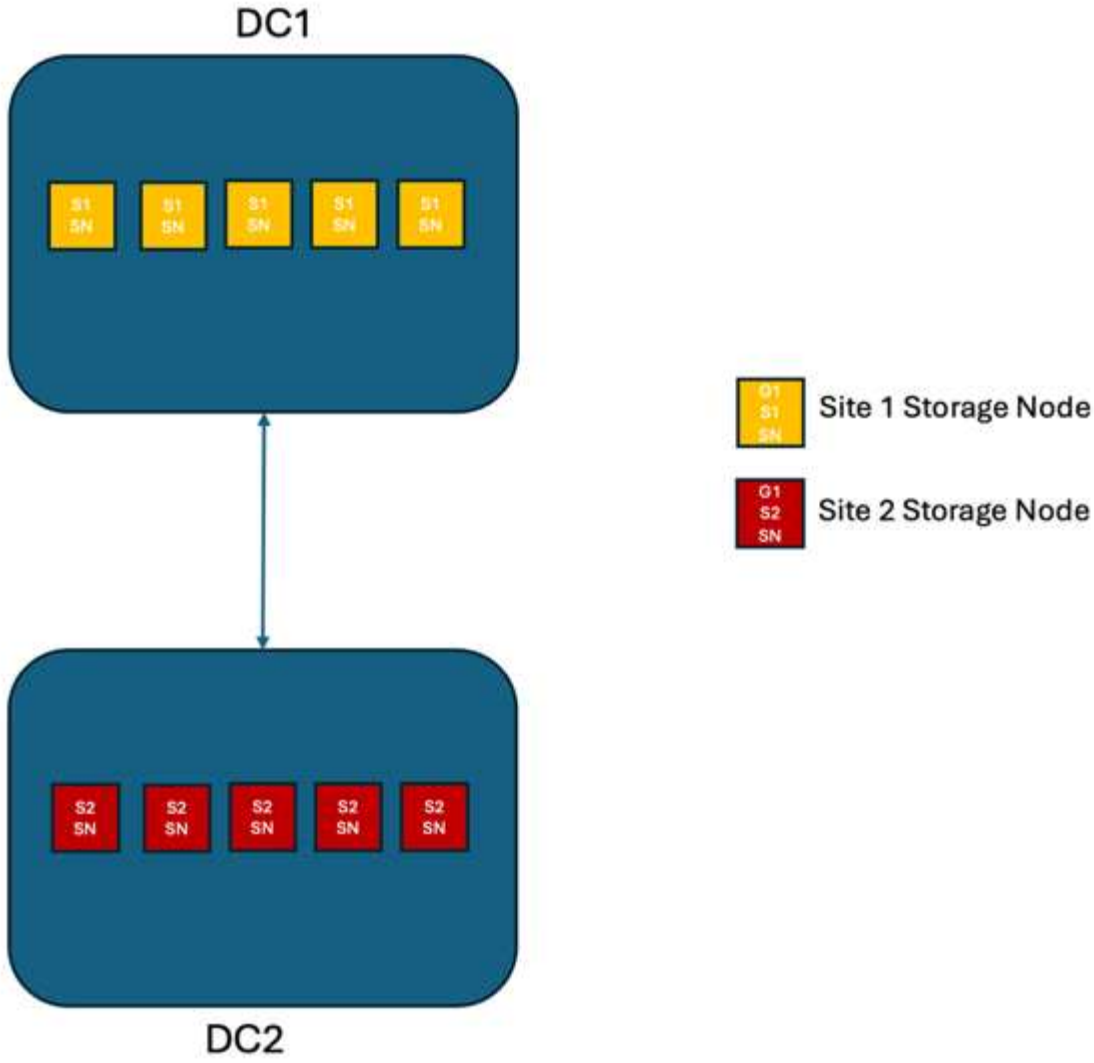
- La réplication intra-grid inclut à la fois la réplication synchrone et asynchrone. Elle peut être configurée à l'aide du comportement d'ingestion ILM et du contrôle de la cohérence des métadonnées.
- La réplication inter-grid est asynchrone uniquement.

Un déploiement multi-site à grille unique

Dans les scénarios suivants, les solutions StorageGRID sont configurées avec un équilibreur de charge externe optionnel gérant les requêtes vers les groupes de haute disponibilité de l'équilibreur de charge intégré. Cela permettra d'obtenir un RTO nul, en plus d'un RPO nul. ILM est configuré avec une protection d'ingestion équilibrée pour le placement synchrone. Chaque compartiment est configuré avec la version Quorum du modèle de cohérence globale forte pour les grilles de 3 sites ou plus et la version Legacy de la cohérence globale forte pour 2 sites.

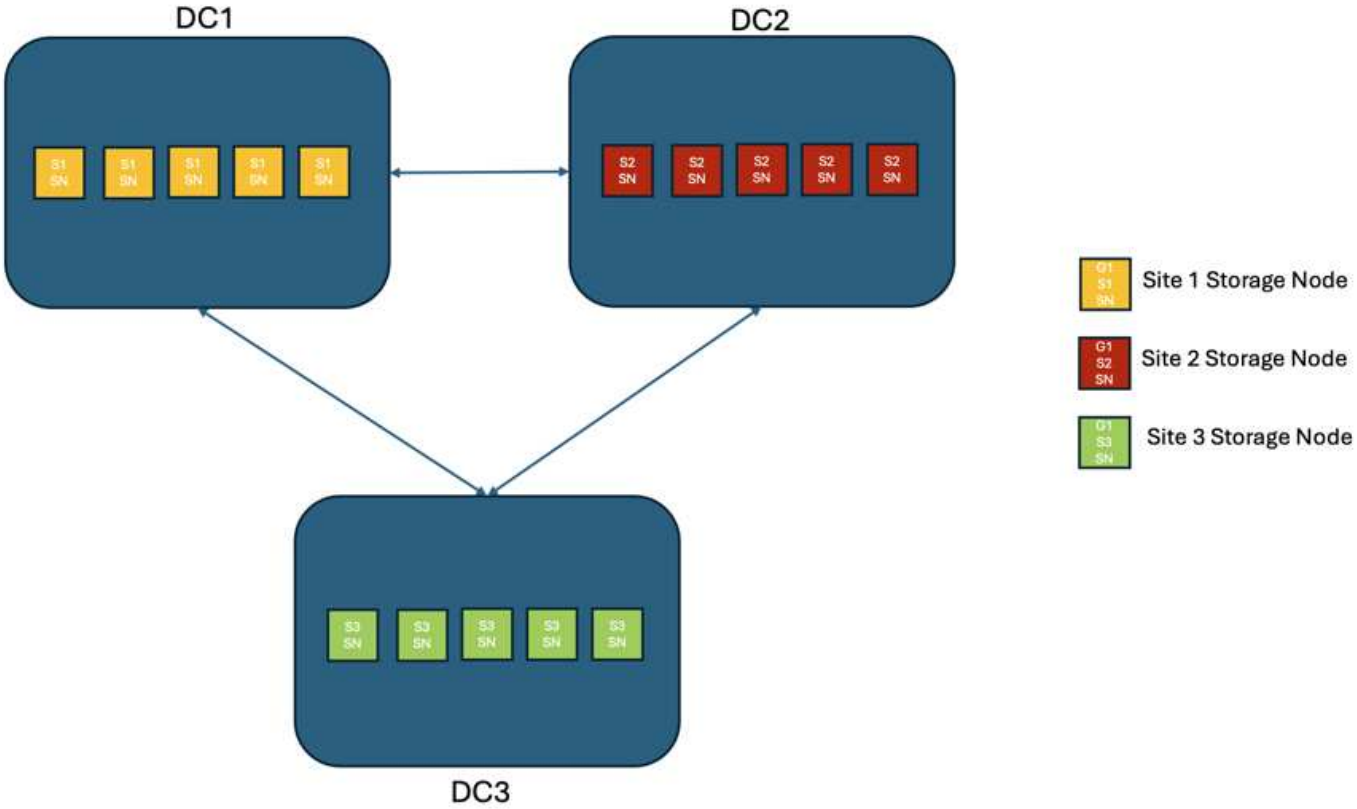
Scénario 1 :

Dans une solution StorageGRID à deux sites, il existe au moins deux répliques de chaque objet et six répliques de toutes les métadonnées. En cas de rétablissement du service, les mises à jour relatives à la panne seront automatiquement synchronisées avec le site/les nœuds rétablis. Avec seulement 2 sites, il est peu probable d'atteindre un RPO nul dans les scénarios de panne autres qu'une perte totale d'un site.



Scénario 2 :

Dans une solution StorageGRID de trois sites ou plus, il existe au moins 3 répliques ou 3 blocs EC de chaque objet et 9 répliques de toutes les métadonnées. En cas de rétablissement du service, les mises à jour relatives à la panne seront automatiquement synchronisées avec le site/les nœuds rétablis. Avec trois sites ou plus, il est possible d'atteindre un RPO nul.



Scénarios de défaillance multisite

Panne	Résultats sur 2 sites + Héritage solide à l'échelle mondiale	Résultat de 3 sites ou plus + Quorum Strong Global
Panne d'un seul nœud de disque	Chaque appliance utilise plusieurs groupes de disques et peut supporter au moins 1 disque par groupe en cas de défaillance sans interruption ni perte de données.	Chaque appliance utilise plusieurs groupes de disques et peut supporter au moins 1 disque par groupe en cas de défaillance sans interruption ni perte de données.
Panne d'un seul nœud sur un site	Aucune interruption des opérations ou perte de données.	Aucune interruption des opérations ou perte de données.
Défaillance de plusieurs nœuds sur un site	Interruption des opérations client dirigées vers ce site, mais aucune perte de données. Les opérations dirigées vers l'autre site restent sans interruption et sans perte de données.	Les opérations sont dirigées vers tous les autres sites, restent sans interruption et sans perte de données.

Panne	Résultats sur 2 sites + Héritage solide à l'échelle mondiale	Résultat de 3 sites ou plus + Quorum Strong Global
Défaillance d'un seul nœud sur plusieurs sites	Aucune perturbation ou perte de données si : • Il existe au moins une copie répliquée dans la grille • Il existe suffisamment de blocs EC dans la grille Activités interrompues et risque de perte de données si : • Il n'existe aucune copie répliquée • Il existe des mandrins EC insuffisants	Aucune perturbation ou perte de données si : • Il existe au moins une copie répliquée dans la grille • Il existe suffisamment de blocs EC dans la grille Activités interrompues et risque de perte de données si : • Il n'existe aucune copie répliquée • Il n'existe pas de mandrins EC suffisants pour récupérer l'objet
Panne sur un seul site	Certaines opérations client seront interrompues jusqu'à ce que la panne soit résolue. Les opérations GET et HEAD se poursuivront sans interruption. Réduisez la cohérence des compartiments à « lecture après nouvelle écriture » ou à un niveau inférieur pour poursuivre les opérations sans interruption dans cet état de défaillance.	Aucune interruption des opérations ou perte de données.
Pannes sur un seul site et sur un seul nœud	Certaines opérations client seront interrompues jusqu'à ce que la panne soit résolue. Les opérations de HEAD se poursuivront sans interruption. Les opérations GET se poursuivront sans interruption s'il existe une copie répliquée ou suffisamment de segments EC. Réduisez la cohérence des compartiments à « lecture après nouvelle écriture » ou à un niveau inférieur pour poursuivre les opérations sans interruption dans cet état de défaillance.	Aucune interruption des opérations ni perte de données. Risque de perte de données en fonction du nombre de copies répliquées. Le codage d'effacement local permet d'éviter la perte de données.

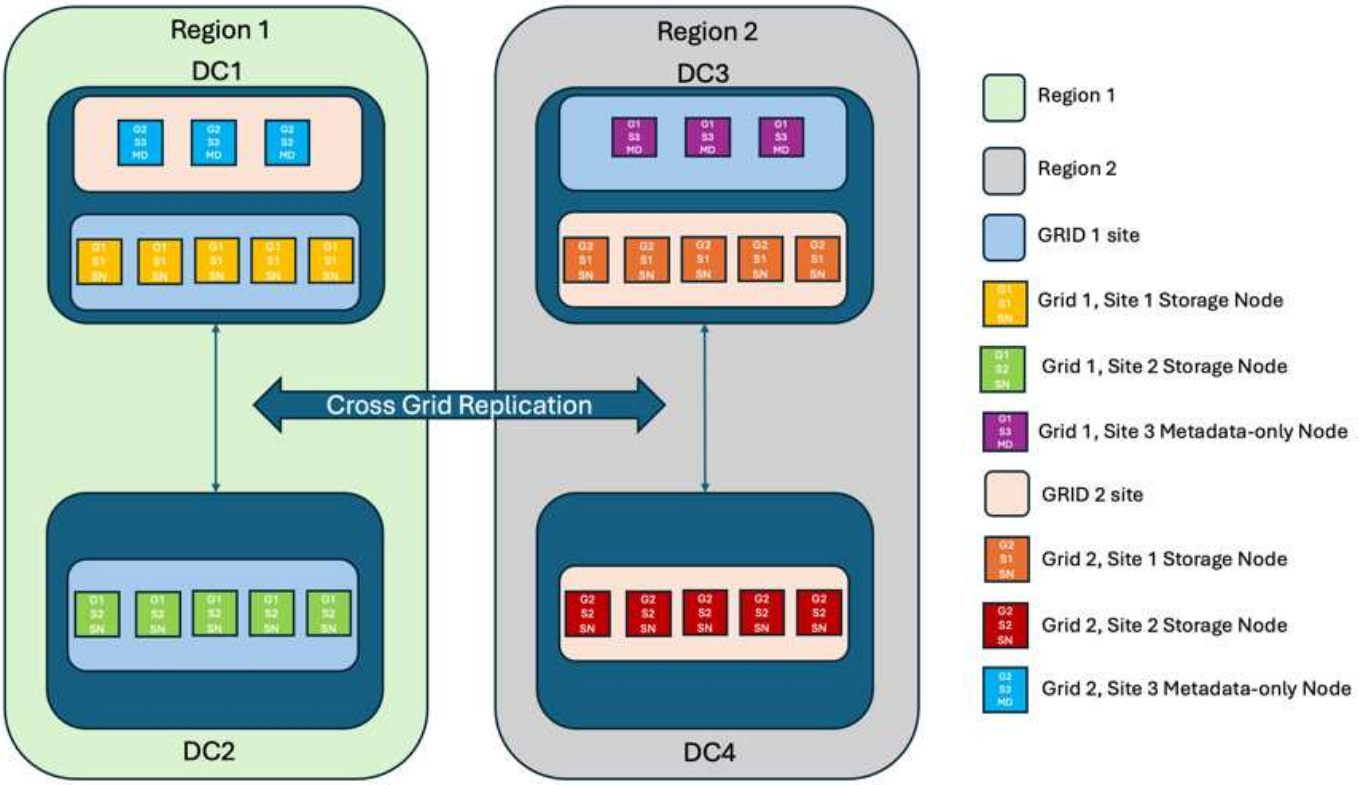
Panne	Résultats sur 2 sites + Héritage solide à l'échelle mondiale	Résultat de 3 sites ou plus + Quorum Strong Global
Un seul site et un nœud pour chaque site restant	Il n'existe que deux sites. Voir : Un seul site et un seul nœud.	Les opérations seront interrompues si le quorum de réplication des métadonnées ne peut être atteint. Réduisez la cohérence des compartiments à « lecture après nouvelle écriture » ou à un niveau inférieur pour poursuivre les opérations sans interruption dans cet état de défaillance. Risque de perte de données en cas de panne permanente, en fonction du nombre de copies répliquées. Le codage d'effacement local permet d'éviter la perte de données.
Panne multisite	Il ne reste plus aucun site opérationnel. Des données seront perdues si au moins un site ne peut être récupéré dans son intégralité.	Les opérations seront interrompues si le quorum de réplication des métadonnées ne peut être atteint. Réduisez la cohérence des compartiments à « lecture après nouvelle écriture » ou à un niveau inférieur pour poursuivre les opérations sans interruption dans cet état de défaillance. Risque de perte de données en cas de panne permanente si le nombre de blocs de données à codage d'effacement est insuffisant. Le codage d'effacement local ou les copies répliquées peuvent empêcher la perte de données.
Isolation réseau d'un site	Les opérations client seront interrompues jusqu'à ce que la panne soit résolue. Réduisez la cohérence des compartiments à « lecture après nouvelle écriture » ou à un niveau inférieur pour poursuivre les opérations sans interruption dans cet état de défaillance. Aucune perte de données	Les opérations seront perturbées sur le site isolé, mais aucune perte de données ne sera à prévoir. Réduisez la cohérence des compartiments à « lecture après nouvelle écriture » ou à un niveau inférieur pour poursuivre les opérations sans interruption dans cet état de défaillance. Aucune interruption des opérations sur les autres sites et aucune perte de données.

Un déploiement multi-sites à plusieurs grilles

Pour ajouter une couche supplémentaire de redondance, ce scénario utilisera deux clusters StorageGRID et utilisera la réplication inter-grille pour les maintenir synchronisés. Pour cette solution, chaque cluster StorageGRID aura trois sites. Deux sites seront utilisés pour le stockage d'objets et les métadonnées tandis que le troisième site sera utilisé uniquement pour les métadonnées. Les deux systèmes seront configurés avec une règle ILM équilibrée pour stocker de manière synchrone les objets à l'aide du codage d'effacement dans

chacun des deux sites de données. Les buckets seront configurés avec le modèle de cohérence global Quorum Strong. Chaque grille sera configurée avec une réplication bidirectionnelle entre grilles sur chaque bucket. Cela fournit la réplication asynchrone entre les régions. En option, un équilibreur de charge global peut être implémenté pour gérer les demandes adressées aux groupes de haute disponibilité de l'équilibreur de charge intégré des deux systèmes StorageGRID afin d'atteindre un RPO nul.

La solution utilisera quatre sites répartis de manière égale en deux régions. La région 1 contiendra les 2 sites de stockage de la grille 1 comme grille principale de la région et le site de métadonnées de la grille 2. La région 2 contiendra les 2 sites de stockage de la grille 2 comme grille principale de la région et le site de métadonnées de la grille 1. Dans chaque région, le même emplacement peut héberger le site de stockage de la grille primaire de la région, ainsi que le site de métadonnées uniquement de la grille des autres régions. L'utilisation de nœuds de métadonnées uniquement comme troisième site permet d'assurer la cohérence requise pour les métadonnées et non de dupliquer le stockage des objets à cet emplacement.



Cette solution avec quatre emplacements distincts assure la redondance complète de deux systèmes StorageGRID distincts qui maintiennent un RPO de 0. Elle utilise à la fois la réplication synchrone multisite et la réplication asynchrone multigrille. Un seul site peut tomber en panne tout en assurant la continuité des opérations client sur les deux systèmes StorageGRID.

Dans cette solution, il existe quatre copies avec code d'effacement de chaque objet et 18 réplicas de toutes les métadonnées. Cela permet de réaliser plusieurs scénarios de défaillance sans impact sur les opérations du client. En cas de panne, les mises à jour de reprise se synchronisent automatiquement avec le ou les sites défaillants.

Scénarios de défaillance multigrille et multisite

Panne	Résultat
Panne d’un seul nœud de disque	Chaque appliance utilise plusieurs groupes de disques et peut supporter au moins 1 disque par groupe en cas de défaillance sans interruption ni perte de données.
Panne d’un seul nœud sur un site d’un grid	Aucune interruption des opérations ou perte de données.
Panne d’un seul nœud sur un site de chaque grid	Aucune interruption des opérations ou perte de données.
Défaillance de plusieurs nœuds dans un site d’une grille	Aucune interruption des opérations ou perte de données.
Défaillance de plusieurs nœuds sur un site de chaque grid	Aucune interruption des opérations ou perte de données.
Défaillance d’un seul nœud sur plusieurs sites d’un grid	Aucune interruption des opérations ou perte de données.
Défaillance d’un seul nœud sur plusieurs sites de chaque grid	Aucune interruption des opérations ou perte de données.
Panne sur un seul site dans une grille	Aucune interruption des opérations ou perte de données.
Panne sur un seul site dans chaque grid	Aucune interruption des opérations ou perte de données.
Pannes sur un seul site et sur un seul nœud dans un grid	Aucune interruption des opérations ou perte de données.
Un seul site et un nœud pour chaque site restant dans une seule grille	Aucune interruption des opérations ou perte de données.
Panne sur un seul emplacement	Aucune interruption des opérations ou perte de données.
Défaillance d’emplacement unique dans chaque grille DC1 et DC3	Les opérations seront interrompues jusqu’à ce que la défaillance soit résolue ou que la cohérence des compartiments soit réduite ; chaque grille a perdu 2 sites Toutes les données existent toujours à 2 emplacements
Défaillance d’emplacement unique dans chaque grille DC1 et DC4 ou DC2 et DC3	Aucune interruption des opérations ou perte de données.
Panne d’emplacement unique dans chaque grille DC2 et DC4	Aucune interruption des opérations ou perte de données.

Panne	Résultat
Isolation réseau d'un site	Les opérations seront interrompues pour le site isolé, mais aucune donnée ne sera perdue Aucune interruption des opérations sur les sites restants et aucune perte de données.

Conclusion

En cas de défaillance sur un site, StorageGRID vise à assurer la durabilité et la disponibilité des données, ainsi que leur disponibilité. Grâce aux stratégies de réplication robustes de StorageGRID, notamment la réplication synchrone multisite et la réplication asynchrone multigrille, les entreprises peuvent assurer la continuité des opérations client et la cohérence des données sur plusieurs sites. La mise en œuvre de règles de gestion du cycle de vie de l'information (ILM) et l'utilisation de nœuds de métadonnées uniquement améliorent encore la résilience et les performances du système. Avec StorageGRID, les entreprises peuvent gérer leurs données en toute confiance et en sachant qu'elles restent accessibles et cohérentes même en cas de défaillance complexe. Cette approche complète de la gestion et de la réplication des données souligne l'importance d'une planification et d'une exécution méticuleuses pour atteindre un objectif de point de récupération nul et protéger les informations précieuses.

Création d'un pool de stockage cloud pour AWS ou Google Cloud

Vous pouvez utiliser un pool de stockage cloud pour déplacer des objets StorageGRID vers un compartiment S3 externe. Le compartiment externe peut appartenir à Amazon S3 (AWS) ou à Google Cloud.

Ce dont vous avez besoin

- StorageGRID 11.6 a été configuré.
- Vous avez déjà configuré un compartiment S3 externe sur AWS ou Google Cloud.

Étapes

1. Dans Grid Manager, accédez à **ILM** > **Storage pools**.
2. Dans la section Cloud Storage pools de la page, sélectionnez **Create**.

   La fenêtre contextuelle Créer un pool de stockage cloud s'affiche.

3. Entrez un nom d'affichage.
4. Sélectionnez **Amazon S3** dans la liste déroulante Type de fournisseur.

   Ce type de fournisseur fonctionne pour AWS S3 ou Google Cloud.

5. Entrez l'URI du compartiment S3 à utiliser pour le pool de stockage cloud.

   Deux formats sont autorisés :

   `https://host:port`

   `http://host:port`

6. Entrez le nom du compartiment S3.

   Le nom que vous spécifiez doit correspondre exactement au nom du compartiment S3. Sinon, la création du pool de stockage cloud échoue. Vous ne pouvez pas modifier cette valeur après l'enregistrement du pool de stockage cloud.

7. Vous pouvez également saisir l'ID de clé d'accès et la clé d'accès secrète.
8. Sélectionnez **ne pas vérifier le certificat** dans la liste déroulante.
9. Cliquez sur **Enregistrer**.

Résultat attendu

Assurez-vous qu'un pool de stockage cloud a été créé pour Amazon S3 ou Google Cloud.

Par Jonathan Wong

Création d'un pool de stockage cloud pour le stockage Azure Blob

Vous pouvez utiliser un pool de stockage cloud pour déplacer des objets StorageGRID vers un conteneur Azure externe.

Ce dont vous avez besoin

- StorageGRID 11.6 a été configuré.
- Vous avez déjà configuré un conteneur Azure externe.

Étapes

1. Dans Grid Manager, accédez à **ILM** > **Storage pools**.
2. Dans la section Cloud Storage pools de la page, sélectionnez **Create**.

   La fenêtre contextuelle Créer un pool de stockage cloud s'affiche.

3. Entrez un nom d'affichage.
4. Sélectionnez **Azure Blob Storage** dans la liste déroulante Type de fournisseur.
5. Entrez l'URI du compartiment S3 à utiliser pour le pool de stockage cloud.

   Deux formats sont autorisés :

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

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

6. Entrez le nom du conteneur Azure.

   Le nom que vous spécifiez doit correspondre exactement au nom du conteneur Azure. Sinon, la création du pool de stockage cloud échoue. Vous ne pouvez pas modifier cette valeur après l'enregistrement du pool de stockage cloud.

7. Vous pouvez également saisir le nom de compte et la clé de compte associés du conteneur Azure pour l'authentification.

8. Sélectionnez **ne pas vérifier le certificat** dans la liste déroulante.
9. Cliquez sur **Enregistrer**.

Résultat attendu

Confirmation de la création d'un pool de stockage cloud pour Azure Blob Storage

Par Jonathan Wong

Utilisation d'un pool de stockage cloud pour la sauvegarde

Vous pouvez créer une règle ILM pour déplacer des objets dans Cloud Storage Pool à des fins de sauvegarde.

Ce dont vous avez besoin

- StorageGRID 11.6 a été configuré.
- Vous avez déjà configuré un conteneur Azure externe.

Étapes

1. Dans Grid Manager, accédez à **ILM** > **règles** > **Créer**.
2. Entrez une description.
3. Entrez un critère pour déclencher la règle.
4. Cliquez sur **Suivant**.
5. Répliquez l'objet dans les nœuds de stockage.
6. Ajoutez une règle de placement.
7. Réplication de l'objet vers le pool de stockage cloud
8. Cliquez sur **Suivant**.
9. Cliquez sur **Enregistrer**.

Résultat attendu

Vérifiez que le diagramme de conservation affiche les objets stockés localement dans StorageGRID et dans un Cloud Storage Pool pour la sauvegarde.

Confirmez que, lorsque la règle ILM est déclenchée, une copie existe dans le pool de stockage cloud et vous pouvez récupérer l'objet localement sans effectuer de restauration d'objet.

Par Jonathan Wong

Configurez le service d'intégration de recherche StorageGRID

Ce guide fournit des instructions détaillées pour la configuration du service d'intégration de recherche NetApp StorageGRID avec le service Amazon OpenSearch ou avec Elasticsearch sur site.

Introduction

StorageGRID prend en charge trois types de services de plateforme.

- **Réplication StorageGRID CloudMirror**. Mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.
- **Notifications**. Notifications d'événements par compartiment pour envoyer des notifications sur des actions spécifiques réalisées sur des objets vers un Amazon simple notification Service (Amazon SNS) externe spécifié.
- **Service d'intégration de recherche**. Envoyez les métadonnées d'objet S3 (simple Storage Service) à un index Elasticsearch spécifique où vous pouvez rechercher ou analyser les métadonnées à l'aide du service externe.

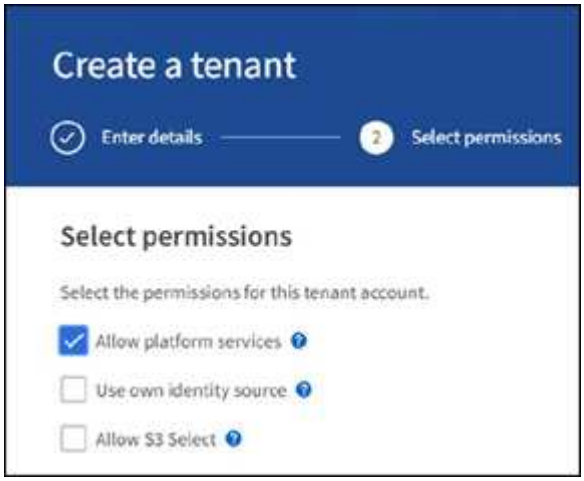
Les services de plateforme sont configurés par le locataire S3 via l'interface du gestionnaire des locataires. Pour plus d'informations, voir "Considérations relatives à l'utilisation des services de plate-forme".

Ce document est un supplément au "Guide des locataires StorageGRID 11.6" et fournit des instructions détaillées et des exemples de configuration du terminal et des compartiments pour les services d'intégration de la recherche. Les instructions d'installation d'Amazon Web Services (AWS) ou de Elasticsearch sur site indiquées ici sont fournies à des fins de test ou de démonstration uniquement.

Les participants doivent maîtriser Grid Manager et le Gestionnaire de locataires, et avoir accès au navigateur S3 pour effectuer des opérations de chargement (PUT) et de téléchargement (GET) de base pour les tests d'intégration de la recherche StorageGRID.

Créez des locataires et activez les services de plateforme

1. Créez un locataire S3 à l'aide de Grid Manager, entrez un nom d'affichage et sélectionnez le protocole S3.
2. Sur la page d'autorisation, sélectionnez l'option Autoriser les services de plate-forme. Vous pouvez également sélectionner d'autres autorisations, si nécessaire.



3. Configurez le mot de passe initial de l'utilisateur root du locataire ou, si la fédération identifier est activée sur la grille, sélectionnez le groupe fédéré disposant d'une autorisation d'accès racine pour configurer le compte du locataire.
4. Cliquez sur se connecter en tant que racine et sélectionnez godet : créer et gérer des godets.

   Vous accédez alors à la page Gestionnaire de locataires.

5. Dans le Gestionnaire des locataires, sélectionnez Mes clés d'accès pour créer et télécharger la clé d'accès S3 pour des tests ultérieurs.

Services d'intégration de recherche avec Amazon OpenSearch

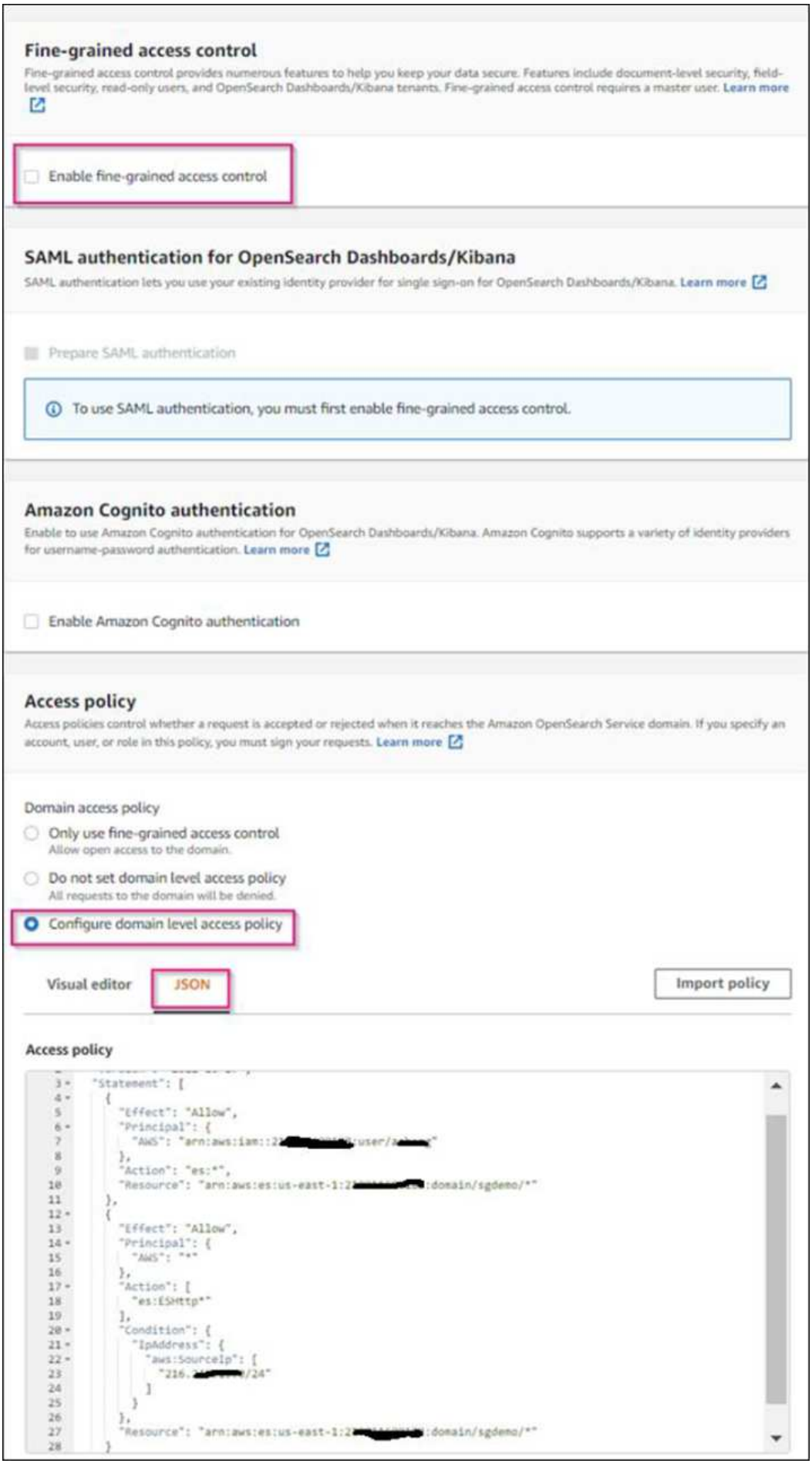
Configuration du service Amazon OpenSearch (anciennement Elasticsearch

Utilisez cette procédure pour une configuration rapide et simple du service OpenSearch à des fins de test/démonstration uniquement. Si vous utilisez Elasticsearch sur site pour des services d'intégration de la recherche, consultez la section Services d'intégration de recherche avec Elasticsearch sur site.

Vous devez disposer d'un identifiant de console AWS valide, d'une clé d'accès, d'une clé d'accès secrète et d'une autorisation pour vous abonner au service OpenSearch.

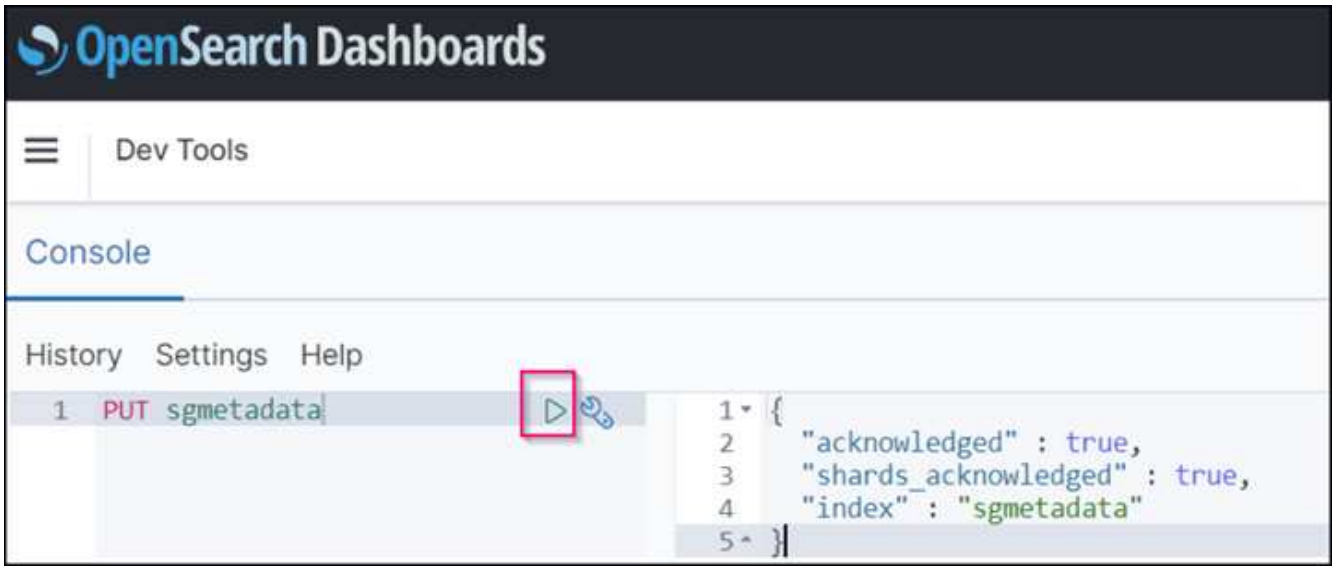
1. Créez un nouveau domaine à l'aide des instructions de "Mise en route du service OpenSearch d'AWS", à l'exception de ce qui suit :
   - Étape 4. Nom de domaine : sgdemo
   - Étape 10. Contrôle d'accès de grain fin : désélectionnez l'option Activer le contrôle d'accès de grain fin.
   - Étape 12. Règle d'accès : sélectionnez configurer la stratégie d'accès de niveau, sélectionnez l'onglet JSON pour modifier la stratégie d'accès en utilisant l'exemple suivant :
     - Remplacez le texte surligné par votre propre ID et nom d'utilisateur AWS Identity and Access Management (IAM).
     - Remplacez le texte en surbrillance (adresse IP) par l'adresse IP publique de votre ordinateur local utilisé pour accéder à la console AWS.
     - Ouvrez un onglet de navigateur pour "https://checkip.amazonaws.com" Pour trouver votre IP publique.

```
{

    "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/*"
        }
    ]
}
```

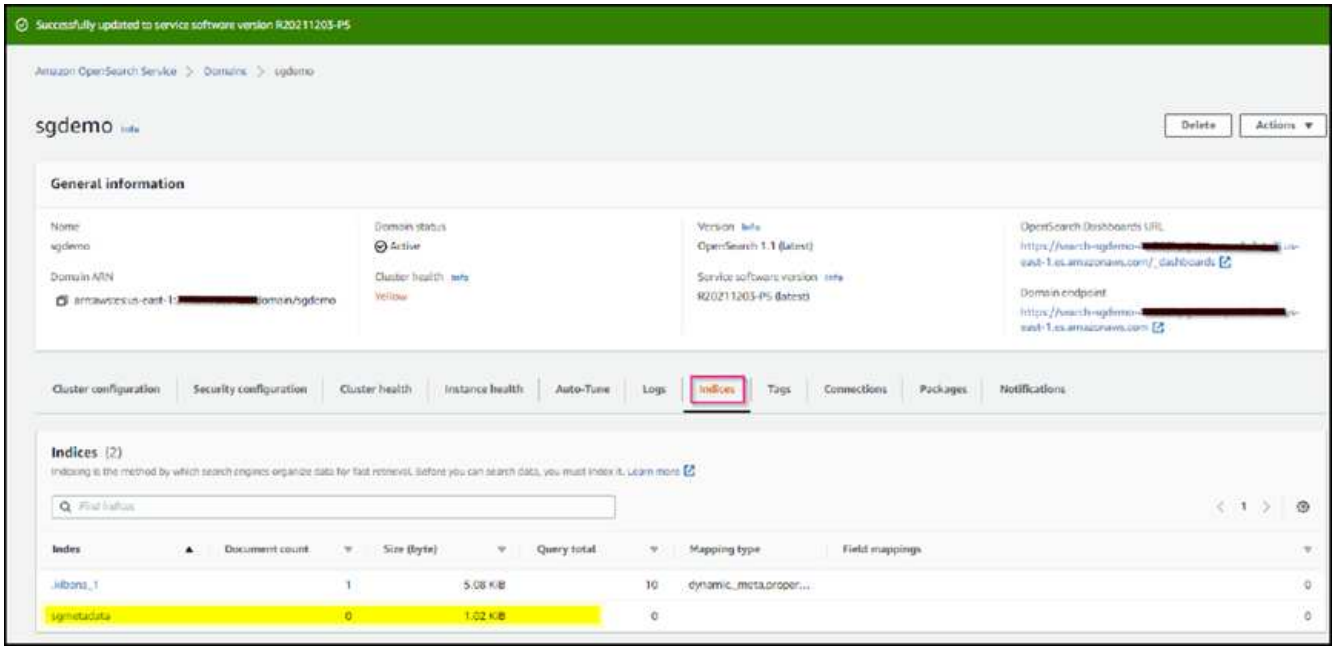

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more
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. Attendez 15 à 20 minutes pour que le domaine devienne actif.

3. Cliquez sur OpenSearch tableaux de bord URL pour ouvrir le domaine dans un nouvel onglet pour accéder au tableau de bord. Si vous obtenez une erreur d'accès refusé, vérifiez que l'adresse IP source de la stratégie d'accès est correctement définie sur l'adresse IP publique de votre ordinateur pour autoriser l'accès au tableau de bord du domaine.
4. Sur la page d'accueil du tableau de bord, sélectionnez Explorer de votre choix. Dans le menu, accédez à Management → Dev Tools
5. Sous Outils de développement → Console , entrez `PUT <index>` Où vous utilisez l'index pour le stockage des métadonnées d'objet StorageGRID. Nous utilisons le nom d'index 'gmetadatas' dans l'exemple suivant. Cliquez sur le petit symbole de triangle pour exécuter la commande PUT. Le résultat attendu s'affiche dans le panneau de droite comme indiqué dans l'exemple d'écran suivant.



6. Vérifiez que l'index est visible depuis l'interface utilisateur Amazon OpenSearch sous sgdomain > indices.

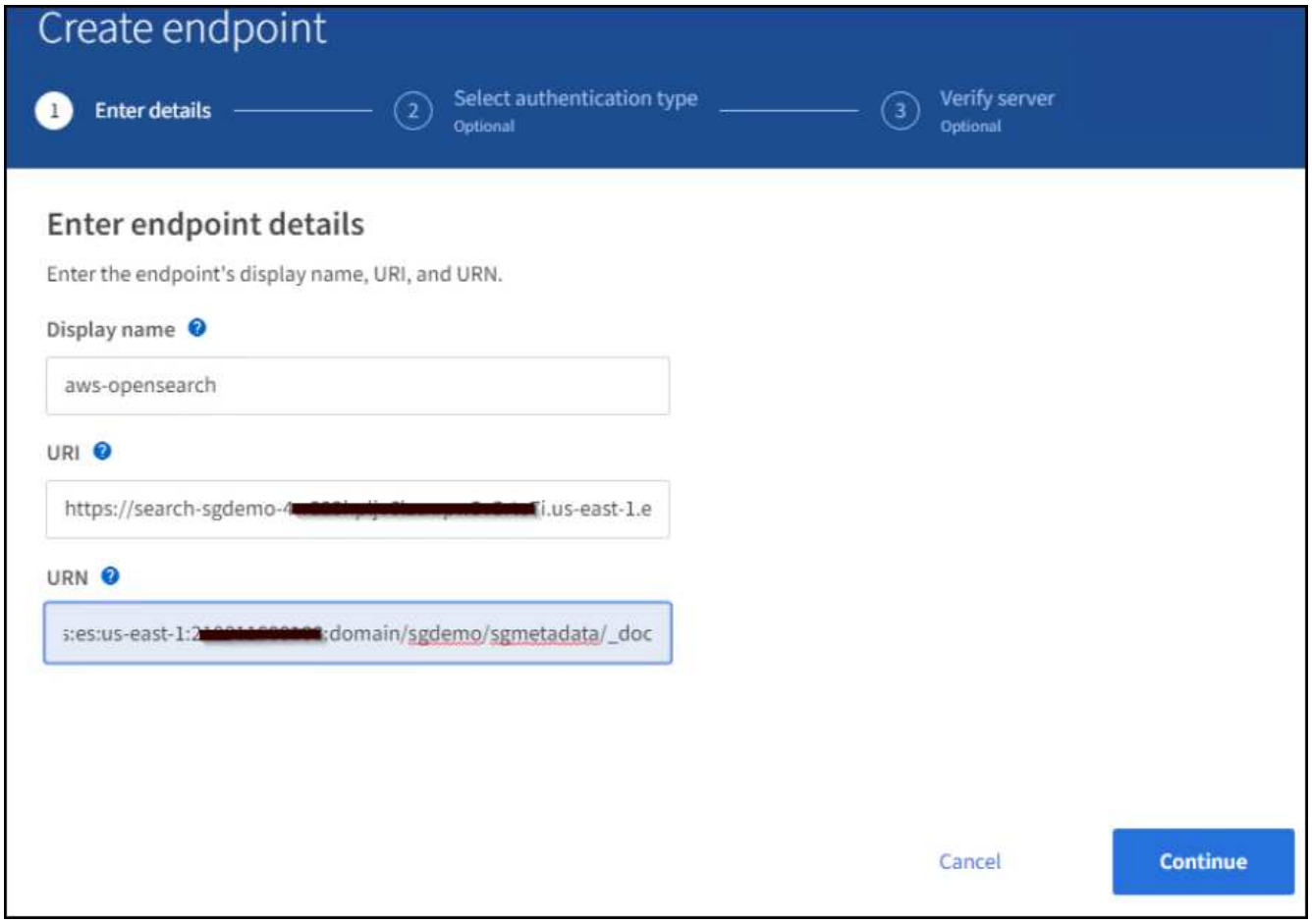


Configuration du terminal des services de plate-forme

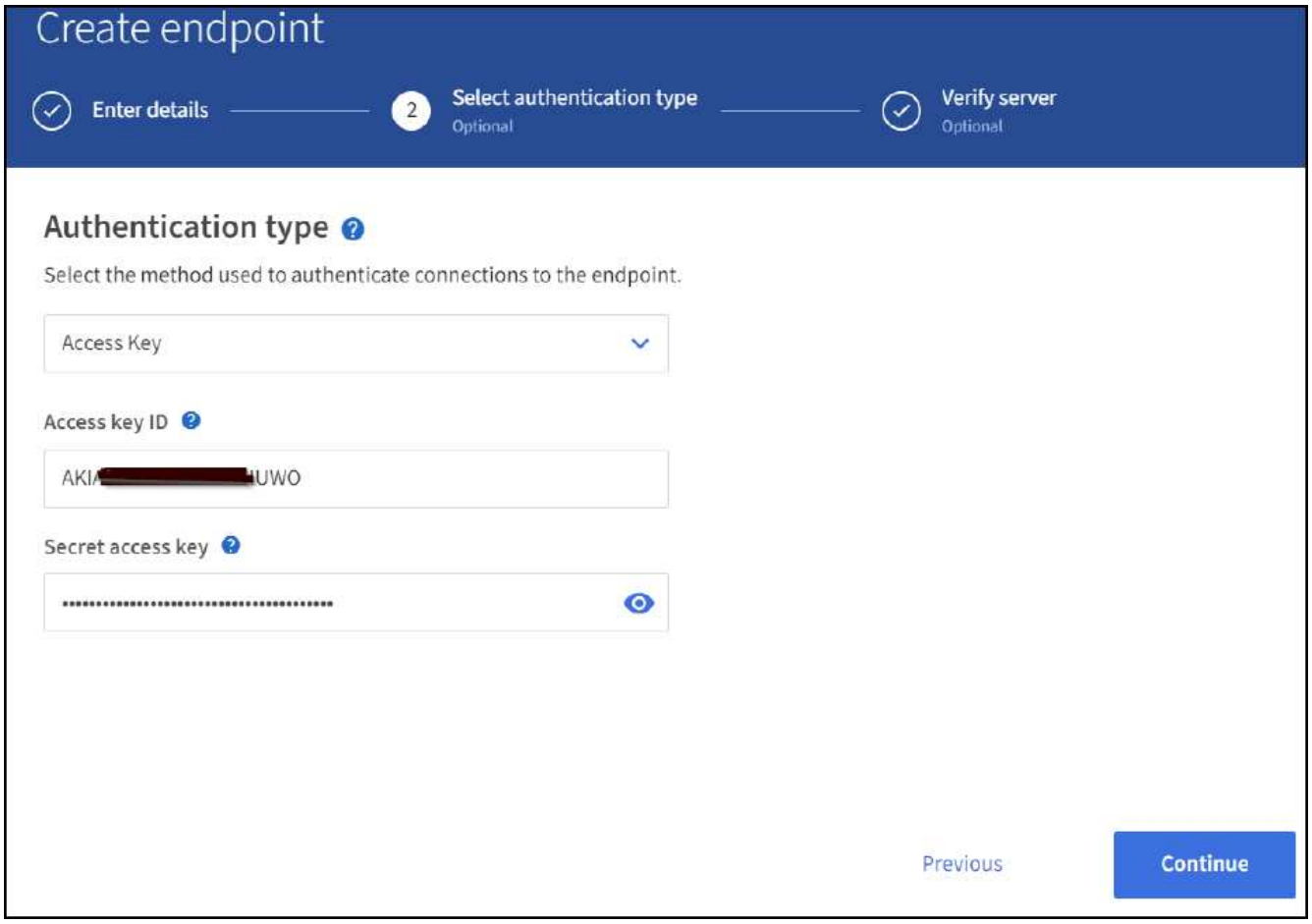
Pour configurer les terminaux des services de plate-forme, procédez comme suit :

1. Dans tenant Manager, accédez à STORAGE(S3) > terminaux des services de plateforme.
2. Cliquez sur Créer un point final, entrez les informations suivantes, puis cliquez sur Continuer :
   - Exemple de nom d'affichage `aws-opensearch`
   - Le noeud final du domaine dans la capture d'écran de l'exemple sous l'étape 2 de la procédure précédente dans le champ URI.
   - Le domaine ARN utilisé à l'étape 2 de la procédure précédente dans le champ URN et ajouter `/<index>/_doc` Jusqu'à la fin de l'ARN.

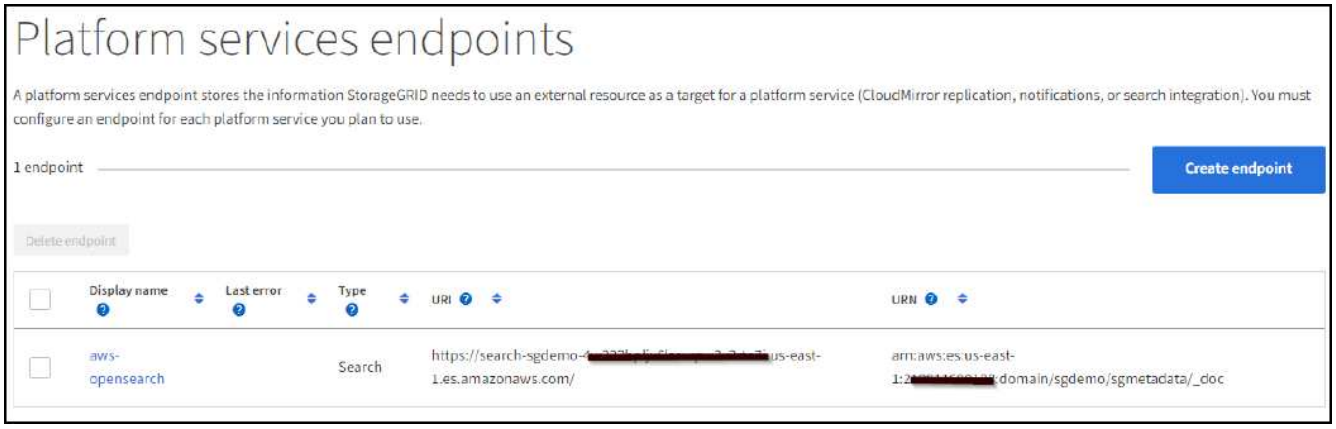
     Dans cet exemple, l'URN devient `arn:aws:es:us-east-1:211234567890:domain/sgdemo/sgmedata/_doc`.



3. Pour accéder au domaine Amazon OpenSearch sgdomain, choisissez Access Key comme type d'authentification, puis entrez la clé d'accès Amazon S3 et la clé secrète. Pour passer à la page suivante, cliquez sur Continuer.



4. Pour vérifier le noeud final, sélectionnez utiliser le certificat CA du système d'exploitation et tester et Créer un noeud final. Si la vérification réussit, un écran de point final similaire à la figure suivante s'affiche. En cas d'échec de la vérification, vérifiez que l'URN inclut `/<index>/_doc` À l'issue du chemin, la clé d'accès AWS et la clé secrète sont correctes.



Services d'intégration de recherche avec Elasticsearch sur site

Configuration Elasticsearch sur site

Cette procédure permet une configuration rapide des données sur site Elasticsearch et Kibana utilisant docker uniquement à des fins de test. Si le serveur Elasticsearch et Kibana existent déjà, passez à l'étape 5.

1. Suivez ceci "Procédure d'installation de Docker" pour installer docker. Nous utilisons le "Procédure d'installation de CentOS Docker" dans cette configuration.

```
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
```

   - Pour démarrer docker après le redémarrage, entrez les informations suivantes :

```
sudo systemctl enable docker
```

   - Réglez le `vm.max_map_count` valeur jusqu'à 262144 :

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

   - Pour conserver le paramètre après le redémarrage, saisissez les informations suivantes :

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

2. Suivez le "Guide de démarrage rapide d'Elasticsearch" Section auto-gérée pour installer et exécuter Elasticsearch et Kibana docker. Dans cet exemple, nous avons installé la version 8.1.

Notez le nom d'utilisateur/mot de passe et le jeton créés par Elasticsearch, vous devez utiliser ces éléments pour démarrer l'interface utilisateur Kibana et l'authentification du terminal de la plateforme 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.

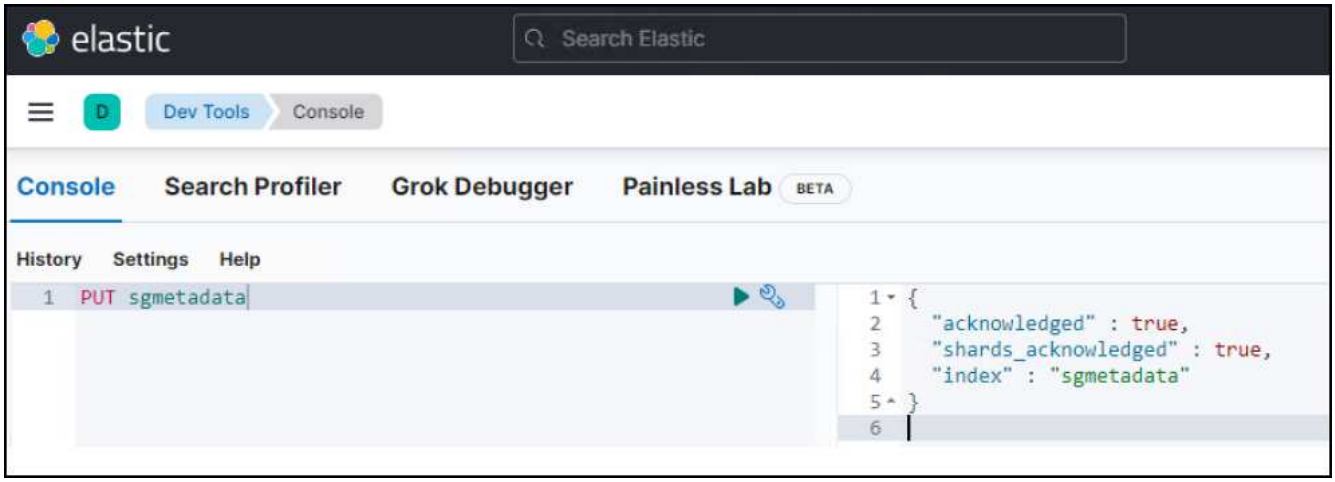
1. In a new terminal session, run:

```
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.

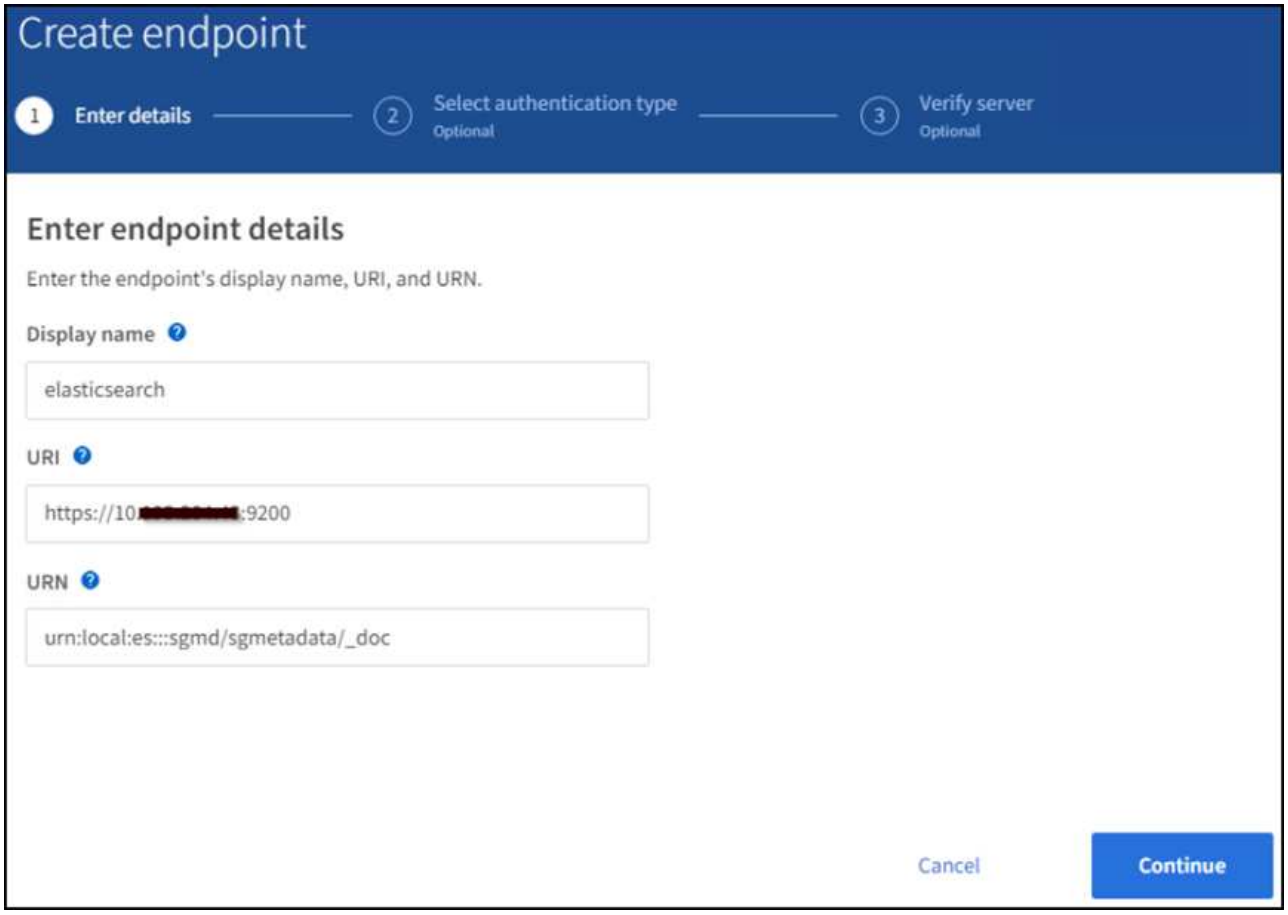
3. Après le démarrage du conteneur kibana docker, le lien URL `https://0.0.0.0:5601` s'affiche dans la console. Remplacez 0.0.0.0 par l'adresse IP du serveur dans l'URL.
4. Connectez-vous à l'interface utilisateur Kibana en utilisant le nom d'utilisateur `elastic` Et le mot de passe généré par Elastic dans l'étape précédente.
5. Pour la première connexion, sur la page d'accueil du tableau de bord, sélectionnez Explorer par vous-même. Dans le menu, sélectionnez gestion > Outils de développement.
6. Sur l'écran Console des outils de développement, entrez `PUT <index>` Où vous utilisez cet index pour stocker les métadonnées des objets StorageGRID. Nous utilisons le nom de l'index `sgmetadata` dans cet exemple. Cliquez sur le petit symbole de triangle pour exécuter la commande PUT. Le résultat attendu s'affiche dans le panneau de droite comme indiqué dans l'exemple d'écran suivant.



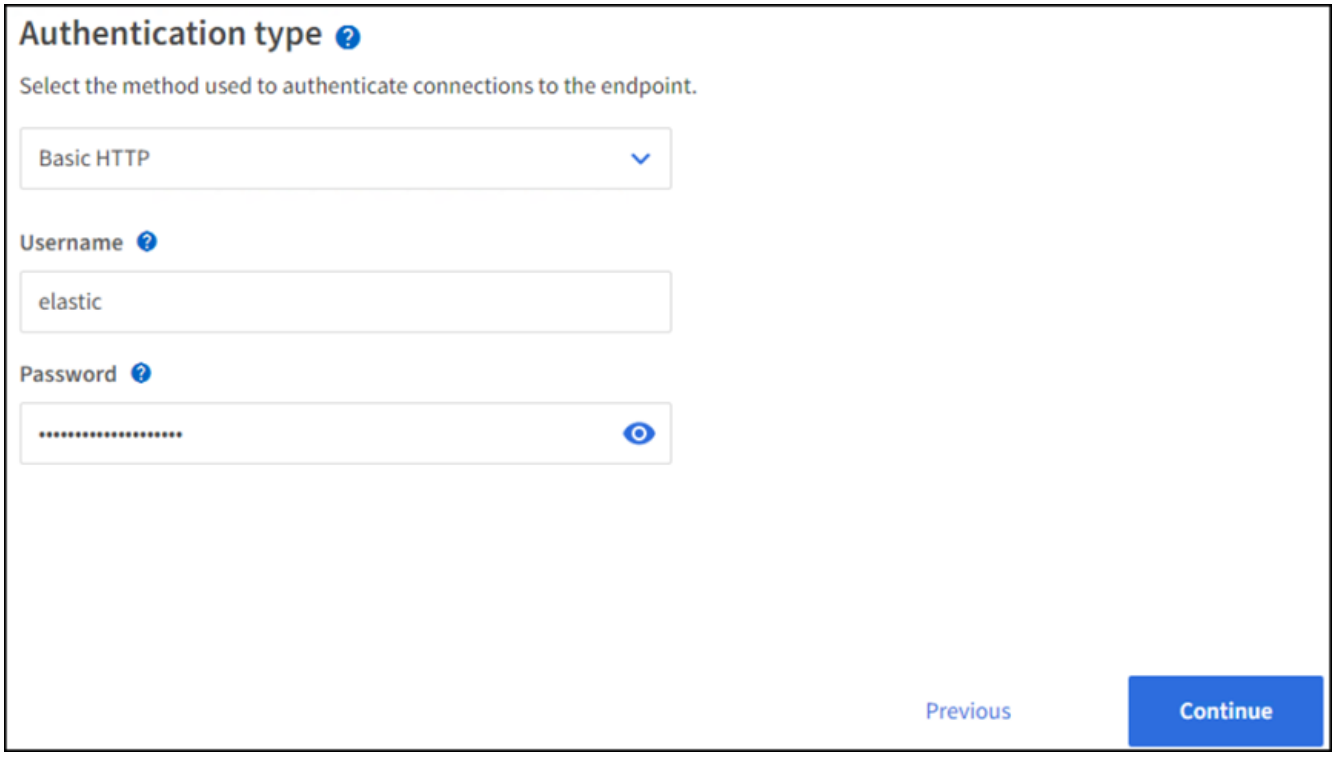
Configuration du terminal des services de plate-forme

Pour configurer les terminaux pour les services de plate-forme, procédez comme suit :

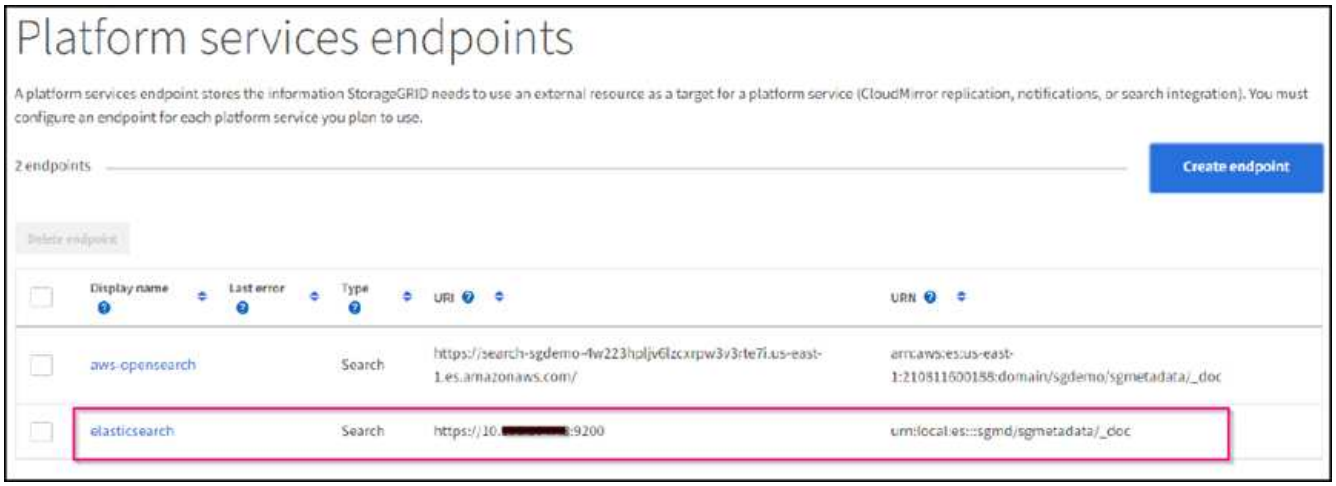
1. Dans tenant Manager, accédez à STORAGE(S3) > terminaux des services de plateforme
2. Cliquez sur Créer un point final, entrez les informations suivantes, puis cliquez sur Continuer :
   - Exemple de nom d'affichage : `elasticsearch`
   - URI : `https://<elasticsearch-server-ip or hostname>:9200`
   - URN : `urn:<something>:es:::<some-unique-text>/<index-name>/_doc` Où l'index-name est le nom que vous avez utilisé sur la console Kibana. Exemple : `urn:local:es:::sgmd/sgmetadata/_doc`



3. Sélectionnez Basic HTTP comme type d'authentification, saisissez le nom d'utilisateur `elastic` Et le mot de passe généré par le processus d'installation Elasticsearch. Pour passer à la page suivante, cliquez sur Continuer.



4. Sélectionnez ne pas vérifier le certificat et le test et Créer un noeud final pour vérifier le noeud final. Si la vérification est réussie, un écran de point final similaire à la capture d'écran suivante s'affiche. Si la vérification échoue, vérifiez que les entrées URN, URI et nom d'utilisateur/mot de passe sont correctes.



Configuration du service d'intégration de la recherche de compartiments

Une fois le terminal du service de plateforme créé, l'étape suivante consiste à configurer ce service au niveau du compartiment pour envoyer les métadonnées d'objet au terminal défini lors de la création ou de la suppression d'un objet, ou encore lors de la mise à jour de ses métadonnées ou balises.

Vous pouvez configurer l'intégration de la recherche à l'aide du Gestionnaire de locataires afin d'appliquer un code XML de configuration StorageGRID personnalisé à un compartiment comme suit :

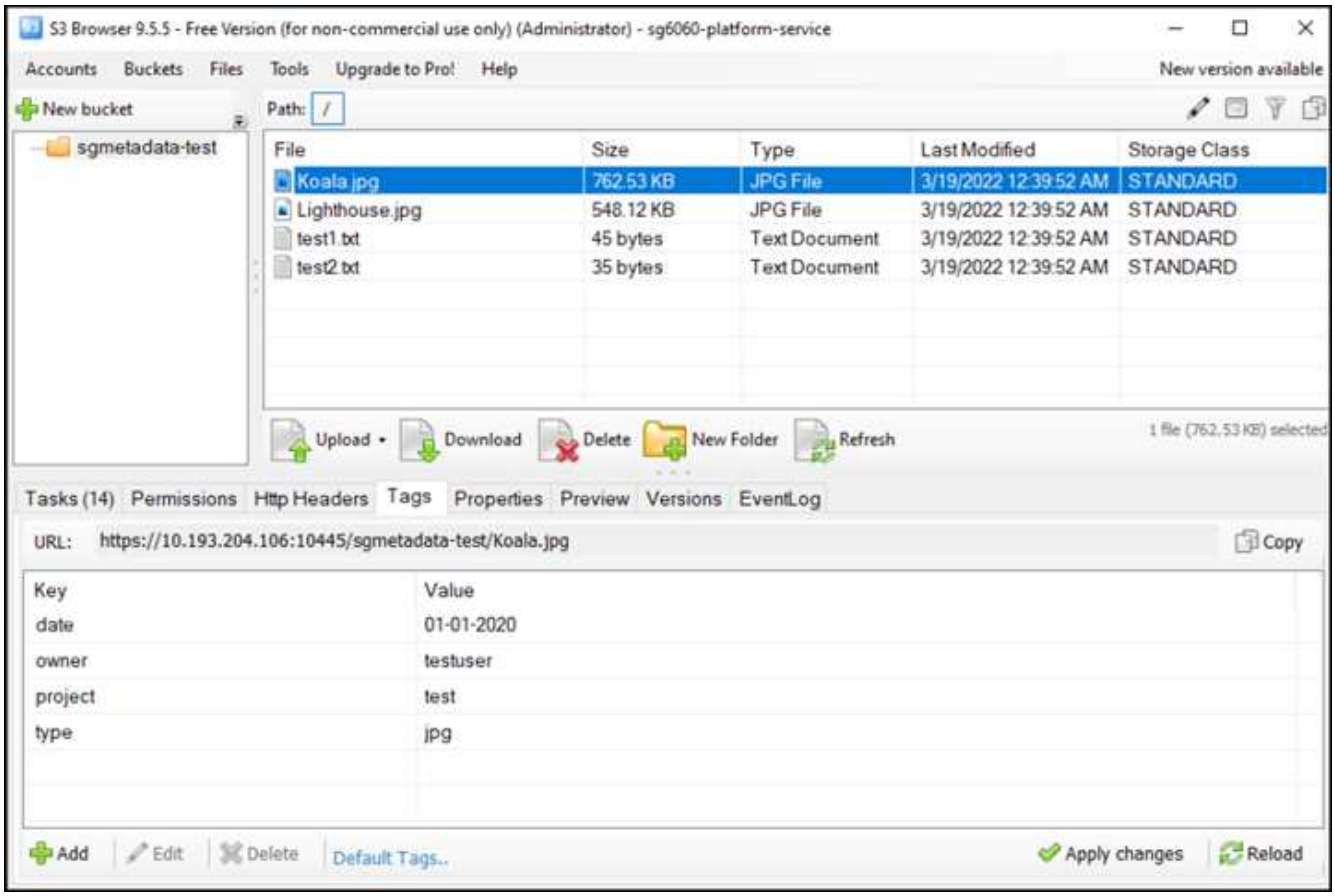
1. Dans le Gestionnaire des locataires, accédez à STORAGE(S3) > compartiments
2. Cliquez sur Créer un compartiment, entrez le nom du compartiment (par exemple, `sgmetadata-test`) et acceptez la valeur par défaut `us-east-1` région.
3. Cliquez sur Continuer > Créer un compartiment.
4. Pour afficher la page de présentation du compartiment, cliquez sur le nom du compartiment, puis sélectionnez Platform Services.
5. Sélectionnez la boîte de dialogue Activer l'intégration de la recherche. Dans la zone XML fournie, entrez le XML de configuration à l'aide de cette syntaxe.

   L'URN mis en surbrillance doit correspondre au terminal des services de plateforme que vous avez défini. Vous pouvez ouvrir un autre onglet du navigateur pour accéder au Gestionnaire de locataires et copier l'URN à partir du noeud final de services de plateforme défini.

   Dans cet exemple, nous n'avons utilisé aucun préfixe, ce qui signifie que les métadonnées de chaque objet de ce compartiment sont envoyées au terminal Elasticsearch précédemment défini.

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

6. Utilisez le navigateur S3 pour vous connecter à StorageGRID avec la clé secrète/d'accès par locataire, et téléchargez les objets de test vers `sgmetadata-test` et ajoutez des balises ou des métadonnées personnalisées aux objets.



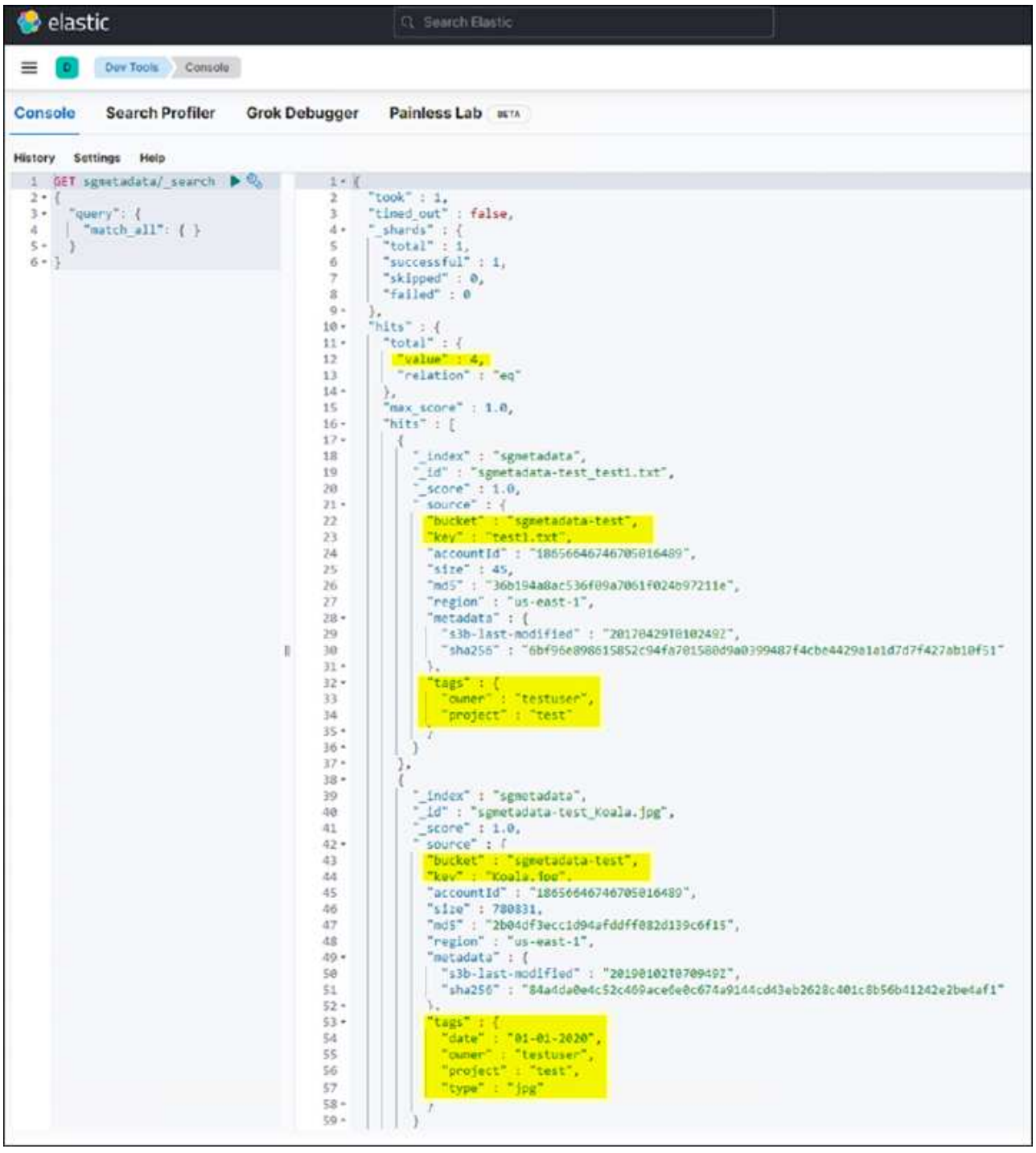
7. Utilisez l'interface utilisateur Kibana pour vérifier que les métadonnées de l'objet ont été chargées dans l'index des métadonnées sgmetadata.

   a. Dans le menu, sélectionnez gestion > Outils de développement.

   b. Collez l'exemple de requête dans le panneau de la console à gauche et cliquez sur le symbole du triangle pour l'exécuter.

      L'exemple de résultat de la requête 1 dans la capture d'écran suivante montre quatre enregistrements. Ceci correspond au nombre d'objets dans le godet.

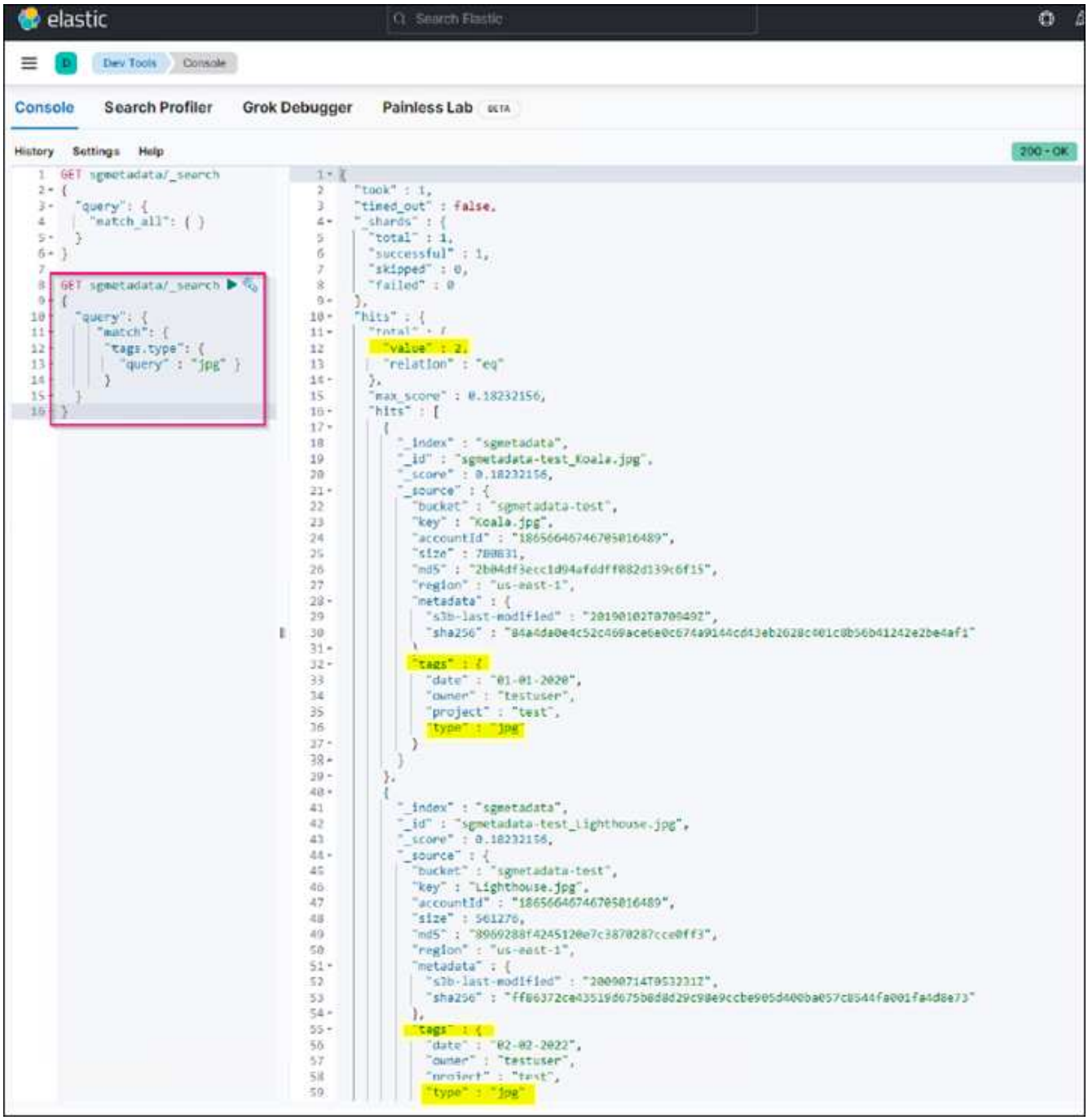
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



Le résultat de l'exemple de requête 2 dans la capture d'écran suivante montre deux enregistrements de type de balise jpg.

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

+



Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- "Qu'est-ce que les services de plateforme"
- "Documentation StorageGRID 11.6"

Par Angela Cheng

Clone de nœud

Considérations et performances sur le clonage des nœuds.

Considérations relatives au clonage de nœuds

Le clone de nœud peut être une méthode plus rapide pour remplacer les nœuds d'appliance existants dans le cadre d'une mise à jour technologique, d'une augmentation de la capacité ou d'une augmentation de la performance du système StorageGRID. Le clone de nœud peut également être utile pour la conversion en chiffrement de nœud avec un KMS ou pour le remplacement d'un nœud de stockage DDP8 par DDP16.

- La capacité utilisée du nœud source n'est pas pertinente pour le temps nécessaire à la fin du processus de clonage. Le clone de nœud est une copie complète du nœud, y compris l'espace libre dans le nœud.
- Les appareils source et cible doivent avoir la même version PGE
- La capacité du nœud de destination doit toujours être supérieure à la source
  - Assurez-vous que la nouvelle appliance de destination possède un lecteur plus grand que la source
  - Si l'appliance de destination possède des lecteurs de même taille et est configurée pour DDP8, vous pouvez configurer la destination pour DDP16. Si la source est déjà configurée pour DDP16, le clone de nœud ne sera pas possible.
  - Lorsque vous utilisez des appliances SG5660 ou SG5760 pour des appliances SG6060, sachez que les SG6060 disposent de 60 disques de capacité lorsque le SG6060 ne présente que 58.
- Le processus de clonage de nœud nécessite que le nœud source soit hors ligne de la grille pendant toute la durée du processus de clonage. Si un nœud supplémentaire se déconnecte pendant ce temps, les services client peuvent être affectés.
- 11.8 et ci-dessous : un nœud de stockage ne peut être hors ligne que pendant 15 jours. Si l'estimation du processus de clonage est proche de 15 jours ou supérieure à 15 jours, utilisez les procédures d'extension et de désaffectation.
  - 11.9: La limite de 15 jours a été supprimée.
- Pour un SG6060 ou un SG6160 avec tiroirs d'extension, vous devez ajouter l'heure de la taille de tiroir appropriée à l'heure de l'appliance de base pour obtenir la durée totale du clone.
- Le nombre de volumes d'une appliance de stockage cible doit être supérieur ou égal au nombre de volumes du nœud source. Vous ne pouvez pas cloner un nœud source avec 16 volumes de magasin d'objets (rangedb) vers une appliance de stockage cible avec 12 volumes de magasin d'objets, même si l'appliance cible a une capacité supérieure au nœud source. La plupart des appliances de stockage disposent de 16 volumes de stockage objet, à l'exception de l'appliance SGF6112 qui ne dispose que de 12 volumes de stockage objet. Par exemple, vous ne pouvez pas cloner à partir d'un SG5760 vers un SGF6112.

Estimations des performances des clones de nœuds

Les tableaux suivants contiennent des estimations calculées pour la durée du clone de nœud. Les conditions varient donc, les entrées dans **BOLD** peuvent risquer de dépasser la limite de 15 jours pour un nœud en panne.

DDP8

SG5612/SG5712/SG5812 → TOUS

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	1 jour	2 jours	2.5 jours	3 jours	4 jours	4.5 jours	5.5 jours
25 GO	1 jour	2 jours	2.5 jours	3 jours	4 jours	4.5 jours	5.5 jours

SG5660 → SG5760/SG5860

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	3.5 jours	7 jours	8.5 jours	10.5 jours	**13,5 jours**	**15,5 jours**	**18,5 jours**
25 GO	3.5 jours	7 jours	8.5 jours	10.5 jours	**13,5 jours**	**15,5 jours**	**18,5 jours**

SG5660 → SG6060/SG6160

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	2.5 jours	4.5 jours	5.5 jours	6.5 jours	9 jours	10 jours	**12 jours**
25 GO	2 jours	4 jours	5 jours	6 jours	8 jours	9 jours	10 jours

SG5760/SG5860 → SG5760/SG5860

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	3.5 jours	7 jours	8.5 jours	10.5 jours	**13,5 jours**	**15,5 jours**	**18,5 jours**
25 GO	3.5 jours	7 jours	8.5 jours	10.5 jours	**13,5 jours**	**15,5 jours**	**18,5 jours**

SG5760/SG5860 → SG6060/SG6160

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	2.5 jours	4.5 jours	5.5 jours	6.5 jours	9 jours	10 jours	**12 jours**
25 GO	2 jours	3.5 jours	4.5 jours	5.5 jours	7 jours	8 jours	9.5 jours

SG6060/SG6160 → SG6060/SG6160

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	2.5 jours	4.5 jours	5.5 jours	6.5 jours	8.5 jours	9.5 jours	11.5 jours
25 GO	2 jours	3 jours	4 jours	4.5 jours	6 jours	7 jours	8.5 jours

DDP16

SG5760/SG5860 → SG5760/SG5860

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	3.5 jours	6.5 jours	8 jours	9.5 jours	**12,5 jours**	**14 jours**	**17 jours**
25 GO	3.5 jours	6.5 jours	8 jours	9.5 jours	**12,5 jours**	**14 jours**	**17 jours**

SG5760/SG5860 → SG6060/SG6160

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	2.5 jours	5 jours	6 jours	7.5 jours	10 jours	11 jours	**13 jours**
25 GO	2 jours	3.5 jours	4 jours	5 jours	6.5 jours	7 jours	8.5 jours

SG6060/SG6160 → SG6060/SG6160

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	3 jours	5 jours	6 jours	7 jours	9.5 jours	10.5 jours	**13 jours**

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
25 GO	2 jours	3.5 jours	4.5 jours	5 jours	7 jours	7.5 jours	9 jours

Tiroir d'extension (à ajouter au-dessus des SG6060/SG6160 pour chaque tiroir de l'appliance source)

Vitesse de l'interface réseau	Taille de disque de 4 To	Taille de disque de 8 To	Taille de disque de 10 To	Taille des disques de 12 To	Taille de disque de 16 To	Taille des disques de 18 To	Taille du disque 22 To
10 GBIT/S.	3.5 jours	5 jours	6 jours	7 jours	9.5 jours	10.5 jours	**12 jours**
25 GO	2 jours	3 jours	4 jours	4.5 jours	6 jours	7 jours	8.5 jours

Par Aron Klein

Procédure de relocalisation du site dans le grid et de modification du réseau à l'échelle du site

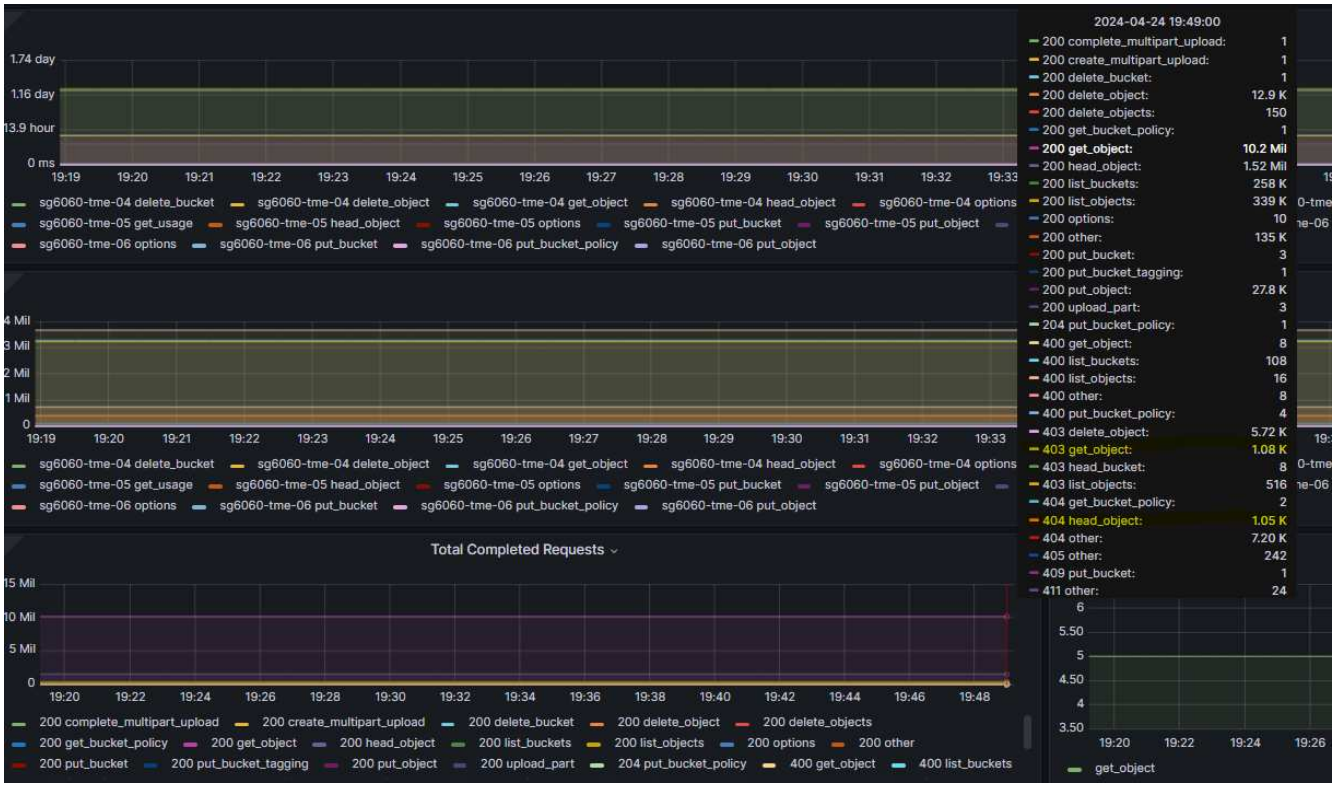
Ce guide décrit la préparation et la procédure à suivre pour déplacer un site StorageGRID dans une grille multi-sites. Vous devez avoir une compréhension complète de cette procédure et prévoir à l'avance pour assurer un processus sans heurt et minimiser l'interruption pour les clients.

Si vous devez modifier le réseau grille de la grille entière, reportez-vous à la section "Modifiez les adresses IP de tous les nœuds de la grille".

Considérations avant la relocalisation du site

- Le déplacement du site doit être terminé et tous les nœuds doivent être en ligne dans les 15 jours pour éviter la reconstruction de la base de données Cassandra.
  "Panne d'un nœud de stockage de plus de 15 jours"
- Si une règle ILM de la règle active utilise un comportement d'ingestion strict, envisagez de la modifier en vue de l'équilibrer ou de la double allocation si le client souhaite continuer à PLACER les objets dans la grille pendant la relocalisation du site.
- Pour les appliances de stockage de 60 disques ou plus, ne déplacez jamais le tiroir avec des disques installés. Étiquetez chaque lecteur de disque et retirez-le du boîtier de stockage avant de le emballer/déplacer.
- Changement d'appliance StorageGRID le réseau local virtuel du réseau de la grille peut être effectué à distance sur le réseau d'administration ou le réseau client. Sinon, prévoyez d'être sur site pour effectuer la modification avant ou après la mutation.
- Vérifiez si l'application client utilise la TÊTE ou si l'objet de non-existence est utilisé avant la MISE. Si oui, remplacez la cohérence du compartiment par site fort pour éviter les erreurs HTTP 500. Si vous n'êtes pas sûr, consultez la présentation S3 graphiques Grafana **Gestionnaire de grille > support > métriques**, placez le curseur de la souris sur le graphique « demande totale terminée ». S'il y a un nombre très élevé de 404 objets GET ou 404 objets Head, une ou plusieurs applications utilisent probablement l'objet Head

ou Get nonexistence. Le compte est cumulatif, passez la souris sur différents chronologies pour voir la différence.



Procédure de modification de l’adresse IP de la grille avant le déplacement du site

Étapes

1. Si un nouveau sous-réseau de réseau Grid sera utilisé au nouvel emplacement, "Ajoutez le sous-réseau à la liste de sous-réseau du réseau Grid"
2. Connectez-vous au nœud d’administration principal, utilisez change-ip pour effectuer une modification de l’adresse IP de la grille. **Stage** doit être effectué avant d’arrêter le nœud pour le déplacement.
   a. Sélectionnez 2 puis 1 pour modification de l’adresse IP de la grille

```
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. sélectionnez 5 pour afficher les modifications

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

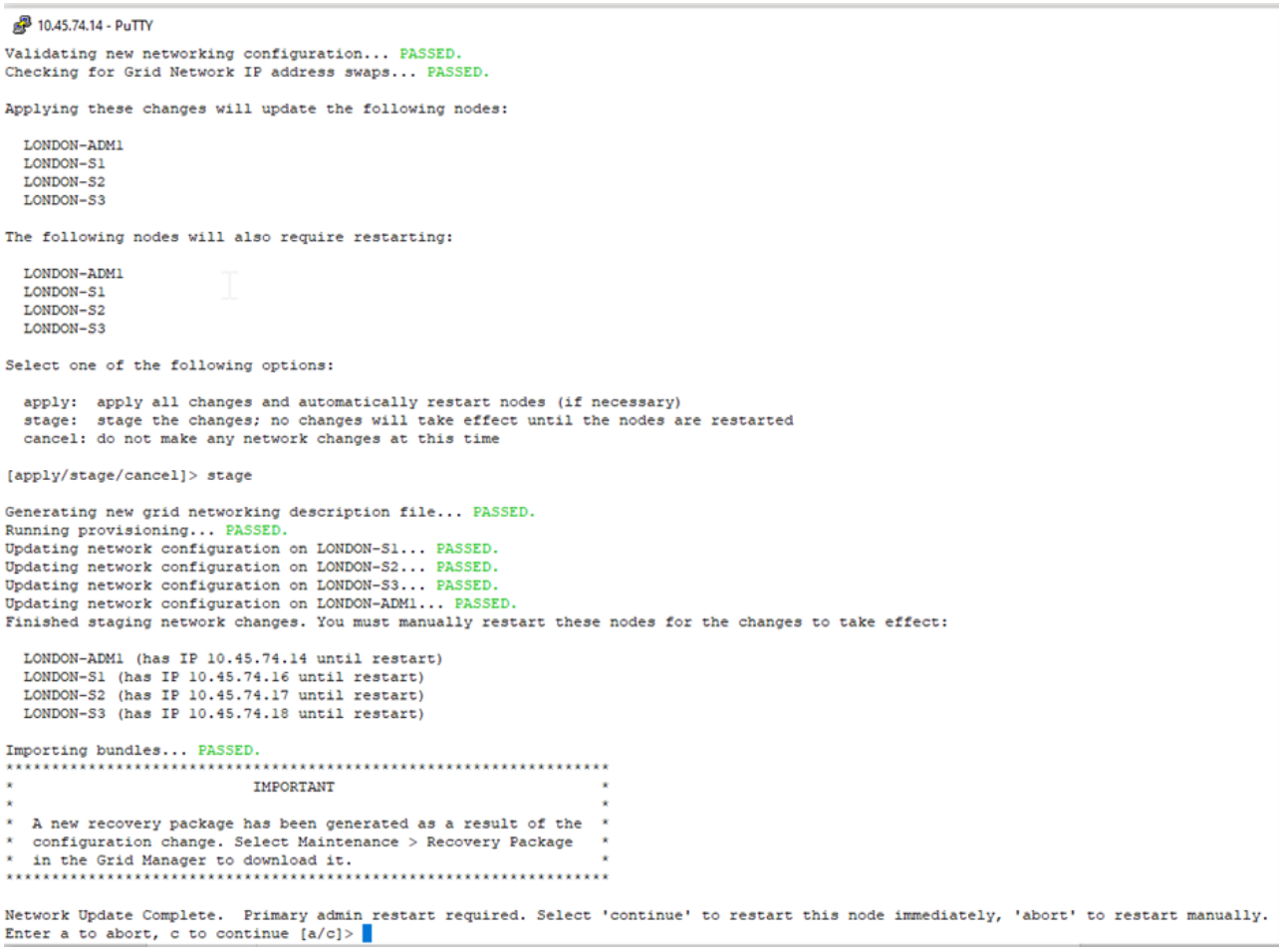
c. sélectionner 10 pour valider et appliquer la modification.

```
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
```

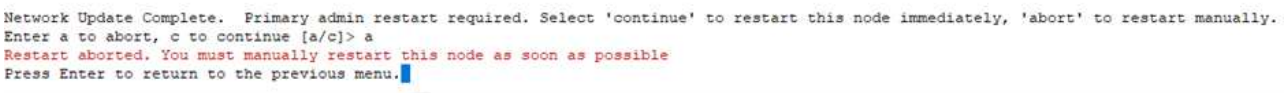
d. Vous devez sélectionner **stage** dans cette étape.

```
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. Si le nœud d'administration principal est inclus dans la modification ci-dessus, entrez **'a' pour redémarrer manuellement le nœud d'administration principal**



f. Appuyez sur ENTER pour revenir au menu précédent et quitter l'interface change-ip.



3. À partir de Grid Manager, téléchargez le nouveau package de récupération. **Grid Manager** > **Maintenance** > **paquet de récupération**
4. Si une modification VLAN est nécessaire sur l'appliance StorageGRID, reportez-vous à la section Modification du VLAN de l'appliance.
5. Arrêtez tous les nœuds et/ou appliances sur le site, étiquetez/retirez les disques si nécessaire, puis démettez, emballez et déplacez-les.
6. Si vous prévoyez de modifier l'adresse ip du réseau d'administration et/ou le VLAN et l'adresse ip du client, vous pouvez effectuer la modification après le déplacement.

Modification du VLAN de l'appliance

La procédure ci-dessous suppose que vous disposez d'un accès à distance au réseau client ou administrateur de l'appliance StorageGRID pour effectuer la modification à distance.

Étapes

1. Avant d'arrêter l'appareil,
"mettez l'appareil en mode de maintenance".

2. Utilisation d'un navigateur pour accéder à l'interface graphique du programme d'installation de l'appliance StorageGRID à l'aide de https://<admin-or-client-network-ip>:8443. Impossible d'utiliser Grid IP car la nouvelle Grid IP est déjà en place une fois que l'appliance est en mode maintenance.
3. Modifiez le VLAN pour le réseau Grid. Si vous accédez à l'appliance sur le réseau client, vous ne pouvez pas modifier le VLAN client pour le moment, vous pouvez le modifier après le déplacement.
4. connectez l'appliance à l'appliance et arrêtez le nœud en utilisant « shutdoown -h now »
5. Une fois les appliances prêtes sur le nouveau site, accédez à l'interface utilisateur graphique du programme d'installation de l'appliance StorageGRID à l'aide de https://<grid-network-ip>:8443. Vérifiez que l'état du stockage est optimal et que la connectivité réseau est assurée par les autres nœuds Grid à l'aide des outils ping/nmap disponibles dans l'interface graphique.
6. Si vous prévoyez de modifier l'adresse IP du réseau client, vous pouvez modifier le VLAN client à ce stade. Le réseau client n'est pas prêt tant que vous n'avez pas mis à jour l'adresse ip du réseau client à l'aide de l'outil change-ip à l'étape suivante.
7. Quittez le mode maintenance. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer dans StorageGRID**.
8. Une fois que tous les nœuds sont actifs et que Grid n'indique aucun problème de connectivité, utilisez change-ip pour mettre à jour le réseau d'administration de l'appliance et le réseau client, si nécessaire.

Migration du stockage basé sur les objets d'ONTAP S3 vers StorageGRID

Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

Démo de migration

Cette démonstration porte sur la migration des utilisateurs et des compartiments d'ONTAP S3 vers StorageGRID.

Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

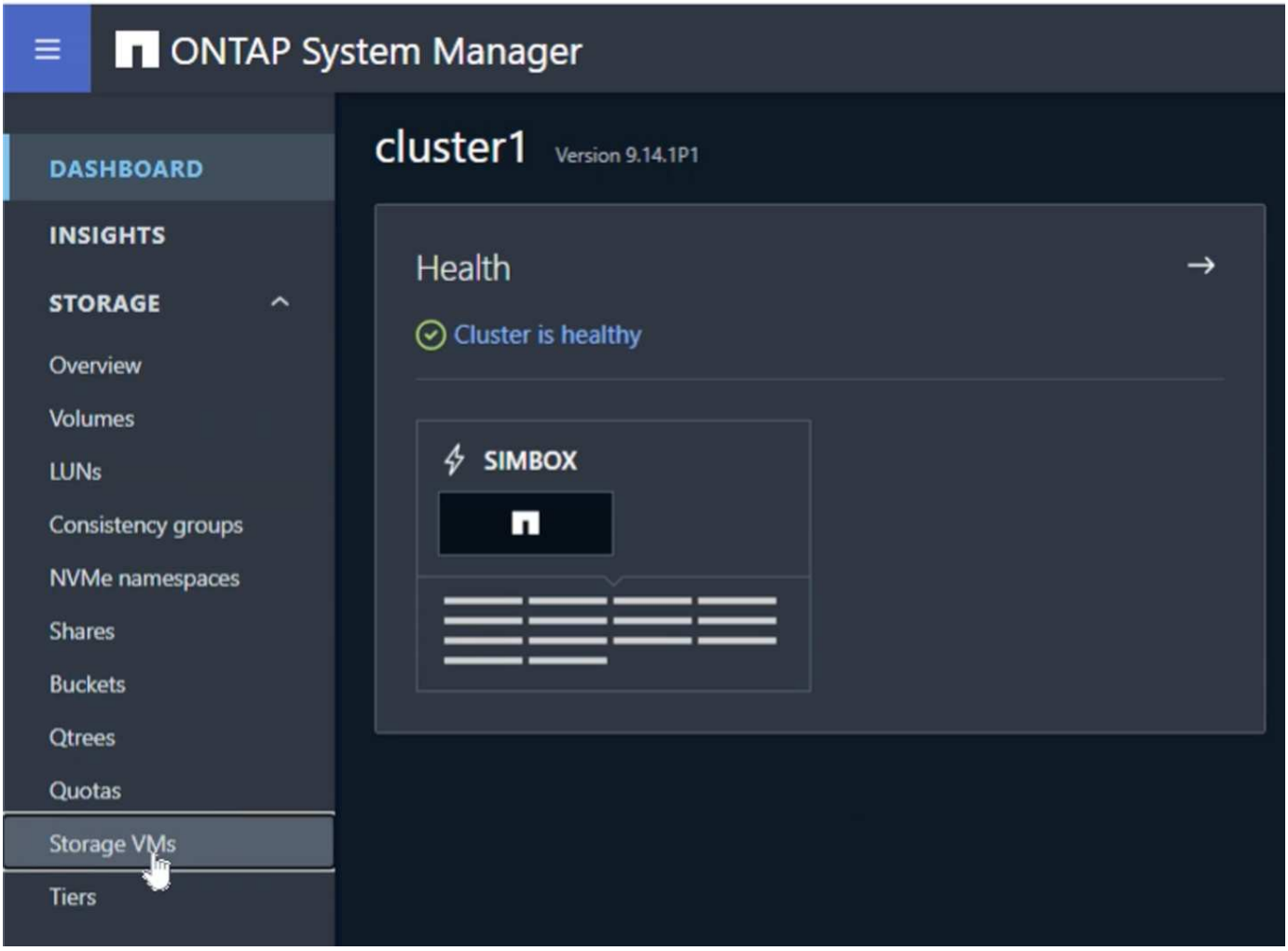
Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

Préparation de ONTAP

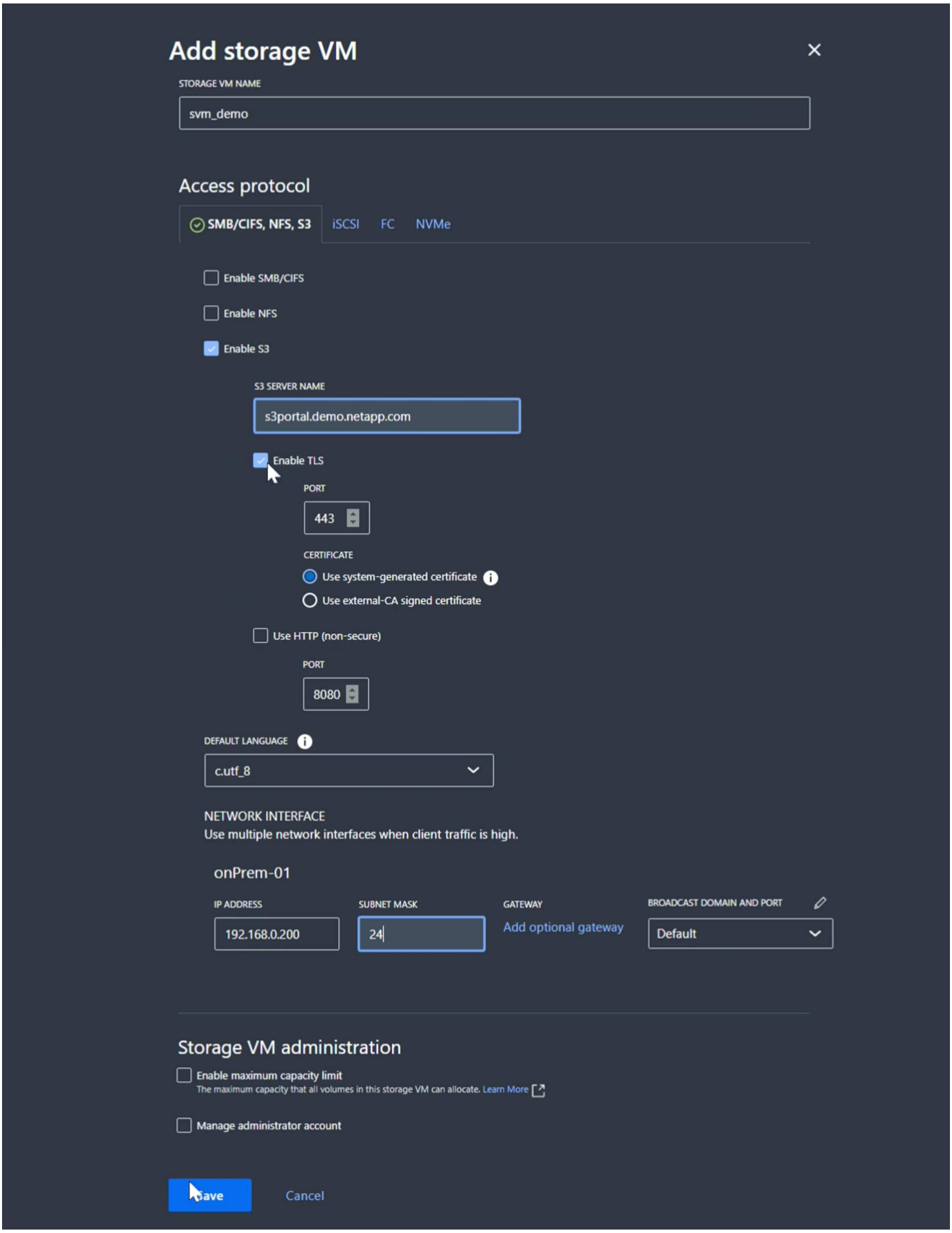
À des fins de démonstration, nous allons créer un serveur de magasin d'objets SVM, un utilisateur, un groupe, une politique de groupe et des compartiments.

Créez la machine virtuelle de stockage

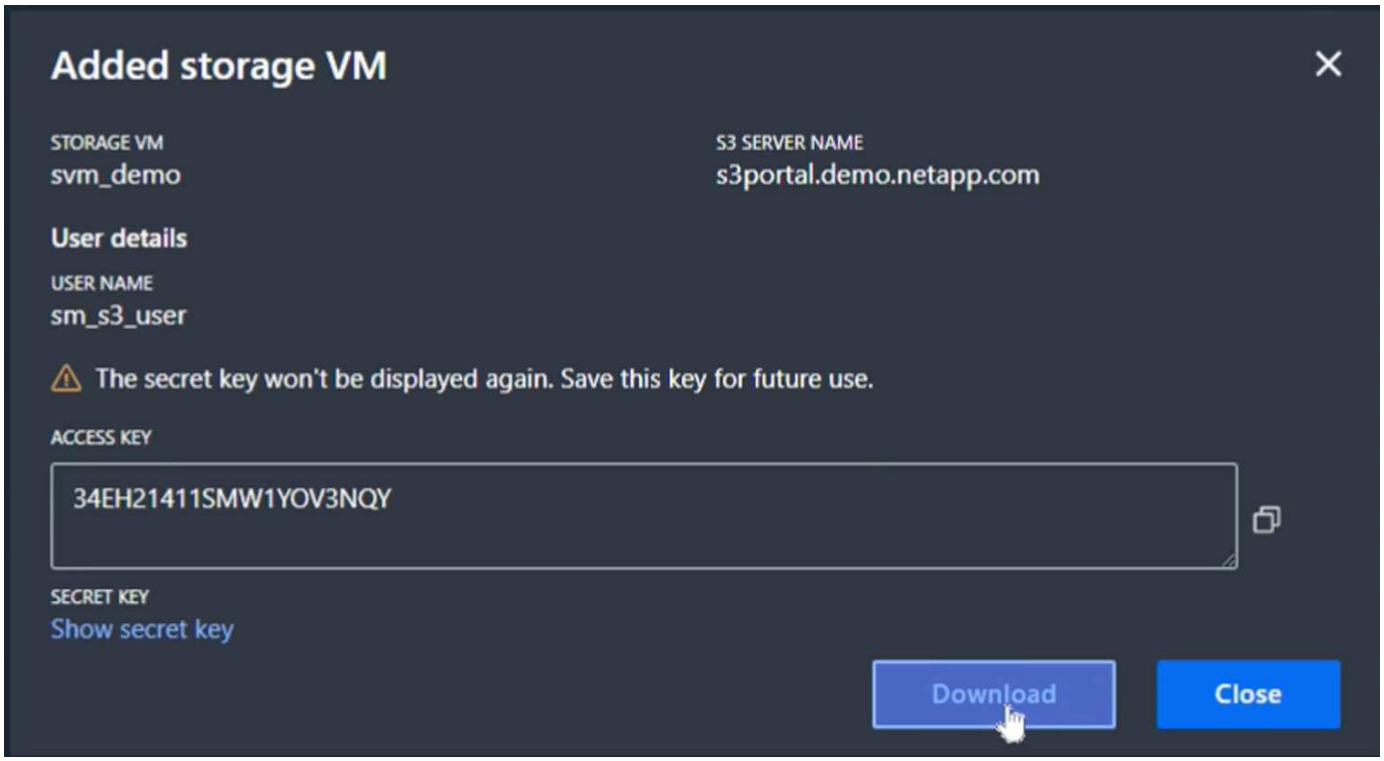
Dans le Gestionnaire système ONTAP, accédez à VM de stockage et ajoutez une nouvelle VM de stockage.



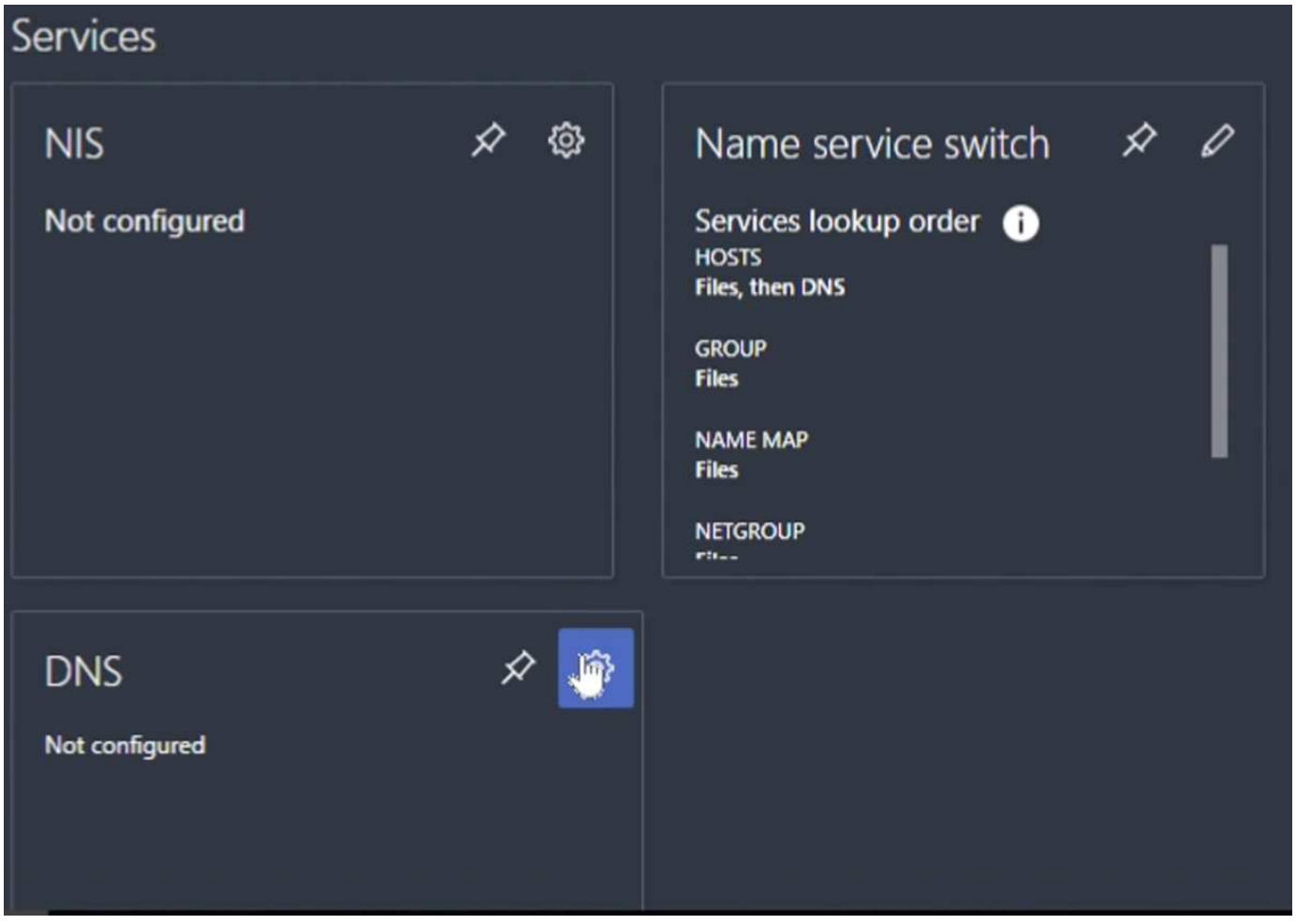
Cochez les cases « Activer S3 » et « Activer TLS » et configurez les ports HTTP(S). Définissez l'adresse IP, le masque de sous-réseau et définissez la passerelle et le domaine de diffusion si vous n'utilisez pas la valeur par défaut ou requise dans votre environnement.



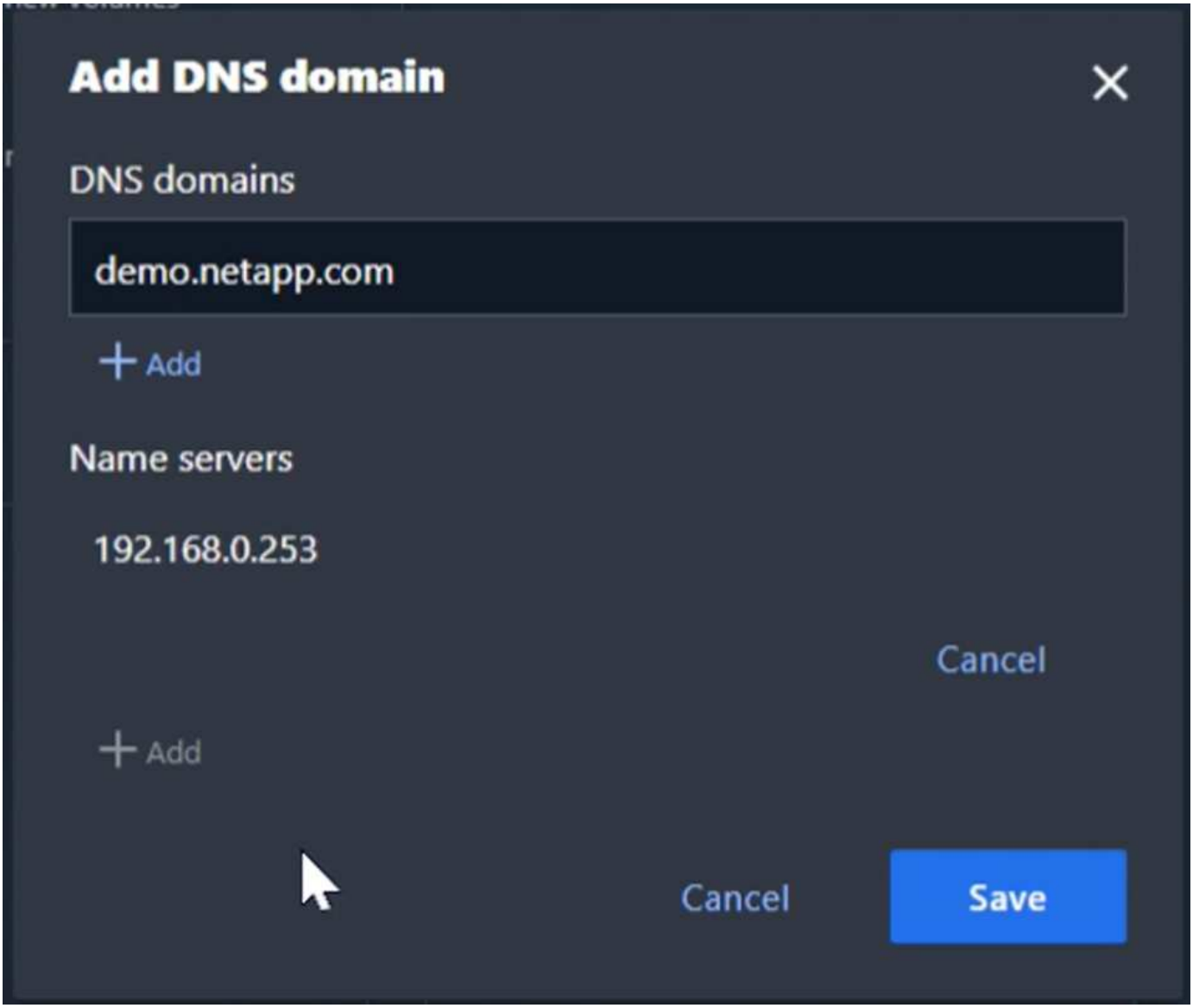
Un utilisateur sera créé dans le cadre de la création de la SVM. Téléchargez les clés S3 pour cet utilisateur et fermez la fenêtre.



Une fois le SVM créé, éditer le SVM et ajouter les paramètres DNS.

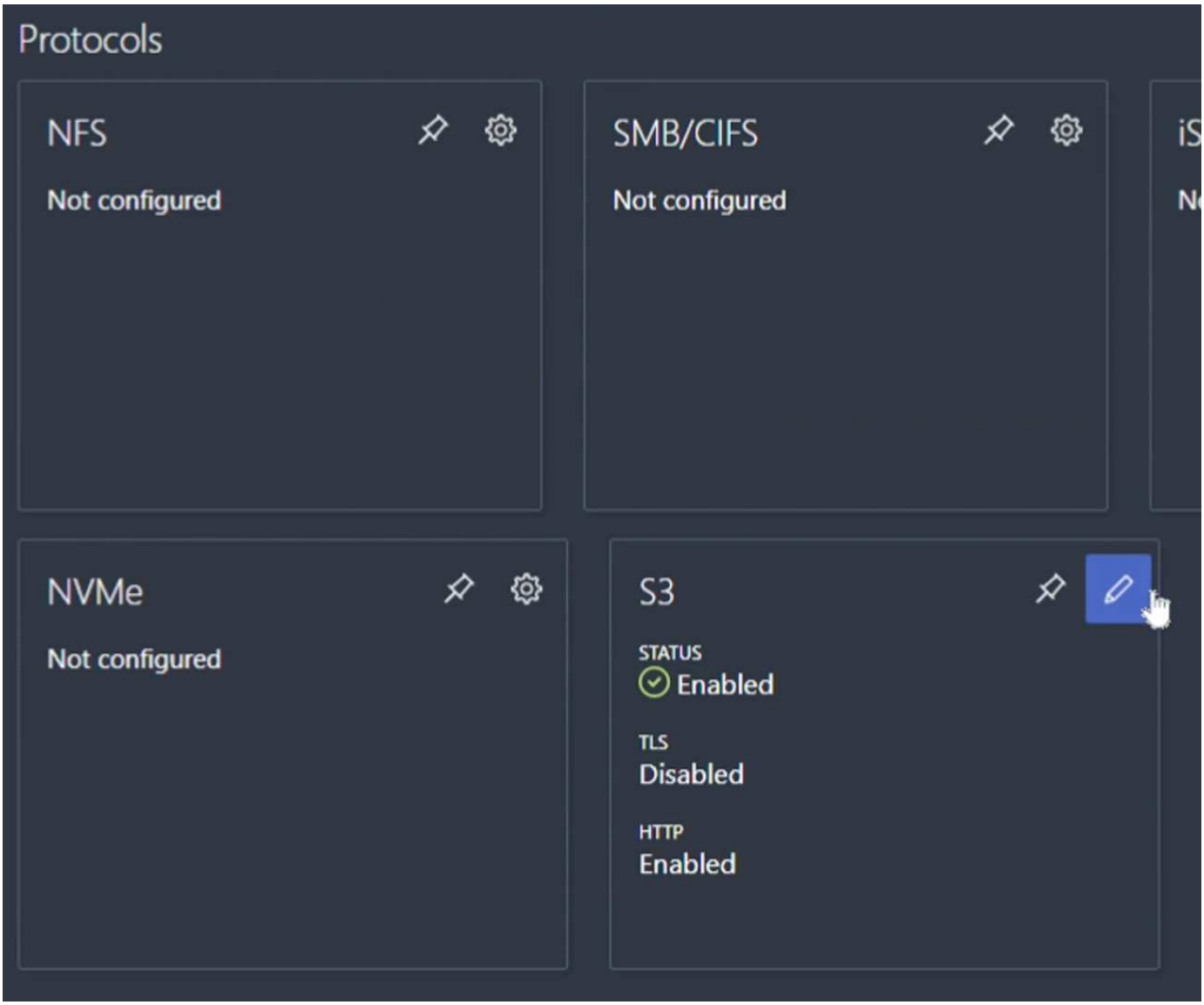


Définissez le nom DNS et l'adresse IP.

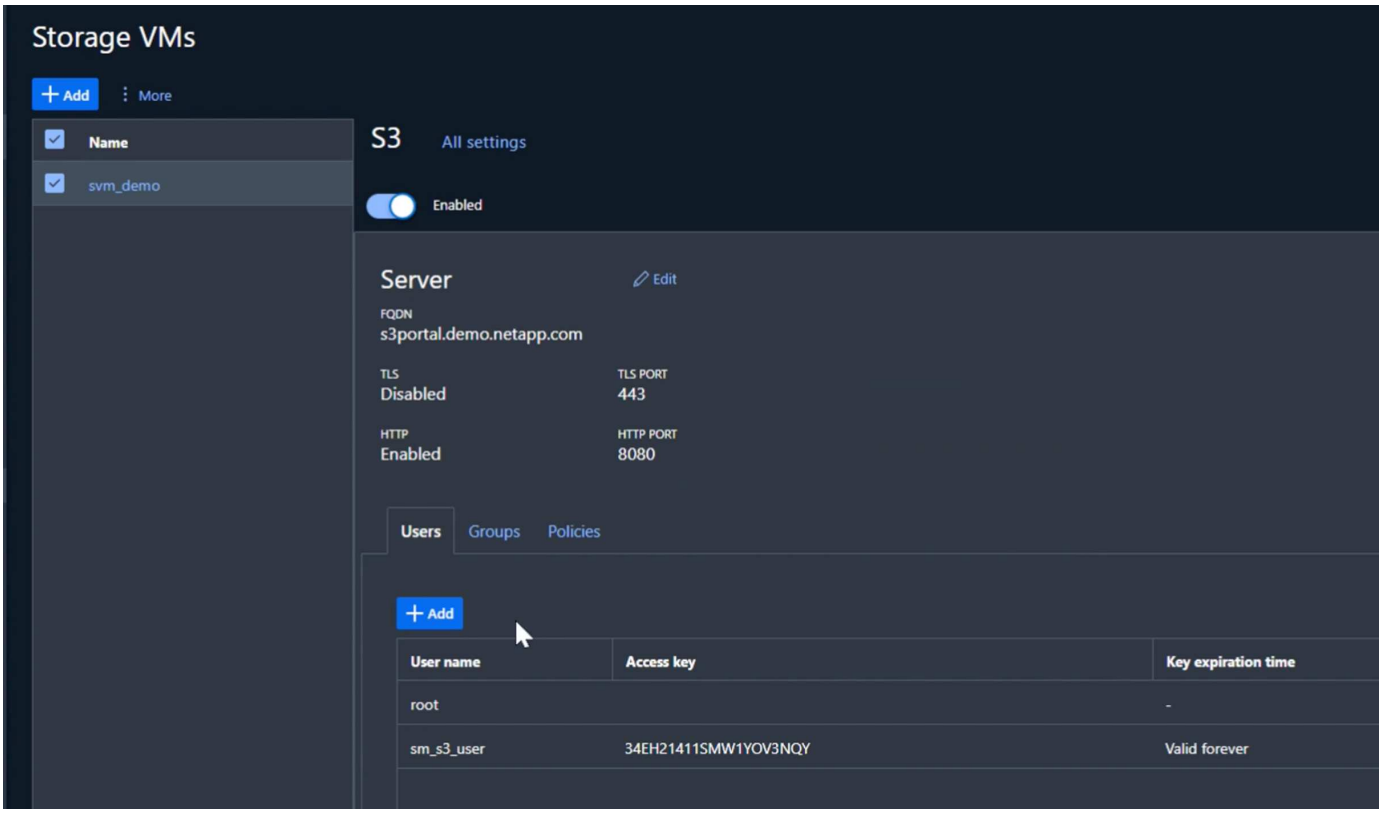


Créer un utilisateur SVM S3

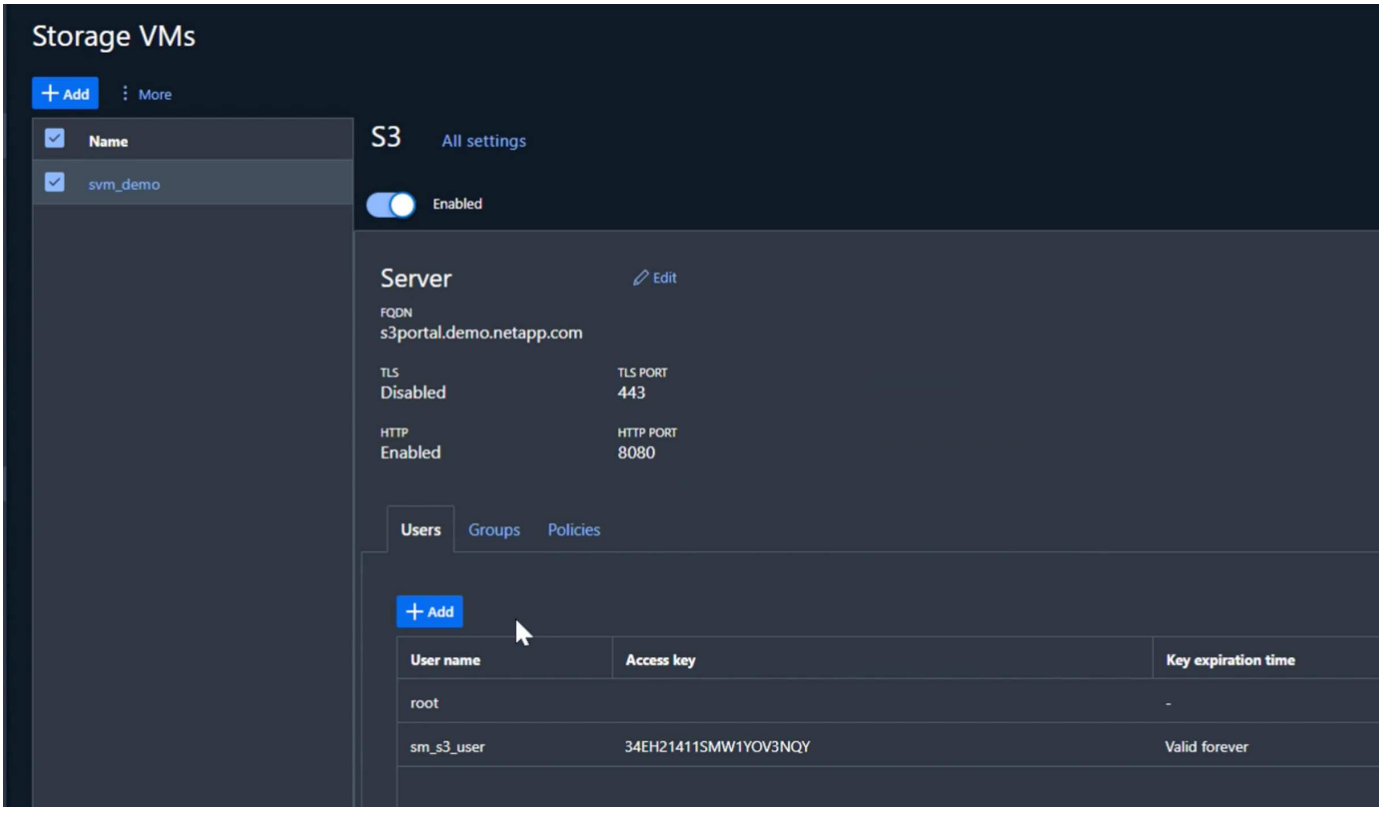
Nous pouvons maintenant configurer les utilisateurs et le groupe S3. Modifiez les paramètres S3.



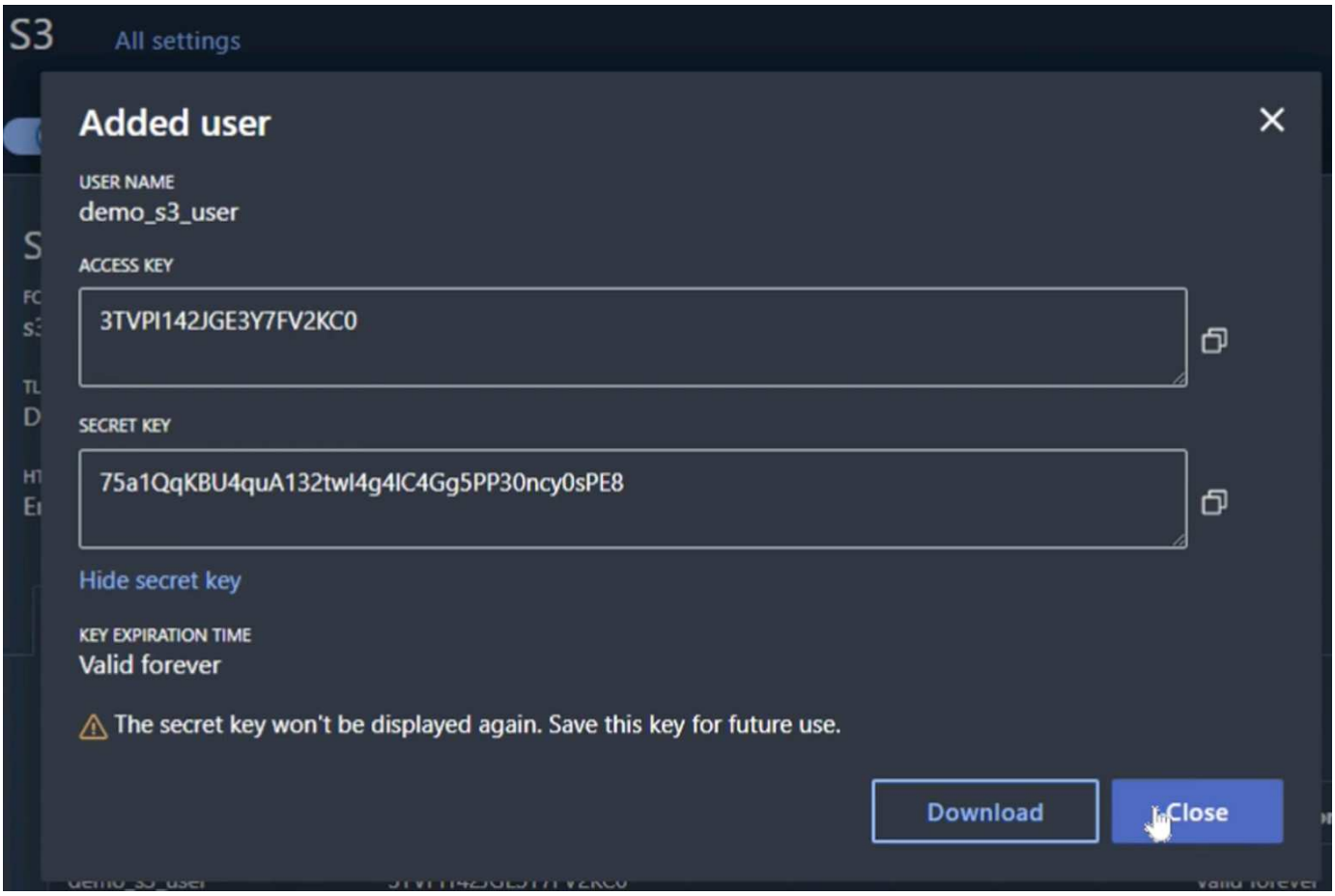
Ajouter un nouvel utilisateur.



Entrez le nom d'utilisateur et l'expiration de la clé.

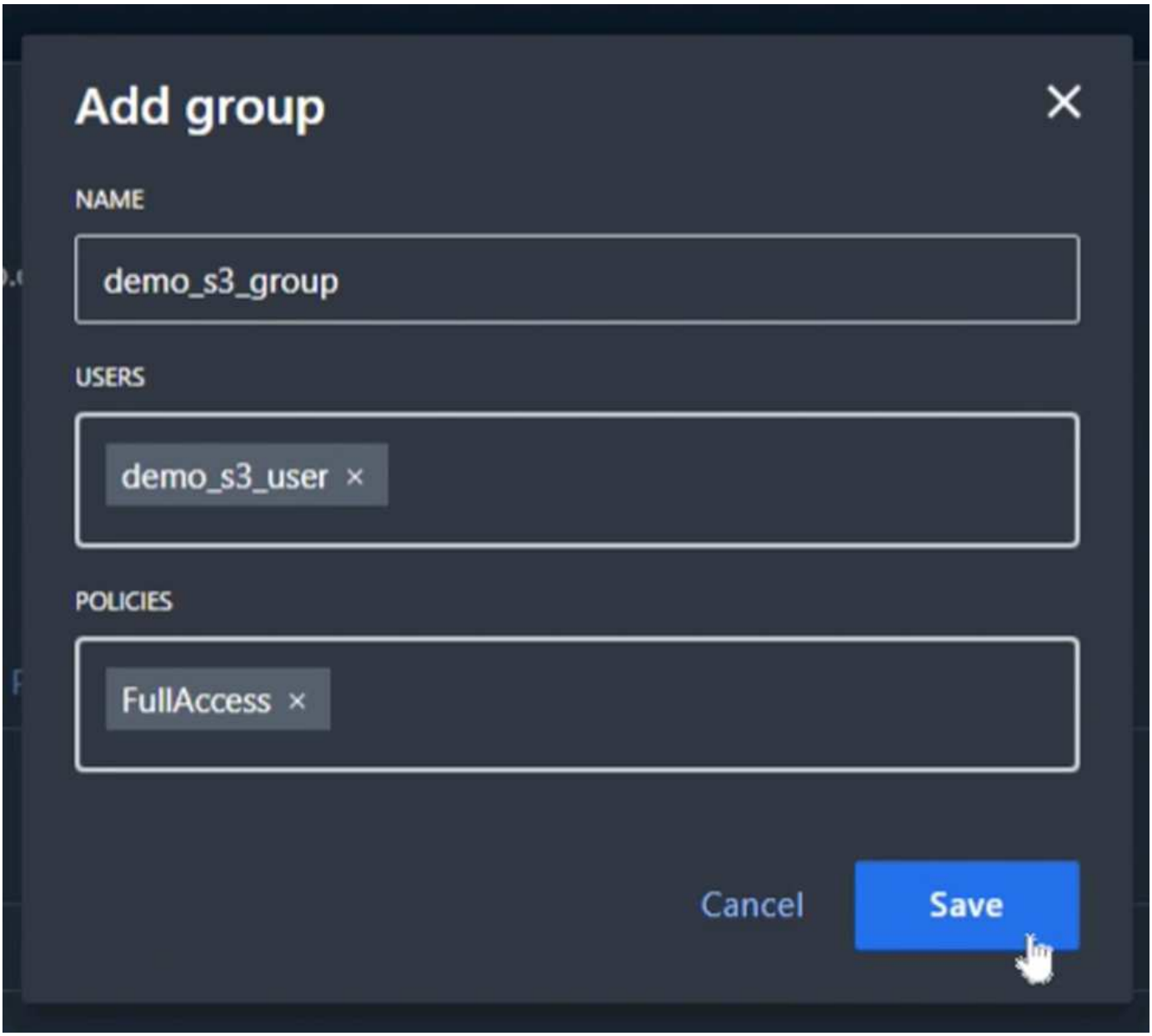


Téléchargez les clés S3 pour le nouvel utilisateur.



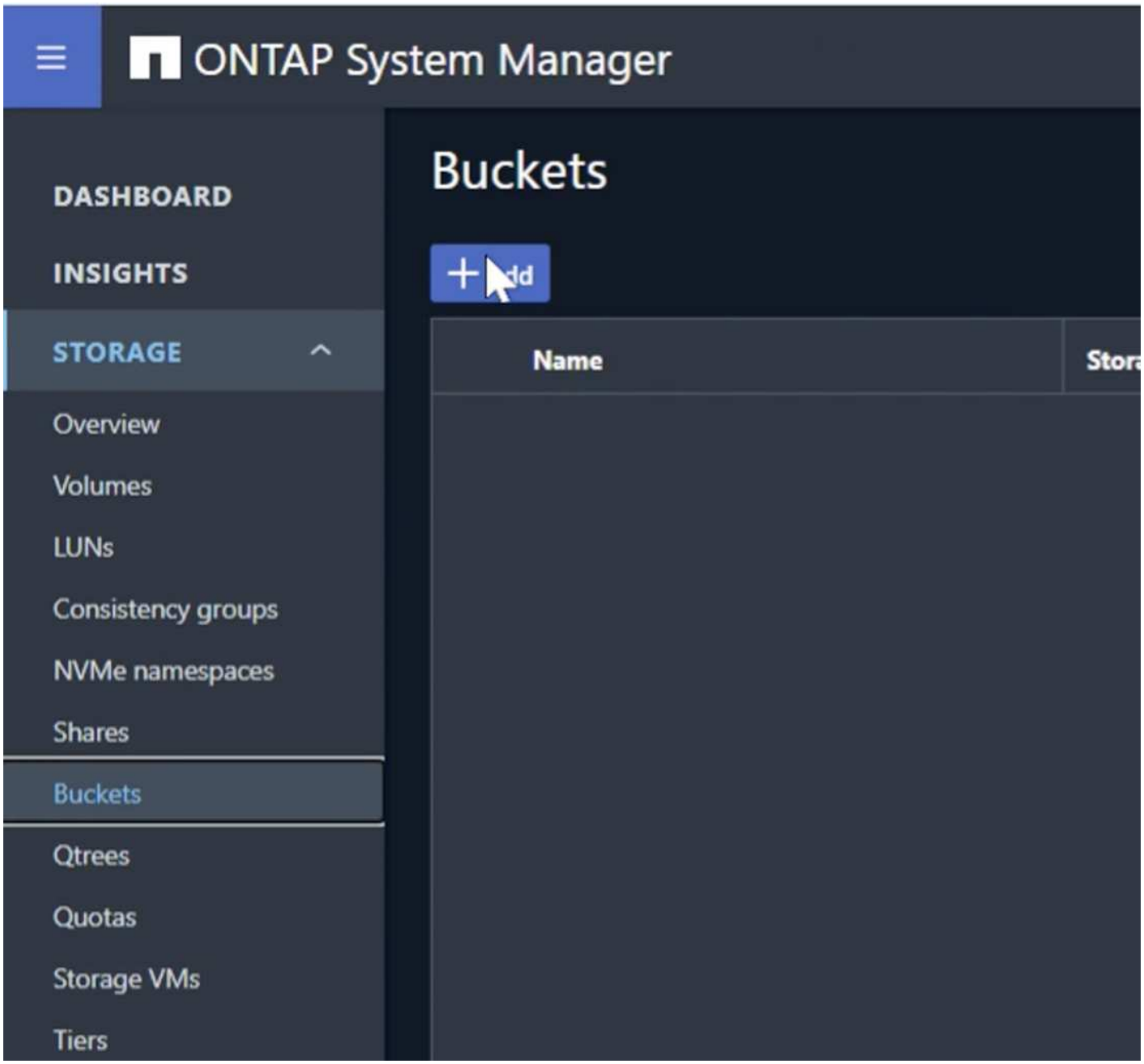
Créer un groupe SVM S3

Dans l'onglet groupes des paramètres du SVM S3, ajoutez un nouveau groupe avec les autorisations utilisateur créé ci-dessus et FullAccess.

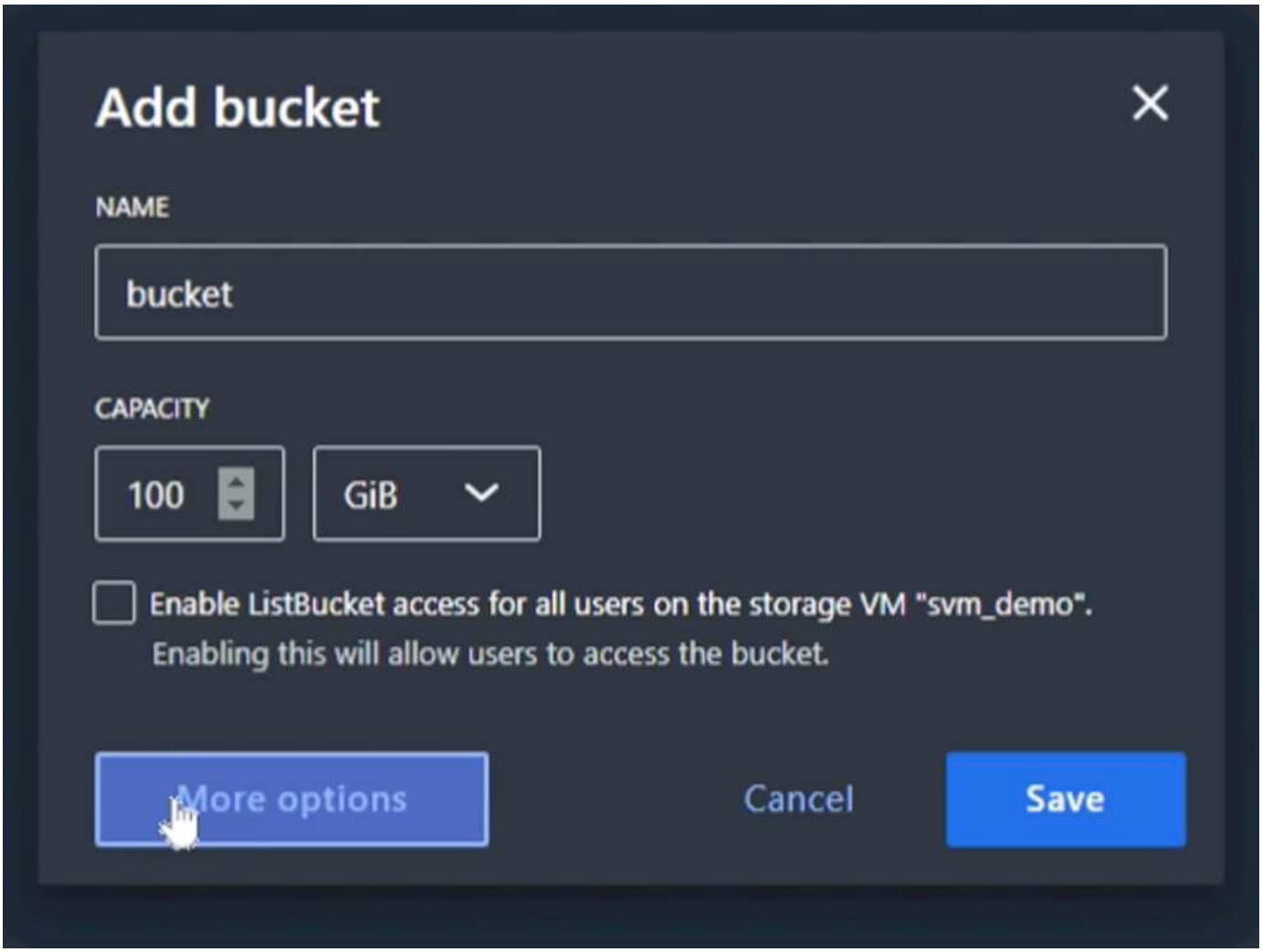


Création de compartiments SVM S3

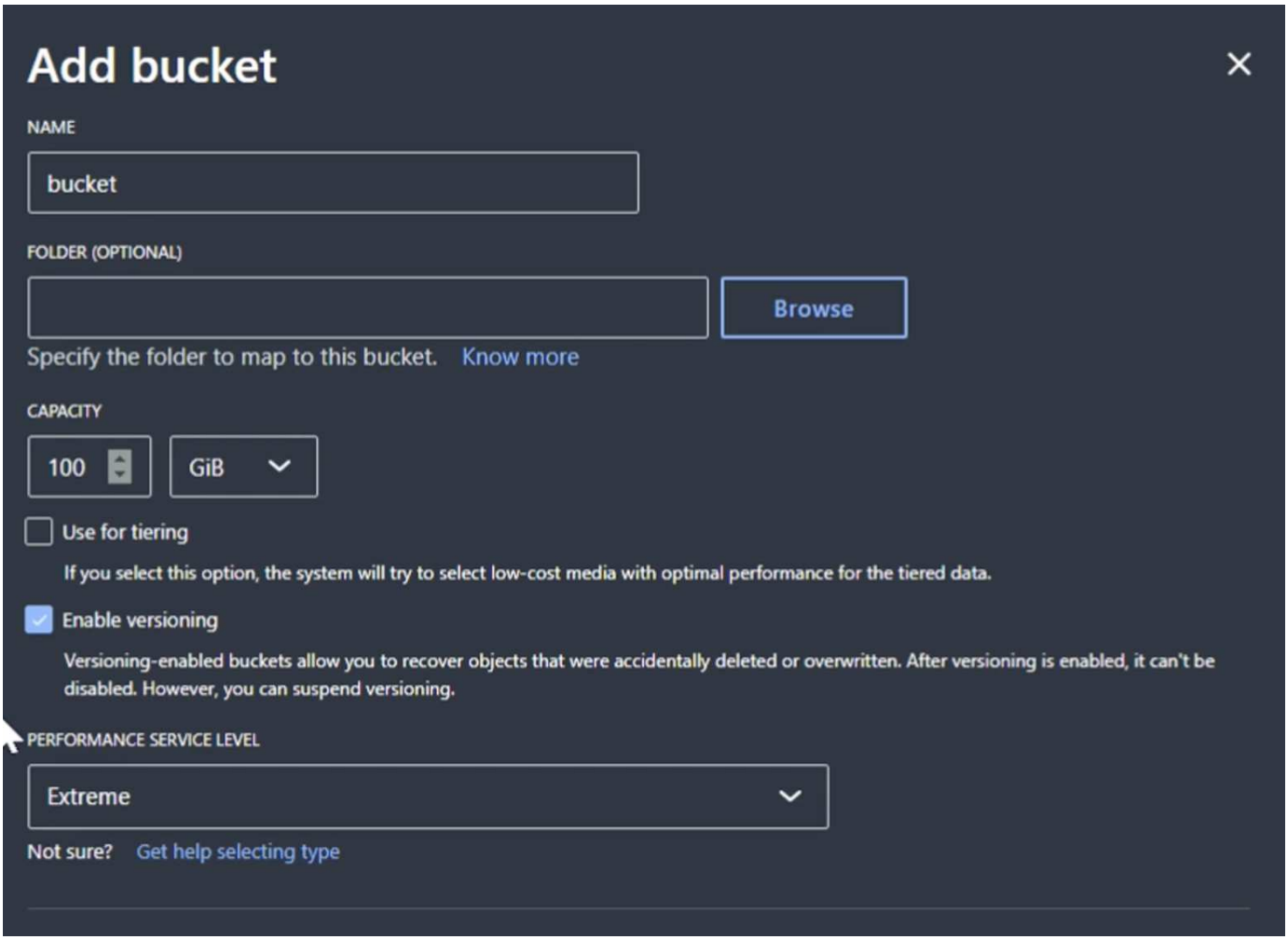
Accédez à la section compartiments et cliquez sur le bouton « + Ajouter ».



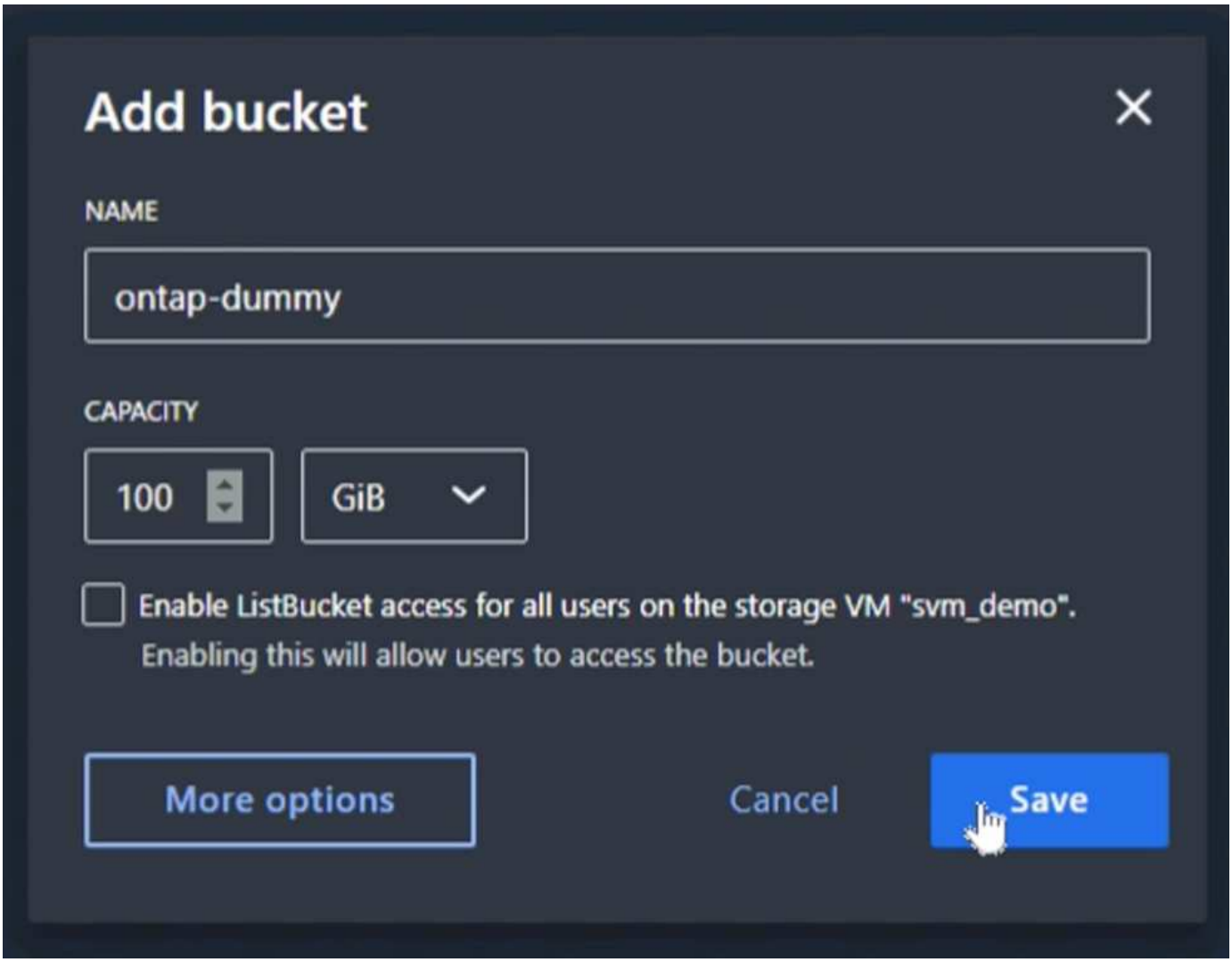
Entrez un nom, une capacité et désélectionnez la case à cocher "Activer l'accès ListBucket…" et cliquez sur le bouton "plus d'options".



Dans la section « autres options », cochez la case Activer la gestion des versions et cliquez sur le bouton « Enregistrer ».



Répétez le processus et créez un second compartiment sans activer la gestion des versions. Entrez un nom, la même capacité que le compartiment un, puis désélectionnez la case à cocher « Activer l'accès à ListBucket… » et cliquez sur le bouton « Enregistrer ».



Par Rafael Guedes, et Aron Klein

Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

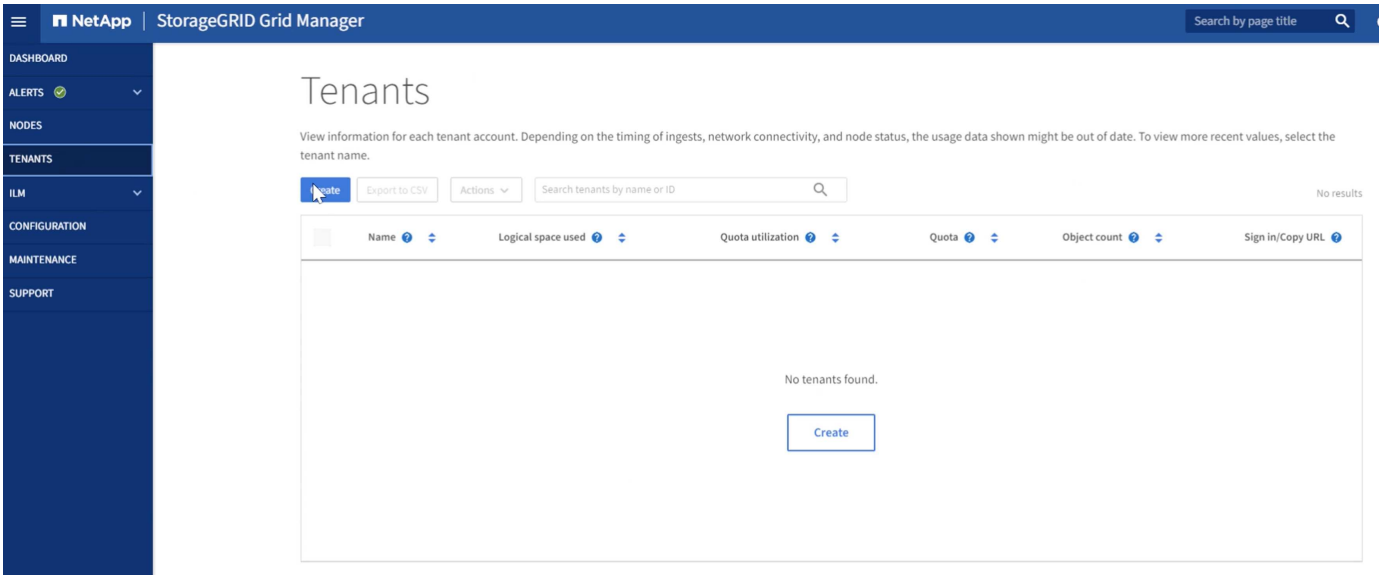
Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

Préparation de StorageGRID

Suite à la configuration de cette démonstration, nous allons créer un tenant, un utilisateur, un groupe de sécurité, une stratégie de groupe et un compartiment.

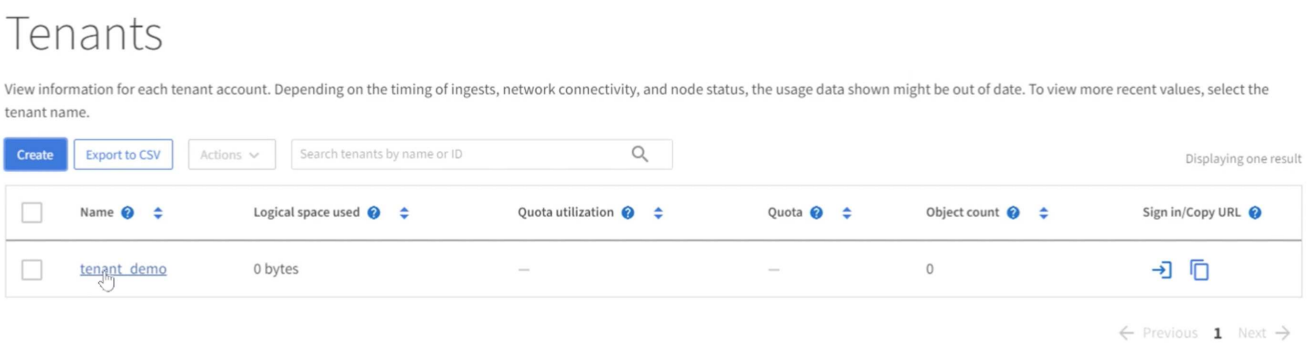
Créez le locataire

Accédez à l'onglet « tenants » et cliquez sur le bouton « create »

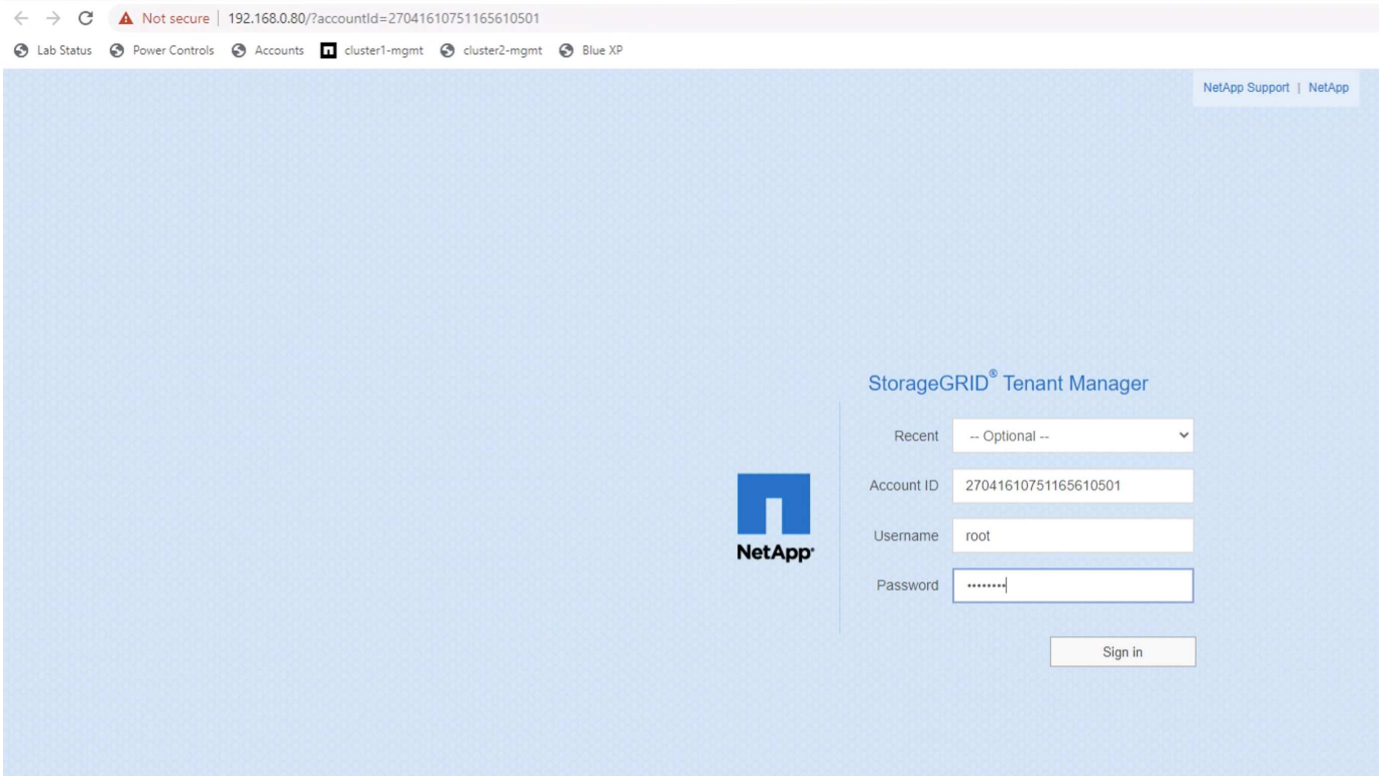


Renseignez les détails du locataire à fournir un nom de locataire, sélectionnez S3 pour le type de client et aucun quota n'est requis. Inutile de sélectionner des services de plateforme ou d'autoriser la sélection S3. Vous pouvez choisir d'utiliser votre propre référentiel d'identité si vous le souhaitez. Définissez le mot de passe racine et cliquez sur le bouton Terminer.

Cliquez sur le nom du locataire pour afficher les détails du locataire. **Vous aurez besoin de l'ID de locataire plus tard, alors copiez-le hors de**. Cliquez sur le bouton se connecter. Vous accédez ainsi au portail des locataires. Enregistrez l'URL pour une utilisation ultérieure.

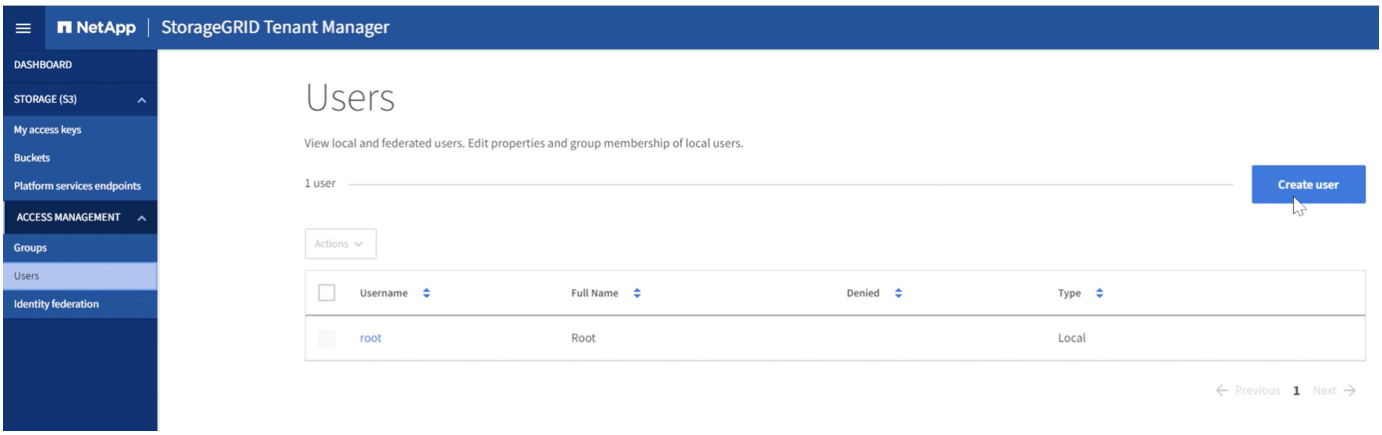


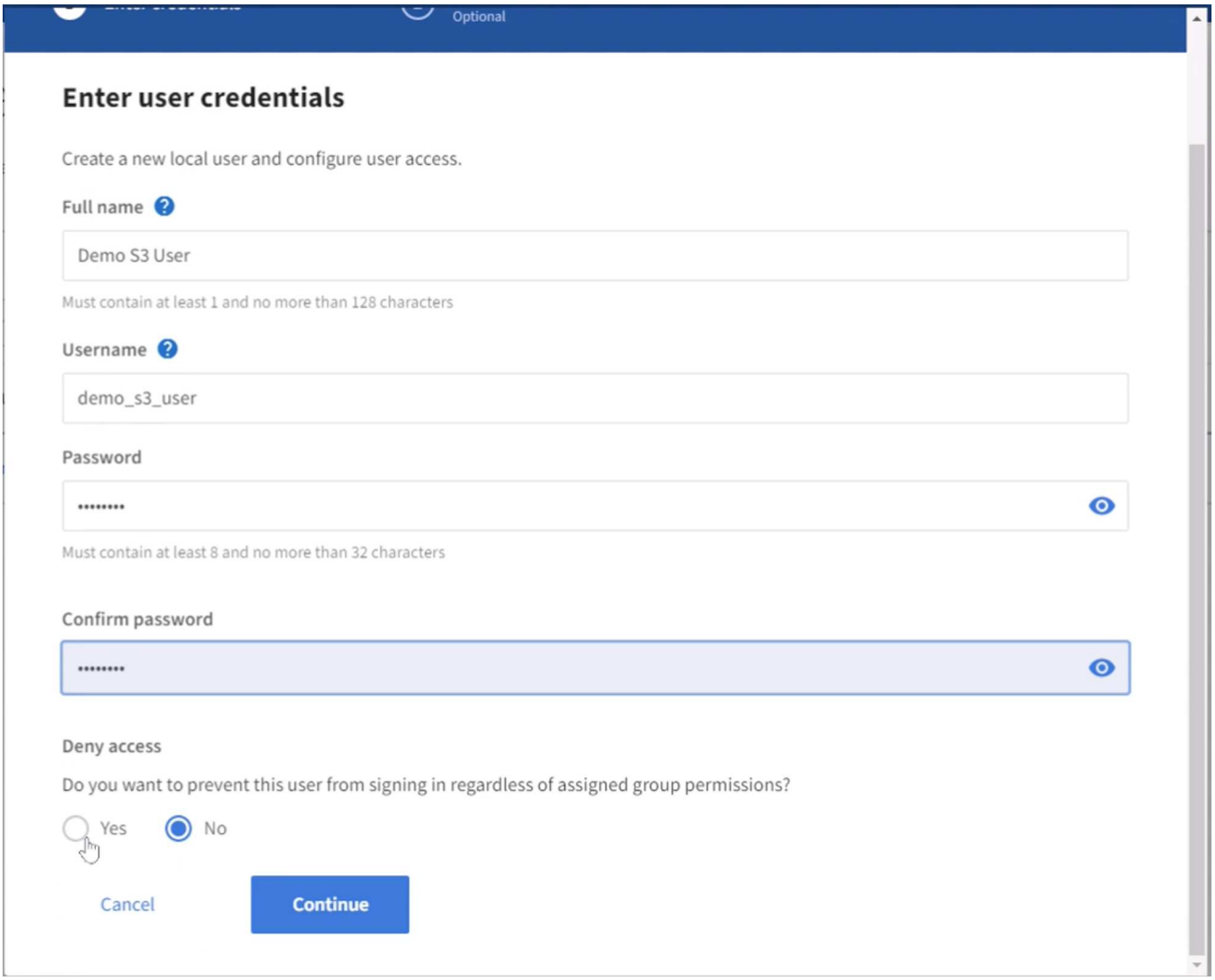
Vous accédez ainsi au portail des locataires. Enregistrez l'URL pour une utilisation ultérieure et entrez les informations d'identification de l'utilisateur root.



Créez l'utilisateur

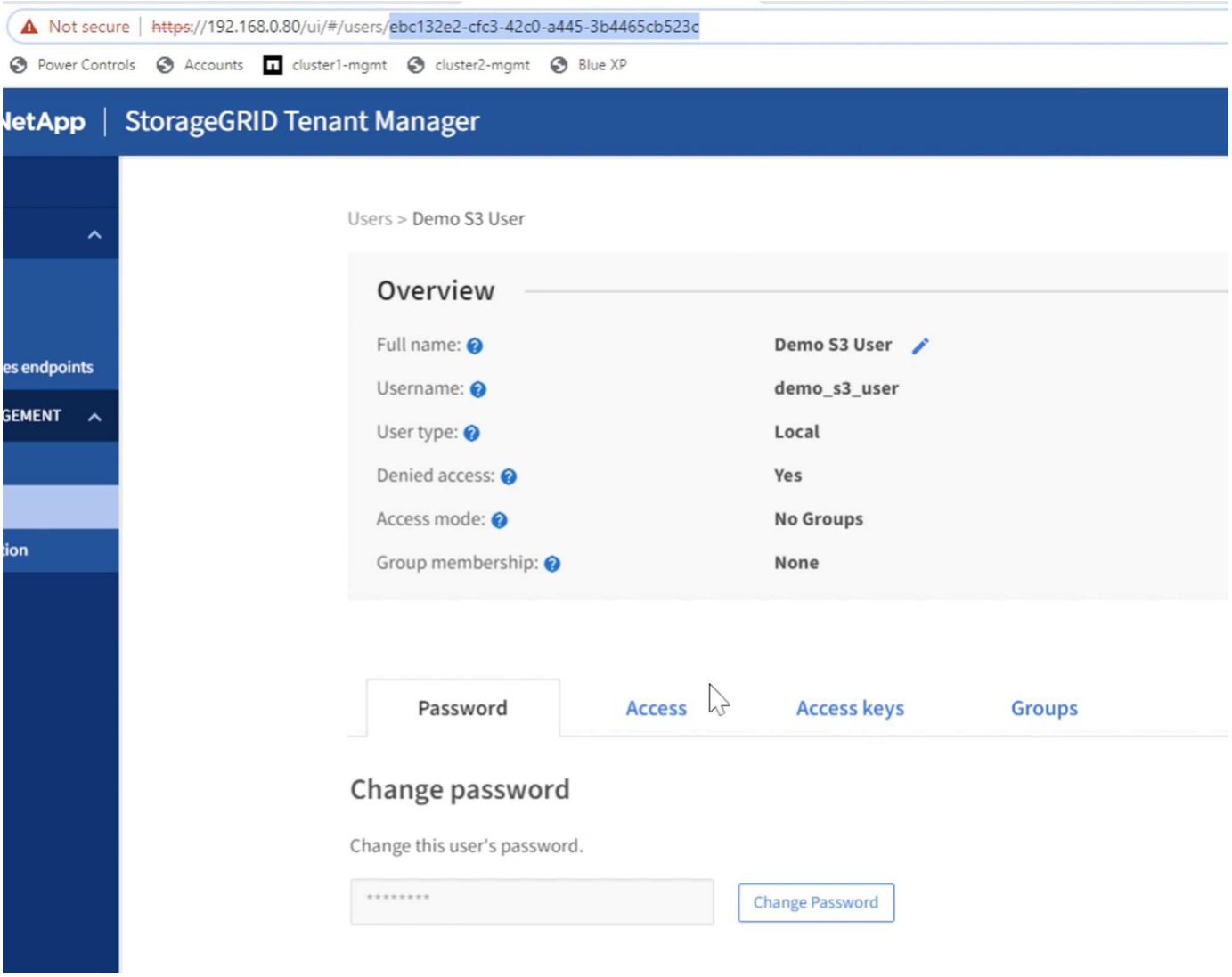
Accédez à l'onglet utilisateurs et créez un nouvel utilisateur.



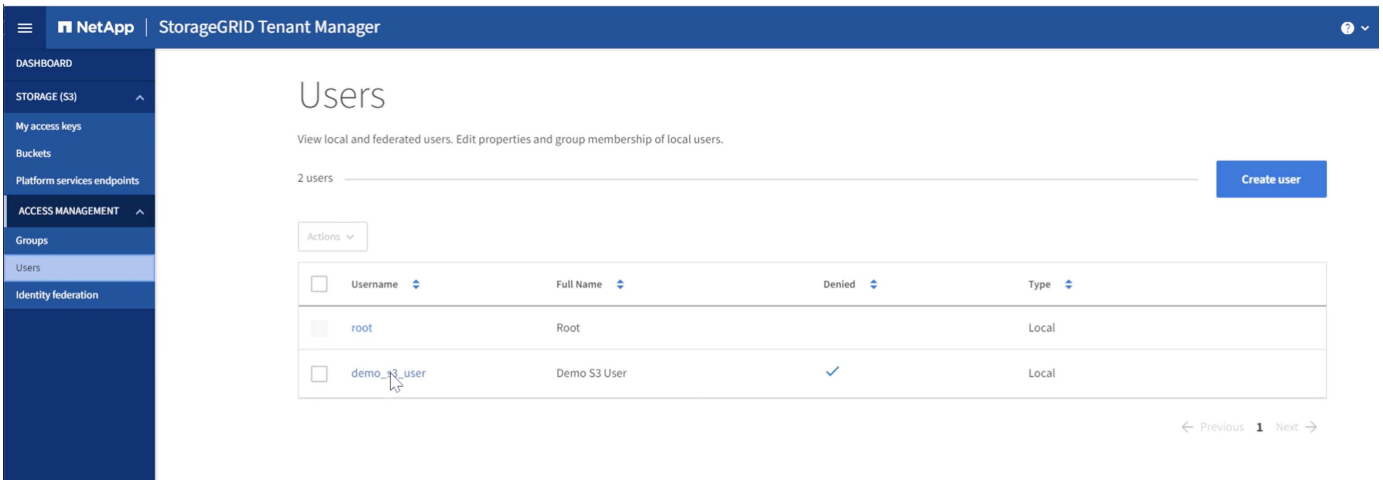


Maintenant que le nouvel utilisateur a été créé, cliquez sur son nom pour ouvrir les détails de l'utilisateur.

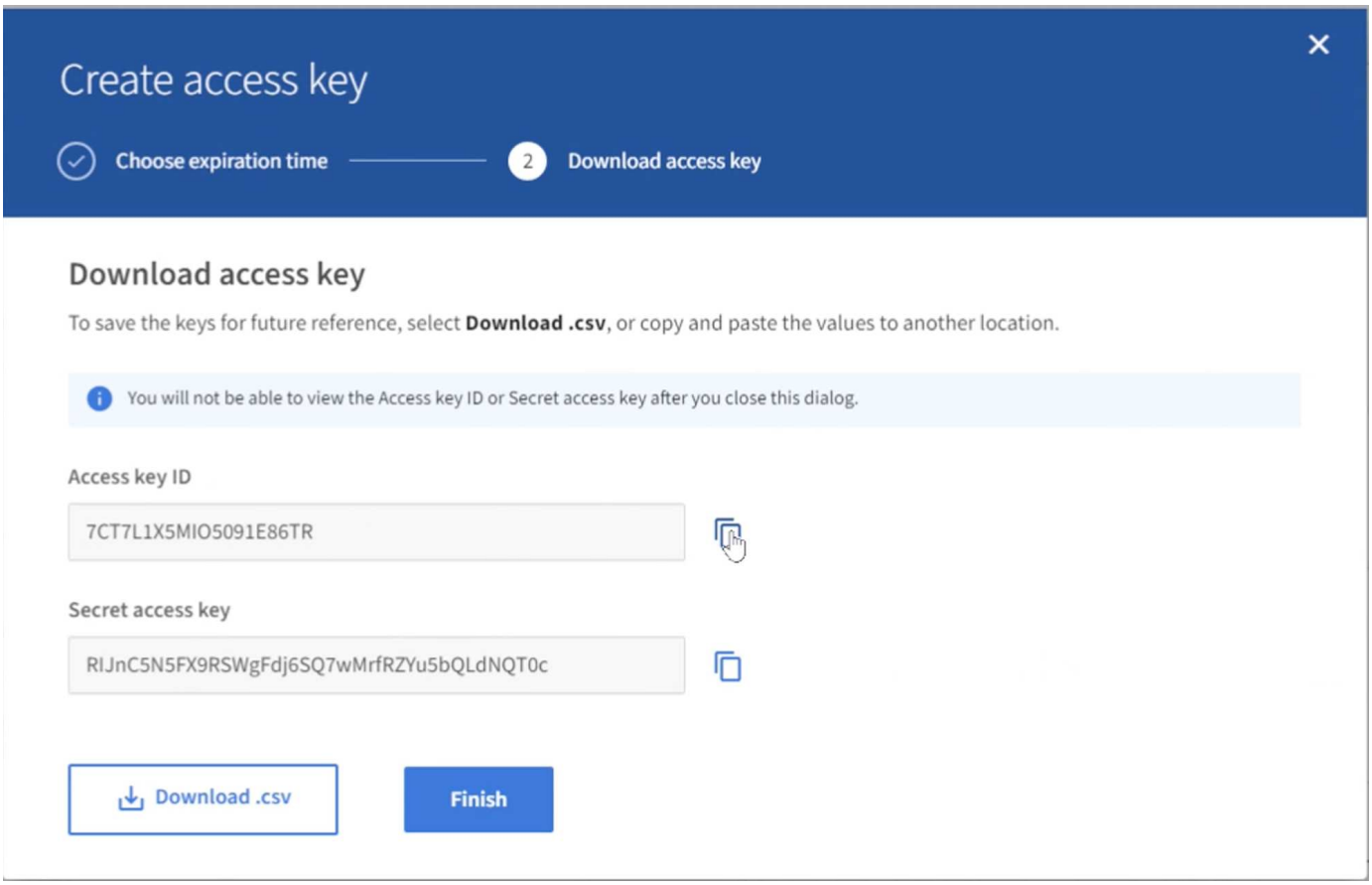
Copiez l'ID utilisateur à partir de l'URL à utiliser ultérieurement.



Pour créer les clés S3, cliquez sur le nom d'utilisateur.

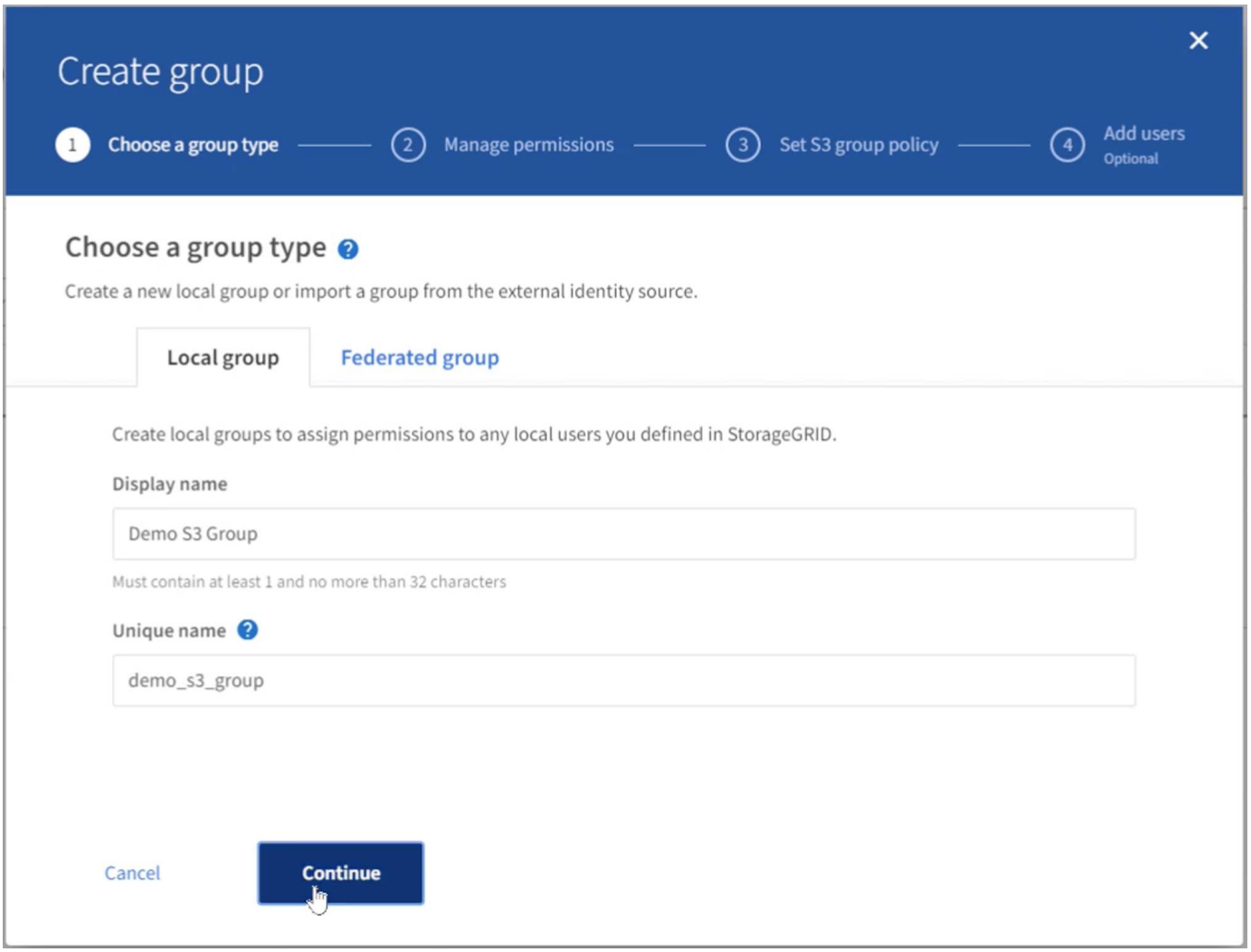


Sélectionnez l'onglet « clés d'accès » et cliquez sur le bouton « Créer une clé ». Il n'est pas nécessaire de définir une heure d'expiration. Téléchargez les clés S3 car elles ne peuvent plus être récupérées une fois la fenêtre fermée.

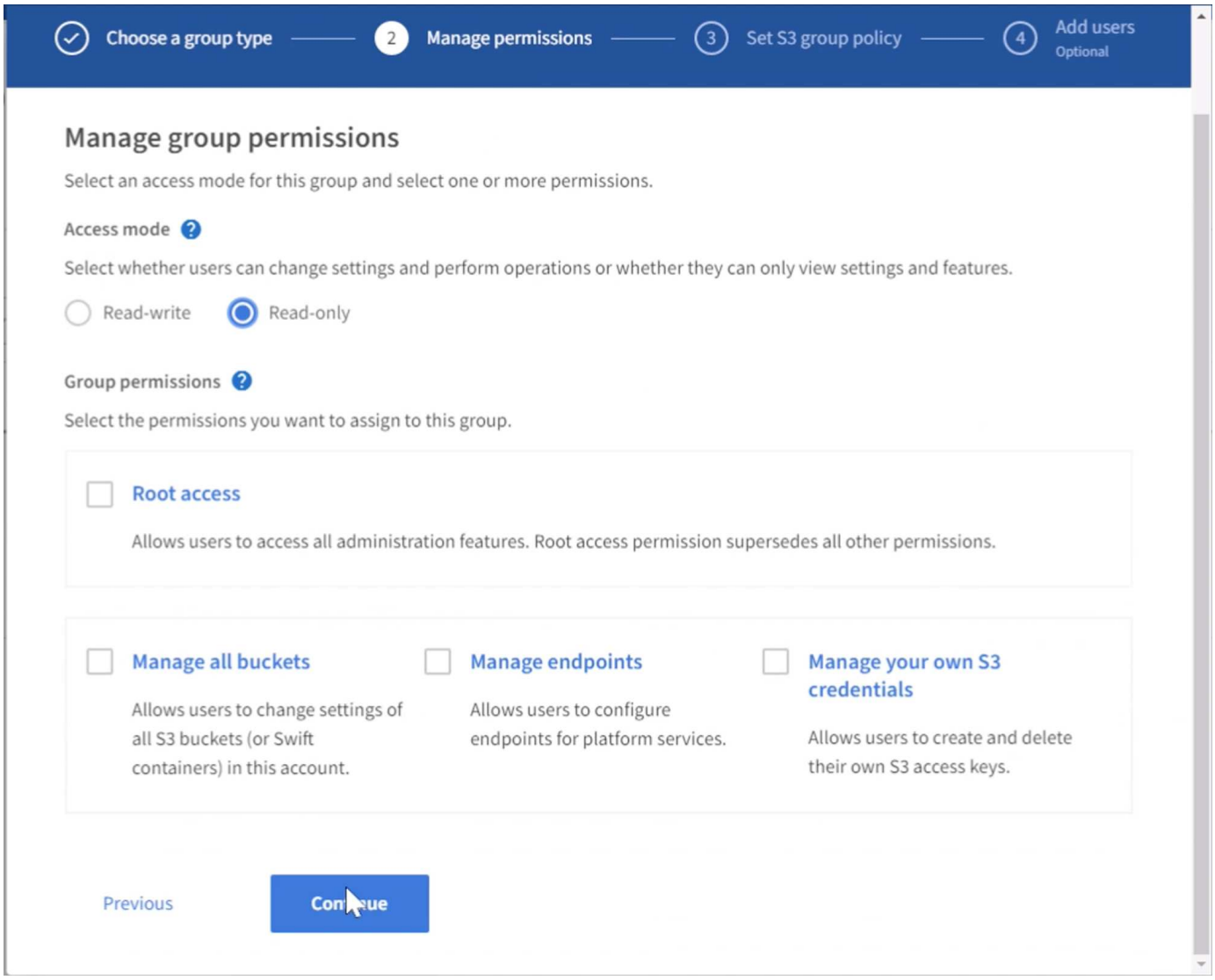


Créez le groupe de sécurité

Allez maintenant à la page groupes et créez un nouveau groupe.

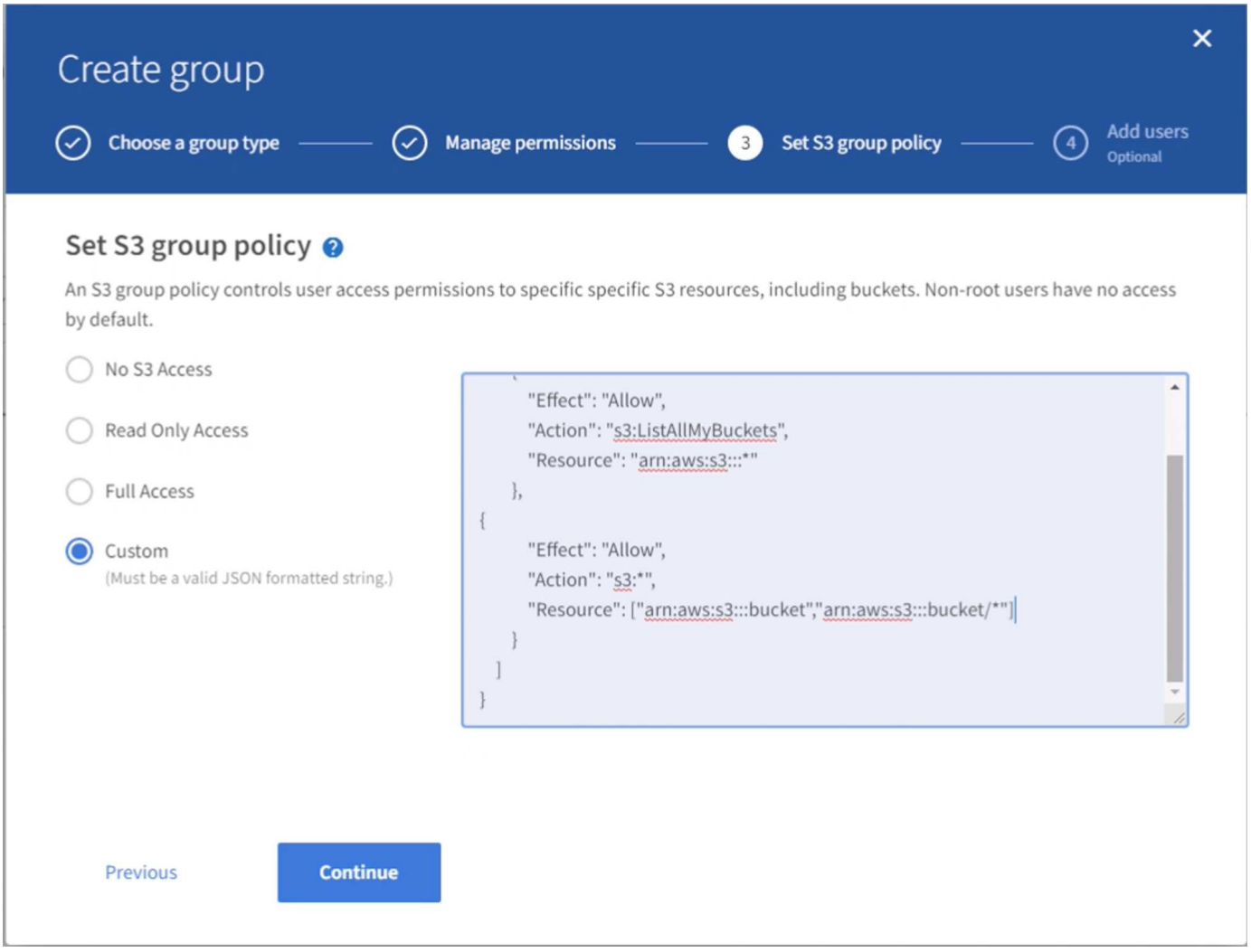


Définissez les autorisations de groupe sur lecture seule. Il s'agit des autorisations de l'interface du locataire, et non des autorisations S3.

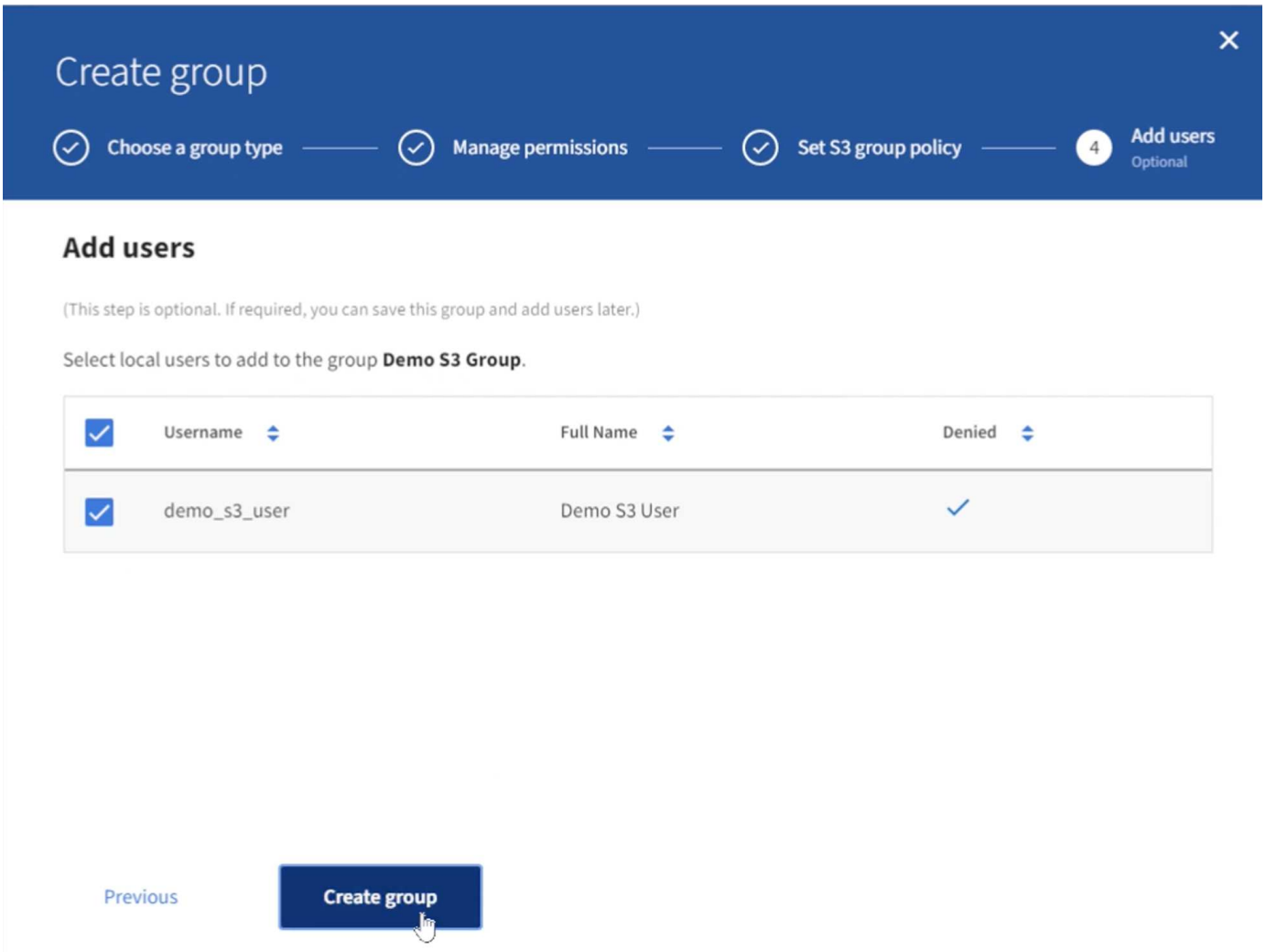


Les autorisations S3 sont contrôlées avec la règle de groupe (IAM Policy). Définissez la stratégie de groupe sur personnalisée et collez la stratégie json dans la zone. Cette règle permet aux utilisateurs de ce groupe de lister les compartiments du locataire et d'effectuer toutes les opérations S3 dans le compartiment nommé « compartiment » ou sous-dossiers du compartiment nommé « compartiment ».

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

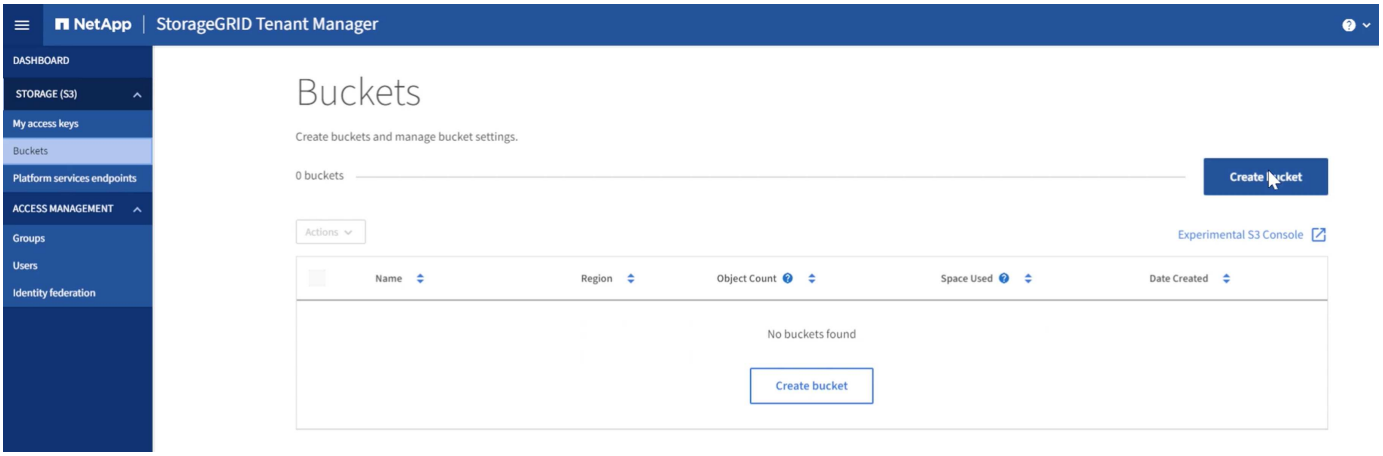


Enfin, ajoutez l'utilisateur au groupe et terminez.

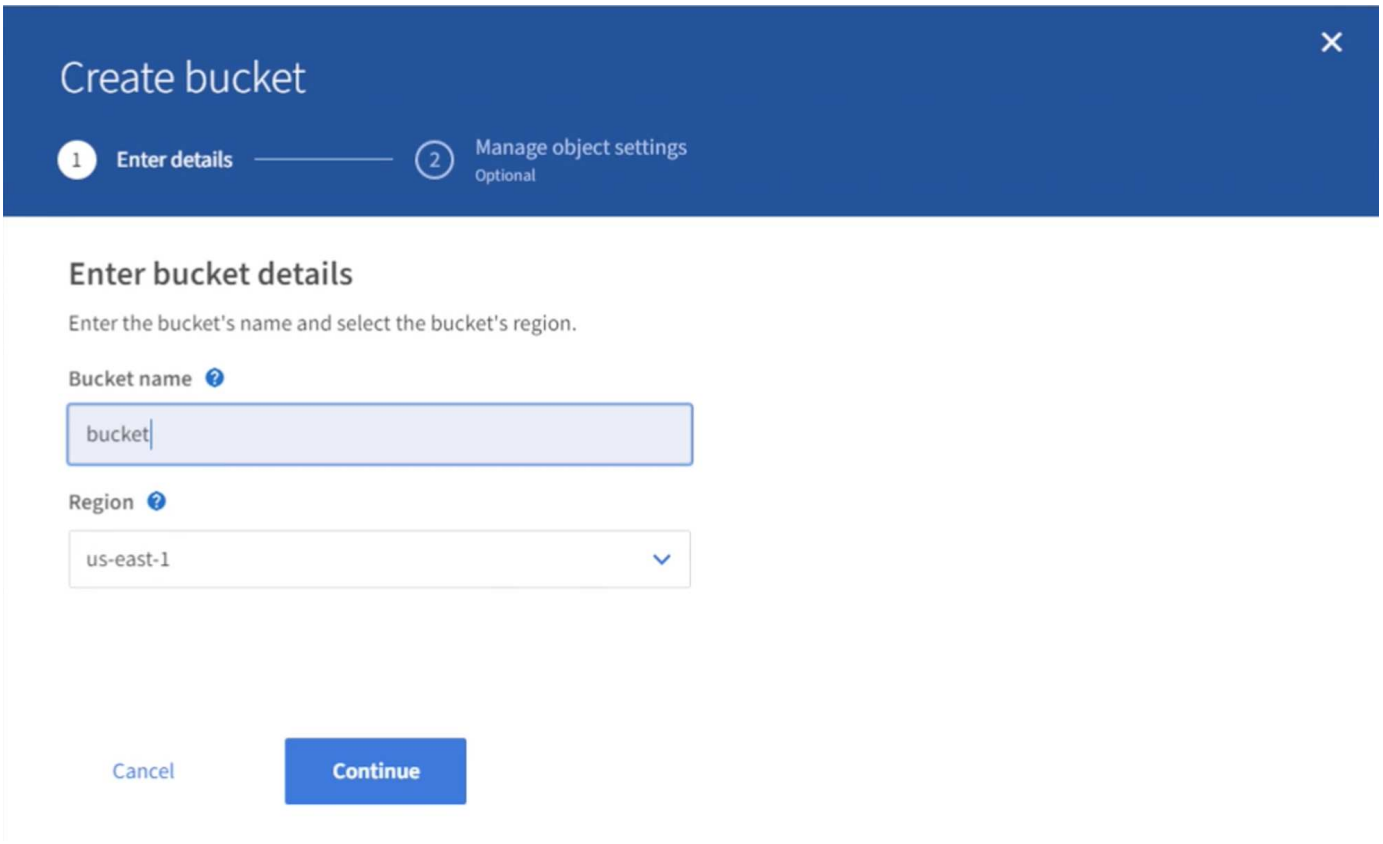


Créer deux compartiments

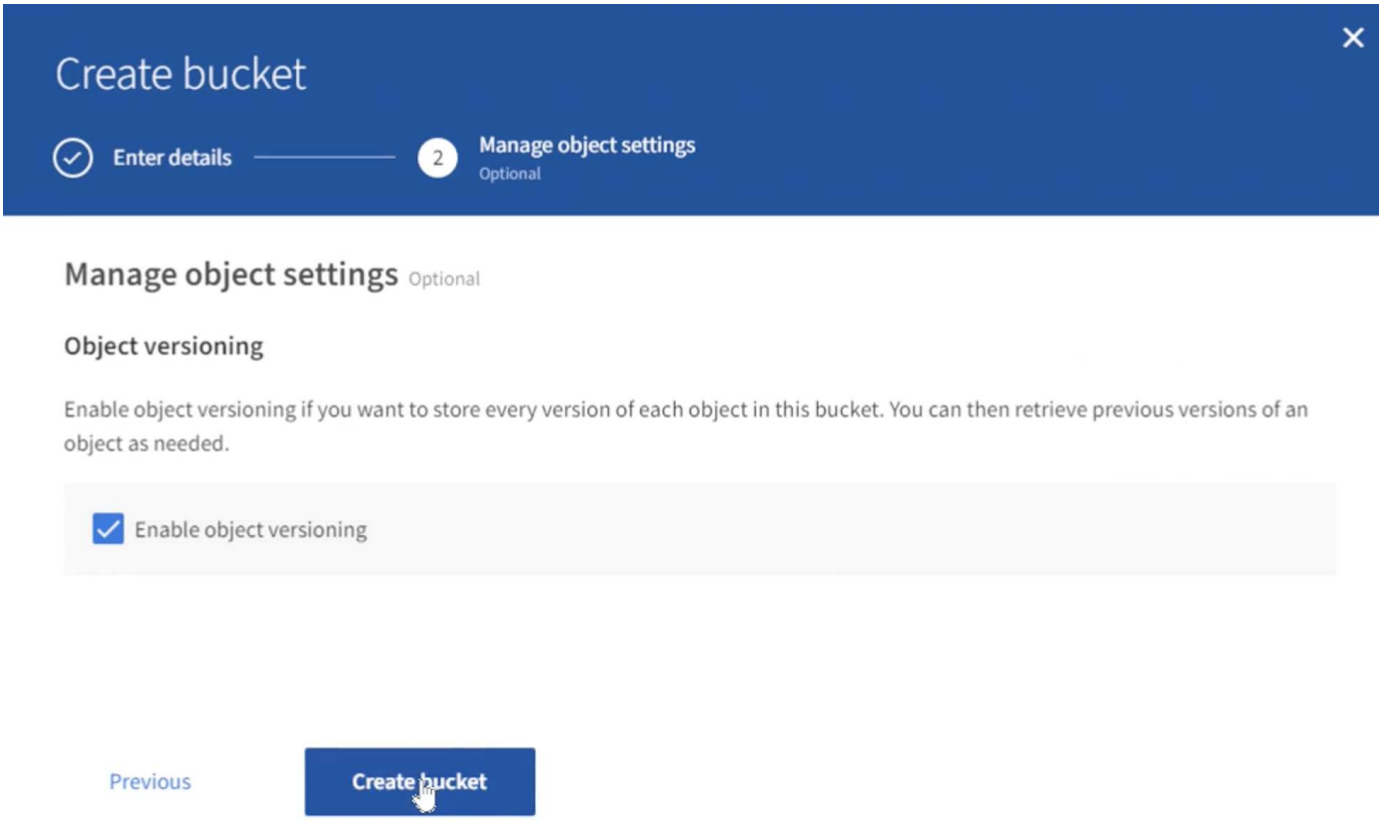
Accédez à l'onglet compartiments et cliquez sur le bouton Créer un compartiment.



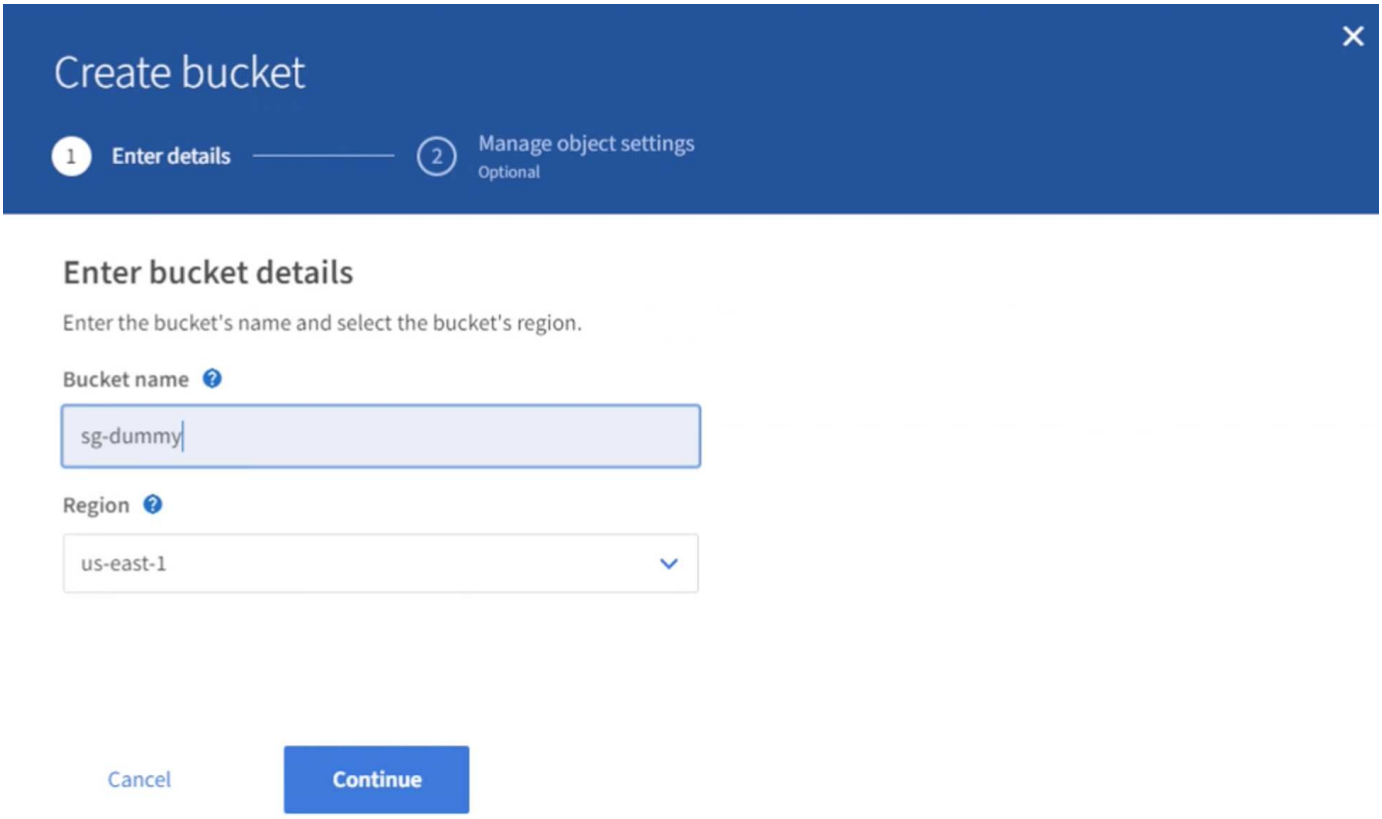
Définissez le nom du compartiment et la région.



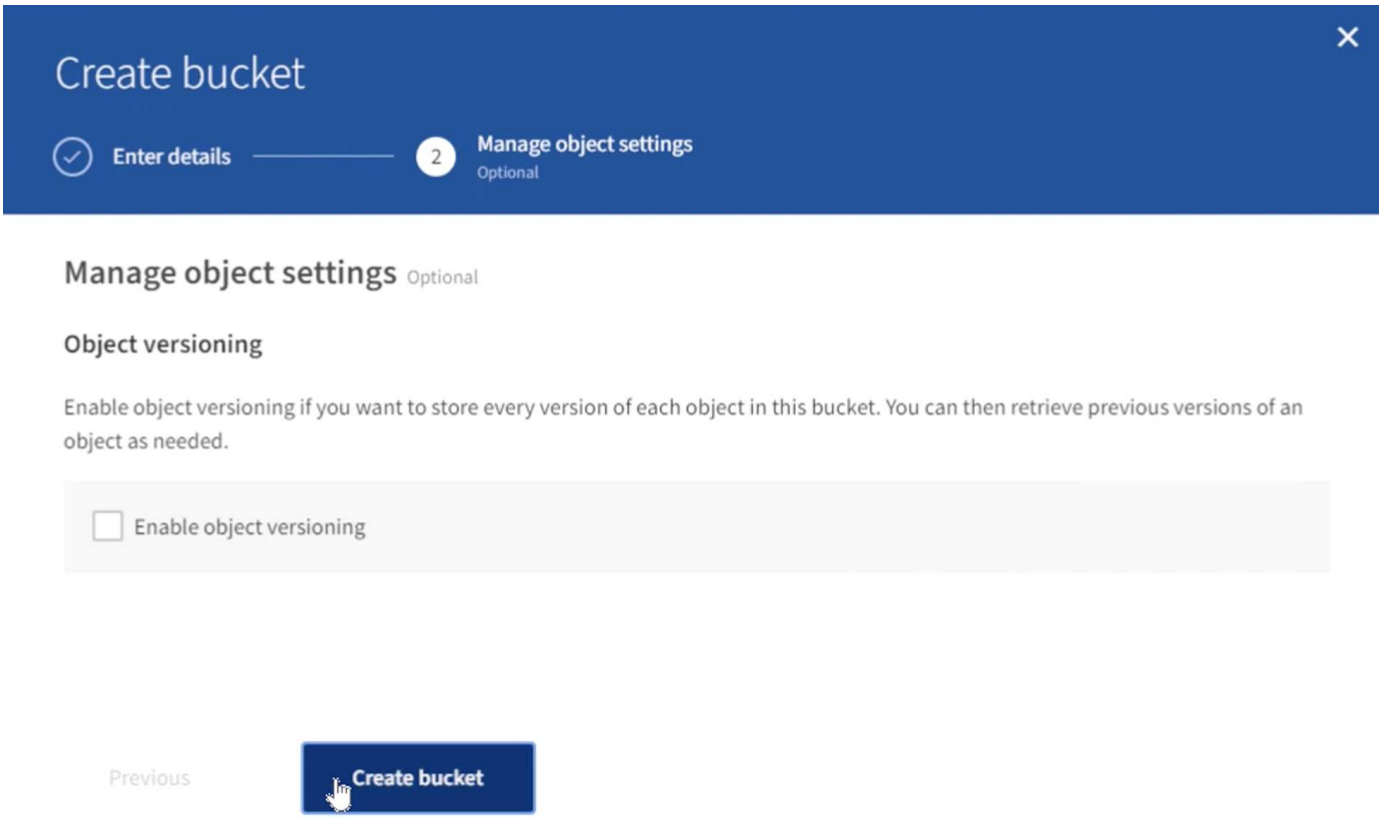
Sur ce premier compartiment, activez la gestion des versions.



Créez à présent un second compartiment sans activation de la gestion des versions.



N’activez pas la gestion des versions sur ce second compartiment.



Par Rafael Guedes, et Aron Klein

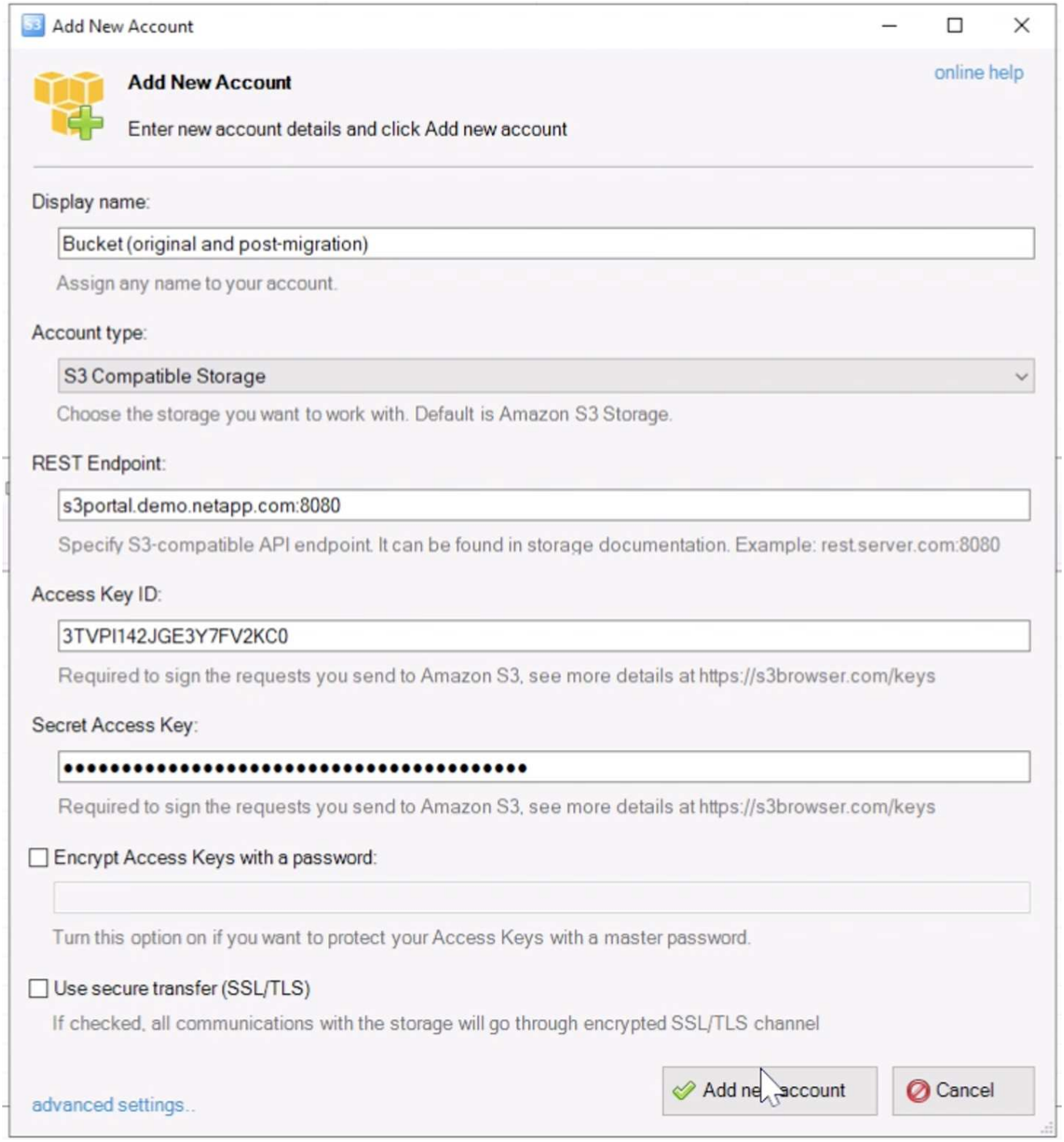
Bénéficiez d’un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d’ONTAP S3 vers StorageGRID

Bénéficiez d’un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d’ONTAP S3 vers StorageGRID

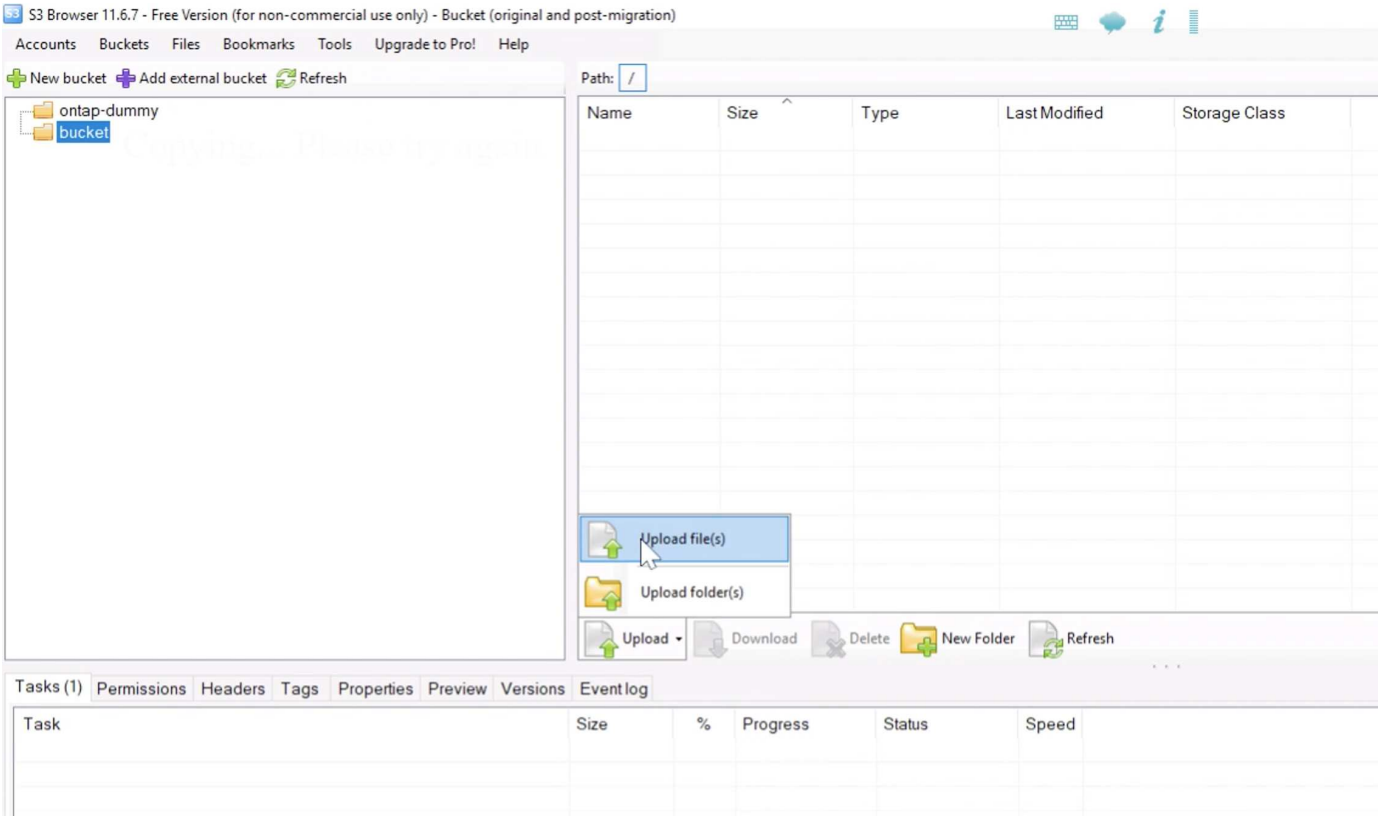
Remplissez le compartiment source

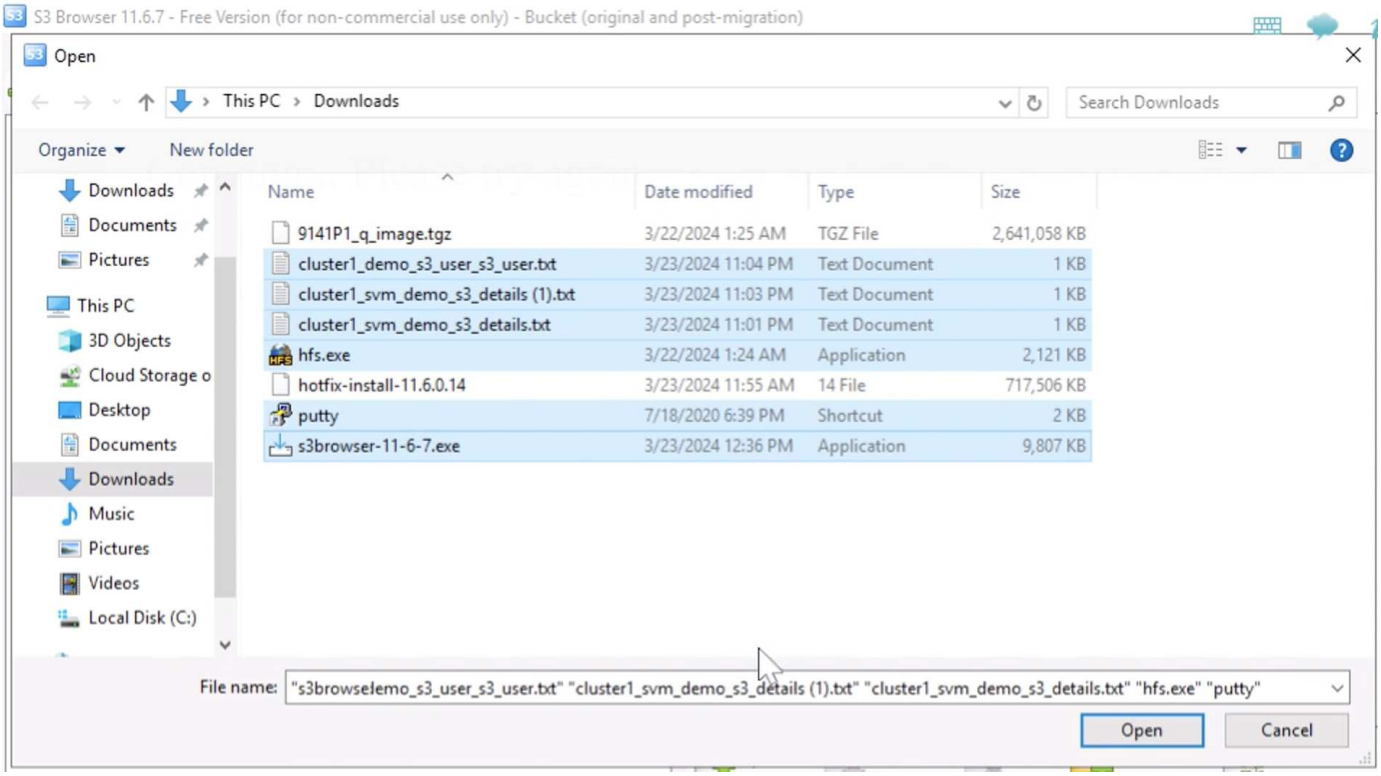
Mettons quelques objets dans le compartiment ONTAP source. Nous utiliserons S3Browser pour cette démo, mais vous pourriez utiliser n’importe quel outil que vous êtes à l’aise avec.

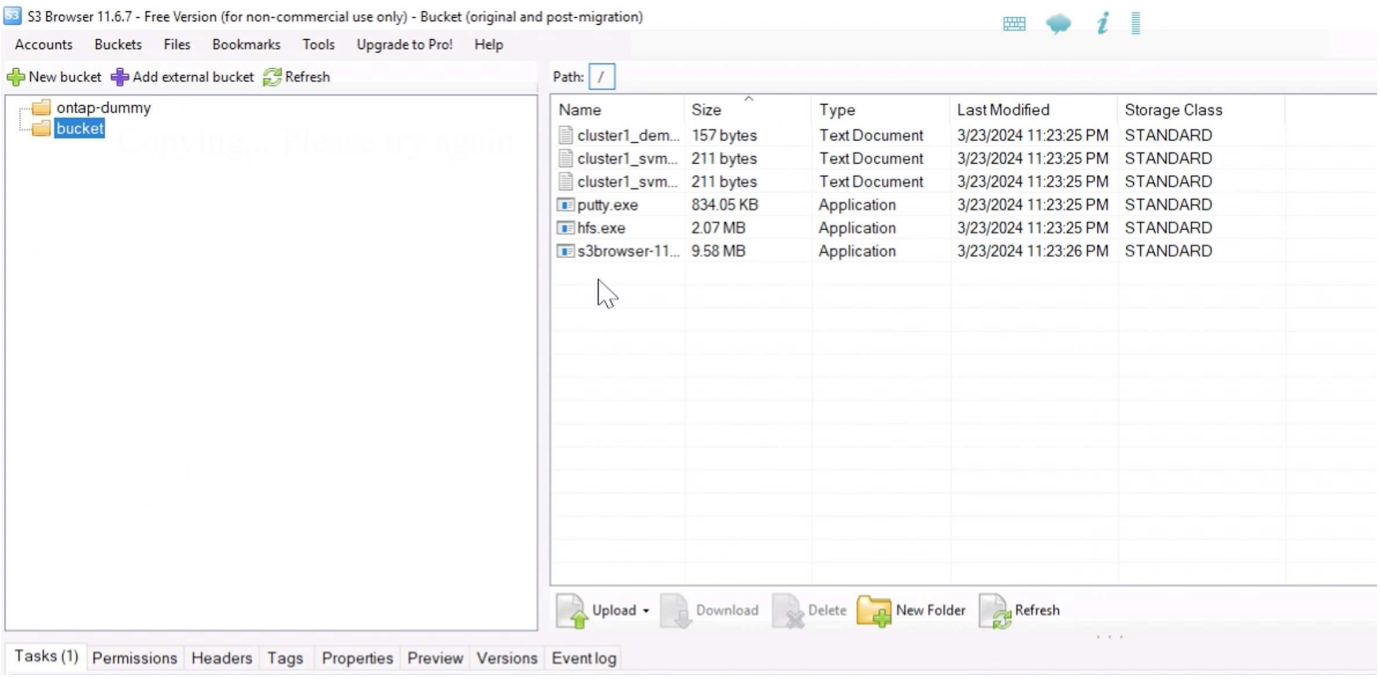
À l’aide des touches ONTAP utilisateur s3 créées ci-dessus, configurez S3Browser pour qu’il se connecte à votre système ONTAP.



Chargeons maintenant certains fichiers dans le compartiment compatible avec la gestion des versions.

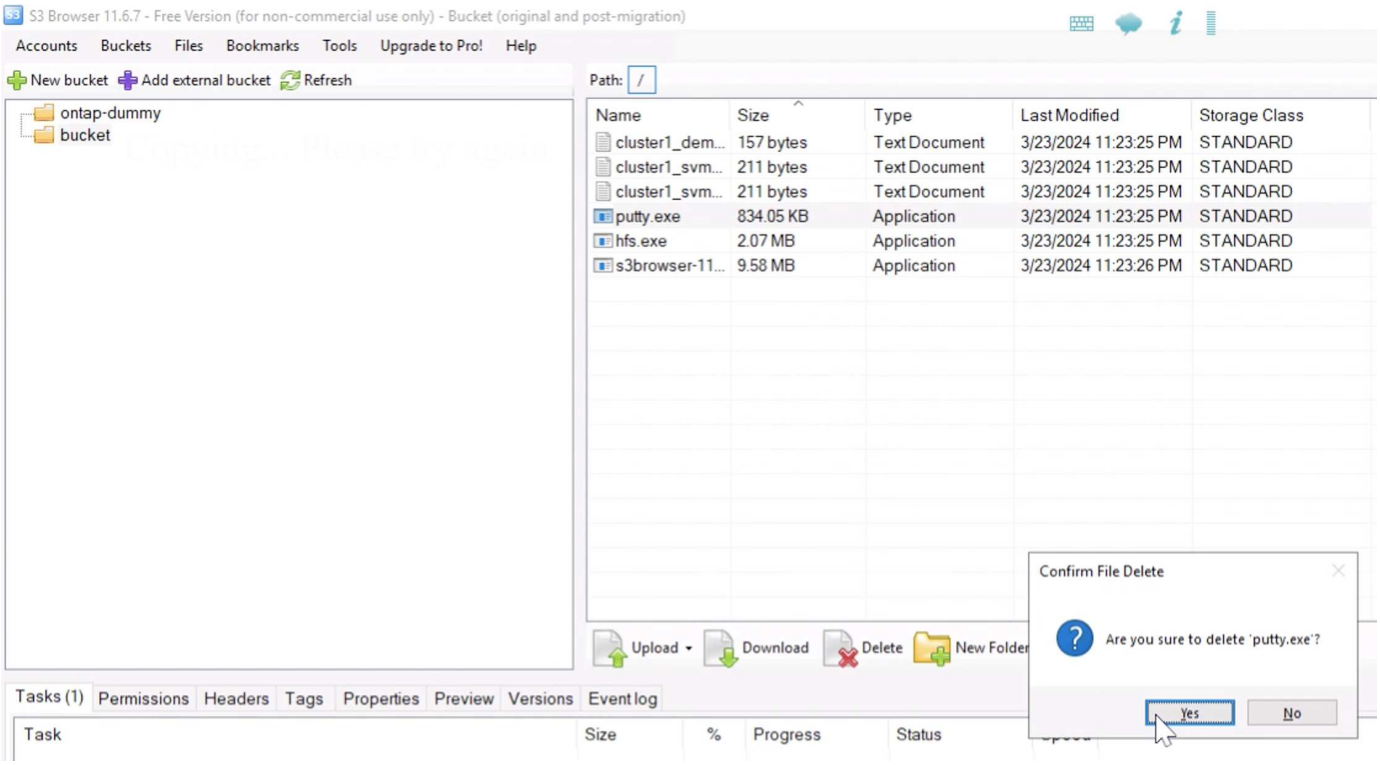

S3 Browser 11.6.7 - Free Version (for non-commercial use only) - Bucket (original and post-migration)
Accounts
Buckets
Files
Bookmarks
Tools
Upgrade to Pro!
Help
New bucket
Add external bucket
Refresh
Path: /
ontap-dummy
bucket
Name
Size
Type
Last Modified
Storage Class
Upload file(s)
Upload folder(s)
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

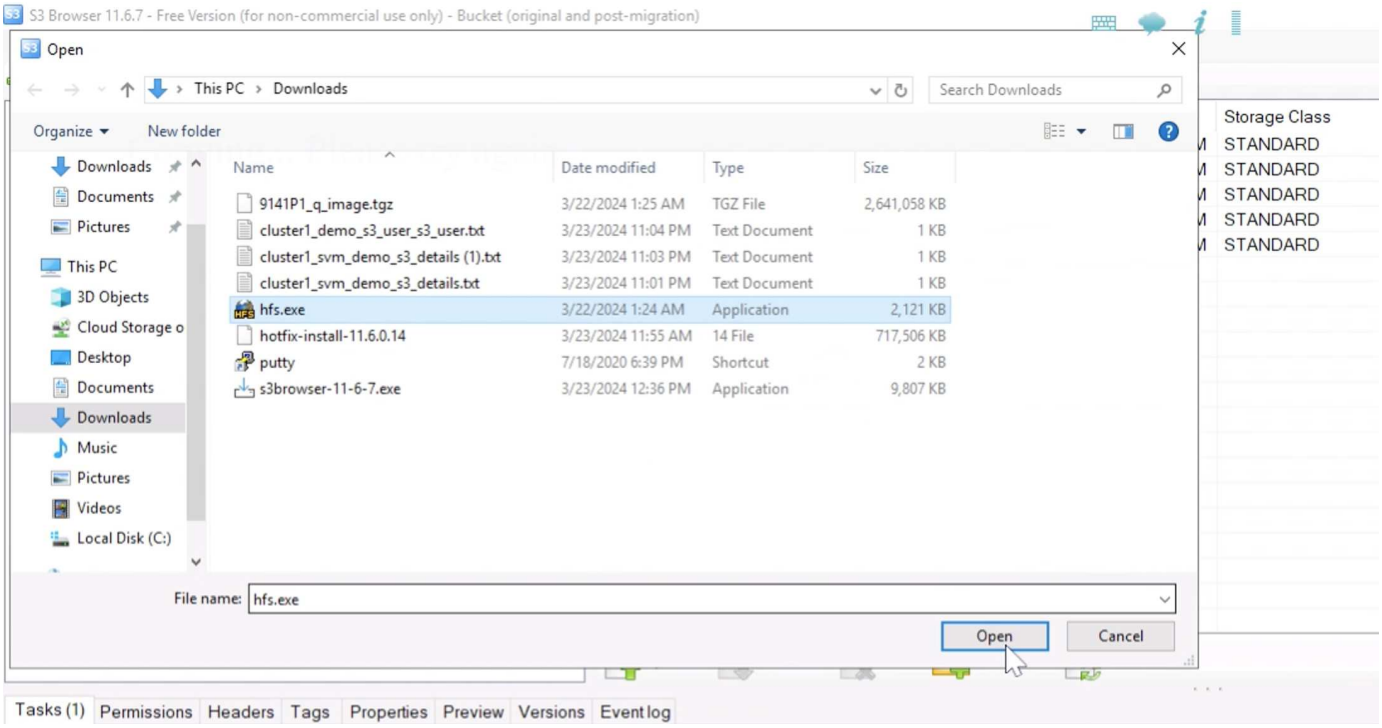


Créons maintenant certaines versions d'objet dans le compartiment.

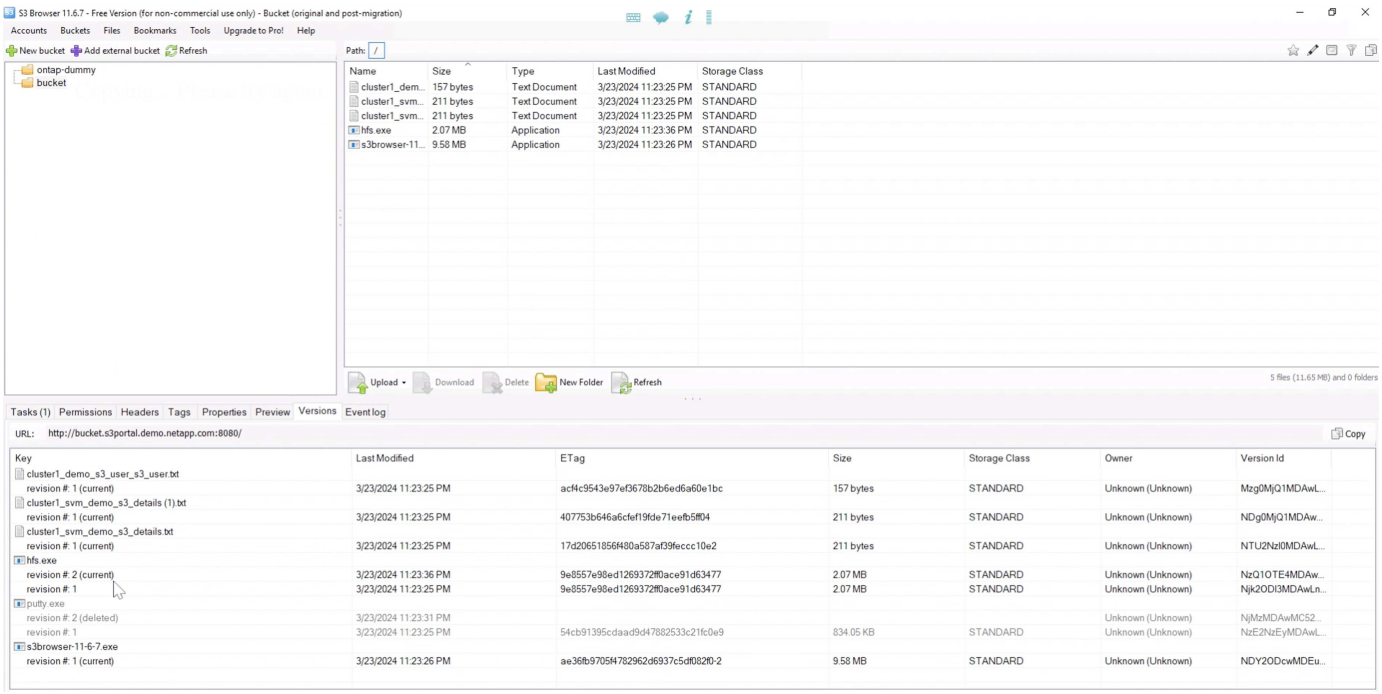
Supprimer un fichier.



Téléchargez un fichier qui existe déjà dans le compartiment pour copier le fichier sur lui-même et en créer une nouvelle version.



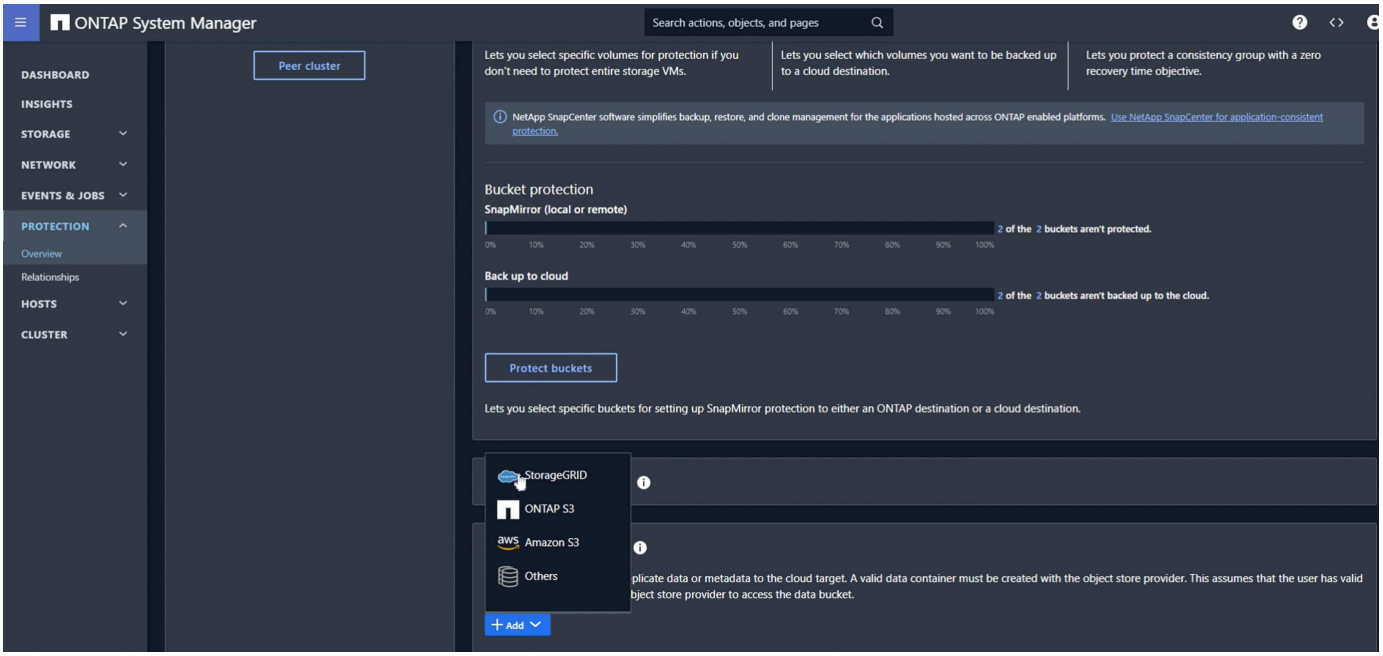
Dans S3Browser, nous pouvons visualiser les versions des objets que nous venons de créer.



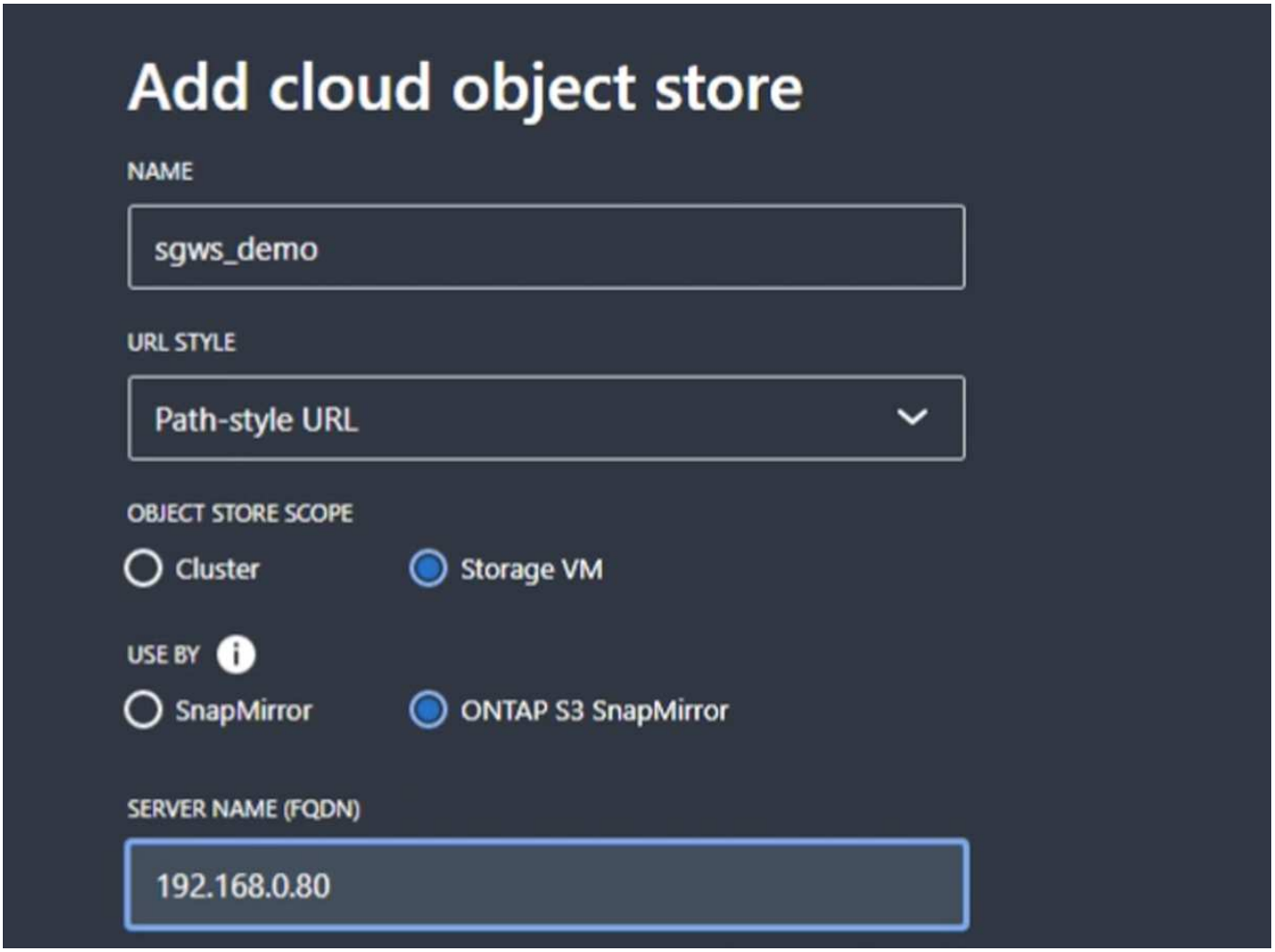
Établissement de la relation de réplication

Commençons à envoyer des données de ONTAP à StorageGRID.

Dans ONTAP System Manager, accédez à protection/Présentation. Faites défiler jusqu'à « Cloud object stores », cliquez sur le bouton « Add » et sélectionnez « StorageGRID ».



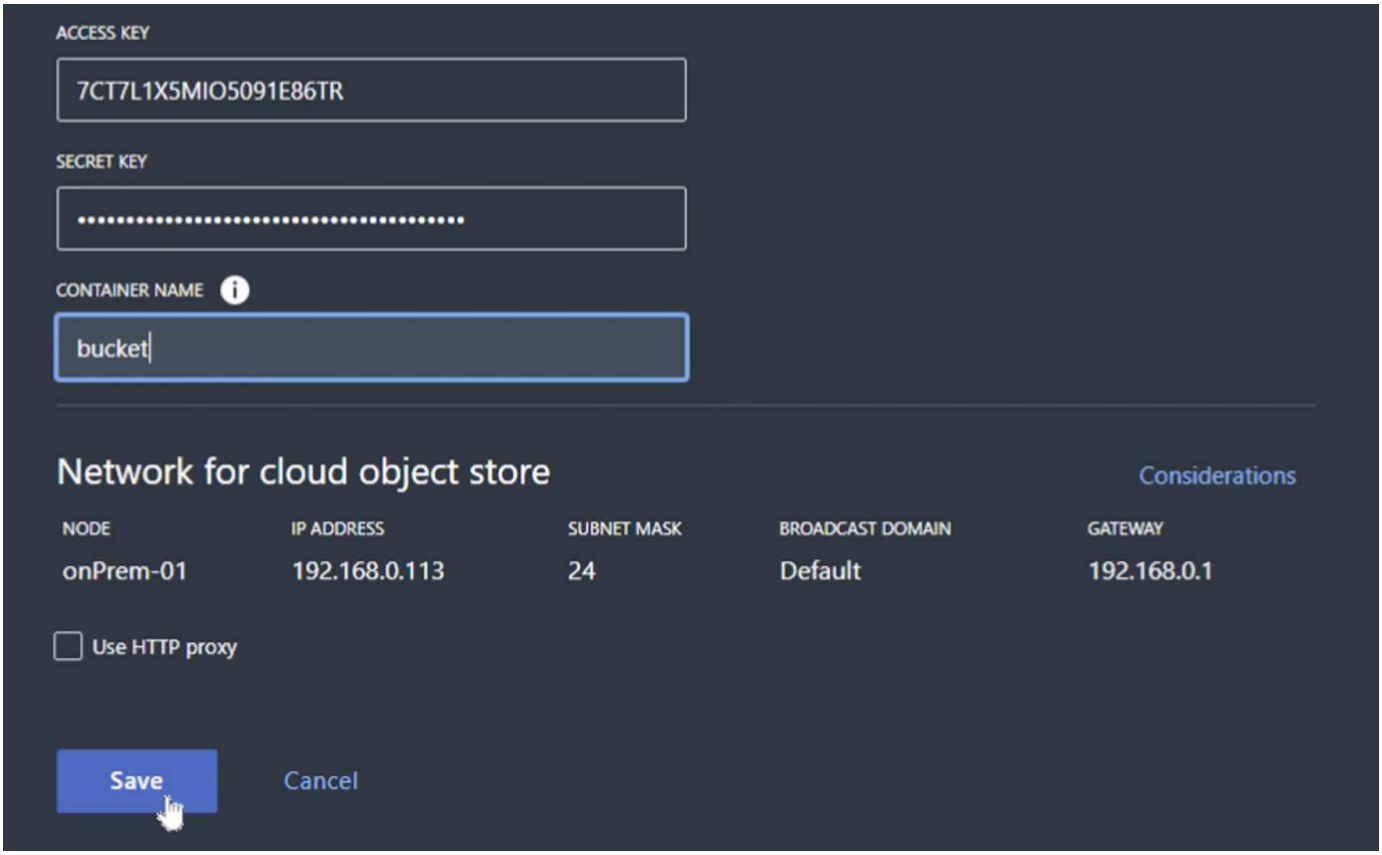
Entrez les informations StorageGRID en fournissant un nom, un style d'URL (pour cette démonstration, nous utiliserons les URL Path-styl). Définissez l'étendue du magasin d'objets sur « Storage VM ».



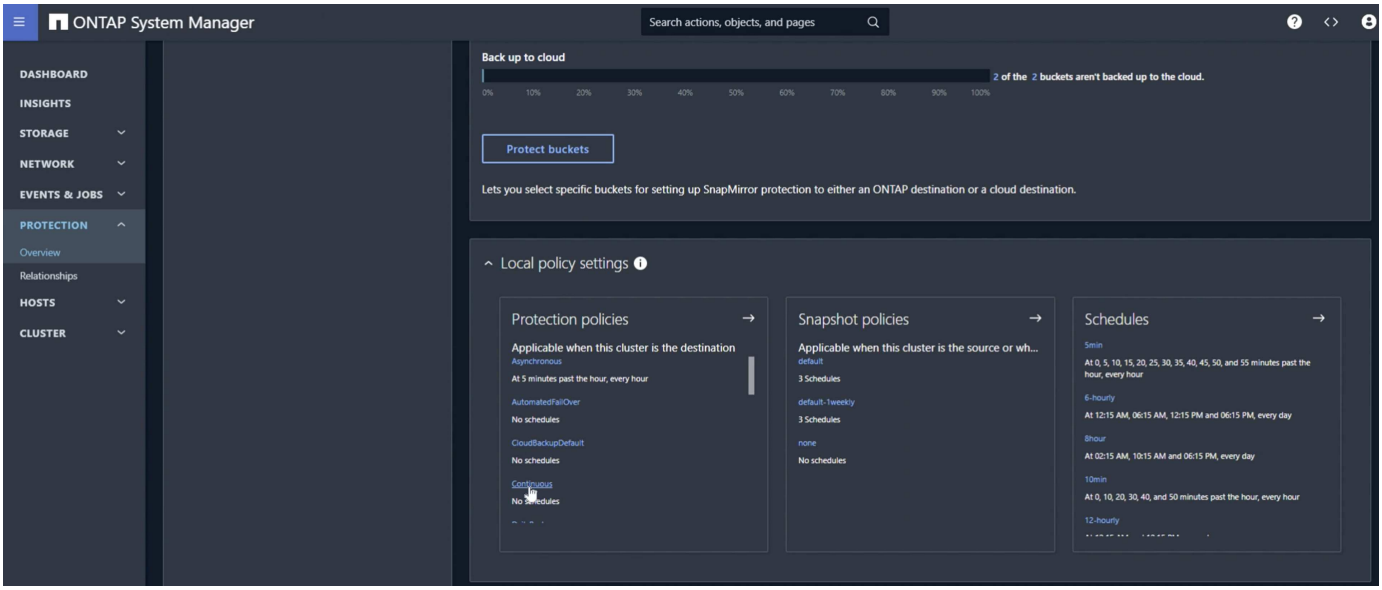
Si vous utilisez SSL, définissez le port du noeud final de l'équilibreur de charge et copiez-le dans le certificat

du noeud final StorageGRID ici. Sinon, décochez la case SSL et entrez le port du noeud final HTTP ici.

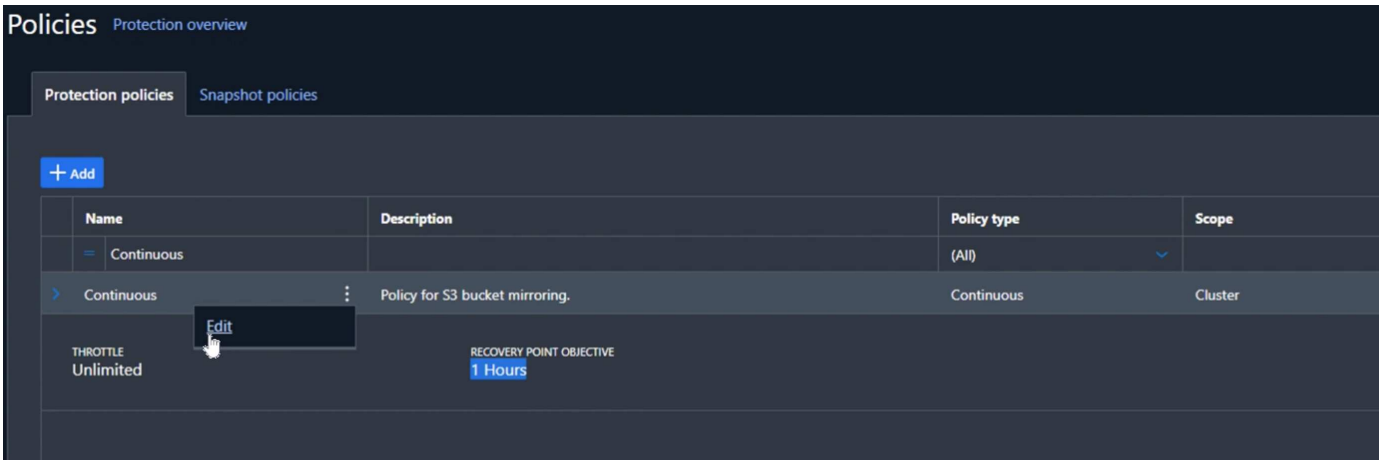
Entrez les clés S3 d'utilisateur StorageGRID et le nom de compartiment dans la configuration StorageGRID ci-dessus pour la destination.



Maintenant qu'une cible de destination est configurée, nous pouvons configurer les paramètres de stratégie pour la cible. Développez « Paramètres de stratégie locale » et sélectionnez « continu ».



Modifiez la stratégie continue et changez l'objectif de point de récupération de « 1 heure » à « 3 secondes ».

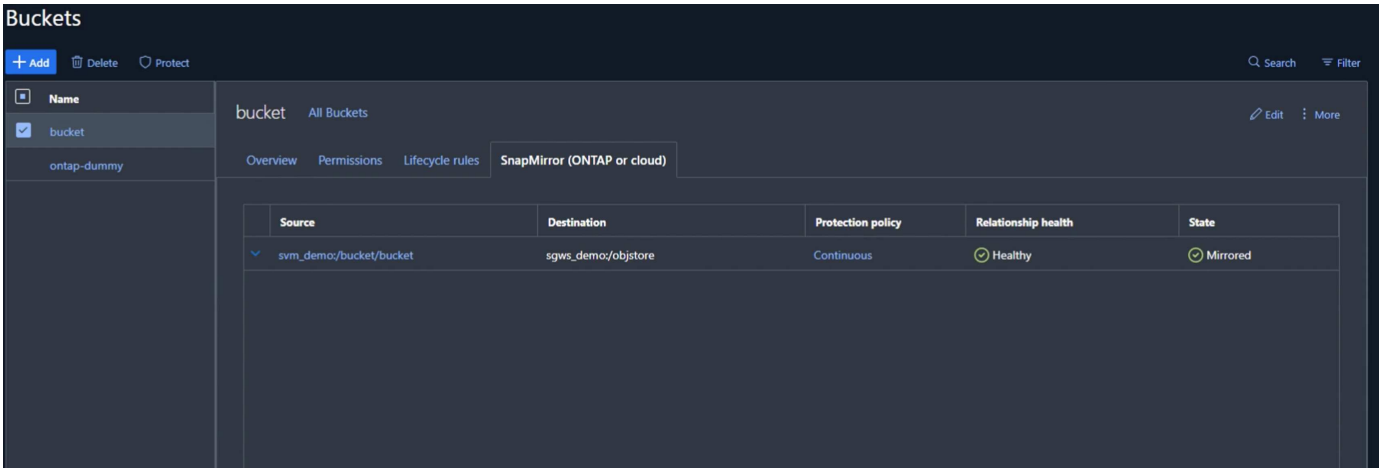


Nous pouvons maintenant configurer SnapMirror pour répliquer le compartiment.

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

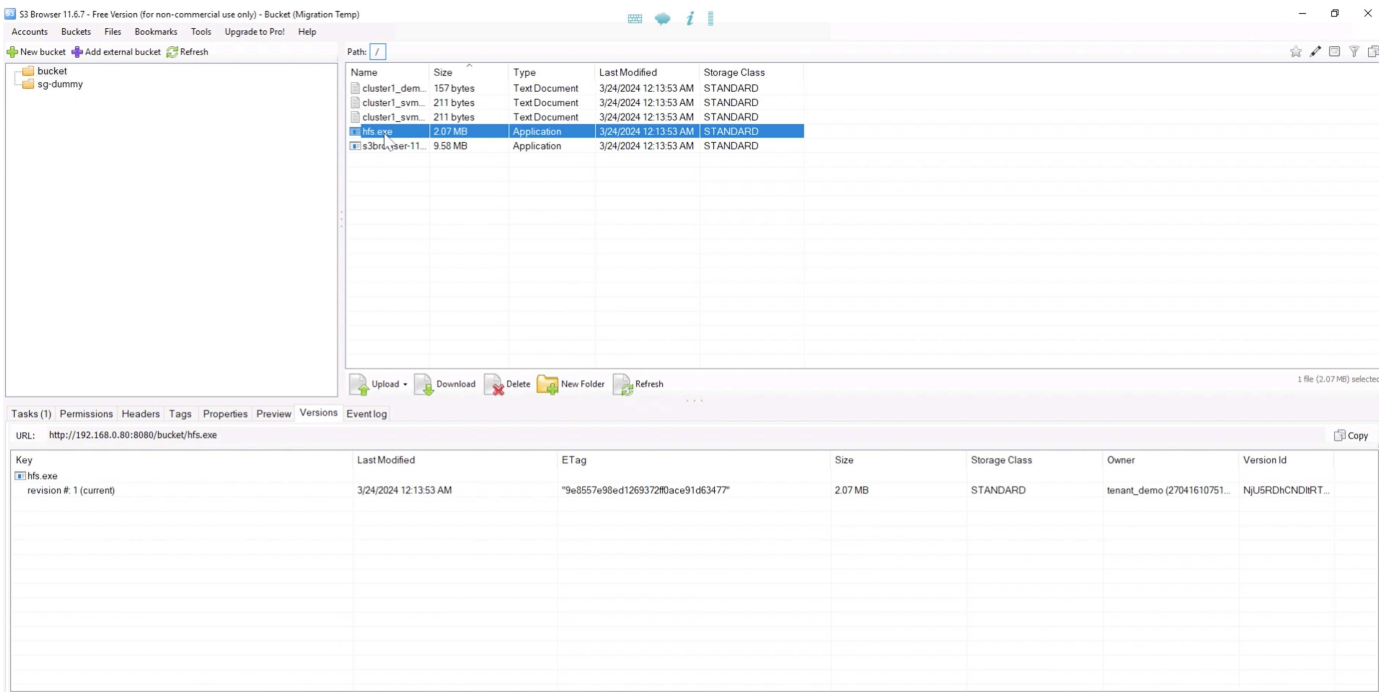
Le compartiment affiche alors un symbole de nuage dans la liste de compartiments sous protection.

Si nous sélectionnons le compartiment et passons à l'onglet SnapMirror (ONTAP ou Cloud), nous verrons le statut de réexpédition SnapMirror.

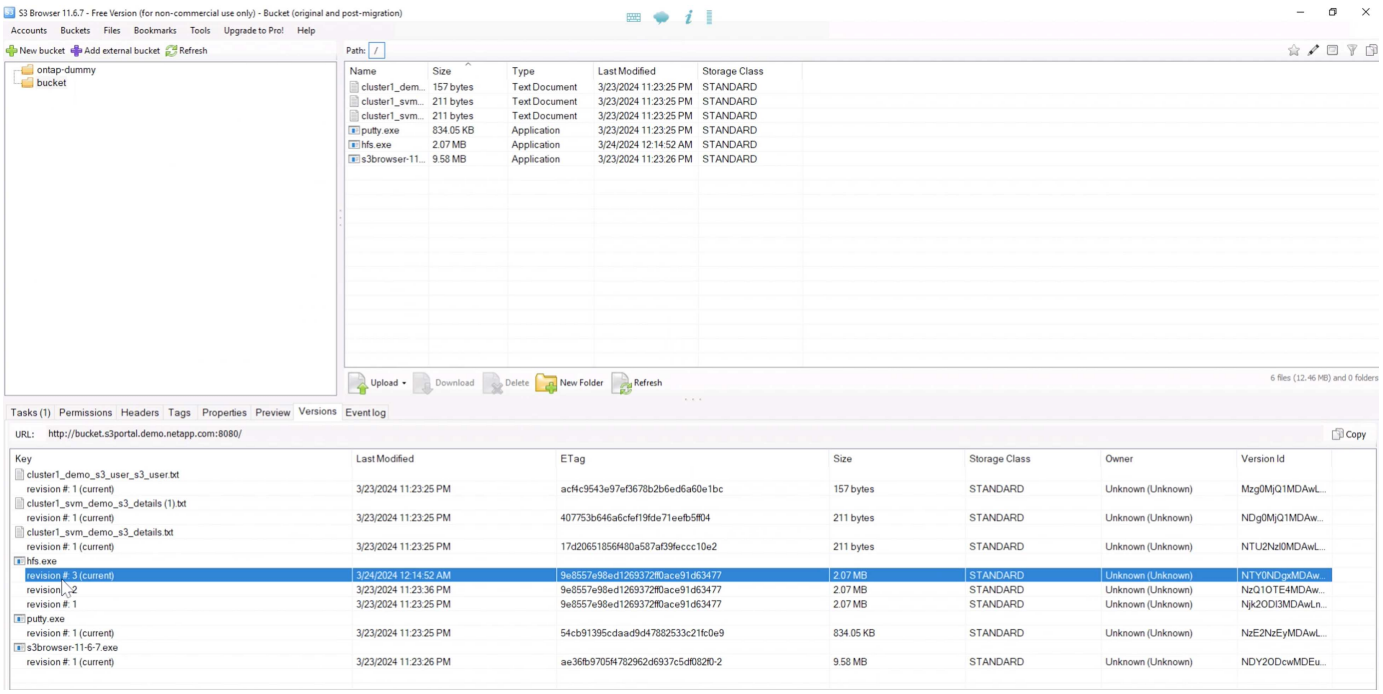


Détails de la réplication

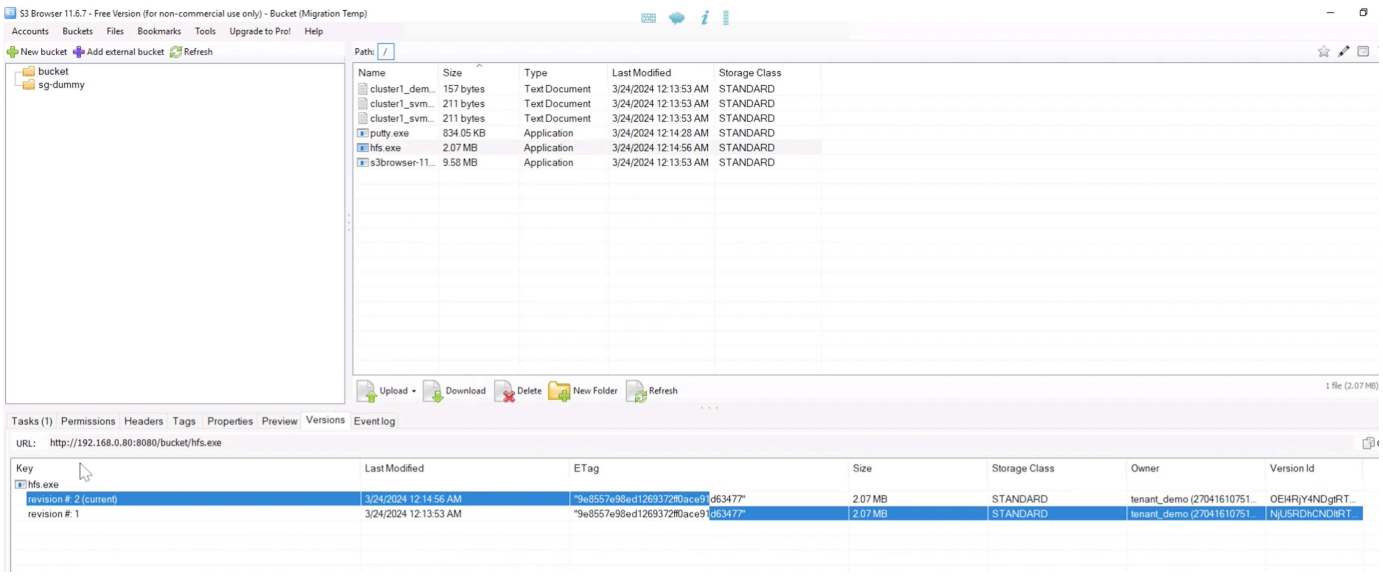
Nous disposons désormais d'un compartiment de réplication réussi de ONTAP vers StorageGRID. Mais qu'est-ce qui se réplique réellement ? La source et la destination sont toutes les deux des compartiments avec version. Les versions précédentes sont-elles également répliquées vers la destination ? Si nous examinons notre compartiment StorageGRID avec S3Browser, nous constatons que les versions existantes ne se répliquent pas et que notre objet supprimé n'existe pas, pas plus qu'un marqueur de suppression pour cet objet. Notre objet dupliqué ne possède qu'une seule version dans le compartiment StorageGRID.



Dans notre compartiment ONTAP, ajoutons une nouvelle version à notre objet que nous avons utilisé précédemment et voyons comment il se réplique.



En ce qui concerne StorageGRID, nous constatons qu'une nouvelle version a également été créée dans ce compartiment, mais qu'elle manque la version initiale d'avant la relation SnapMirror.



En effet, le processus ONTAP SnapMirror S3 ne réplique que la version actuelle de l'objet. C'est pourquoi nous avons créé un compartiment versionné côté StorageGRID pour être la destination. De cette façon, StorageGRID peut conserver un historique des versions des objets.

Par Rafael Guedes, et Aron Klein

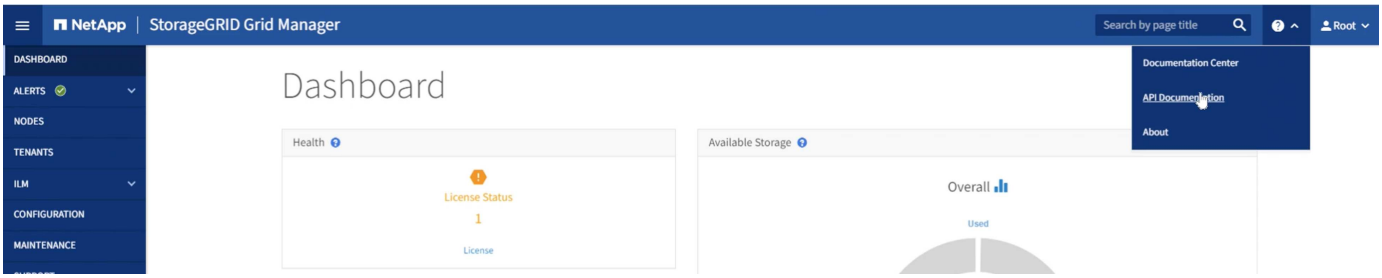
Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

Bénéficiez d'un stockage S3 haute performance en migrant de manière fluide le stockage basé sur les objets d'ONTAP S3 vers StorageGRID

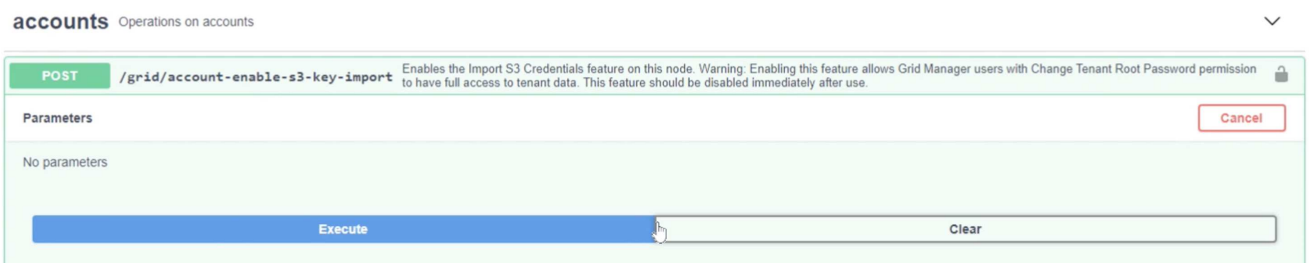
Migrer les clés S3

Pour une migration, la plupart du temps, vous voudrez migrer les informations d'identification des utilisateurs plutôt que de générer de nouvelles informations d'identification côté destination. StorageGRID fournit des api qui permettent d'importer des clés s3 vers un utilisateur.

Se connecter à l'interface utilisateur de gestion de StorageGRID (et non à l'interface du gestionnaire de locataires) ouvre la page swagger de documentation de l'API.

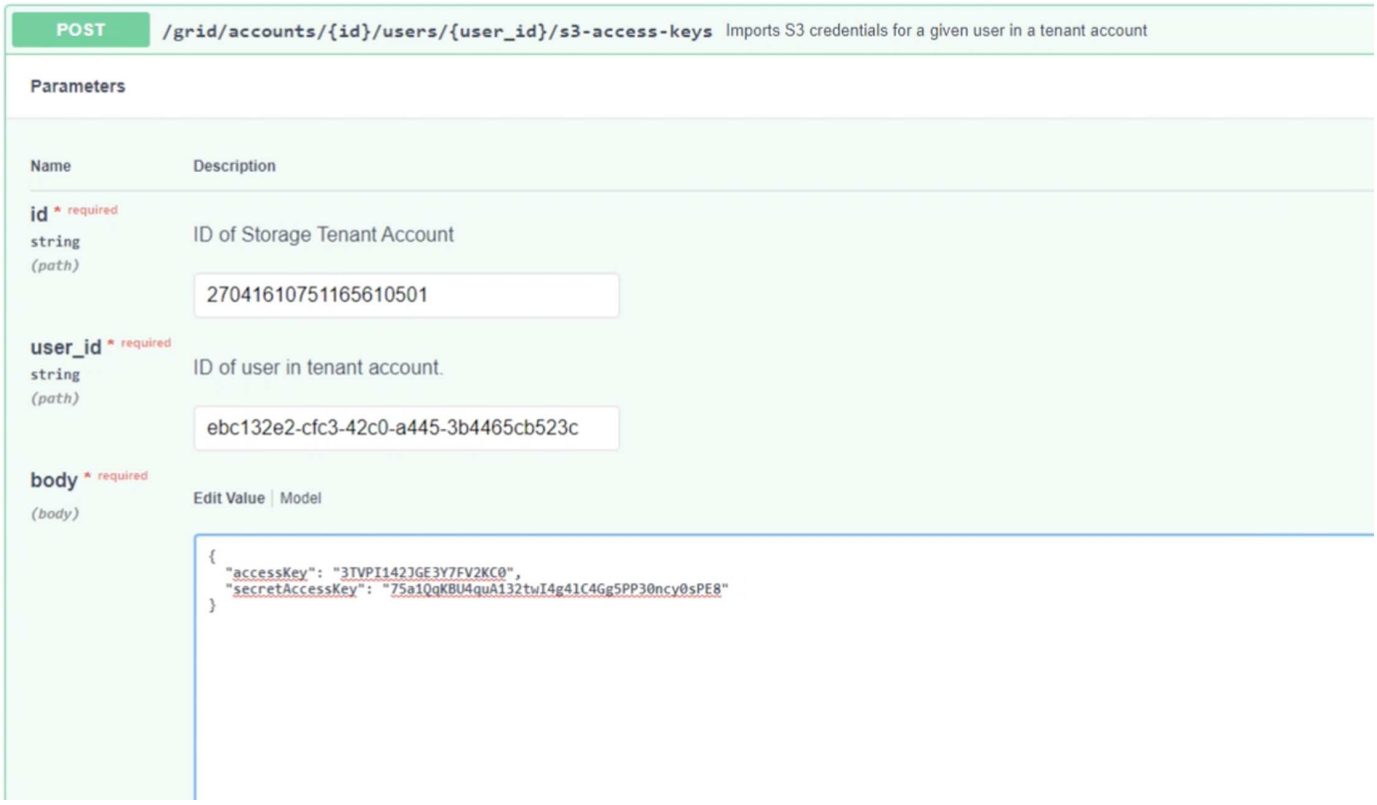


Développez la section « comptes », sélectionnez « POST /grid/account-enable-s3-key-import », cliquez sur le bouton « essayer », puis cliquez sur le bouton exécuter.

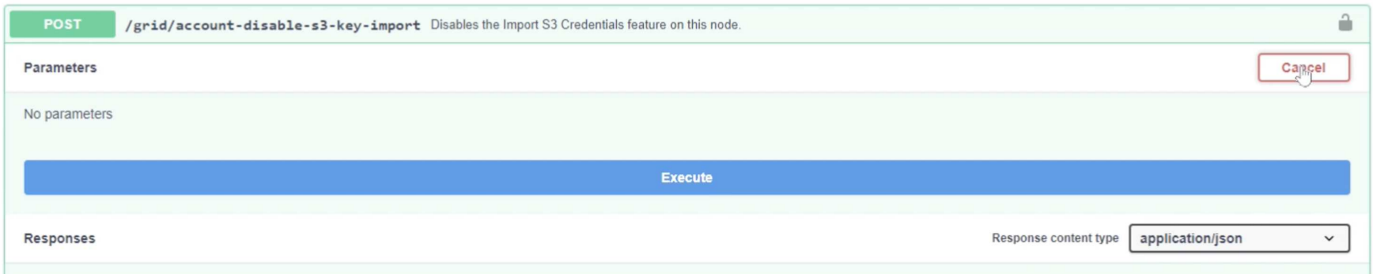


Faites défiler la page encore sous « Accounts » jusqu'à « POST /grid/accounts/{ID}/users/{user_ID}/s3-Access-keys ».

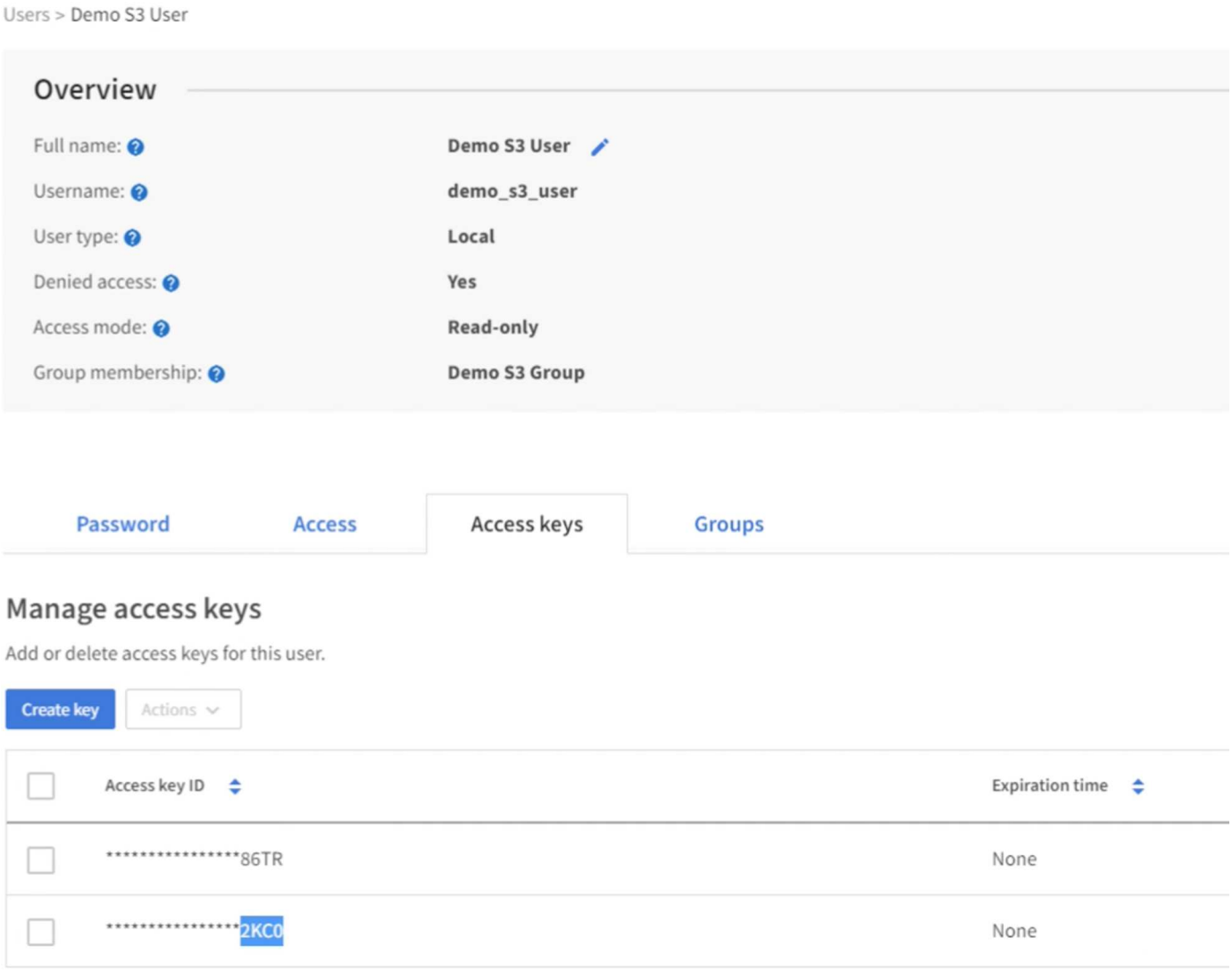
Voici où nous allons entrer l'ID de locataire et l'ID de compte d'utilisateur que nous avons recueillis plus tôt. Remplissez les champs et les clés de notre utilisateur ONTAP dans la boîte json. Vous pouvez définir l'expiration des clés ou supprimer " , "expire": 123456789" et cliquez sur execute.



Une fois que vous avez terminé toutes les importations de clés utilisateur, vous devez désactiver la fonction d'importation de clés dans « Accounts » « POST /grid/account-disable-s3-key-import ».



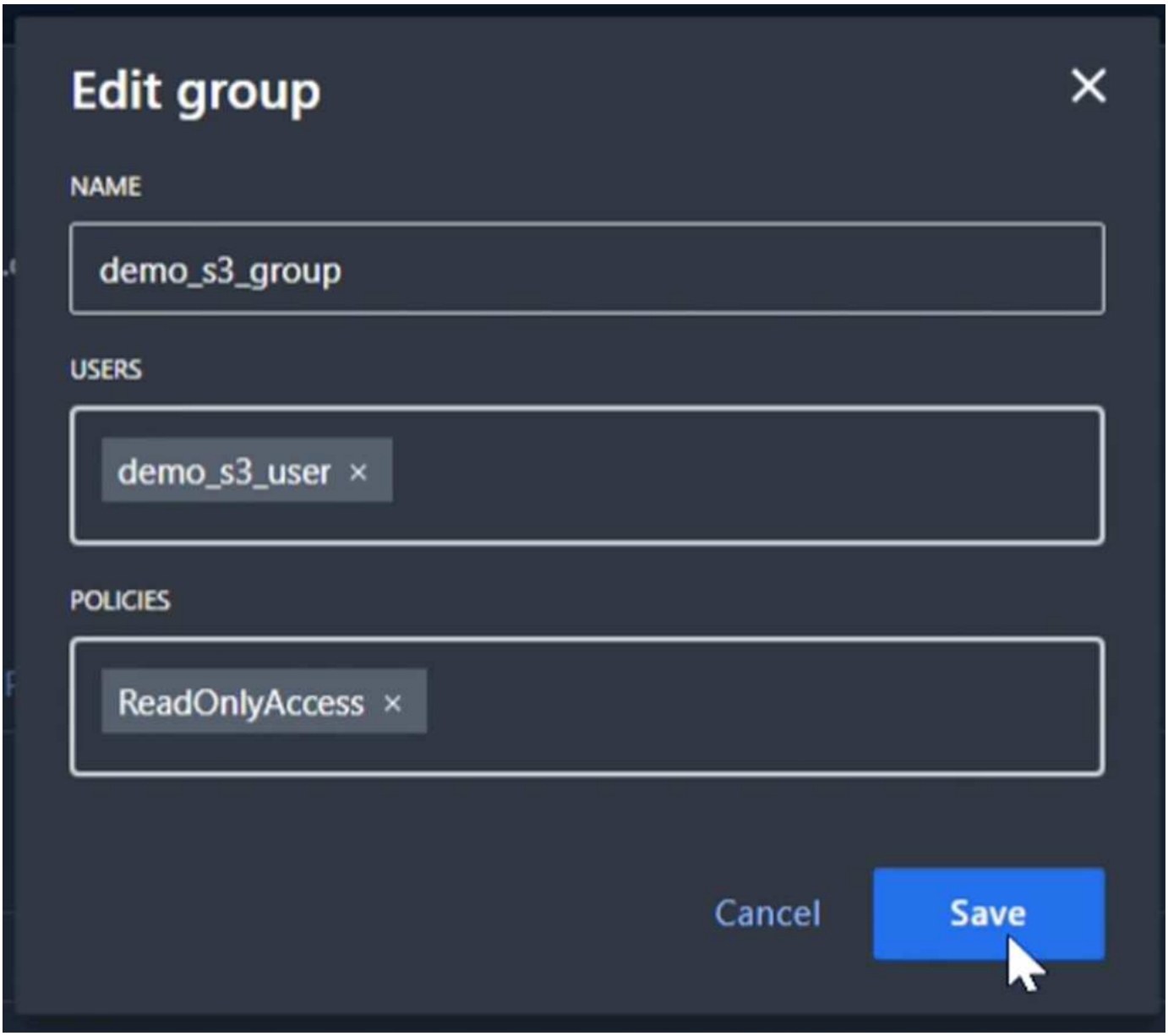
Si nous examinons le compte d'utilisateur dans l'interface utilisateur du gestionnaire de locataires, la nouvelle clé a été ajoutée.



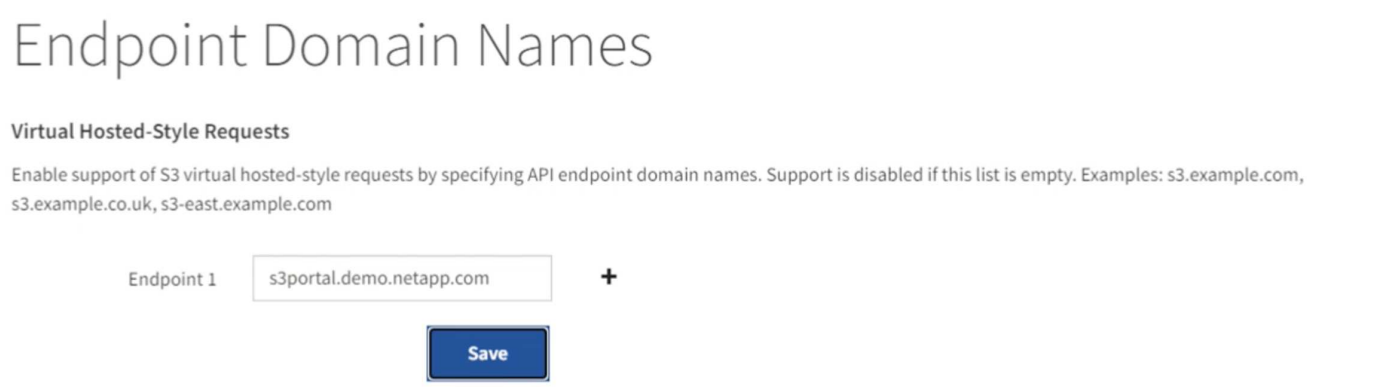
Le basculement final

Si vous avez l'intention de répliquer sans cesse un compartiment de ONTAP vers StorageGRID, vous pouvez terminer ici. S'il s'agit d'une migration d'ONTAP S3 vers StorageGRID, il est temps de mettre fin à cette migration et de la couper.

Dans le gestionnaire système ONTAP, modifiez le groupe S3 et définissez-le sur « ReadOnlyAccess ». Cela empêchera les utilisateurs d'écrire dans le compartiment ONTAP S3.



Il ne reste plus qu'à configurer le DNS pour qu'il pointe du cluster ONTAP vers le terminal StorageGRID. Assurez-vous que votre certificat de noeud final est correct et si vous avez besoin de requêtes de type hébergement virtuel, ajoutez les noms de domaine de noeud final dans StorageGRID



Vos clients devront soit attendre l'expiration du TTL, soit vider le DNS pour résoudre le problème sur le nouveau système afin que vous puissiez tester que tout fonctionne. Il ne reste plus qu'à nettoyer les clés S3 temporaires initiales que nous avons utilisées pour tester l'accès aux données StorageGRID (ET NON les clés importées), supprimer les relations SnapMirror et supprimer les données ONTAP.

Par Rafael Guedes, et Aron Klein

Guides d’utilisation et d’outils

Utilisez le connecteur Cloudera Hadoop S3A avec StorageGRID

Par Angela Cheng

Hadoop est devenu l’un des préférés des data Scientists depuis un certain temps. Hadoop permet le traitement distribué d’importants jeux de données sur des clusters d’ordinateurs à l’aide d’infrastructures de programmation simples. Hadoop a été conçu pour évoluer verticalement de serveurs uniques à des milliers de machines, chaque machine étant en possession de ressources de calcul et de stockage locales.

Pourquoi utiliser S3A pour les flux de travail Hadoop ?

Comme le volume de données a augmenté au fil du temps, l’approche qui consiste à ajouter de nouveaux ordinateurs avec leurs propres ressources de calcul et de stockage est devenue inefficace. L’évolutivité linéaire engendre des défis pour utiliser les ressources efficacement et gérer l’infrastructure.

Pour relever ces challenges, le client Hadoop S3A propose des E/S haute performance par rapport au stockage objet S3. L’implémentation d’un workflow Hadoop avec S3A vous permet d’exploiter le stockage objet en tant que référentiel de données et de séparer les ressources de calcul et de stockage. Vous pouvez ainsi faire évoluer indépendamment les ressources de calcul et de stockage. Qui dissocie le calcul et le stockage pour vous permettre de consacrer la quantité de ressources adaptée à vos tâches de calcul, et d’assurer la capacité en fonction de la taille de votre jeu de données. Par conséquent, vous pouvez réduire votre TCO global pour les workflows Hadoop.

Configurer le connecteur S3A pour utiliser StorageGRID

Prérequis

- Une URL de terminal StorageGRID S3, une clé d’accès s3 pour un locataire et une clé secrète pour le test de connexion à Hadoop S3A.
- Un cluster Cloudera ainsi que l’autorisation root ou sudo pour chaque hôte du cluster afin d’installer le package Java.

En avril 2022, Java 11.0.14 avec Cloudera 7.1.7 a été testé contre StorageGRID 11.5 et 11.6. Cependant, le numéro de version de Java peut être différent au moment d’une nouvelle installation.

Installez le package Java

1. Vérifier le "Matrice de support Cloudera" Pour la version JDK prise en charge.
2. Téléchargez le "Package Java 11.x" Correspondant au système d’exploitation du cluster Cloudera. Copiez ce package sur chaque hôte du cluster. Dans cet exemple, le progiciel rpm est utilisé pour CentOS.
3. Connectez-vous à chaque hôte en tant que root ou en utilisant un compte avec l’autorisation sudo. Effectuez les étapes suivantes sur chaque hôte :
   a. Installez le package :

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

b. Vérifiez l'emplacement d'installation de Java. Si plusieurs versions sont installées, définissez la nouvelle version installée par défaut :

```
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. Ajoutez cette ligne à la fin de `/etc/profile`. Le chemin doit correspondre au chemin de la sélection ci-dessus :

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

d. Exécutez la commande suivante pour que le profil prenne effet :

```
source /etc/profile
```

Configuration HDFS S3A de Cloudera

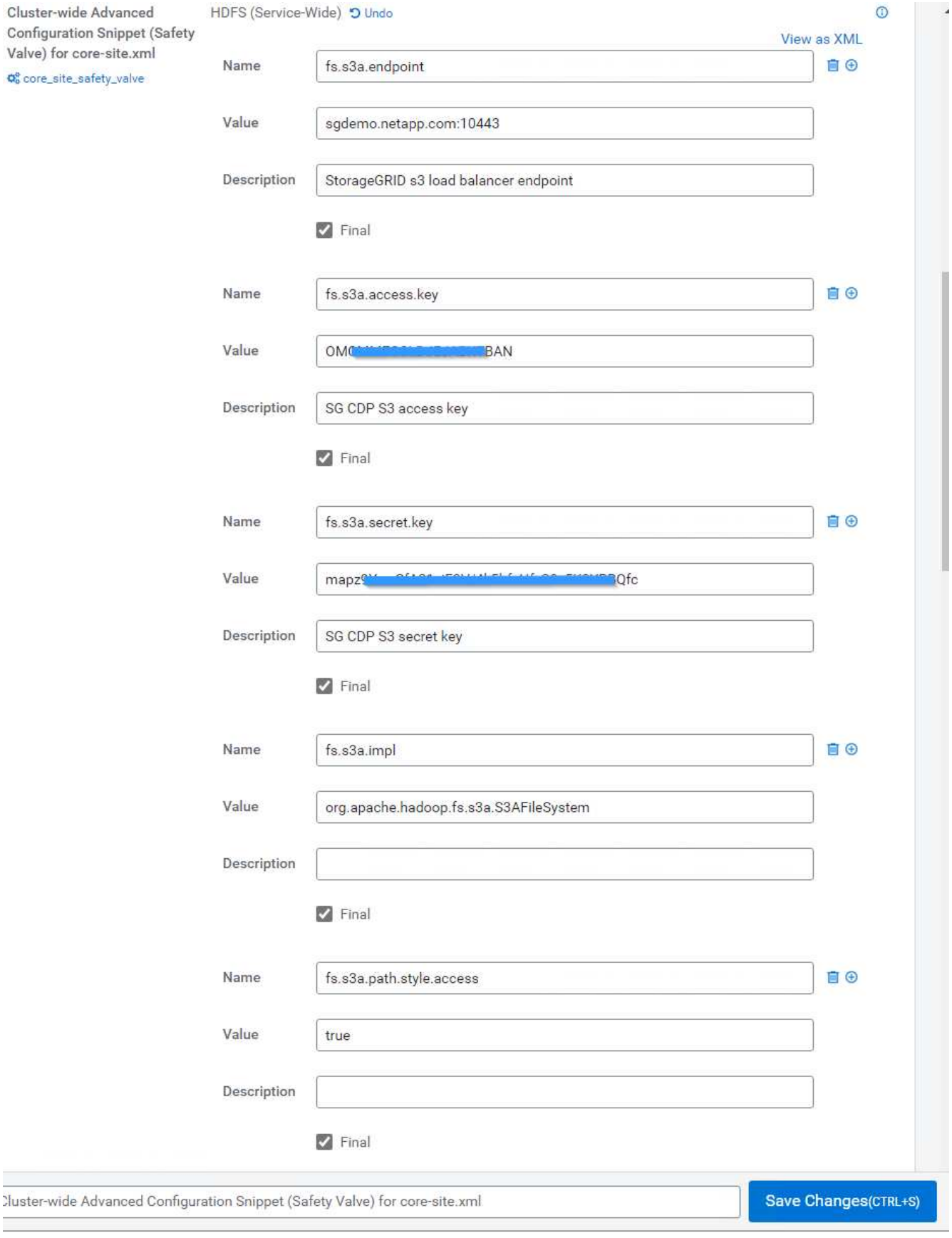
Étapes

1. Dans l'interface graphique Cloudera Manager, sélectionnez clusters > HDFS et sélectionnez Configuration.
2. Sous CATÉGORIE, sélectionnez Avancé, puis faites défiler vers le bas pour rechercher `Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml`.
3. Cliquez sur le signe (+) et ajoutez les paires de valeurs suivantes.

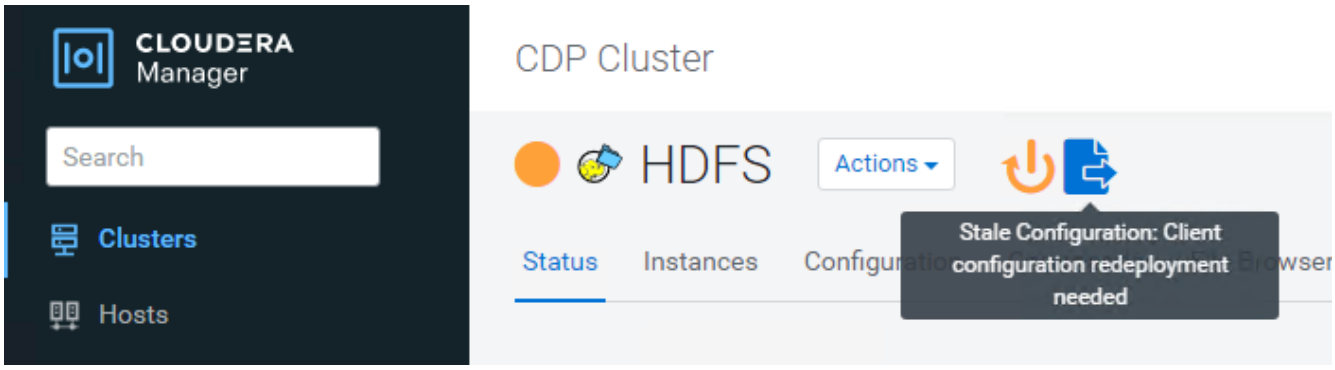
Nom	Valeur
fs.s3a.access.key	*<clé d'accès s3 de StorageGRID>*
fs.s3a.secret.key	*<clé secrète S3 du locataire StorageGRID>*
fs.s3a.connection.ssl.enabled	[vrai ou faux] (la valeur par défaut est https si cette entrée est manquante)
fs.s3a.endpoint	*<noeud final StorageGRID S3:port>*

Nom	Valeur
fs.s3a.impl	ORG.apache.hadoop.fs.s3a.S3AFileSystem
fs.s3a.path.style.access	[vrai ou faux] (le style d'hôte virtuel par défaut est défini si cette entrée est manquante)

Exemple de capture d'écran



4. Cliquez sur le bouton Enregistrer les modifications. Sélectionnez l'icône Configuration obsolète dans la barre de menus HDFS, sélectionnez redémarrer les services obsolètes sur la page suivante, puis sélectionnez redémarrer maintenant.



Tester la connexion S3A à StorageGRID

Effectuer un test de connexion de base

Connectez-vous à l'un des hôtes du cluster Cloudera, puis entrez `hadoop fs -ls s3a://<bucket-name>/`.

L'exemple suivant utilise le chemin syle avec un compartiment hdfs-test pré-existant et un objet 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.
```

Dépannage

Scénario 1

Utilisez une connexion HTTPS à StorageGRID et obtenez un `handshake_failure` erreur après un délai de 15 minutes.

Raison : ancienne version JRE/JDK utilisant la suite de chiffrement TLS obsolète ou non prise en charge pour la connexion à StorageGRID.

Exemple de message d'erreur

```
[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
```

Résolution : Assurez-vous que JDK 11.x ou version ultérieure est installé et défini par défaut la bibliothèque Java. Reportez-vous à la Installez le package Java pour plus d'informations.

Scénario 2 :

Impossible de se connecter à StorageGRID avec message d'erreur `Unable to find valid certification path to requested target`.

Raison: le certificat du serveur de noeuds finaux StorageGRID S3 n'est pas approuvé par le programme Java.

Exemple de message d'erreur :

```
[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
```

Resolution: NetApp recommande d'utiliser un certificat de serveur délivré par une autorité de signature de certificat public connu pour s'assurer que l'authentification est sécurisée. Vous pouvez également ajouter un certificat d'autorité de certification ou de serveur personnalisé au magasin de confiance Java.

Procédez comme suit pour ajouter une autorité de certification ou un certificat de serveur personnalisé StorageGRID au magasin d'approbation Java.

1. Sauvegardez le fichier Java cacerts existant par défaut.

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

2. Importez le certificat de noeud final StorageGRID S3 dans le magasin de confiance 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>
```

Conseils de dépannage

1. Augmentez le niveau de journalisation hadoop pour DÉBOGUER.

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

2. Exécutez la commande et dirigez les messages du journal vers error.log.

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

Par Angela Cheng

Utilisez S3cmd pour tester et démontrer l'accès S3 sur StorageGRID

Par Aron Klein

S3cmd est un outil de ligne de commande gratuit et un client pour les opérations S3. Vous pouvez utiliser s3cmd pour tester et démontrer l'accès s3 avec StorageGRID.

Installez et configurez S3cmd

Pour installer S3cmd sur un poste de travail ou un serveur, téléchargez-le à partir de "Client S3 en ligne de commande". S3cmd est préinstallé sur chaque nœud StorageGRID comme outil pour faciliter le dépannage.

Étapes de configuration initiale

1. s3cmd --configure
2. Fournissez uniquement Access_Key et secret_key, pour le reste conservez les valeurs par défaut.
3. Tester l'accès avec les informations d'identification fournies ? [O/n] : n (ignorer le test car il échouera)
4. Enregistrer les paramètres ? [o/N] y
   a. Configuration enregistrée dans '/root/.s3cfg'
5. Dans les champs .s3cfg, rendre vide Host_base et Host_bucket après le signe "=" :
   a. host_base =
   b. host_bucket =

> Si vous spécifiez Host_base et Host_bucket à l'étape 4, il n'est pas nécessaire de spécifier un noeud final avec --host dans la CLI. Exemple :

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

Exemples de commandes de base

- **Créer un compartiment :**

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

- **Liste de tous les compartiments:**

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

- **Liste de tous les compartiments et de leur contenu:**

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

- **Liste des objets dans un compartiment spécifique :**

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

- **Supprimer un compartiment :**

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

- **Mettre un objet:**

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

- **Obtenir un objet:**

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

- **Supprimer un objet:**

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

Base de données en mode Vertica Eon utilisant NetApp StorageGRID comme stockage communautaire

Par Angela Cheng

Ce guide décrit la procédure de création d'une base de données Vertica Eon mode avec stockage communautaire sur NetApp StorageGRID.

Introduction

Vertica est un logiciel de gestion de base de données analytique. C'est une plateforme de stockage orientée colonnes conçue pour gérer d'importants volumes de données, permettant ainsi des performances d'interrogation très rapides dans un scénario très intensif. Une base de données Vertica s'exécute dans l'un des deux modes suivants : EON ou Enterprise. Vous pouvez déployer les deux modes sur site ou dans le cloud.

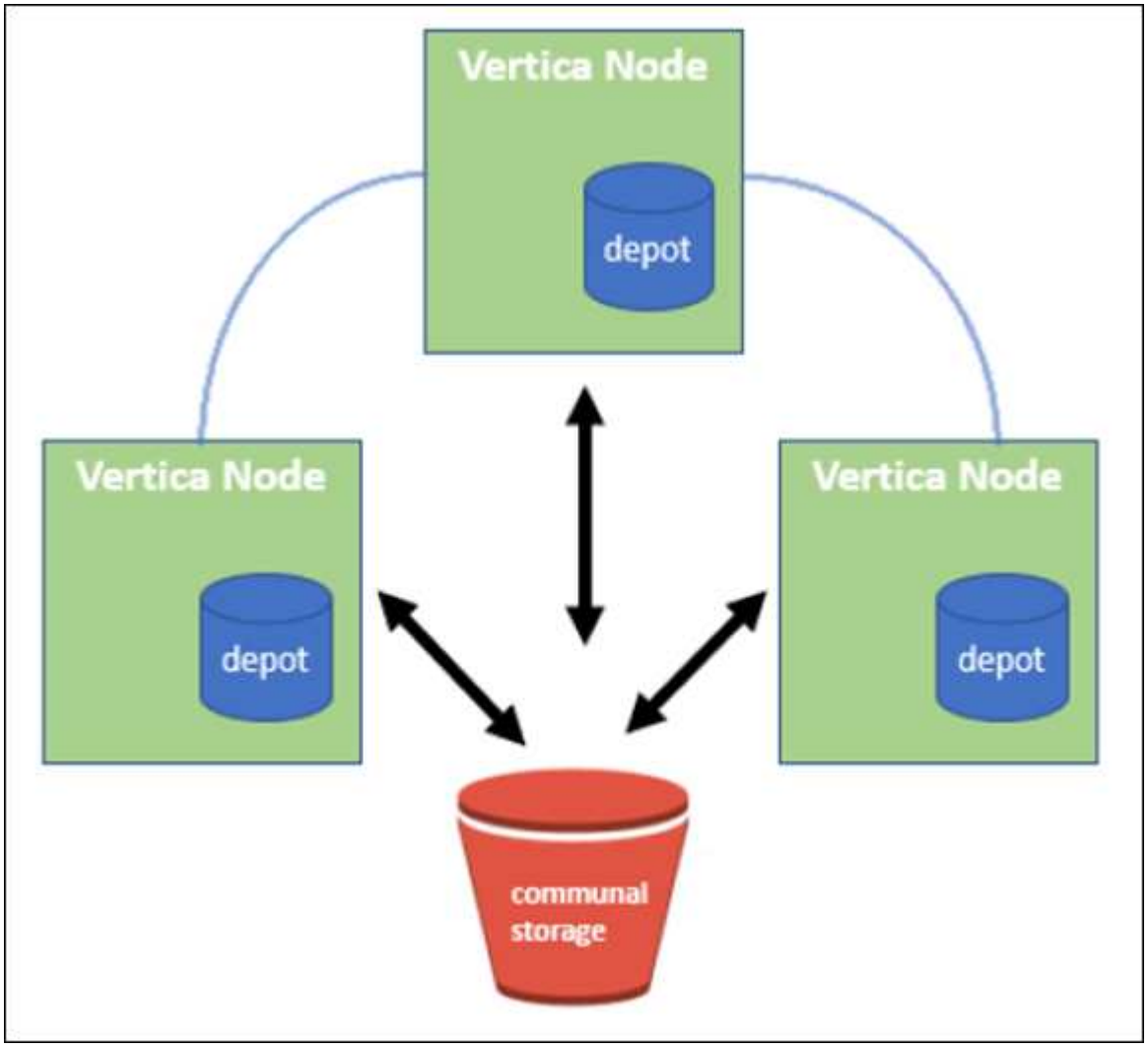
Les modes EON et Enterprise diffèrent principalement lorsqu'ils stockent des données :

- Les bases de données du mode EON utilisent le stockage communautaire pour leurs données. Ceci est recommandé par Vertica.
- Les bases de données Enterprise mode stockent les données localement dans le système de fichiers des nœuds qui composent la base de données.

Architecture du mode EON

Le mode EON sépare les ressources de calcul de la couche de stockage communautaire de la base de données, ce qui permet l'évolutivité séparée du calcul et du stockage. Vertica en mode Eon est optimisé pour traiter des charges de travail variables et les isoler les unes des autres à l'aide de ressources de calcul et de stockage distinctes.

EON mode stocke les données dans un magasin d'objets partagés appelé stockage communal : un compartiment S3, hébergé sur site ou sur Amazon S3.



Stockage communautaire

Au lieu de stocker les données localement, le mode Eon utilise un emplacement de stockage commun unique pour toutes les données et le catalogue (métadonnées). Le stockage communal est l'emplacement de stockage centralisé de la base de données, partagé entre les nœuds de base de données.

Le stockage communal a les propriétés suivantes :

- Le stockage communautaire dans le cloud ou dans un stockage objet sur site est plus résilient et moins vulnérable aux pertes de données dues à des défaillances de stockage que sur un stockage sur disque sur des machines individuelles.
- Toutes les données peuvent être lues par n'importe quel nœud utilisant le même chemin d'accès.
- La capacité n'est pas limitée par l'espace disque sur les nœuds.
- Les données étant stockées dans la communauté, vous pouvez faire évoluer votre cluster en toute flexibilité pour répondre aux besoins changeants. Si les données étaient stockées localement sur les nœuds, ajouter ou supprimer des nœuds nécessiterait un déplacement de grandes quantités de données entre les nœuds pour les déplacer hors des nœuds supprimés, ou vers les nœuds nouvellement créés.

Le dépôt

La vitesse est un inconvénient du stockage commun. L'accès aux données à partir d'un emplacement cloud partagé est plus lent que la lecture à partir d'un disque local. En outre, la connexion au stockage commun peut former un goulot d'étranglement si de nombreux nœuds lisent les données à partir de ce stockage en même temps. Pour améliorer la vitesse d'accès aux données, les nœuds d'une base de données en mode Eon maintiennent un cache de disque local de données appelé dépôt. Lors de l'exécution d'une requête, les nœuds vérifient d'abord si les données dont ils ont besoin se trouvent dans le dépôt. Si c'est le cas, il termine la requête en utilisant la copie locale des données. Si les données ne se trouvent pas dans le dépôt, le nœud extrait les données du stockage commun et enregistre une copie dans le dépôt.

Recommandations de NetApp StorageGRID

Vertica stocke les données de base de données dans le stockage objet sous la forme de milliers (ou de millions) d'objets compressés (dont la taille observée est de 200 à 500 Mo par objet). Lorsqu'un utilisateur exécute des requêtes de base de données, Vertica récupère la plage de données sélectionnée à partir de ces objets compressés en parallèle à l'aide de l'appel GET de plage d'octets. Chaque PLAGE d'octets GET est d'environ 8 Ko.

Lors du test de requêtes utilisateur externes au dépôt de bases de données de 10 To, 4,000 à 10,000 REQUÊTES GET (OCTET-plage) par seconde ont été envoyées dans la grille. Lors de l'exécution de ce test avec des appliances SG6060, si le taux d'utilisation du processeur par nœud d'appliance est faible (environ 20 à 30 %), 2/3 le temps du processeur est en attente des E/S. Un très faible pourcentage (0 % à 0.5 %) d'attente d'E/S est observé sur le SGF6024.

En raison de la forte demande en IOPS peu élevées avec des latences très faibles (la moyenne doit être inférieure à 0.01 secondes), NetApp recommande l'utilisation du système SFG6024 pour les services de stockage objet. Si le SG6060 est nécessaire pour des bases de données très volumineuses, le client doit travailler avec l'équipe des comptes Vertica sur le dimensionnement du dépôt pour prendre en charge le dataset très interrogé.

Pour le nœud d'administration et le nœud de passerelle d'API, le client peut utiliser le SG100 ou le SG1000. Le choix dépend du nombre de requêtes des utilisateurs en parallèle et de la taille de la base de données. Si le client préfère utiliser un équilibreur de charge tiers, NetApp recommande un équilibreur de charge dédié pour une charge de travail hautes performances. Pour connaître le dimensionnement StorageGRID, consultez l'équipe de gestion de compte NetApp.

D'autres recommandations concernant la configuration de StorageGRID incluent :

- **Topologie de grille**. Ne mélangez pas le SGF6024 avec d'autres modèles d'appliance de stockage sur le même site de réseau. Si vous préférez utiliser le SG6060 pour la protection de l'archivage à long terme,

conservez le SGF6024 avec un équilibreur de charge dédié dans son propre site de grid (site physique ou logique) pour une base de données active afin d'améliorer les performances. L'utilisation de différents modèles d'appliance sur le même site réduit les performances globales sur le site.

- **Protection des données**. Utilisez des copies répliquées pour la protection. N'utilisez pas le code d'effacement pour une base de données active. Le client peut utiliser un code d'effacement pour protéger à long terme les bases de données inactives.
- **N'activez pas la compression de grille**. Vertica compresse les objets avant de les stocker dans le stockage objet. L'activation de la compression grid n'entraîne pas d'économie supplémentaire en matière d'utilisation du stockage et réduit considérablement les performances GET de plage d'octets.
- **Connexion de terminal HTTP et HTTPS S3**. Lors du test de banc d'essai, nous avons observé une amélioration des performances d'environ 5 % lors de l'utilisation d'une connexion HTTP S3 du cluster Vertica vers le point de terminaison de l'équilibreur de charge StorageGRID. Ce choix doit être basé sur les exigences de sécurité du client.

Les recommandations pour une configuration Vertica sont les suivantes :

- **Les paramètres de dépôt par défaut de la base de données Vertica sont activés (valeur = 1) pour les opérations de lecture et d'écriture**. NetApp recommande fortement de maintenir ces paramètres de dépôt activés pour améliorer les performances.
- **Désactiver les limitations de diffusion**. Pour plus de détails sur la configuration, reportez-vous à la section Désactivation des restrictions de diffusion en continu.

Installation du mode Eon sur site avec stockage communautaire sur StorageGRID

Les sections suivantes décrivent la procédure, dans l'ordre, d'installation du mode Eon sur site avec un stockage communautaire sur StorageGRID. La procédure de configuration du stockage objet compatible S3 (simple Storage Service) sur site est similaire à la procédure décrite dans le guide Vertica, "Installez une base de données en mode Eon sur site".

La configuration suivante a été utilisée pour le test fonctionnel :

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- Trois machines virtuelles (VM) avec CentOS 7.x OS pour les nœuds Vertica afin de former un cluster. Cette configuration est destinée uniquement au test fonctionnel, pas au cluster de base de données de production Vertica.

Ces trois nœuds sont configurés avec une clé Secure Shell (SSH) afin de permettre SSH sans mot de passe entre les nœuds du cluster.

Informations requises par NetApp StorageGRID

Pour installer Eon mode sur site avec un stockage communautaire sur StorageGRID, vous devez disposer des informations de prérequis suivantes.

- Adresse IP ou nom de domaine complet (FQDN) et numéro de port du terminal StorageGRID S3. Si vous utilisez HTTPS, utilisez un certificat SSL personnalisé (autorité de certification) ou un certificat SSL auto-signé mis en œuvre sur le terminal StorageGRID S3.
- Nom du compartiment. Il doit exister au préalable et être vide.
- L'ID de clé et la clé d'accès secrète avec un accès en lecture et en écriture au compartiment.

Création d'un fichier d'autorisation pour accéder au terminal S3

Les prérequis suivants s'appliquent lors de la création d'un fichier d'autorisation pour accéder au terminal S3 :

- Vertica est installé.
- Un cluster est configuré, configuré et prêt pour la création de bases de données.

Pour créer un fichier d'autorisation pour accéder au terminal S3, effectuez la procédure suivante :

1. Connectez-vous au nœud Vertica sur lequel vous allez exécuter `admintools` Pour créer la base de données du mode Eon.

   L'utilisateur par défaut est `dbadmin`, Créé lors de l'installation du cluster Vertica.

2. Utilisez un éditeur de texte pour créer un fichier sous le `/home/dbadmin` répertoire. Le nom du fichier peut être tout ce que vous voulez, par exemple, `sg_auth.conf`.
3. Si le terminal S3 utilise un port HTTP standard 80 ou HTTPS 443, ignorez le numéro de port. Pour utiliser HTTPS, définissez les valeurs suivantes :

   ◦ `awsenablehttps = 1`, sinon, définissez la valeur sur `0`.

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

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

   Pour utiliser un certificat SSL personnalisé ou auto-signé pour la connexion HTTPS du noeud final StorageGRID S3, spécifiez le chemin d'accès complet au fichier et le nom du fichier du certificat. Ce fichier doit se trouver au même emplacement sur chaque nœud de la Vertica et avoir des droits d'accès en lecture pour tous les utilisateurs. Ignorez cette étape si le certificat SSL du terminal StorageGRID S3 est signé par une autorité de certification publique.

   - `awscafile = <filepath/filename>`

   Par exemple, consultez le fichier d'exemple suivant :

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

+

> Dans un environnement de production, le client doit implémenter un certificat de serveur signé par une autorité de certification publique sur un terminal d'équilibrage de charge StorageGRID S3.

Sélection d'un chemin de dépôt sur tous les nœuds de la Vertica

Choisissez ou créez un répertoire sur chaque nœud pour le chemin de stockage du dépôt. Le répertoire que vous fournissez pour le paramètre chemin de stockage du dépôt doit avoir les éléments suivants :

- Le même chemin sur tous les nœuds du cluster (par exemple, `/home/dbadmin/depot`)
- Être lisible et inscriptible par l'utilisateur dbadmin
- Un stockage suffisant

  Par défaut, Vertica utilise 60 % de l'espace du système de fichiers contenant le répertoire pour le stockage du dépôt. Vous pouvez limiter la taille du dépôt en utilisant le `--depot-size` argument dans le `create_db` commande. Voir "Dimensionnement du cluster Vertica pour une base de données en mode Eon" article pour les directives générales de dimensionnement de la Vertica ou consultez votre gestionnaire de compte Vertica.

  Le `admintools create_db` l'outil tente de créer le chemin de dépôt pour vous si celui-ci n'existe pas.

Création de la base de données Eon sur site

Pour créer la base de données Eon sur site, procédez comme suit :

1. Pour créer la base de données, utilisez le `admintools create_db` outil.

   La liste suivante fournit une brève explication des arguments utilisés dans cet exemple. Consultez le document Vertica pour obtenir une explication détaillée de tous les arguments requis et facultatifs.

   - -x <chemin/nom de fichier d'autorisation créé dans « Création d'un fichier d'autorisation pour accéder au noeud final S3 » >.

     Les détails d'autorisation sont stockés dans la base de données après la création. Vous pouvez supprimer ce fichier pour éviter d'exposer la clé secrète S3.

   - --emplacement-communautaire-stockage <s3://storagegrid buckname>
   - -S <liste séparée par des virgules des nœuds de la Vertica à utiliser pour cette base de données>
   - -d <nom de la base de données à créer>
   - -p <mot de passe à définir pour cette nouvelle base de données>. Par exemple, reportez-vous à la commande d'exemple suivante :

     ```
     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 création d'une nouvelle base de données prend plusieurs minutes en fonction du nombre de nœuds de la base de données. Lors de la création de la base de données pour la première fois, vous serez invité à accepter le contrat de licence.

Par exemple, reportez-vous à l'exemple de fichier d'autorisation suivant et `create db` commande :

```
[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.
```

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
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

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
40	s3://vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31_0_0.dfs
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

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
33	s3://vertica/acd/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29_0_0.dfs
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

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
8937984	s3://vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002187a.tar
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

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
254	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c13_13/completed
2958	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c2_2/chkpt_1.cat.gz
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

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0016/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/chkpt_1.cat.gz
232	s3://vertica/metadata/VMart/nodes/v_vmart_node0017/Catalog/859703b06a3456d95d0be28575a673/Checkpoints/c14_7/completed
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

Taille de l'objet (octet)	Chemin d'accès complet de la clé de compartiment/objet
0	s3://vertica/metadata/VMart/nodes/v_vmart_node0018/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat

Désactivation des restrictions de diffusion en continu

Cette procédure est basée sur le guide Vertica pour d'autres systèmes de stockage objet sur site et doit s'appliquer à StorageGRID.

1. Après avoir créé la base de données, désactivez le `AWSStreamingConnectionPercentage` paramètre de configuration en le définissant sur `0`. Ce paramètre n'est pas nécessaire pour une installation sur site en mode Eon avec stockage communautaire. Ce paramètre de configuration contrôle le nombre de connexions au magasin d'objets utilisé par Vertica pour les lectures en continu. Dans un environnement cloud, ce paramètre évite que les données en streaming à partir du magasin d'objets utilisent tous les descripteurs de fichier disponibles. Certains poignées de fichiers restent disponibles pour d'autres opérations de stockage d'objets. En raison de la faible latence des magasins d'objets sur site, cette option n'est pas nécessaire.
2. Utiliser un `vsql` instruction permettant de mettre à jour la valeur du paramètre. Le mot de passe est le mot de passe de la base de données que vous avez défini dans la section "création de la base de données Eon sur site". Par exemple, reportez-vous à l'exemple de résultat suivant :

```
[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
```

Vérification des paramètres du dépôt

Les paramètres de dépôt par défaut de la base de données Vertica sont activés (valeur = 1) pour les opérations de lecture et d'écriture. NetApp recommande fortement de maintenir ces paramètres de dépôt activés pour améliorer les performances.

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

Chargement des données d'échantillon (facultatif)

Si cette base de données est destinée aux tests et sera supprimée, vous pouvez charger des données

d'échantillon dans cette base de données pour les tests. Vertica est fourni avec un exemple de jeu de données, VMart, sous `/opt/vertica/examples/VMart_Schema/` Sur chaque nœud Vertica. Vous trouverez plus d'informations sur cet exemple de jeu de données "ici".

Procédez comme suit pour charger les données d'échantillon :

1. Connectez-vous en tant que dbadmin à l'un des nœuds de la Vertica : cd /opt/vertica/sou/VMart_Schema/
2. Chargez les exemples de données dans la base de données et entrez le mot de passe de la base de données lorsque vous y êtes invité dans les sous-étapes c et d :
   a. `cd /opt/vertica/examples/VMart_Schema`
   b. `./vmart_gen`
   c. `vsql < vmart_define_schema.sql`
   d. `vsql < vmart_load_data.sql`
3. Il existe plusieurs requêtes SQL prédéfinies, vous pouvez les exécuter pour confirmer que les données de test sont chargées correctement dans la base de données. Par exemple : `vsql < vmart_queries1.sql`

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- "Documentation du produit NetApp StorageGRID 11.7"
- "Fiche technique StorageGRID"
- "Documentation produit de Vertica 10.1"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Septembre 2021	Version initiale.

Par Angela Cheng

Analyse des journaux StorageGRID à l'aide de la pile ELK

Par Angela Cheng

Grâce à la fonction de transfert syslog StorageGRID, vous pouvez configurer un serveur syslog externe pour collecter et analyser les messages journaux StorageGRID. ELK (Elasticsearch, Logstash, Kibana) est devenu l'une des solutions d'analytique des journaux les plus populaires. Regardez la "Analyse du journal StorageGRID à l'aide de la vidéo ELK" pour afficher un exemple de configuration ELK et découvrir comment elle peut être utilisée pour identifier et dépanner les requêtes S3 ayant échoué. StorageGRID 11.9 prend en charge l'exportation du journal d'accès aux noeuds finaux de l'équilibreur de charge vers le serveur syslog externe. Regardez cette "Vidéo YouTube" vidéo pour en savoir plus sur cette nouvelle fonctionnalité. Cet article fournit des exemples de fichiers de configuration Logstash, de requêtes Kibana, de graphiques et de tableau de bord, pour vous offrir un démarrage rapide de la gestion des journaux et de l'analytique StorageGRID.

De formation

- StorageGRID 11.6.0.2 ou version ultérieure
- ELK (Elasticsearch, Logstash et Kibana) 7.1x ou plus installé et en fonctionnement

Exemples de fichiers

- "Téléchargez le paquet Logstash 7.x." + **md5 checksum** 148c23d0021d9a4bb4a6c0287464deab + **sha256 checksum** f51ec9e2e3f842d5a781566b167a561b4373038b4e7bb3c8b5d52f2f2d2f2f2f2f2d2f2f2f2f2f2f2f2f6f6f
- "Téléchargez le paquet Logstash 8.x." + **md5 checksum** e11bae3a662f87c310ef363d0fe06835 + **total de contrôle sha256** 5c670755742cfdfd5aa723a596ba087e0153a65bcaef3934afdb682f61cd278d
- "Téléchargez le paquet Logstash 8.x des fichiers d'exemple pour StorageGRID 11.9" + **somme de contrôle md5** 41272857c4a54600f95995f6ed74800d + **somme de contrôle sha256** 67048ee8661052719990851e1ad960d4902fe537a6e135e8600177188da677c9

Hypothèse

Les lecteurs connaissent la terminologie et les opérations de StorageGRID et d'ELK.

Instructions

Deux exemples de versions sont fournis en raison des différences de noms définies par des motifs grk. + par exemple, le modèle SYSLOGBASE grok dans le fichier de configuration Logstash définit les noms de champs différemment en fonction de la version Logstash installée.

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

Logstash 7.17 échantillon

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

Logstash 8.23 échantillon

Table JSON

Search field names

Actions	Field	Value
	_id	yuhOiIEBVP6KX4EwqcyU
	_index	sglog-2022.06.21
	# _score	-
	@timestamp	Jun 21, 2022 @ 18:07:45.444
	t event.original	<28>Jun 21 22:07:45 SITE2-S3 ADE: syslog messages being dropped
	t host.hostname	SITE2-S3
	t msg-details	syslog messages being dropped
	t process.name	ADE
	t syslog_pri	28
	t timestamp	Jun 21 22:07:45

Étapes

1. Décompressez l'échantillon fourni en fonction de la version ELK installée. + l'exemple de dossier inclut deux exemples de configuration de Logstash : + **sglog-2-file.conf:** ce fichier de configuration envoie des messages de journal StorageGRID vers un fichier sur Logstash sans transformation de données. Vous pouvez l'utiliser pour confirmer que Logstash reçoit des messages StorageGRID ou pour vous aider à comprendre les modèles de journaux StorageGRID. + **sglog-2-es.conf:** ce fichier de configuration transforme les messages du journal StorageGRID en utilisant divers modèles et filtres. Il comprend des exemples d'instructions de DROP, qui sont basées sur des motifs ou des filtres. Le résultat est envoyé à Elasticsearch pour l'indexation. + Personnalisez le fichier de configuration sélectionné en fonction de l'instruction dans le fichier.
2. Testez le fichier de configuration personnalisé :

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

   Si la dernière ligne renvoyée est similaire à la ligne ci-dessous, le fichier de configuration n'a pas d'erreurs de syntaxe :

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

3. Copiez le fichier conf personnalisé dans la configuration du serveur Logstash : /etc/logstash/conf.d + si vous n'avez pas activé config.reload.automatic dans /etc/logstash/logstash.yml, redémarrez le service Logstash. Dans le cas contraire, attendez que l'intervalle de rechargement de la configuration s'écoule.

```
 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. Vérifiez /var/log/logstash/logstash-plain.log et assurez-vous qu'il n'y a pas d'erreur lors du démarrage de Logstash avec le nouveau fichier de configuration.
5. Vérifiez que le port TCP est démarré et que vous écoutez. + dans cet exemple, le port TCP 5000 est utilisé.

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

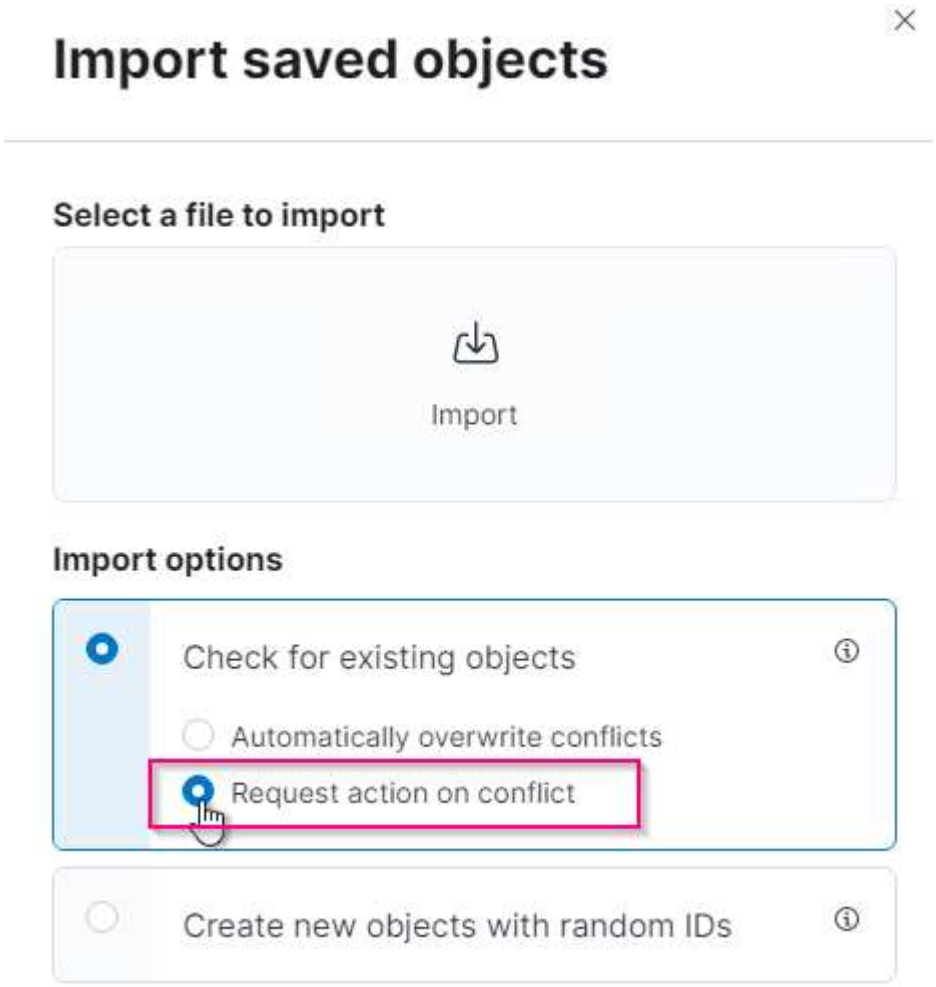
6. À partir de l'interface graphique du gestionnaire StorageGRID, configurez le serveur syslog externe pour envoyer des messages de journal à Logstash. Reportez-vous au "vidéo de démonstration" pour plus de détails.
7. Vous devez configurer ou désactiver le pare-feu sur le serveur Logstash pour autoriser la connexion des

nœuds StorageGRID au port TCP défini.

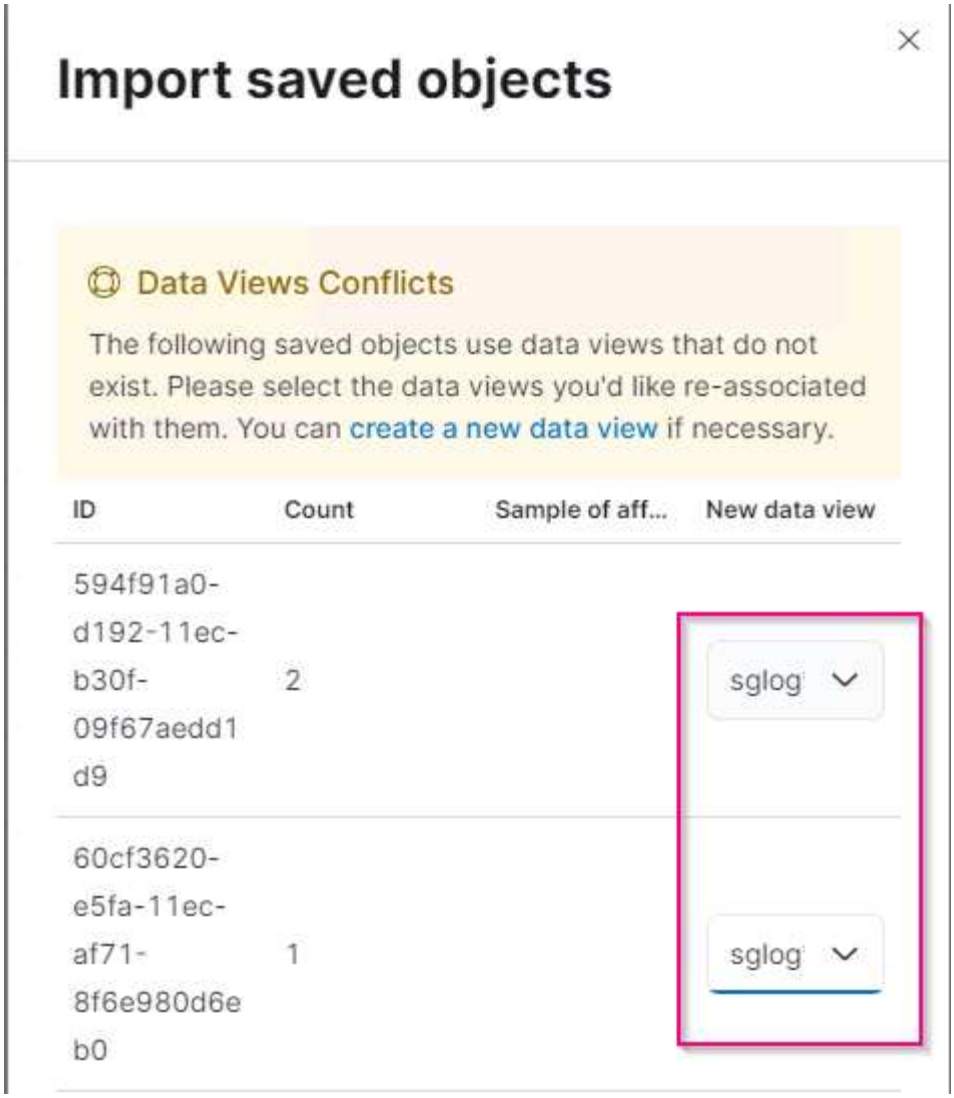
8. Dans l'interface graphique Kibana, sélectionnez Management → Dev Tools. Sur la page Console, exécutez cette commande OBTENIR pour confirmer la création de nouveaux index sur Elasticsearch.

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

9. A partir de l'interface graphique Kibana, créez un motif d'index (ELK 7.x) ou une vue de données (ELK 8.x).
10. Dans l'interface utilisateur graphique de Kibana, entrez « objets lavés » dans la zone de recherche située en haut au centre. + sur la page objets enregistrés, sélectionnez Importer. Sous Options d'importation, sélectionnez « demander une action en cas de conflit »



Importez elk<version>-query-chart-sample.ndjson. + lorsque vous êtes invité à résoudre le conflit, sélectionnez le modèle d'index ou la vue de données que vous avez créé à l'étape 8.



Les objets Kibana suivants sont importés : + **Query** + * audit-msg-s3rq-orlm + * bycast log s3 messages liés + * loglevel warning or above + * échec de l'événement de sécurité + bycast.log * nginx-gw journal d'accès au point final (disponible uniquement dans elk8-sample-for-sgg.zip) + **Chart** analyse de type de sécurité + nombre moyen de messages HTTP * s3 sur la base du tableau de temps de réponse * s3 * s3 + nombre de demandes supérieur à la demande * s3 *.

Vous êtes maintenant prêt à effectuer une analyse des journaux StorageGRID à l'aide de Kibana.

Ressources supplémentaires

- "syslog101"
- "Qu'est-ce que la pile ELK"
- "Liste des répétitions Grok"
- "Guide débutant de Logstash: Grok"
- "Guide pratique de Logstash : plongée en profondeur syslog"
- "Guide Kibana - Explorez le document"
- "Référence des messages du journal d'audit StorageGRID"

Grâce à Prometheus et Grafana, vous pouvez renforcer la conservation des metrics

Par Aron Klein

Ce rapport technique fournit des instructions détaillées pour la configuration de NetApp StorageGRID avec les services externes Prometheus et Grafana.

Introduction

StorageGRID stocke les metrics à l'aide de Prometheus et fournit des visualisations de ces metrics via des tableaux de bord intégrés. Vous pouvez accéder en toute sécurité aux metrics Prometheus depuis StorageGRID en configurant des certificats d'accès client et en activant l'accès prometheus pour le client spécifié. Aujourd'hui, la conservation de ces données de mesure est limitée par la capacité de stockage du nœud d'administration. Pour gagner plus de temps et pouvoir créer des visualisations personnalisées de ces metrics, nous déploierons un nouveau serveur Prometheus et Grafana, configurerons notre nouveau serveur afin de grattez les metrics à partir de l'instance IDS, et nous concevons un tableau de bord avec les mesures importantes. Vous pouvez obtenir plus d'informations sur les metrics Prometheus collectés dans la "Documentation StorageGRID".

Fédérer Prometheus

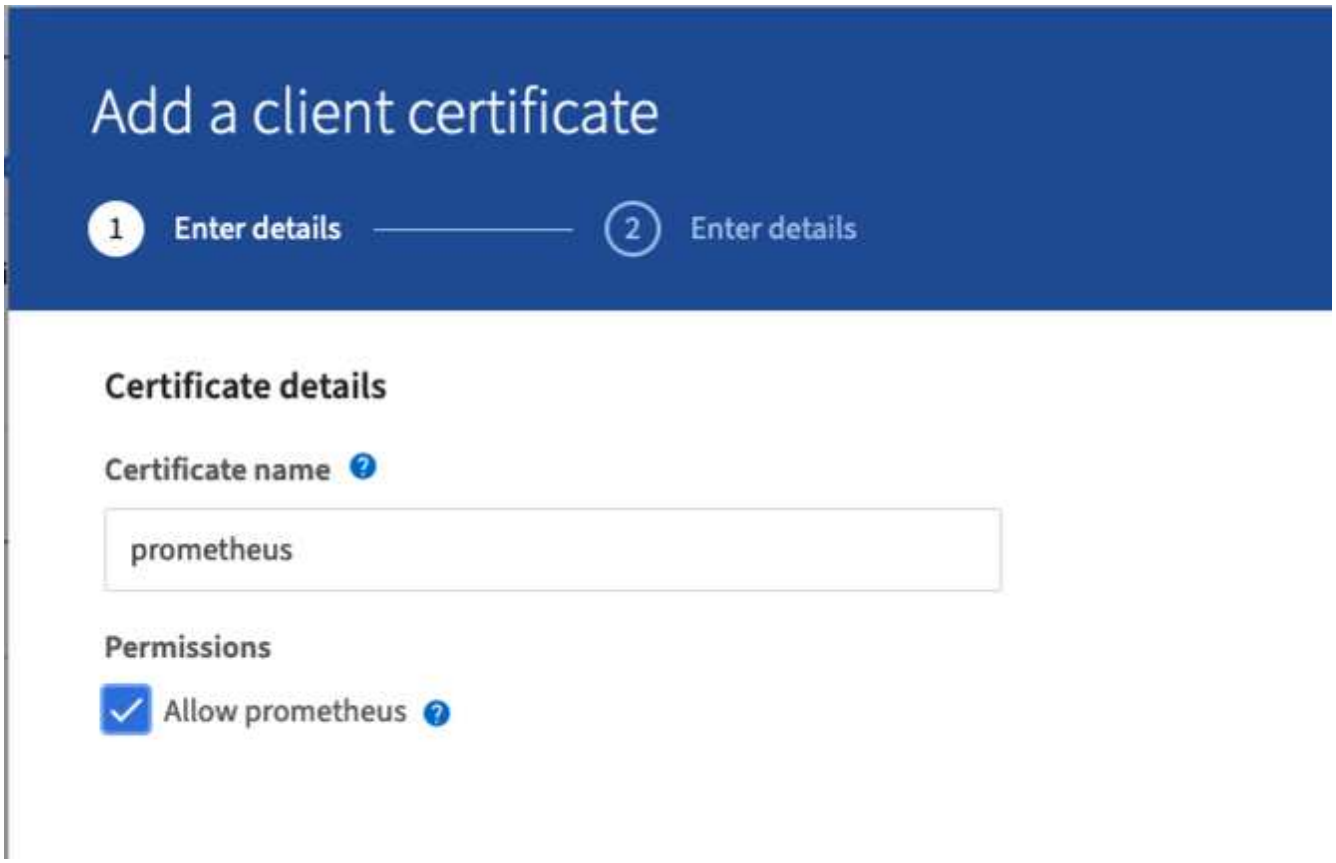
Détails de laboratoire

Pour les besoins de cet exemple, j'utiliserai toutes les machines virtuelles pour les nœuds StorageGRID 11.6 et un serveur Debian 11. L'interface de gestion StorageGRID est configurée avec un certificat d'autorité de certification public approuvé. Cet exemple ne passera pas par l'installation et la configuration du système StorageGRID ou de l'installation de Debian linux. Vous pouvez utiliser toutes les versions Linux que vous souhaitez prendre en charge par Prometheus et Grafana. Prometheus et Grafana peuvent être installés en tant que conteneurs docker, qu'ils soient issus de la source ou binaires précompilés. Dans cet exemple, je vais installer les binaires Prometheus et Grafana directement sur le même serveur Debian. Téléchargez et suivez les instructions d'installation de base sur https://prometheus.io et https://grafana.com/grafana/ respectivement.

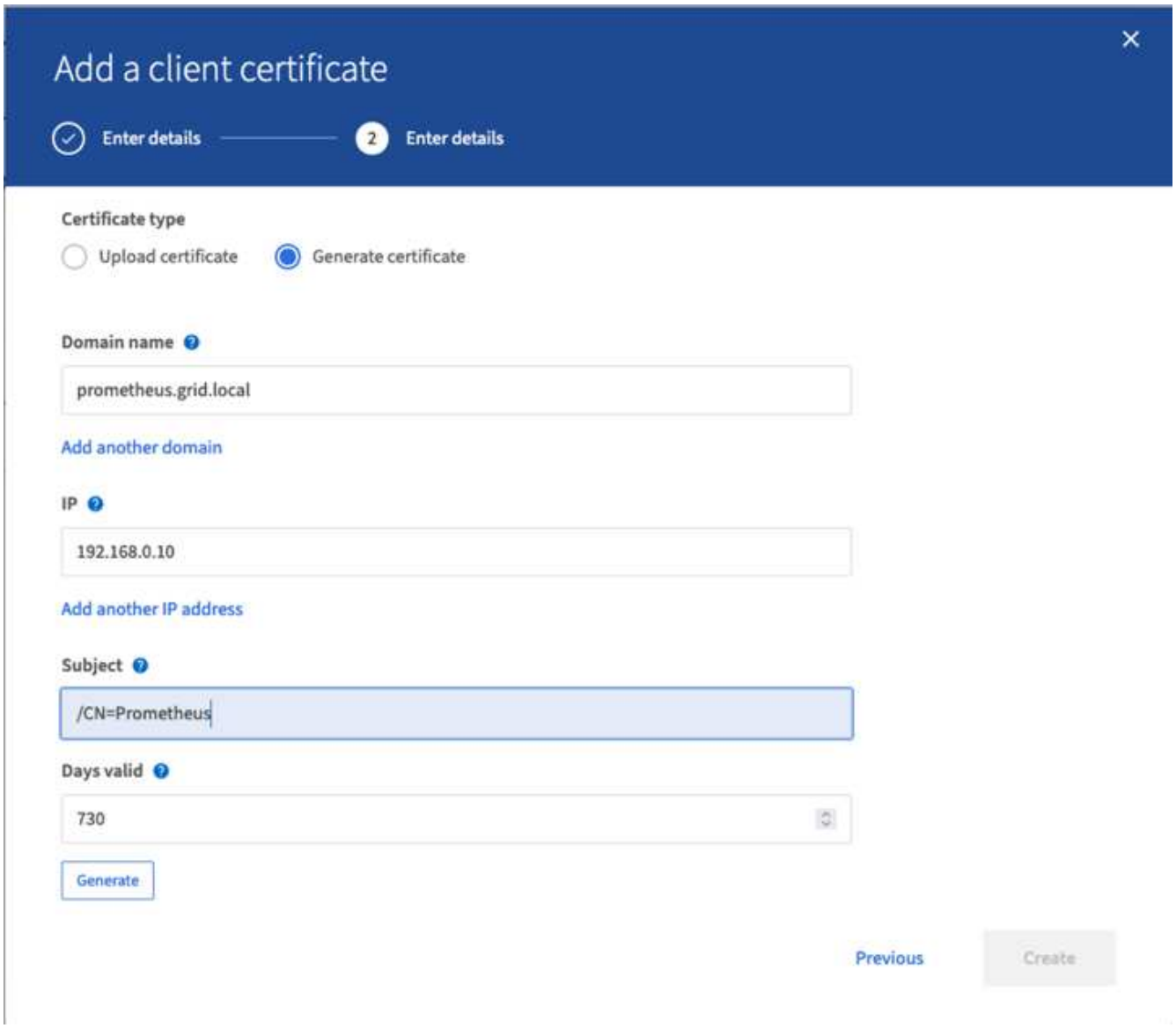
Configurez StorageGRID pour l'accès client Prometheus

Afin d'accéder aux identifiants de paramètres de la mémoire de la solution, vous devez générer ou télécharger un certificat client avec une clé privée et activer l'autorisation pour le client. L'interface de gestion StorageGRID doit posséder un certificat SSL. Ce certificat doit être approuvé par le serveur prometheus soit par une autorité de certification approuvée, soit manuellement approuvé s'il est auto-signé. Pour en savoir plus, consultez le "Documentation StorageGRID".

1. Dans l'interface de gestion StorageGRID, sélectionnez « CONFIGURATION » en bas à gauche, puis dans la deuxième colonne sous « sécurité », cliquez sur certificats.
2. Sur la page certificats, sélectionnez l'onglet « client » et cliquez sur le bouton « Ajouter ».
3. Indiquez un nom pour le client auquel l'accès sera accordé et utilisez ce certificat. Cliquez sur la case sous "permissions", devant "Autoriser Prometheus" et cliquez sur le bouton Continuer.

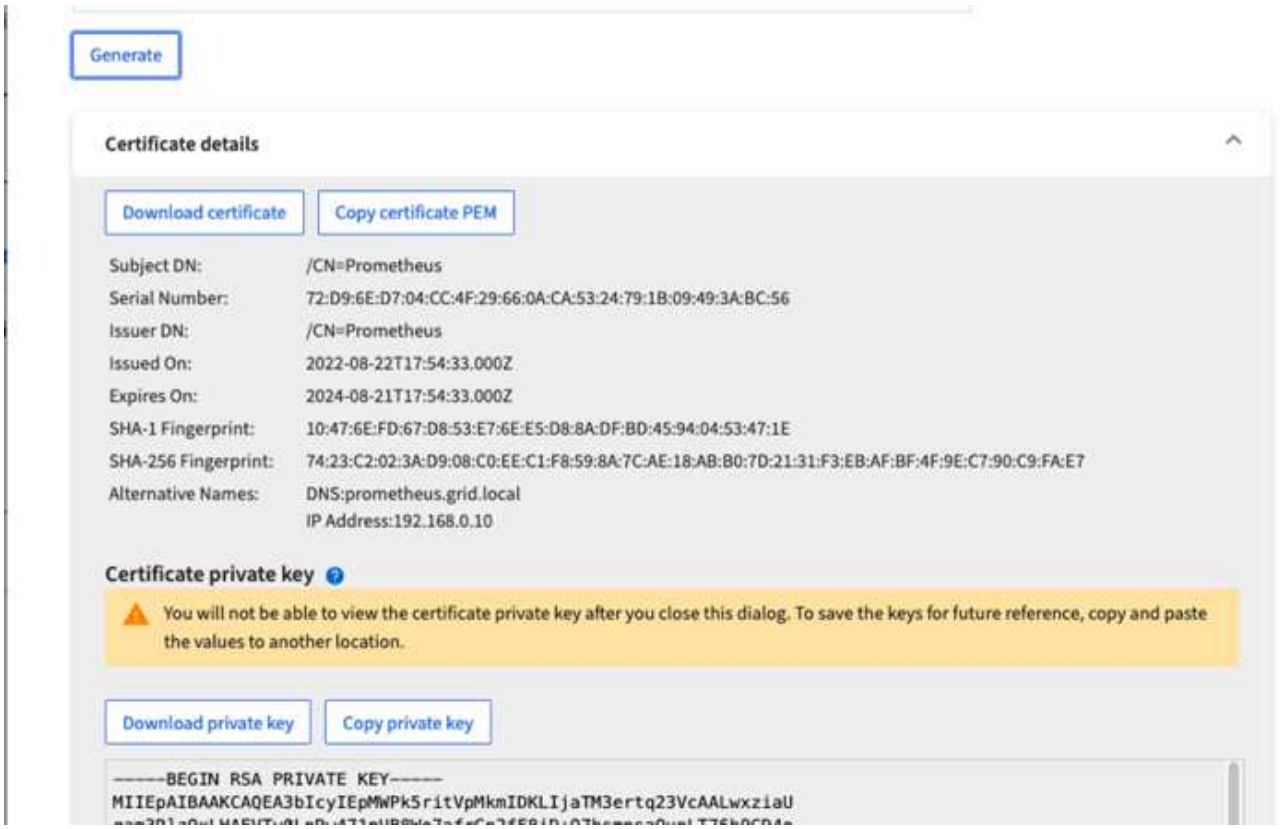


4. Si vous disposez d'un certificat signé par l'autorité de certification, vous pouvez sélectionner le bouton radio « Télécharger le certificat », mais dans notre cas, nous allons permettre à StorageGRID de générer le certificat client en sélectionnant le bouton radio « générer le certificat ». Les champs obligatoires s'affichent pour être renseignés. Saisissez le FQDN du serveur client, l'adresse IP du serveur, l'objet et les jours valides. Cliquez ensuite sur le bouton « générer ».



> 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. Téléchargez le fichier pem de certificat et le fichier pem de clé privée.



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

Préparez le serveur Linux pour l'installation de Prometheus

Avant d'installer Prometheus, je souhaite préparer mon environnement avec un utilisateur Prometheus, la structure de répertoires et configurer la capacité pour l'emplacement de stockage des metrics.

1. Créez l'utilisateur Prometheus.

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

2. Créez les répertoires pour les données Prometheus, les certificats client et les metrics.

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

3. J'ai formaté le disque que j'utilise pour la rétention des metrics avec un système de fichiers ext4.

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

4. Je ai ensuite monté le système de fichiers dans le répertoire des metrics de Prometheus.

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

5. Obtenez l'UUID du disque que vous utilisez pour les données de metrics.

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

6. Ajout d'une entrée dans /etc/fstab/ pour que le montage persiste entre les redémarrages à l'aide de l'UUID de /dev/sdb.

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

Installez et configurez Prometheus

Lorsque le serveur est prêt, je peux commencer l'installation de Prometheus et configurer le service.

1. Extraire le pack d'installation Prometheus

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

2. Copiez les binaires dans /usr/local/bin et modifiez la propriété de l'utilisateur prometheus créé précédemment

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

3. Copiez les consoles et les bibliothèques dans /etc/prometheus

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

4. Copiez le certificat client et les fichiers pem de clé privée téléchargés précédemment de StorageGRID vers /etc/prometheus/certs
5. Créez le fichier yaml de configuration prometheus

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

6. Insérez la configuration suivante. Le nom du travail peut être tout ce que vous souhaitez. Remplacez les « cibles : ['] » par le FQDN du nœud admin, et si vous avez modifié les noms des certificats et des fichiers de clé privée, mettez à jour la section tls_config pour qu'elle corresponde. enregistrez ensuite le fichier. Si votre interface de gestion de grille utilise un certificat auto-signé, téléchargez le certificat et placez-le avec un nom unique, et dans la section tls_config, ajoutez ca_file: /Etc/prometheus/cert/UIcert.pem

   a. Dans cet exemple, je collecterai tous les metrics commençant par alertManager, cassandra, nœud et StorageGRID. Vous trouverez plus d'informations sur les metrics Prometheus dans la "Documentation 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']
```

Si votre interface de gestion du grid utilise un certificat auto-signé, téléchargez le certificat et placez-le avec le certificat client portant un nom unique. Dans la section tls_config, ajoutez le certificat au-dessus du certificat client et des lignes de clé privée

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

1. Modifiez la propriété de tous les fichiers et répertoires dans /etc/prometheus et /var/lib/prometheus pour l'utilisateur prometheus

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

2. Créez un fichier de service prometheus dans /etc/systemd/system

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

3. Insérez les lignes suivantes, notez le --Storage.tsdb.rerétention=1A qui définit la conservation des données de mesure sur 1 an. Vous pouvez également utiliser --Storage.tsdb.Retention.size=300 Gio pour la conservation sur les limites de stockage. C'est le seul emplacement pour définir la conservation des métriques.

```
[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. Rechargez le service systemd pour enregistrer le nouveau service prometheus. démarrez et activez ensuite le service prometheus.

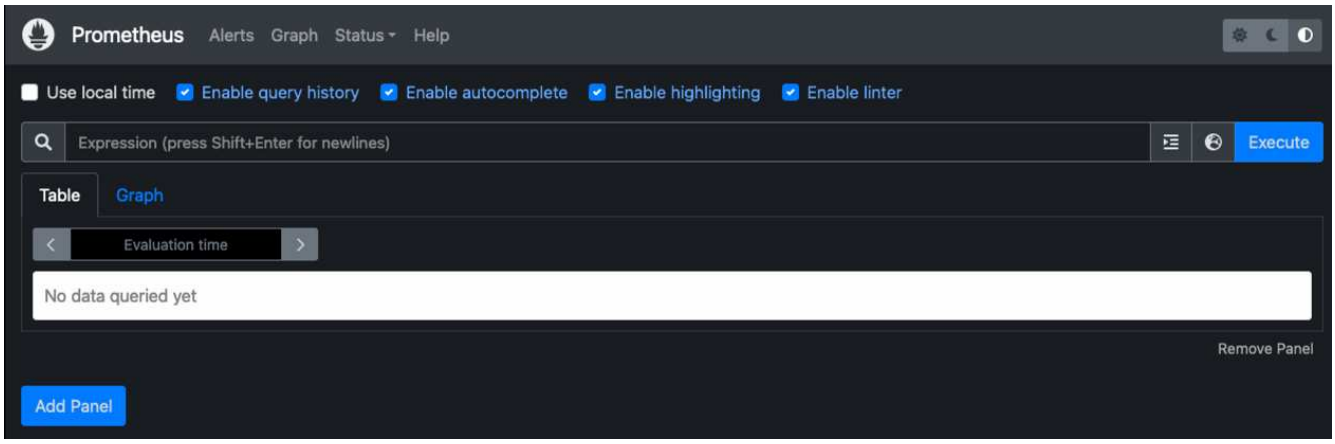
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. Vérifiez que l'entretien fonctionne correctement

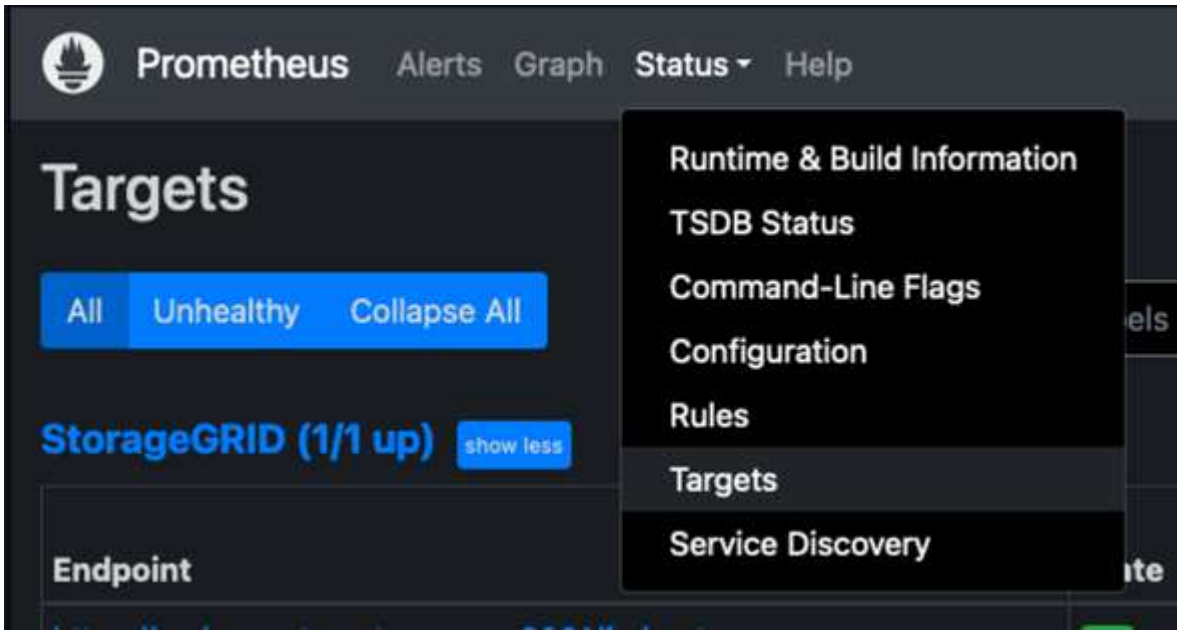
```
sudo systemctl status prometheus
```

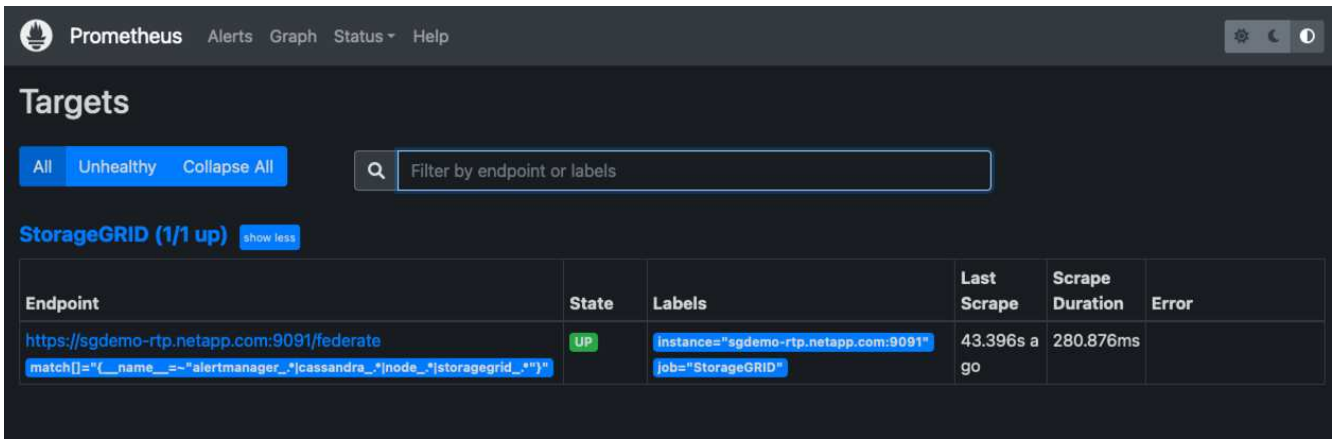
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 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. Vous devez maintenant pouvoir naviguer vers l'interface du serveur prometheus http://Prometheus-server:9090 Et voir l'interface utilisateur

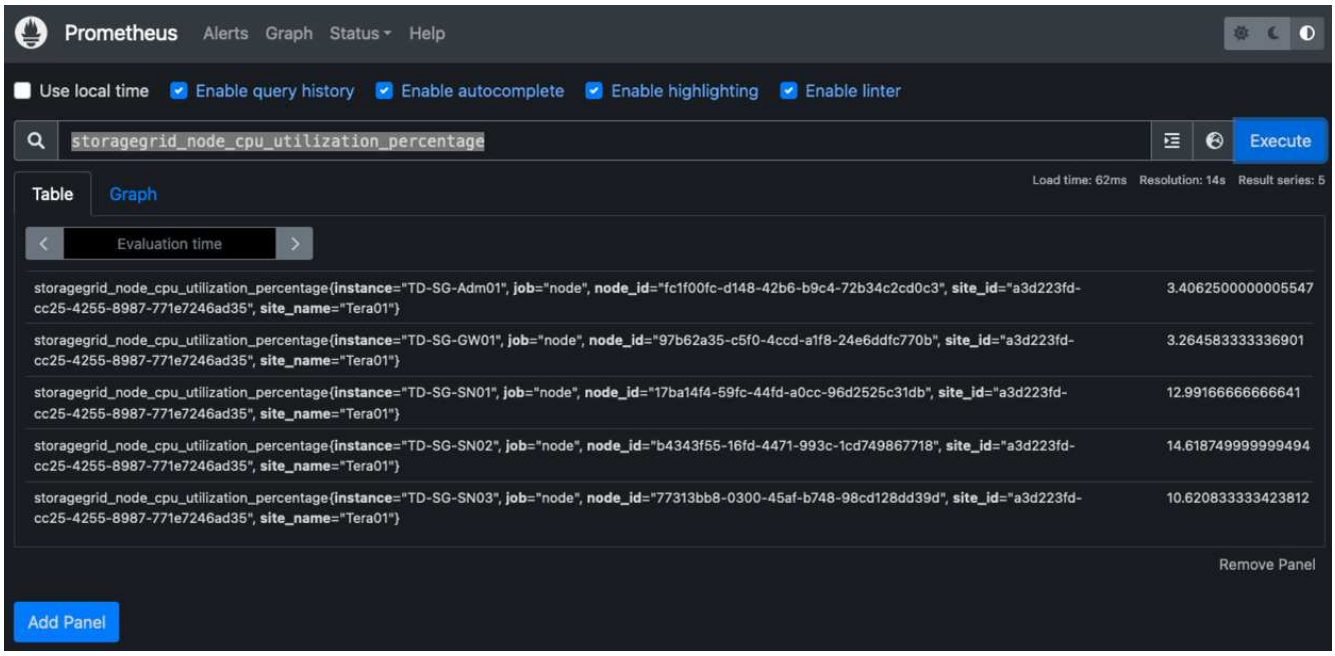


7. Sous cibles « Status », vous pouvez consulter le statut du noeud final StorageGRID configuré dans prometheus.yml





8. Sur la page graphique, vous pouvez exécuter une requête de test et vérifier que les données sont scrapées avec succès. Par exemple, entrez « storagegrid_node_cpu_usage_percent » dans la barre de requêtes et cliquez sur le bouton Exécuter.



Installer et configurer Grafana

Vous pouvez désormais installer Grafana et configurer un tableau de bord

Grafana Installation

1. Installez la dernière édition Enterprise de 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. Ajouter ce référentiel pour les versions stables :

```
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. Après avoir ajouté le référentiel.

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

4. Rechargez le service systemd pour enregistrer le nouveau service grafana. Démarrez et activez ensuite le service Grafana.

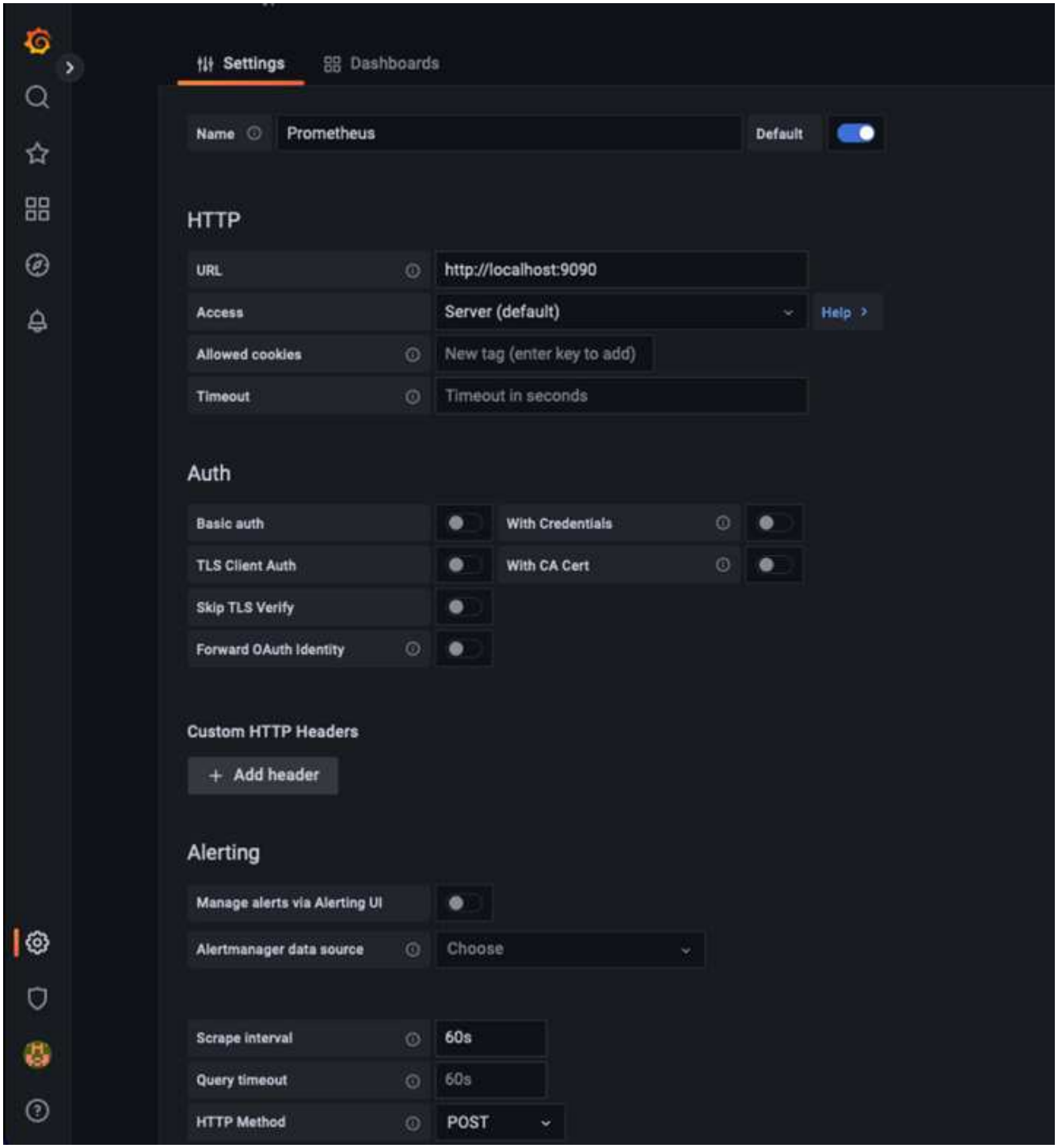
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. Grafana est désormais installé et exécuté. Lorsque vous ouvrez un navigateur vers HTTP://Prometheus-Server:3000, vous êtes accueilli par la page de connexion de Grafana.
6. Les informations d'identification par défaut sont admin/admin et vous devez définir un nouveau mot de passe à mesure qu'il vous invite à.

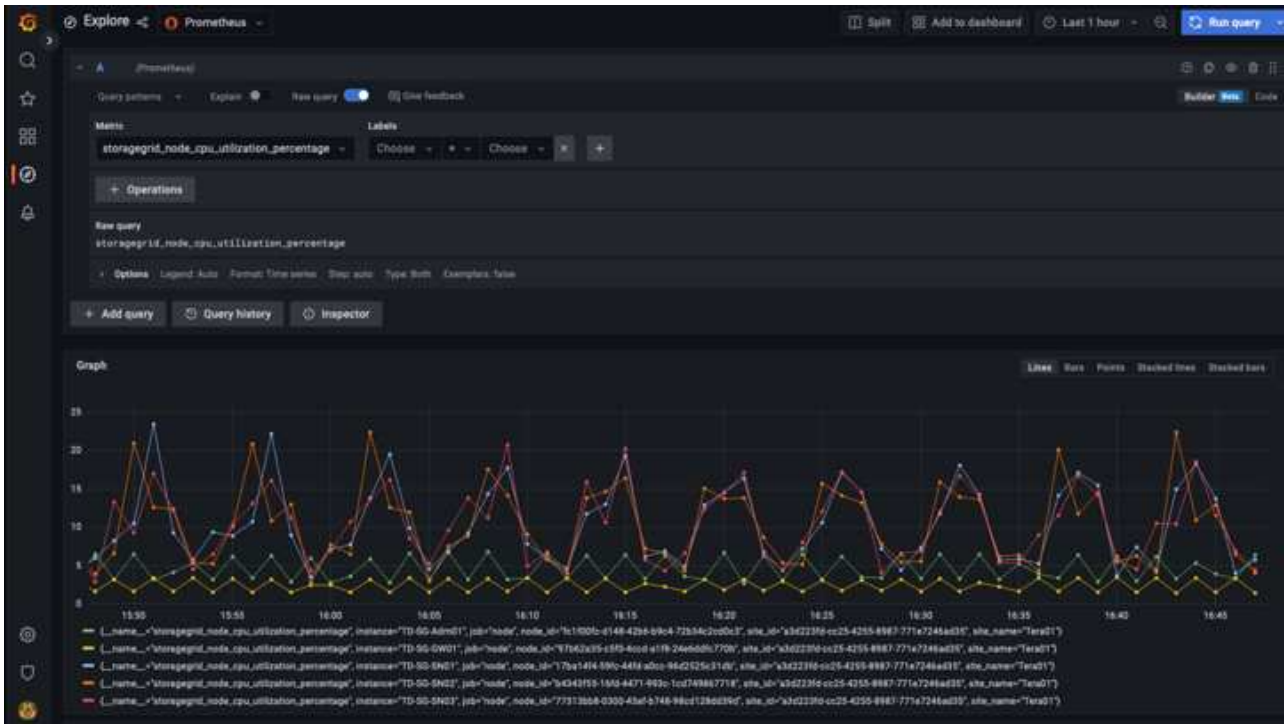
Créez un tableau de bord Grafana pour StorageGRID

Lorsque vous installez et exécutez Grafana et Prometheus, vous pouvez désormais vous connecter en créant une source de données et en créant un tableau de bord

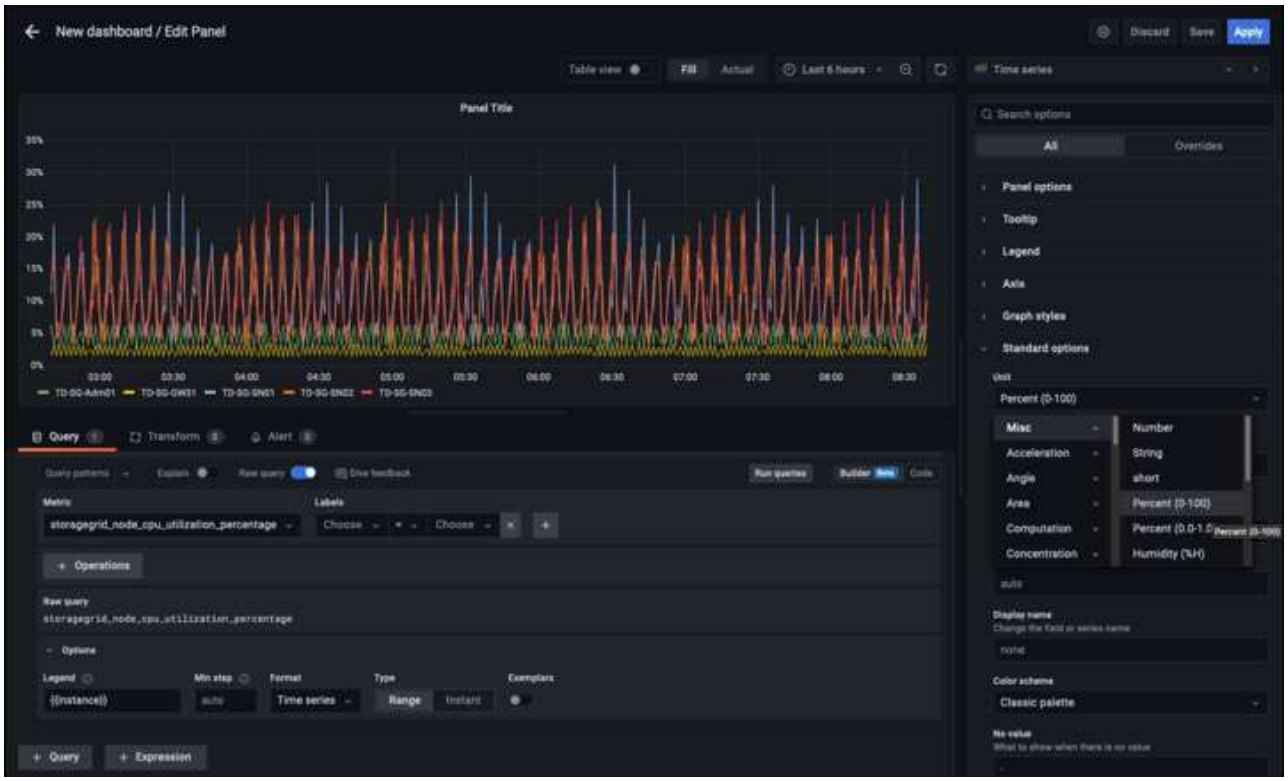
1. Dans le volet de gauche, développez « Configuration » et sélectionnez « sources de données », puis cliquez sur le bouton « Ajouter une source de données »
2. Prometheus est une des principales sources de données. Si ce n'est pas le cas, utilisez la barre de recherche pour trouver Prometheus
3. Configurez la source Prometheus en entrant l'URL de l'instance prometheus et l'intervalle de récupération en fonction de l'intervalle Prometheus. J'ai également désactivé la section d'alertes car je n'ai pas configuré le gestionnaire d'alertes sur prometheus.



4. Une fois les paramètres souhaités saisis, faites défiler l'écran vers le bas et cliquez sur « Enregistrer et tester ».
5. Une fois le test de configuration réussi, cliquez sur le bouton Explorer.
    a. Dans la fenêtre d'exploration, vous pouvez utiliser la même mesure que Prometheus testée avec « storagegrid_node_cpu_use_percent », puis cliquez sur le bouton Run Query



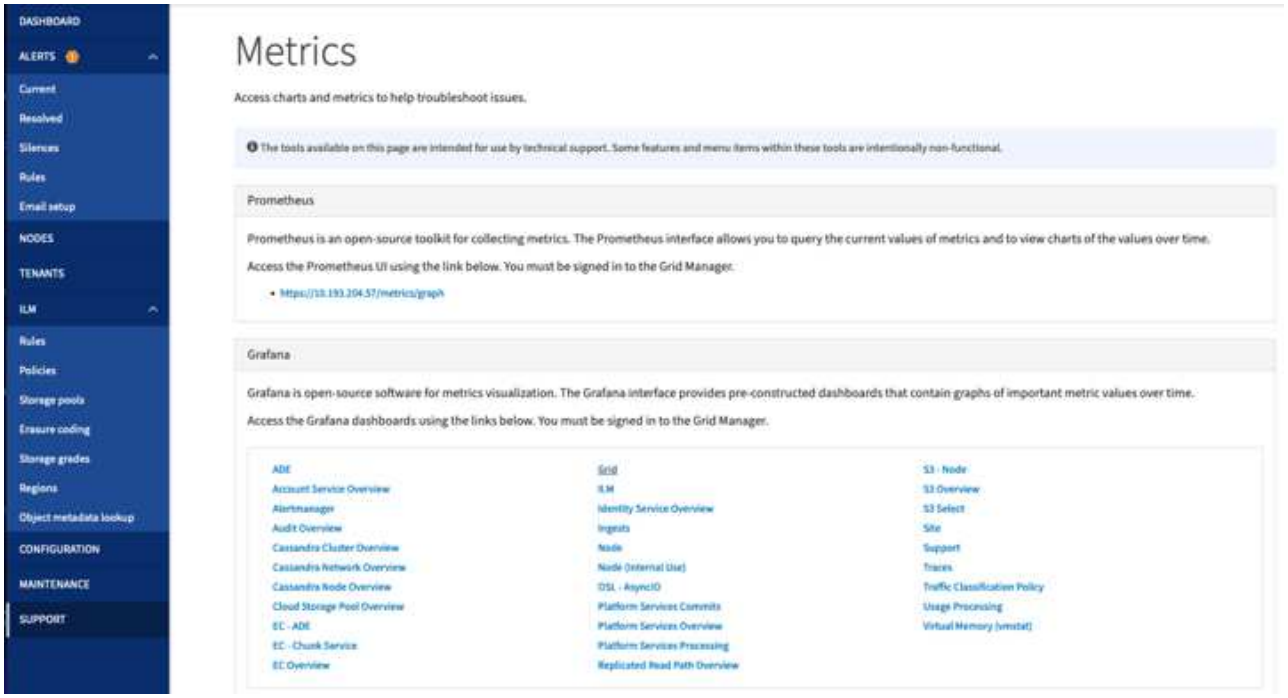
6. Comme la source de données est configurée, nous pouvons créer un tableau de bord.
   a. Dans le volet de gauche, développez « tableaux de bord » et sélectionnez « + nouveau tableau de bord ».
   b. Sélectionnez « Ajouter un nouveau panneau »
   c. Configurez le nouveau panneau en sélectionnant une mesure, puis j'utiliserai à nouveau « storagegrid_node_cpu_use_percentage », saisissez un titre pour le panneau, développez « Options » en bas et pour changer de légende en personnalisé et entrez «{{instance} » pour définir les noms de nœud, et à droite sous « Options standard » définissez « unité » sur « 100 % ». Cliquez ensuite sur « appliquer » pour enregistrer le panneau dans le tableau de bord.



7. Nous pouvons continuer à concevoir notre tableau de bord de ce type pour chaque metric souhaité, mais heureusement que StorageGRID dispose déjà de tableaux de bord avec des panneaux que nous pouvons copier dans nos tableaux de bord personnalisés.

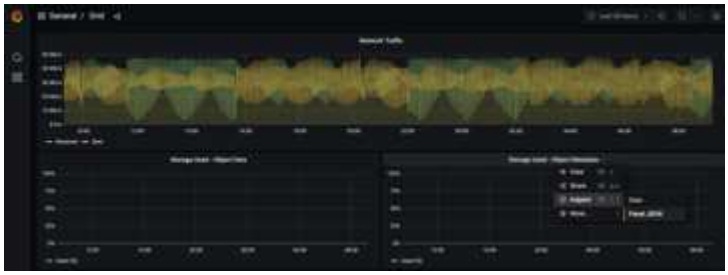
   a. Dans le volet gauche de l'interface de gestion StorageGRID, sélectionnez « support », et en bas de la colonne « Outils », cliquez sur métriques.

   b. Dans les mesures, je vais sélectionner le lien « grille » en haut de la colonne centrale.



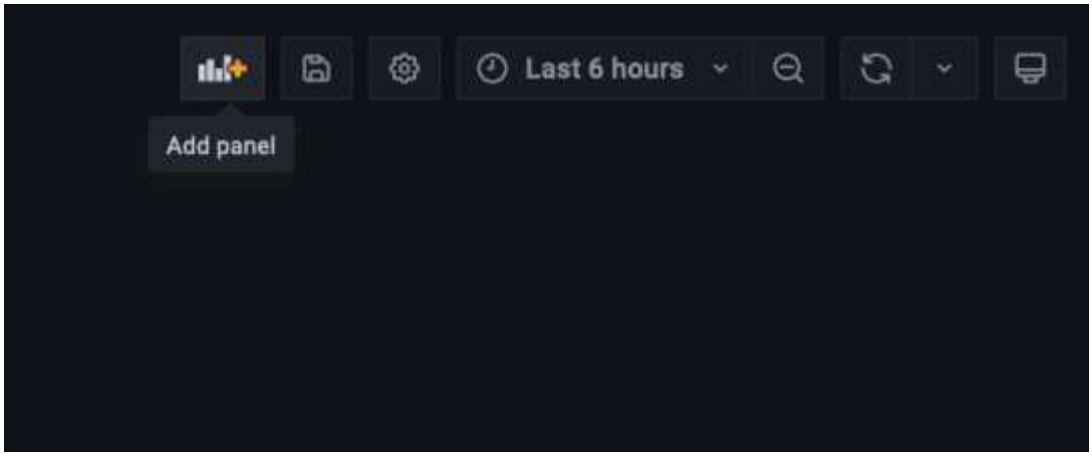
   c. Dans le tableau de bord Grid, sélectionnez le panneau « stockage utilisé - métadonnées de l'objet ».

Cliquez sur la petite flèche vers le bas et sur la fin du titre du panneau pour faire descendre un menu. Dans ce menu, sélectionnez « inspection » et « panneau JSON ».



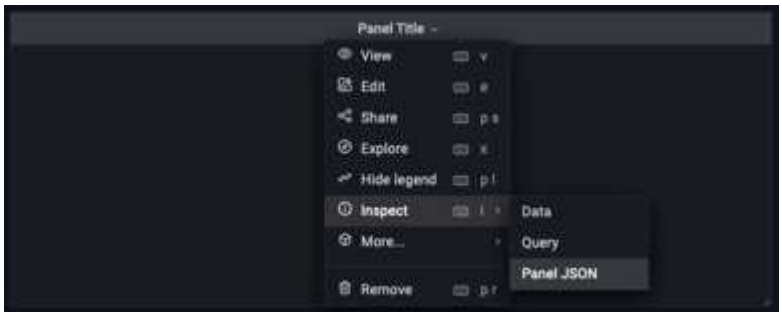
d. Copiez le code JSON et fermez la fenêtre.

e. Dans notre nouveau tableau de bord, cliquez sur l’icône pour ajouter un nouveau panneau.

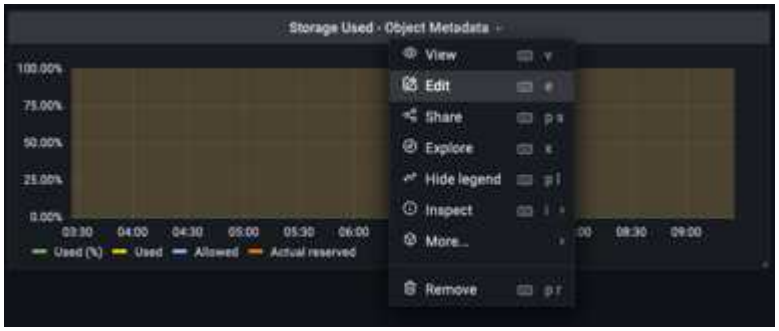


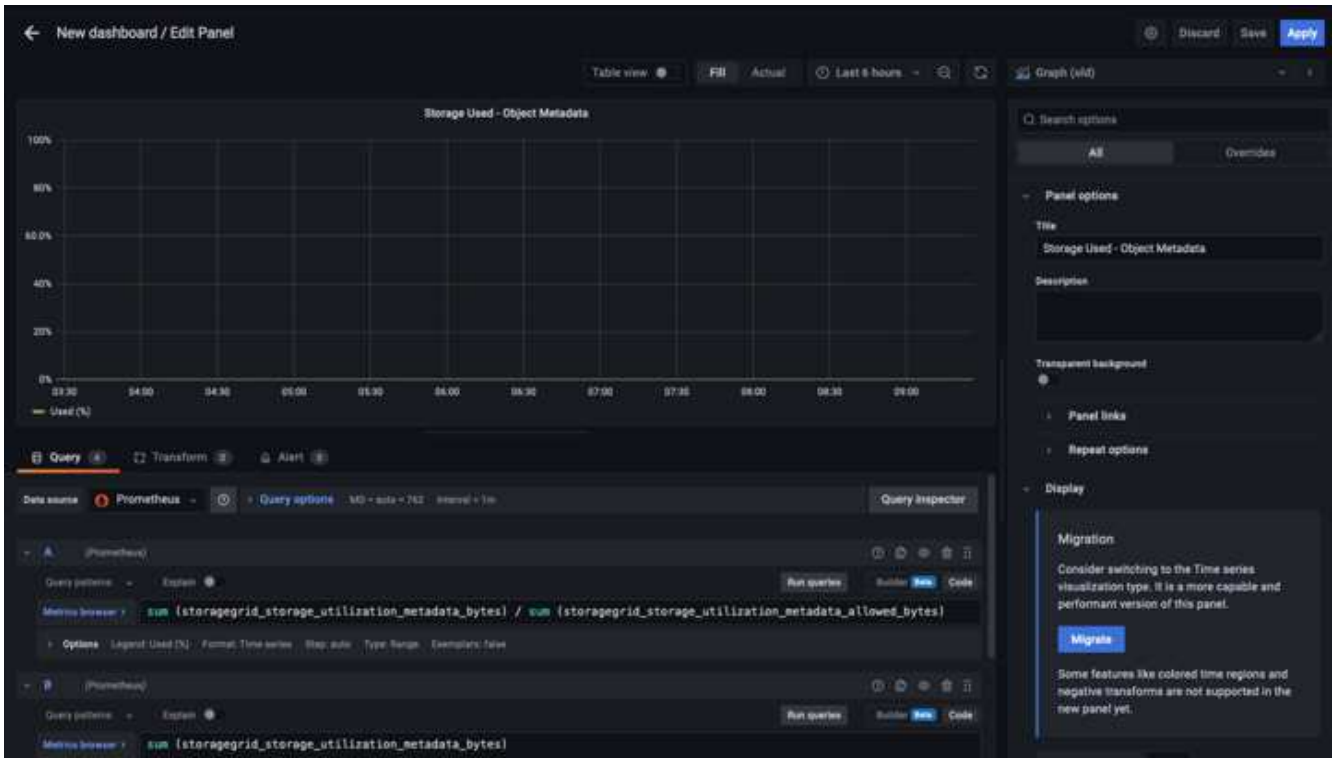
f. Appliquez le nouveau panneau sans apporter de modifications

g. Inspecter le fichier JSON, et tout comme dans le panneau StorageGRID. Supprimez tout code JSON et remplacez-le par le code copié du panneau StorageGRID.



h. Modifiez le nouveau panneau et, à droite, un message migration s'affiche avec un bouton « migrer ». Cliquez sur le bouton, puis sur le bouton « appliquer ».





8. Une fois tous les panneaux en place et configurés comme vous le souhaitez. Enregistrez le tableau de bord en cliquant sur l'icône du disque dans le coin supérieur droit et donnez un nom à votre tableau de bord.

Conclusion

Nous disposons désormais d'un serveur Prometheus avec une capacité de stockage et de conservation des données personnalisables. Grâce à cela, nous pouvons continuer à élaborer nos propres tableaux de bord avec les mesures les plus pertinentes pour nos opérations. Vous pouvez obtenir plus d'informations sur les metrics Prometheus collectés dans la "Documentation StorageGRID".

Utilisez F5 DNS pour équilibrer la charge globale de StorageGRID.

Par Steve Gorman (F5)

Ce rapport technique fournit des instructions détaillées pour configurer NetApp StorageGRID avec les services DNS F5 pour l'équilibrage de charge global afin d'offrir une meilleure disponibilité des données, une plus grande cohérence des données et d'optimiser le routage des transactions S3 lorsque votre grille est distribuée sur plusieurs sites et/ou groupes HA.

Introduction

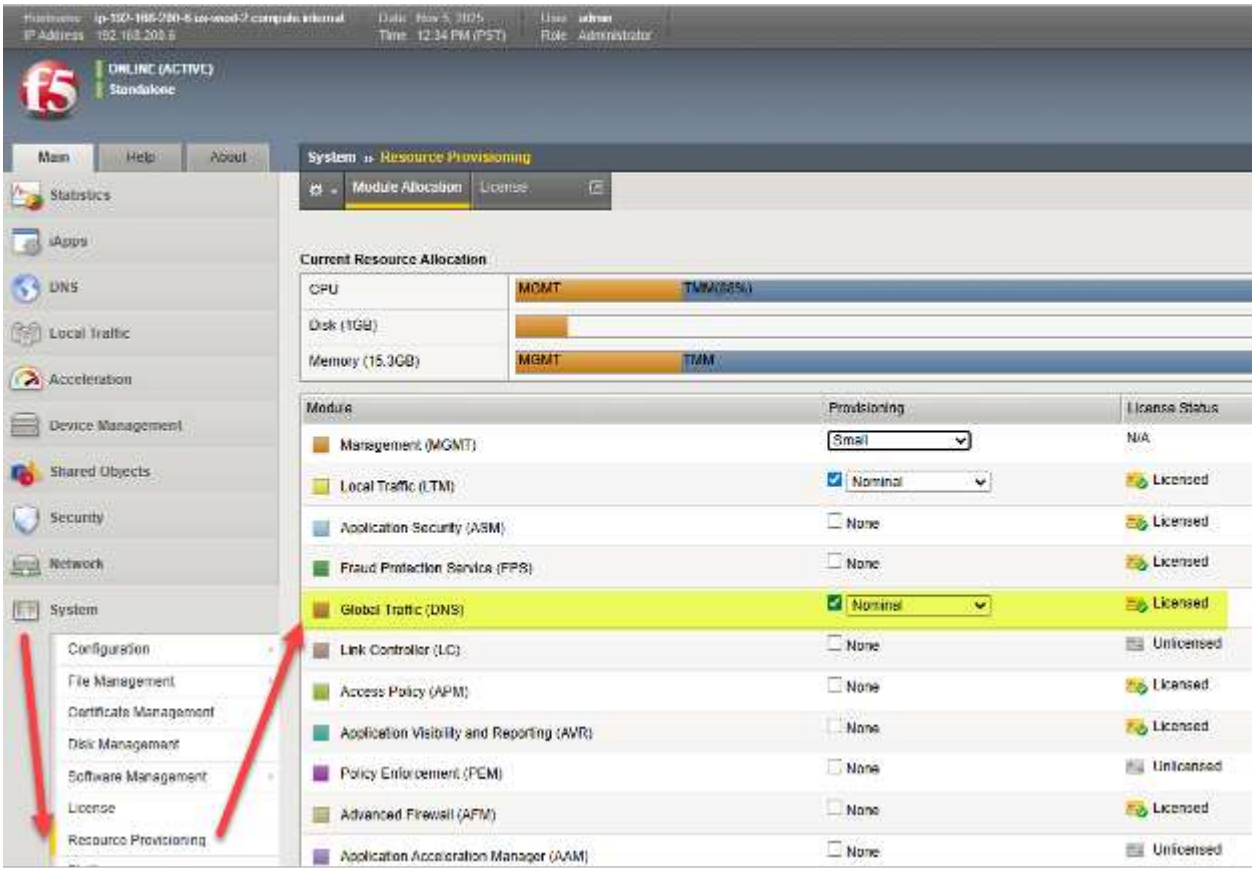
La solution F5 BIG-IP DNS, anciennement appelée BIG-IP GTM (Global Traffic Manager) et GSLB (Global Server Load Balancing), permet un accès transparent à travers plusieurs groupes HA actifs-actifs et des solutions StorageGRID multisites actives-actives.

Configuration F5 BIG-IP StorageGRID multisite

Quel que soit le nombre de sites StorageGRID à prendre en charge, au moins deux appliances BIG-IP, physiques ou virtuelles, doivent avoir le module DNS BIG-IP activé et configuré. Plus une entreprise dispose de serveurs DNS, plus son degré de redondance sera élevé.

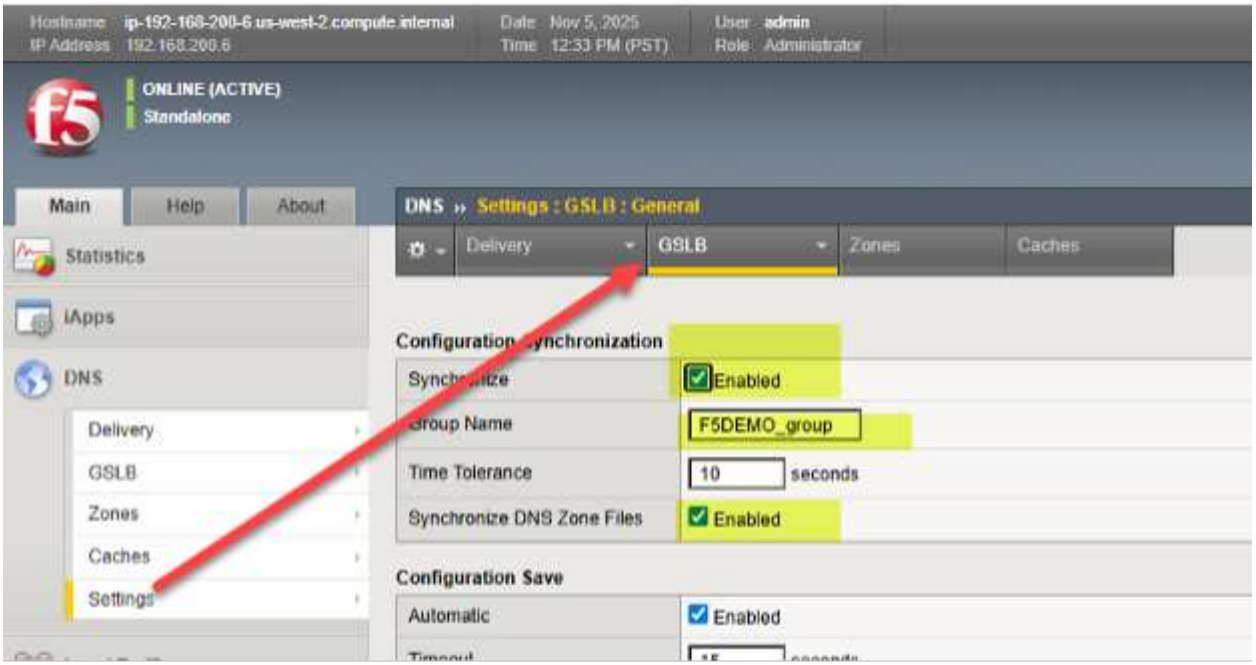
BIG-IP DNS - Premiers pas de la configuration initiale

Une fois que l'appliance BIG-IP a subi au moins la configuration initiale, utilisez un navigateur Web pour vous connecter à l'interface TMUI (interface graphique BIG-IP) et choisissez Système → Provisionnement des ressources. Comme indiqué, assurez-vous que le module « Trafic global (DNS) » est coché et qu'il est bien sous licence. Notez, comme sur l'image, qu'il est courant que le « trafic local (LTM) » puisse être provisionné sur le même appareil.

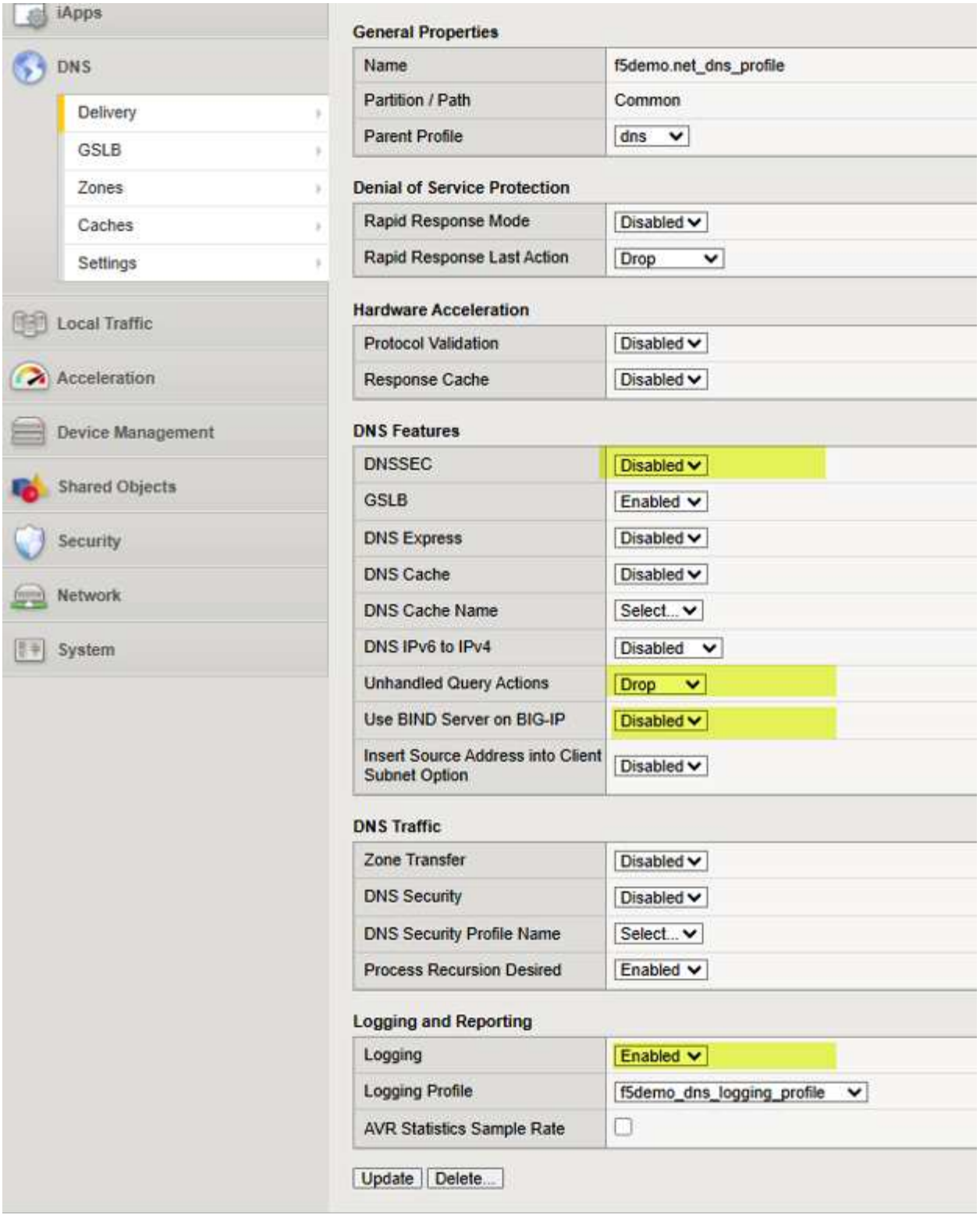


Configurer les éléments fondamentaux du protocole DNS

La première étape vers la gestion du trafic global pour les sites StorageGRID consiste à choisir l'onglet DNS, où sera configurée la quasi-totalité du routage du trafic global, puis à sélectionner Paramètres → GLSB. Activez les deux options de synchronisation et choisissez un nom de groupe DNS qui sera partagé entre les appliances BIG-IP participantes.



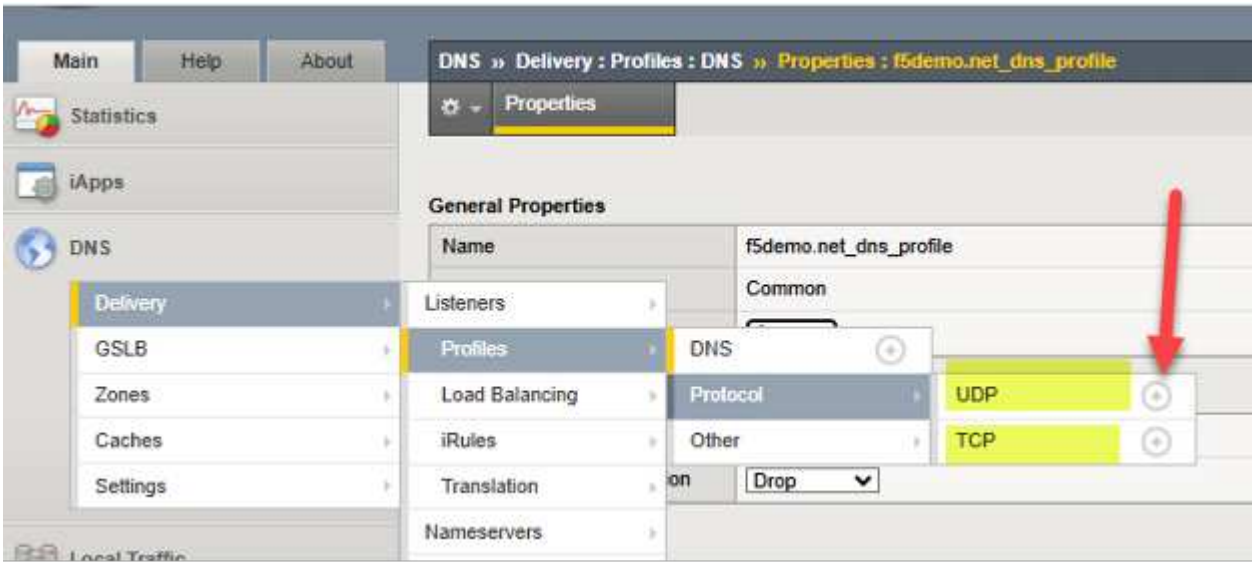
Ensuite, accédez à DNS > Distribution > Profils > DNS : Créer et créez un profil qui gérera les fonctionnalités DNS que vous souhaitez activer ou désactiver. Consultez le lien précédent pour accéder au guide pédagogique DNS si la génération de journaux DNS spécifiques vous intéresse. Voici un exemple de profil DNS fonctionnel ; notez les quatre éléments mis en évidence qui représentent des paramètres importants. Pour plus d'informations, chaque configuration possible est expliquée dans l'article suivant de la base de connaissances F5. "ici".



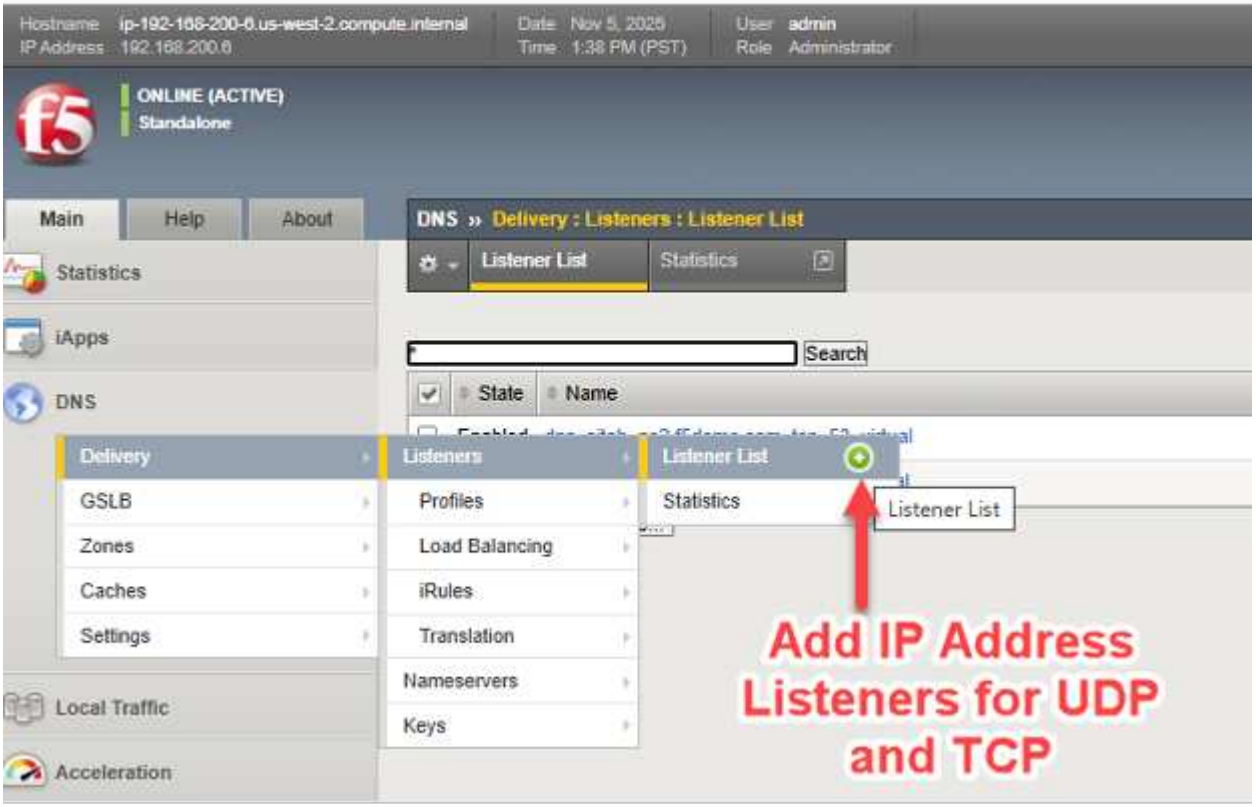
À ce stade, nous pouvons ajuster les caractéristiques des protocoles UDP et TCP, grâce à des « profils » créés, qui peuvent tous deux transporter du trafic DNS impliquant BIG-IP. Il suffit de créer un nouveau profil pour UDP et TCP. Partant du principe que le trafic DNS transitera par des liaisons WAN, une bonne pratique consiste simplement à hériter des caractéristiques UDP et TCP reconnues pour leurs bonnes performances dans les environnements WAN. Pour ajouter chaque protocole, cliquez simplement sur l'icône « + » située à côté de celui-ci, puis définissez le profil parent comme suit :

UDP → utiliser le profil « parent » « udp_gtm_dns »

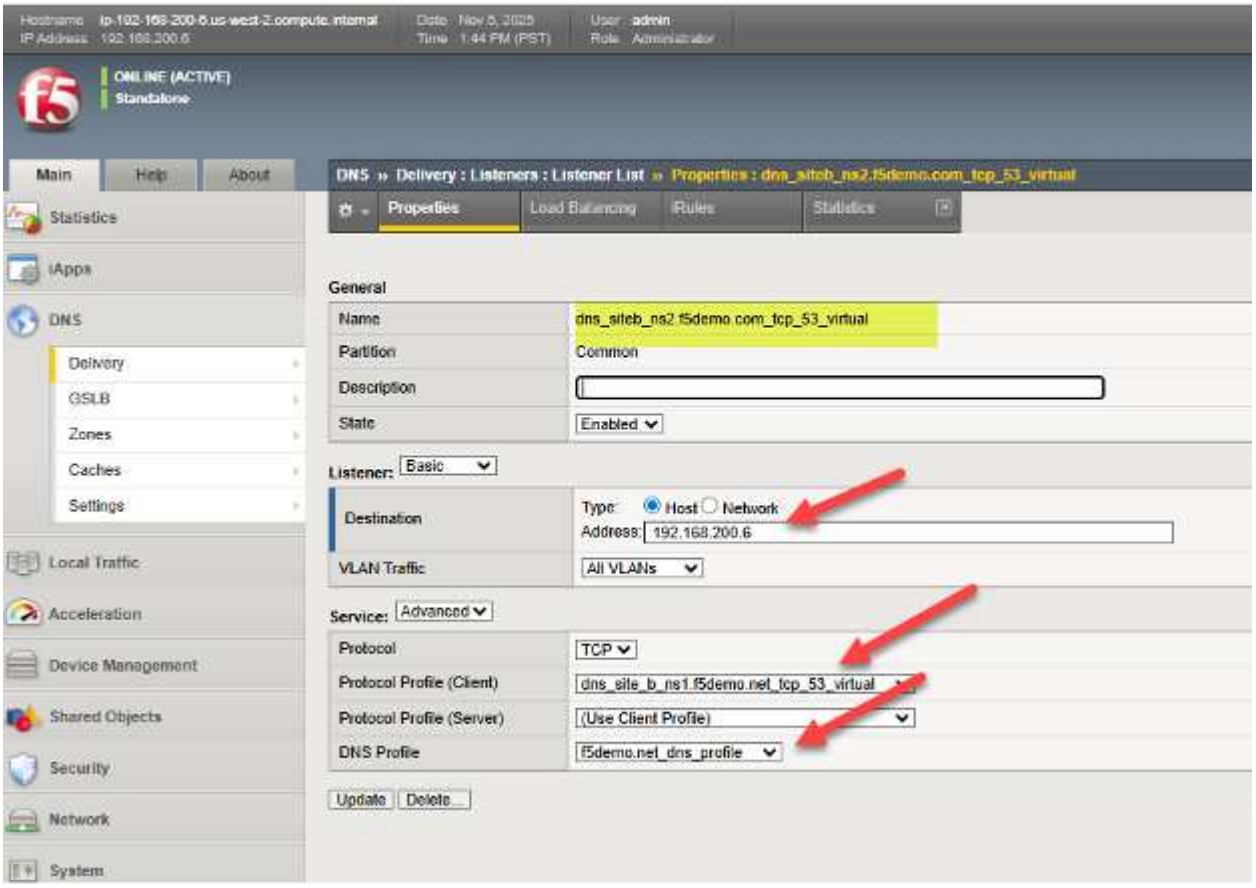
TCP → utiliser le profil « parent » « f5-tcp-wan »



Il nous suffit maintenant d'attribuer une adresse IP au trafic UDP et TCP impliquant le DNS BIG-IP. Pour ceux qui connaissent BIG-IP LTM, il s'agit essentiellement de la création de serveurs virtuels DNS, et les serveurs virtuels ont besoin d'adresses IP « d'écoute ». Comme indiqué dans la capture d'écran, suivez les flèches pour créer des serveurs d'écoute/virtuels pour DNS/UDP et DNS/TCP.



Voici un exemple tiré d'un serveur DNS BIG-IP en production ; on y voit les paramètres d'écoute du serveur virtuel TCP et on peut constater comment ils relient plusieurs des étapes précédentes. Cela inclut la référence au profil DNS et au profil de protocole (TCP), ainsi que la configuration d'une adresse IP valide que le DNS pourra utiliser. Comme pour tous les objets créés avec BIG-IP, il est utile d'utiliser un nom significatif qui permette d'identifier l'objet, comme dns/siteb/TCP53 dans l'exemple donné.



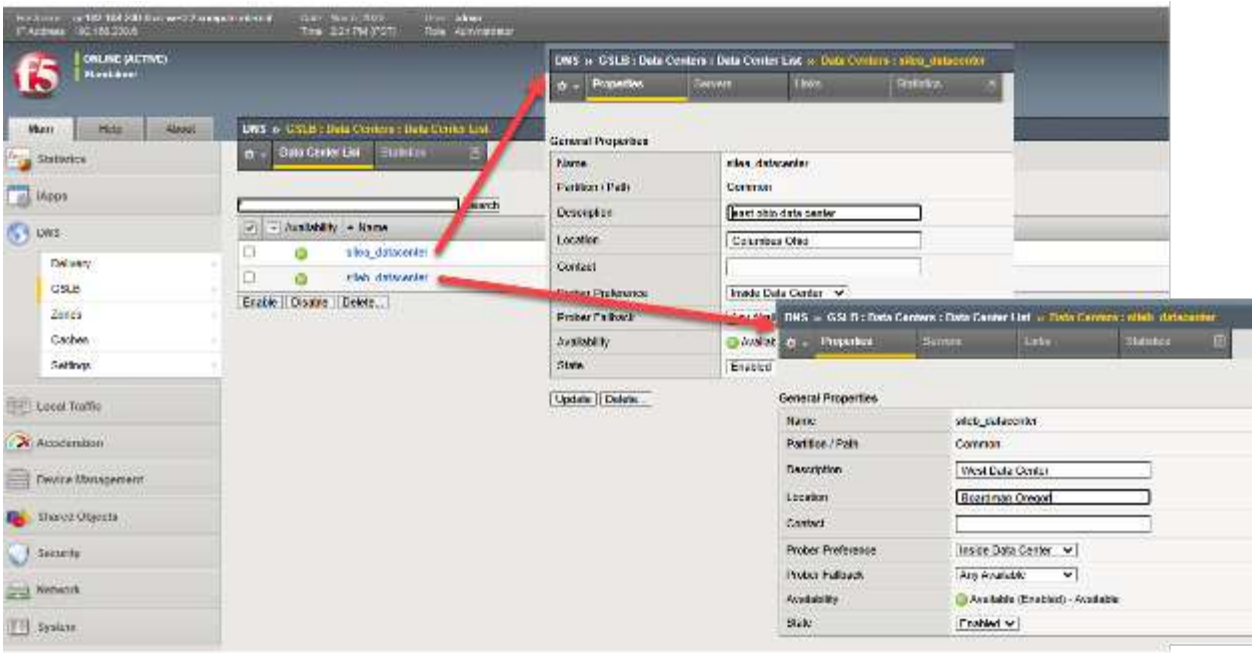
Ceci conclut les étapes préliminaires, généralement « uniques », de configuration d'un dispositif BIG-IP avec le module DNS activé. Nous sommes maintenant prêts à aborder les détails de la mise en place d'une solution globale de gestion du trafic avec nos appliances, qui sera bien sûr liée aux caractéristiques des sites StorageGRID .

Mise en place de sites de centres de données et établissement de communications inter-BIG-IP en quatre étapes

Première étape : Créer des centres de données

Chaque site qui hébergera des groupes de nœuds à équilibrer localement la charge par BIG-IP LTM doit être enregistré dans le DNS BIG-IP. Cette opération ne doit être effectuée que sur un seul serveur DNS BIG-IP, car nous créons un groupe DNS synchronisé pour la gestion du trafic ; cette configuration sera donc partagée entre les membres DNS du groupe.

Dans l'interface graphique TMUI, sélectionnez DNS > GSLB > Centres de données > Liste des centres de données et créez une entrée pour chacun des sites StorageGRID . Si vous utilisez une configuration réseau alignée sur la figure 1, un dispositif DNS situé sur d'autres sites non StorageGRID , ajoutez des centres de données pour ces sites en plus des sites de stockage. Dans cet exemple, les sites a et b sont créés dans l'Ohio et l'Oregon, les BIG-IP sont des appliances double DNS et LTM.



Deuxième étape : Créer des serveurs (Liste de tous les équipements BIG-IP de la solution)

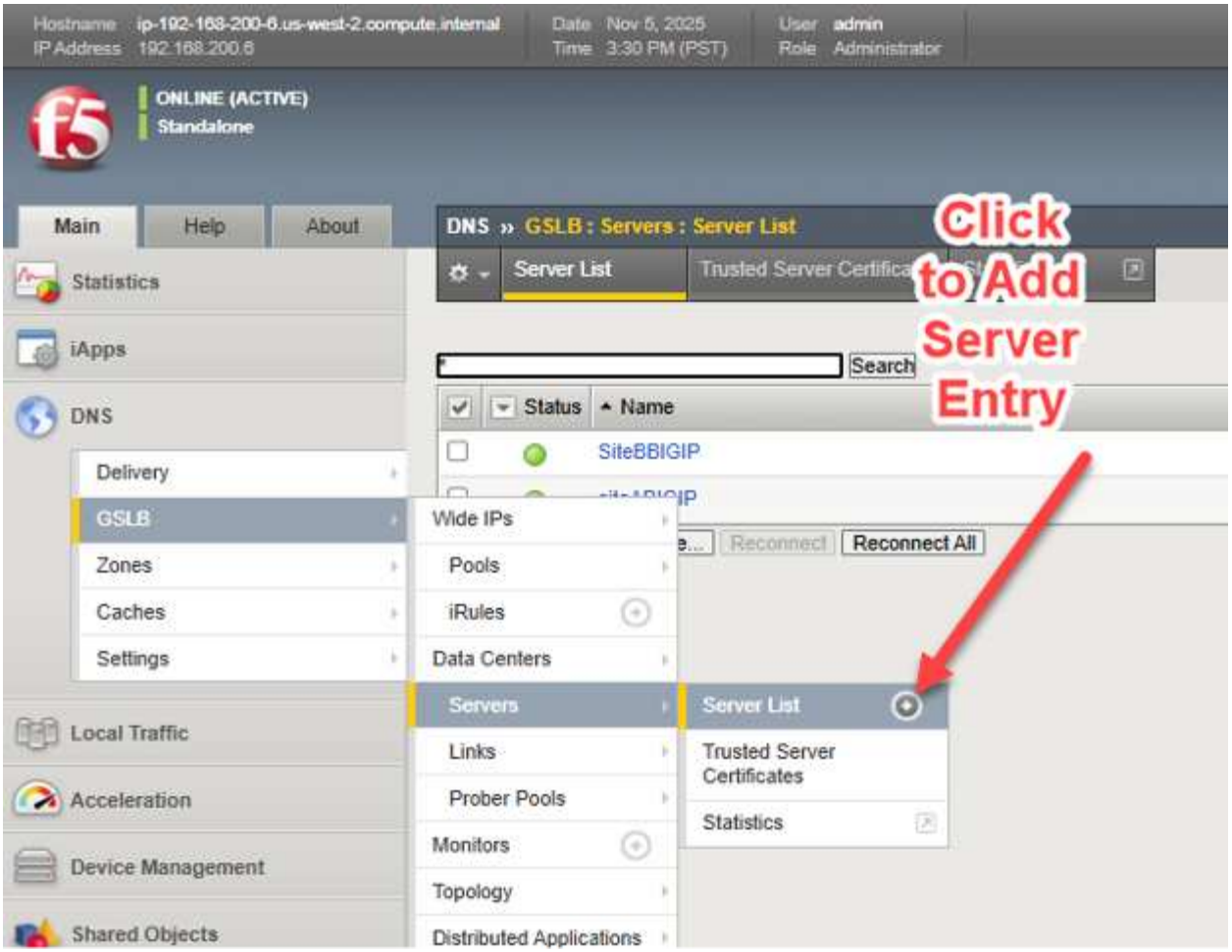
Nous sommes maintenant prêts à connecter les clusters de sites StorageGRID individuels à la configuration DNS BIG-IP. Rappelons que le dispositif BIG-IP de chaque site effectuera l'équilibrage de charge réel du trafic S3, grâce à la configuration de serveurs virtuels qui lient une adresse IP/port accessible « front-end » à un ensemble de « pool » de dispositifs Storage Node « back-end », en utilisant des adresses IP/ports « back-end ».

Si, par exemple, tous les nœuds de stockage d'un pool sont mis hors ligne administrativement, peut-être pour la mise hors service d'un site, ou de manière inattendue suite à des contrôles d'intégrité en temps réel ayant échoué, le trafic sera dirigé vers d'autres sites en modifiant les réponses aux requêtes DNS.

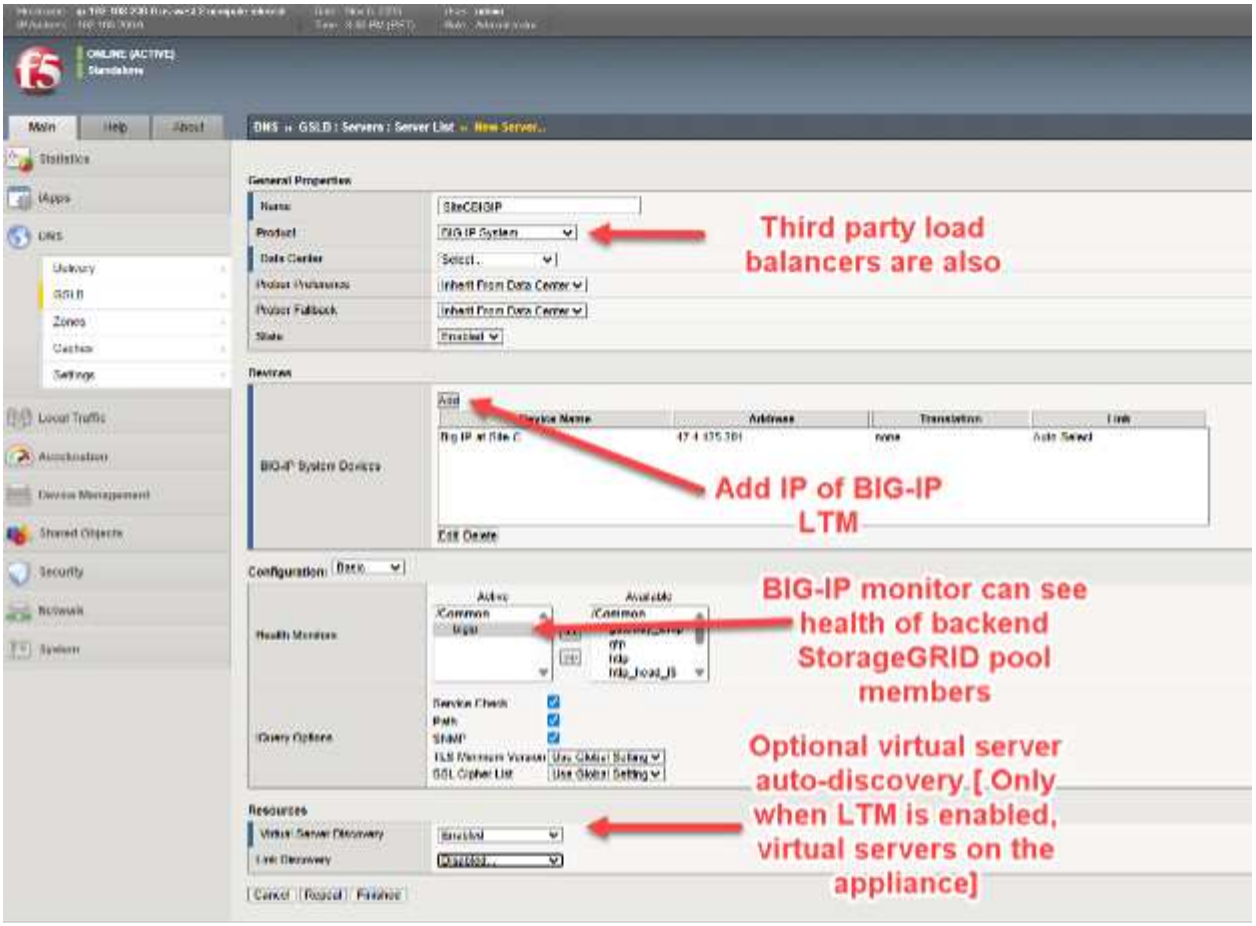
Pour intégrer les sites StorageGrid, et plus précisément les serveurs virtuels locaux, à la configuration DNS BIG-IP sur chaque appliance, la configuration n'est nécessaire qu'une seule fois. L'ensemble des appliances DNS BIG-IP seront configurées dans une prochaine étape.

En termes simples, nous allons créer une liste, appelée liste de serveurs, de tous nos équipements BIG-IP, qu'ils soient sous licence pour DNS, LTM ou les deux (DNS et LTM). Cette liste principale sera synchronisée avec tous les équipements DNS BIG-IP une fois la liste complétée.

Sur un appareil BIG-IP DNS sous licence, choisissez DNS > GSLB > Serveurs > Liste des serveurs et choisissez le bouton ajouter (+).



Les quatre éléments clés lors de l'ajout de chaque BIG-IP sont les suivants : * Sélectionner BIG-IP dans le menu déroulant des produits ; d'autres équilibreurs de charge sont possibles, mais ils manquent généralement de réactivité en temps réel lorsque l'état des nœuds backend se détériore sur chaque site. Ajoutez l'adresse IP du serveur DNS BIG-IP. Lors du premier ajout d'un serveur DNS BIG-IP, l'adresse sera probablement celle du serveur accessible via l'interface graphique ; pour les serveurs suivants, il s'agira des autres serveurs de la solution. * Choisissez un moniteur d'intégrité, utilisez toujours « BIG-IP » lorsque l'équilibreur de charge ajouté est un dispositif BIG-IP, pour tenir compte de l'intégrité du nœud StorageGRID en arrière-plan. * En option, demandez la découverte automatique du serveur virtuel si l'appliance est une appliance double DNS/LTM.

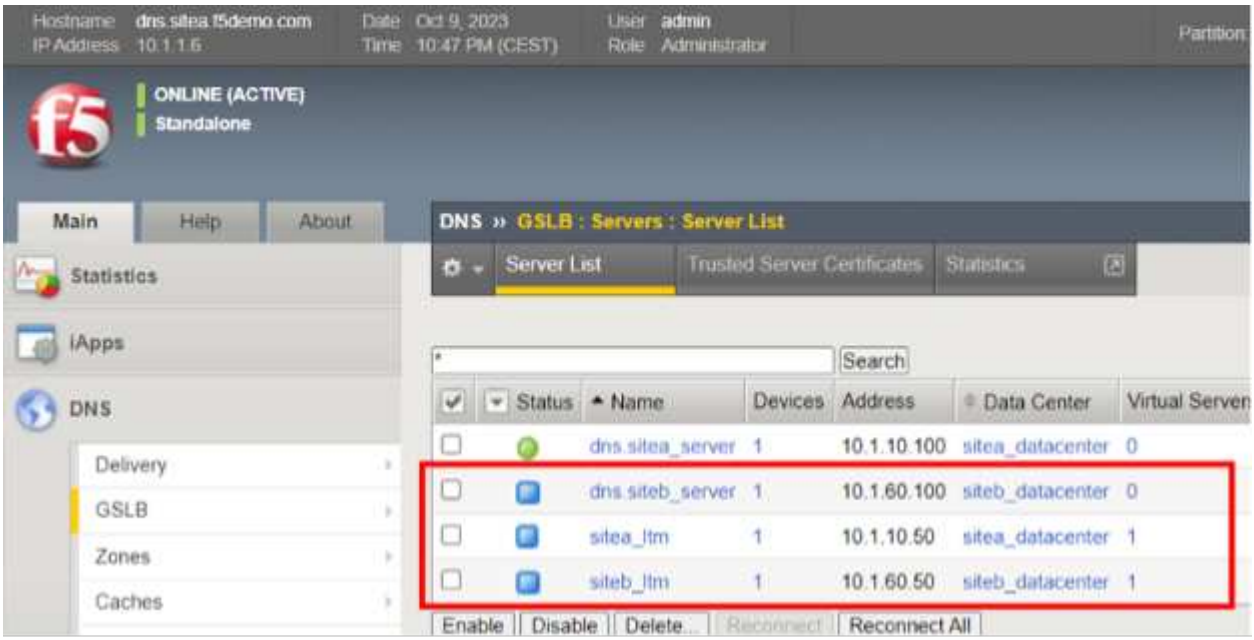


Dans certaines situations, comme des problèmes de réseau transitoires ou des règles ACL de pare-feu entre les emplacements du réseau, lors de l'ajout d'un dispositif distant à ce stade, la découverte du serveur virtuel peut ne pas afficher les entrées pour les dispositifs distants avec LTM configuré. Dans de tels cas, après avoir ajouté le nouvel appareil (« serveur »), on peut ajouter manuellement les serveurs virtuels comme indiqué ci-dessous. Si vous ajoutez un dispositif BIG-IP DNS uniquement, aucun serveur virtuel ne sera découvert ni ajouté à ce dispositif.

Nous devons ajouter ces entrées de serveur pour chaque appareil de notre solution sur tous les sites, y compris les appareils BIG-IP DNS, les appareils BIG-IP LTM et tous les appareils assurant les rôles à la fois d'unités DNS et LTM.

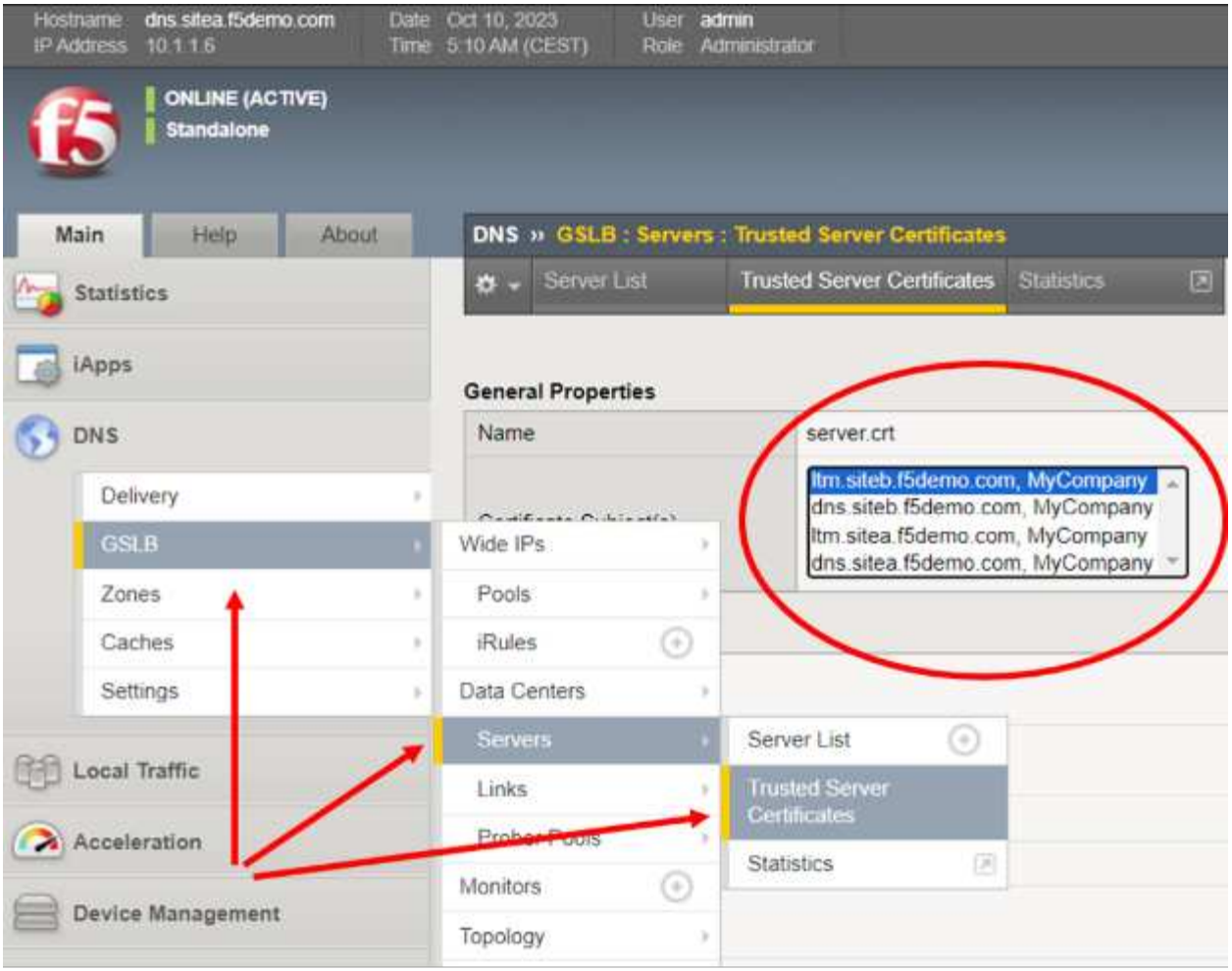
Troisième étape : Établir la confiance entre tous les équipements BIG-IP

Dans l'exemple suivant, quatre appareils ont été ajoutés en tant que serveurs ; ils sont répartis sur deux sites. Notez que chaque site dispose d'un serveur DNS BIG-IP et d'un serveur LTM BIG-IP dédiés. Cependant, tous les appareils, à l'exception de celui sur lequel je suis actuellement connecté, affichent des icônes bleues dans la colonne « État ». Cela signifie qu'une relation de confiance n'a pas encore été établie avec les autres appliances BIG-IP.



Pour ajouter de la confiance, connectez-vous en SSH au BIG-IP où les détails de configuration viennent d'être saisis via l'interface graphique, et utilisez le compte « root » pour accéder à l'interface de ligne de commande du BIG-IP. Saisissez la commande unique suivante à l'invite : *bigip_add*

La commande « bigip_add » récupère le certificat de gestion des périphériques BIG-IP de destination afin de l'utiliser lors de la configuration du canal chiffré « iQuery » entre les serveurs GSLB du cluster. Par défaut, iQuery utilise le port TCP 4353 et sert de signal de synchronisation permettant aux membres DNS BOG-IP de rester synchronisés. Il utilise XML et gzip dans le canal chiffré. Lorsque vous exécutez la commande « bigip_add » sans aucune option, elle sera exécutée sur tous les périphériques BIGIP de la liste des serveurs GSLB en utilisant le nom d'utilisateur actuel pour se connecter aux points de terminaison. Pour vérifier rapidement que tout a bien fonctionné, retournez simplement à l'interface graphique de BIG-IP et assurez-vous que tous les serveurs possèdent désormais des certificats listés dans le menu déroulant affiché.



Étape 4 : Synchroniser tous les appliances DNS BIG-IP avec le groupe DNS

La dernière étape permettra de configurer entièrement tous les équipements DNS BIG-IP en utilisant simplement l'interface graphique TMUI d'une seule unité. Dans un cas concret, où il existe deux sites StorageGRID , cela signifie désormais utiliser SSH pour accéder à la ligne de commande du DNS BIG-IP de l'**autre** site. Après vous être connecté en tant que root et avoir vérifié que les règles de pare-feu/ACL autorisent les deux périphériques BIG-IP DNS à communiquer sur les ports TCP 22 (SSH), 443 (HTTPS) et 4354 (protocole F5 iQuery), saisissez la commande suivante à l'invite : *gtm_add <adresse IP du premier serveur BIG-IP DNS du site où toutes les étapes de l'interface graphique ont été effectuées précédemment>*

À ce stade, toute configuration DNS supplémentaire peut être effectuée sur n'importe quel dispositif DNS BIG-IP ajouté au groupe. La commande ci-dessus, gtm_add, n'a pas besoin d'être appliquée aux membres de l'appliance qui sont uniquement LTM. Seuls les appareils prenant en charge le DNS nécessitent cette commande pour faire partie du groupe DNS synchronisé.

Mise en place de sites de centres de données et établissement de communications inter-BIG-IP

À ce stade, toutes les étapes nécessaires à la création du groupe d'appliances DNS BIG-IP sous-jacent et sain sont terminées. Nous pouvons maintenant procéder à la création de noms, FQDN, qui pointent vers nos services web/S3 distribués exposés dans chaque centre de données StorageGRID .

Ces noms sont appelés « Wide IPs », ou WIP en abrégé, et ce sont des noms de domaine pleinement qualifiés (FQDN) DNS normaux avec des enregistrements de ressources DNS de type A. Cependant, au lieu de pointer vers un serveur comme un enregistrement de ressource A traditionnel, ils pointent en interne vers des pools de serveurs virtuels BIG-IP. Chaque pool peut, individuellement, être constitué d'un ou plusieurs

serveurs virtuels. Un client S3 demandant une résolution d'adresse IP vers un nom recevra l'adresse du serveur virtuel S3 sur le site StorageGRID optimal sélectionné par la politique.

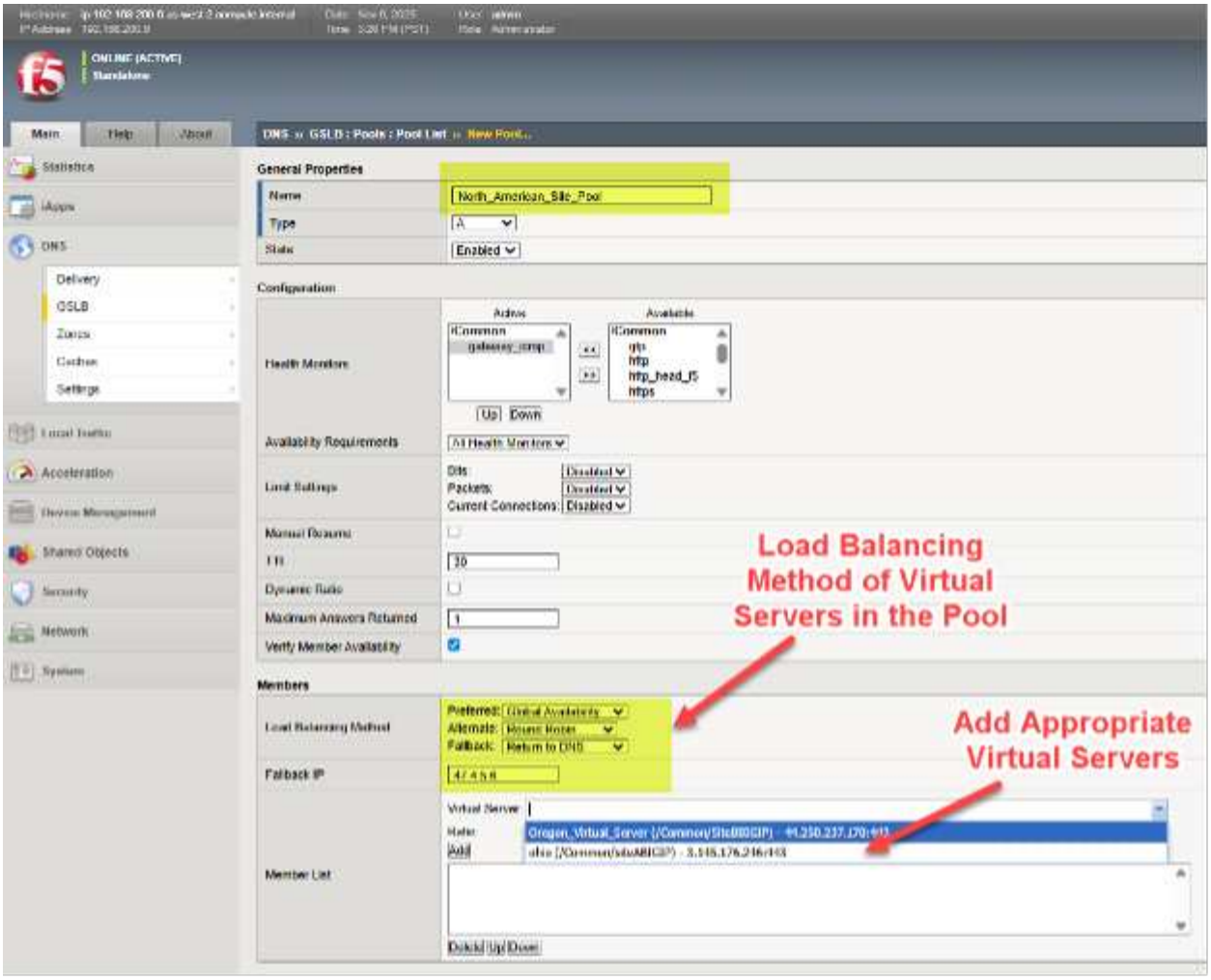
En bref : adresses IP étendues, pools et serveurs virtuels

Pour donner un exemple simple et fictif, un WIP pour le nom **storage.quantumvault.com** pourrait voir la solution DNS BIG-IP liée à deux pools de serveurs virtuels potentiels. Le premier groupe pourrait être composé de 4 sites en Amérique du Nord ; le second groupe pourrait être composé de 3 sites en Europe.

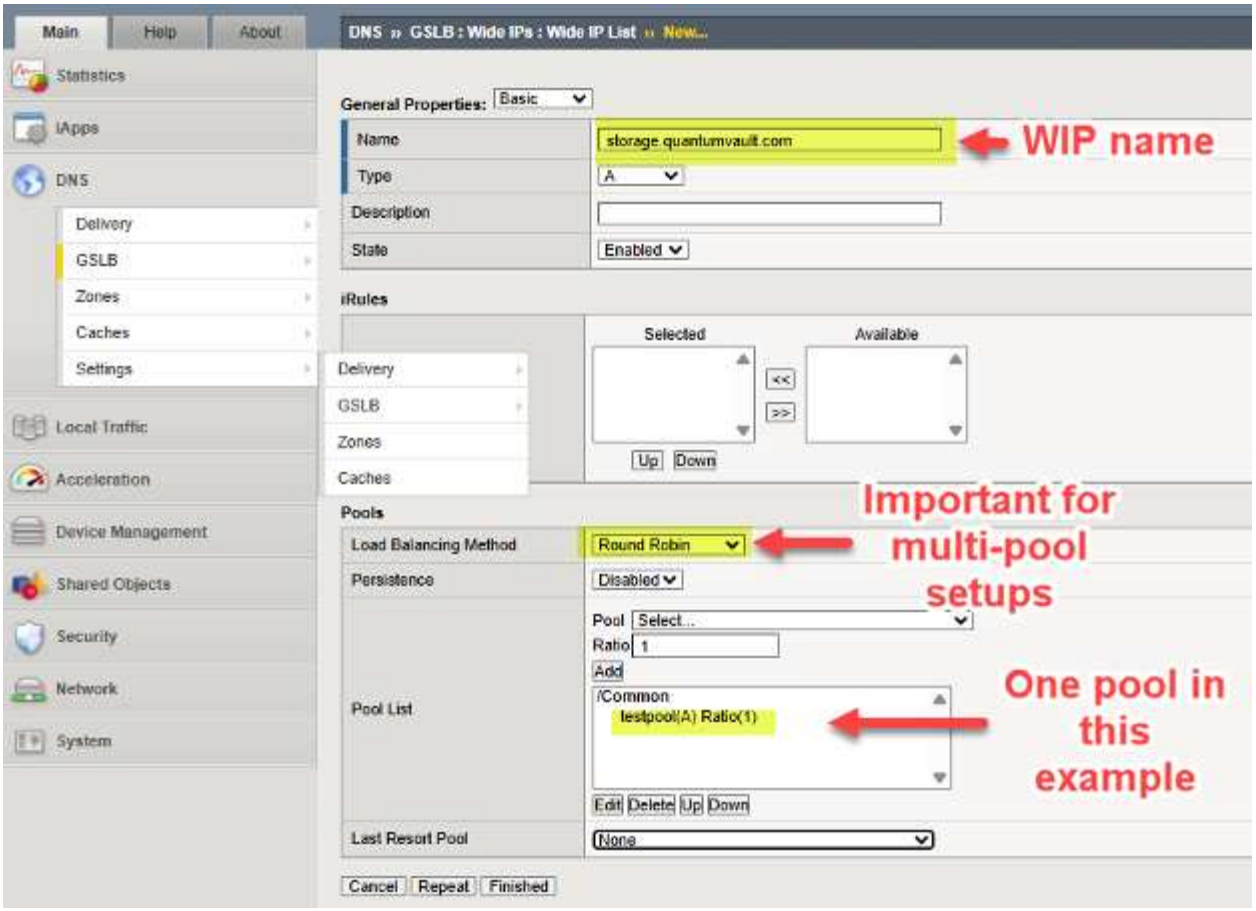
Le choix du pool sélectionné pourrait résulter d'une série de décisions politiques ; un simple ratio de 5:1 pourrait par exemple être utilisé pour diriger la majeure partie du trafic vers les sites StorageGRID nord-américains. Plus probablement, un choix basé sur la topologie où le pool est choisi de telle sorte que, par exemple, tout le trafic S3 d'origine européenne soit dirigé vers des sites européens, et le reste du trafic S3 mondial vers des centres de données nord-américains.

Une fois qu'un pool est trouvé par BIG-IP DNS, supposons que le pool nord-américain ait été sélectionné, l'enregistrement de ressource DNS A réel renvoyé pour résoudre storage.quantumvault.com peut être l'un des 4 serveurs virtuels pris en charge par BIG-IP LTM dans l'un des 4 sites nord-américains. Là encore, le choix est guidé par des politiques ; des approches « statiques » simples comme Round-Robin existent, tandis que des sélections « dynamiques » plus avancées, telles que des sondes de performance pour mesurer la latence de chaque site à partir des résolveurs DNS locaux, sont maintenues et utilisées comme critères de sélection des sites.

Pour configurer un pool de serveurs virtuels sur un BIG-IP DNS, suivez le chemin de menu **DNS > GSLB > Pools > Pool List > Add (+)**. Dans cet exemple, nous pouvons voir que différents serveurs virtuels nord-américains sont ajoutés à un pool et que l'approche privilégiée en matière d'équilibrage de charge, lorsque ce pool est sélectionné, est choisie de manière hiérarchisée.



Nous ajoutons le WIP (Wide IP), le nom de notre service qui sera résolu par DNS, à un déploiement en suivant DNS > GSLB > Wide IPs > Liste des Wide IP > Créer (+). Dans l'exemple suivant, nous fournissons un exemple de travail en cours pour un service de stockage compatible S3.



Ajuster le DNS pour prendre en charge la gestion du trafic global

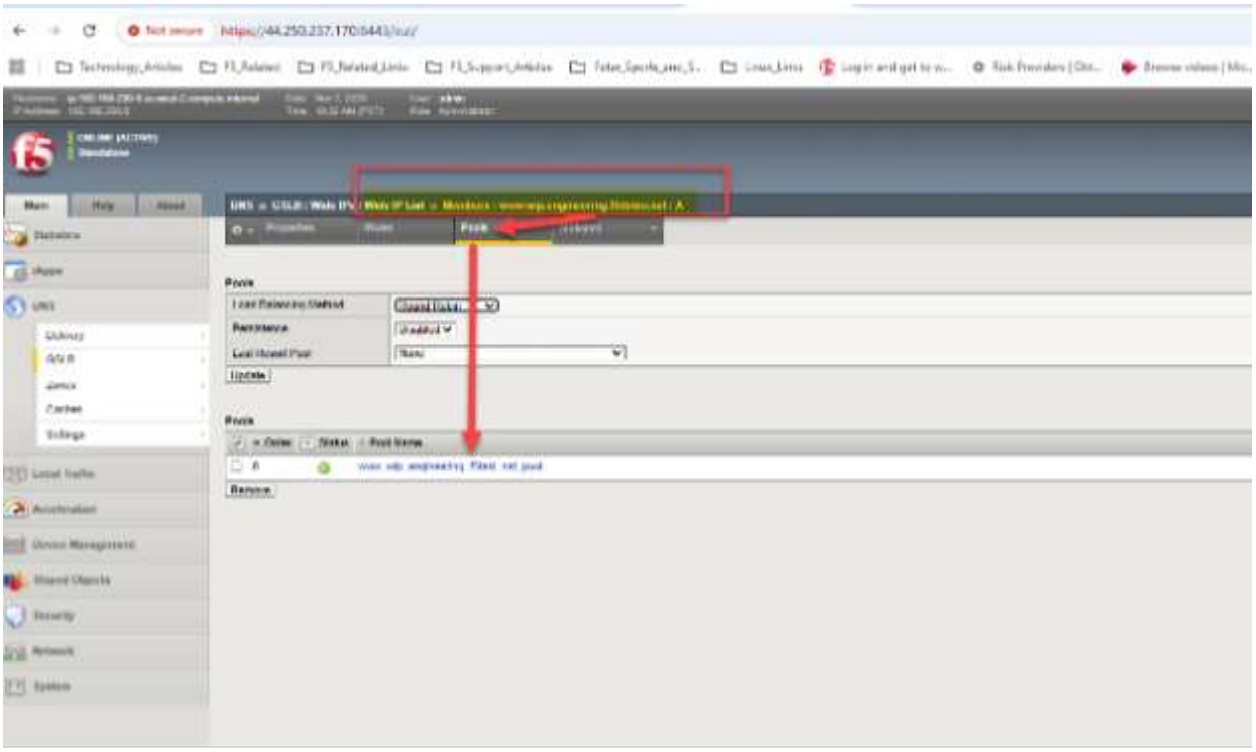
À ce stade, tous nos équipements BIG-IP sous-jacents sont prêts à effectuer le GSLB (équilibrage de charge global des serveurs). Il nous suffit d'ajuster et d'attribuer les noms utilisés pour les flux de trafic S3 pour tirer parti de la solution. L'approche générale consiste à déléguer une partie d'un domaine DNS existant d'une entreprise au contrôle de BIG-IP DNS. Cela revient à « découper » une section de l'espace de noms, un sous-domaine, et à déléguer le contrôle de ce sous-domaine aux appliances DNS BIG-IP. Techniquement, cela se fait en s'assurant que les appliances DNS BIG-IP possèdent des enregistrements de ressources DNS de type A (RR) dans le DNS de l'entreprise, puis en faisant de ces noms/adresses des enregistrements de ressources DNS de serveur de noms (NS) pour le domaine délégué.

Il existe aujourd'hui différentes manières pour les entreprises de gérer leur DNS, dont une solution entièrement hébergée. Un exemple de ceci serait l'exploitation et la gestion du DNS via Windows Server 2025. Une autre solution consiste pour une entreprise à tirer parti de fournisseurs de DNS cloud comme AWS Route53 ou Squarespace.

Voici un exemple fictif à titre d'illustration. Nous disposons StorageGRID prenant en charge la lecture et l'écriture d'objets via le protocole S3 avec un domaine existant géré par AWS Route53 ; le domaine d'exemple existant est f5demo.net.

Nous souhaiterions attribuer le sous-domaine engineering.f5demo.net aux appliances DNS BIG-IP pour la gestion du trafic global. Pour ce faire, nous créons un nouvel enregistrement de ressource NS (serveur de noms) pour engineering.f5demo.net et le faisons pointer vers la liste des noms d'appliances DNS BIG-IP. Dans notre exemple, nous avons deux appliances DNS BIG-IP, et nous créons donc deux enregistrements de ressources A pour chacune d'elles.

Nous allons maintenant, à titre d'exemple, configurer un Wide IP (WIP) dans notre DNS BIG-IP. Étant donné que le DNS utilise la synchronisation de groupe, nous n'avons besoin de l'ajuster qu'à l'aide de l'interface graphique d'un seul appareil. Dans l'interface graphique DNS de BIG-IP, accédez à **DNS > GSLB > Wide IPs > Wide IP List (+)**. Rappelons que, dans une configuration DNS FQDN traditionnelle, on entrerait une ou plusieurs adresses IPv4 ; dans notre cas, nous pointons simplement vers un ou plusieurs pools de serveurs virtuels StorageGRID .

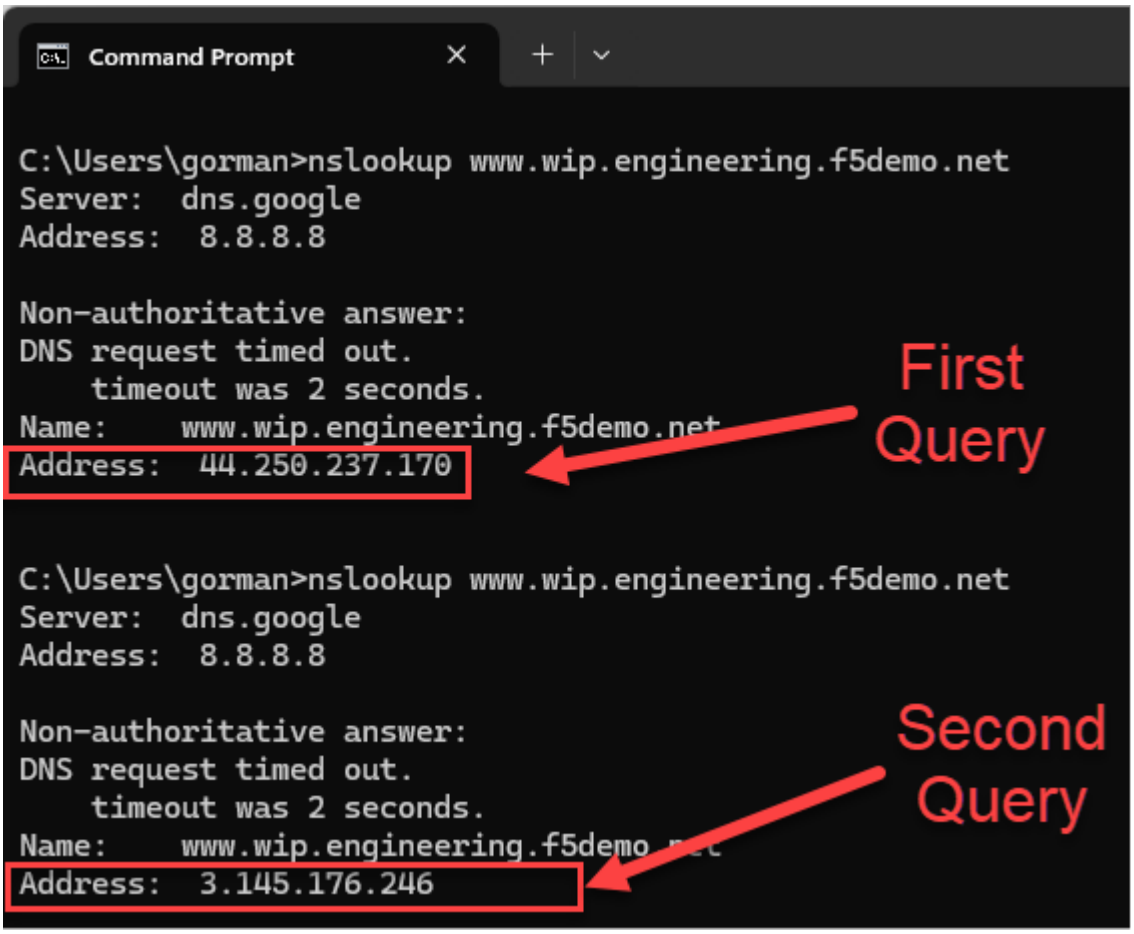


Dans notre exemple, nous avons des serveurs web HTTPS génériques situés à la fois dans l'Ohio et dans l'Oregon. Avec une simple approche de type « round robin », nous devrions pouvoir voir le DNS global répondre aux requêtes concernant les mappages d'enregistrements de ressources A pour

www.wip.engineering.f5demo.net avec les deux adresses IP du serveur virtuel.

Un test simple peut être effectué avec des navigateurs web ou, dans le cas de S3 utilisant StorageGRID, éventuellement avec des outils graphiques comme S3Browser. Chaque requête DNS verra le prochain site de centre de données du pool utilisé comme cible pour le trafic suivant, en raison de notre choix de Round Robin au sein du pool.

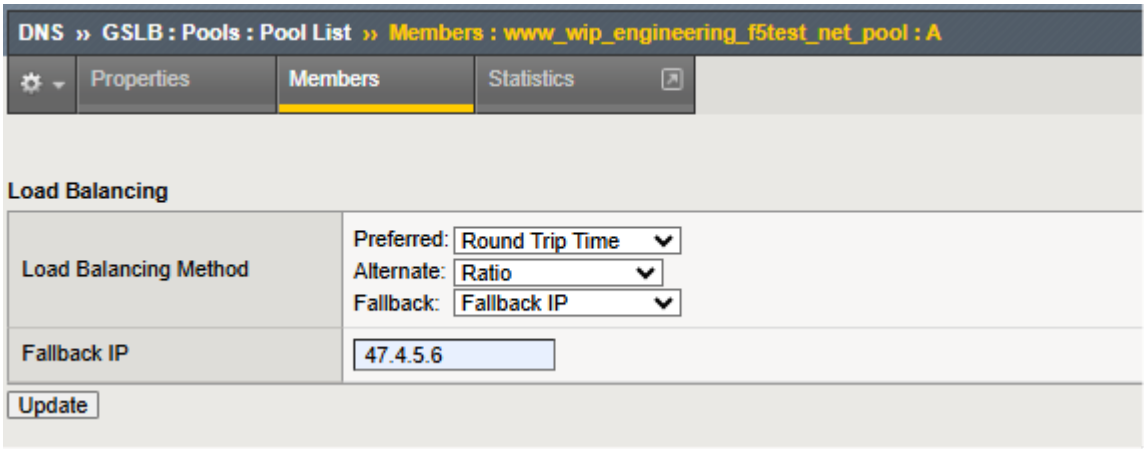
Dans notre exemple de configuration, nous pouvons utiliser dig ou nslookup pour générer rapidement une série de deux requêtes DNS et nous assurer que BIG-IP DNS effectue bien un équilibrage de charge round robin, ce qui permet aux deux sites de recevoir du trafic au fil du temps.



Exploration suggérée pour des techniques plus avancées

L'une des nombreuses approches possibles consisterait à utiliser le mode « Disponibilité globale » plutôt que le simple exemple de « Round Robin » donné ci-dessus. Avec la disponibilité globale, l'ordre séquentiel des pools, ou des serveurs virtuels au sein d'un seul pool, peut recevoir du trafic dirigé vers celui-ci. De cette manière, tout le trafic S3 pourrait, par défaut, être dirigé vers, par exemple, un site situé à New York.

Si les contrôles d'intégrité indiquent un problème de disponibilité des nœuds StorageGRID sur ce site, le trafic pourrait alors être redirigé vers Saint-Louis. Si Saint-Louis rencontrait des problèmes sanitaires, un site à Francfort pourrait alors commencer à recevoir des transactions de lecture ou d'écriture S3. Ainsi, la disponibilité globale est une approche de la résilience globale de la solution S3 StorageGRID . Une autre approche consiste à combiner différentes méthodes d'équilibrage de charge, en utilisant une approche par paliers.



Dans cet exemple, l'option « dynamique » est le premier choix d'équilibrage de charge pour les sites du pool configuré. Dans l'exemple présenté, une approche de mesure continue utilisant un sondage actif des performances du résolveur DNS local est maintenue et sert de catalyseur pour la sélection du site. Si cette approche n'est pas possible, les sites individuels peuvent être sélectionnés en fonction du ratio attribué à chacun. Grâce à ce ratio, les sites StorageGRID plus grands et à bande passante plus élevée peuvent recevoir plus de transactions S3 que les sites plus petits. Enfin, dans le cadre d'un scénario de reprise après sinistre, si tous les sites du pool deviennent défaillants, l'adresse IP de secours spécifiée est utilisée comme site de dernier recours. L'une des méthodes d'équilibrage de charge les plus intéressantes de BIG-IP DNS est la « topologie », selon laquelle la source entrante des requêtes DNS, le résolveur DNS local de l'utilisateur S3, est observée et, à l'aide des informations de topologie Internet, le site apparemment le plus « proche » est sélectionné dans le pool.

Enfin, si les sites sont répartis sur l'ensemble du globe, il peut être judicieux d'envisager l'utilisation de la technologie de « sonde » dynamique décrite en détail dans le manuel DNS F5 BIG-IP. Grâce aux sondes, il est possible de surveiller les sources fréquentes de requêtes DNS, par exemple un partenaire commercial dont le trafic utilise généralement le même résolveur DNS local. Les sondes DNS BIG-IP peuvent être lancées depuis le BIG-IP LTM dans chaque site du monde entier, afin de déterminer de manière générale quel site potentiel serait susceptible d'offrir la latence la plus faible pour les transactions S3. De ce fait, le trafic en provenance d'Asie pourrait être mieux pris en charge par les sites StorageGRID asiatiques que par les sites situés en Amérique du Nord ou en Europe.

Conclusion

L'intégration de F5 BIG-IP avec NetApp StorageGRID répond aux défis techniques liés à la disponibilité et à la cohérence des données sur plusieurs sites et à l'optimisation du routage des transactions S3. Le déploiement de cette solution améliore la résilience, les performances et la fiabilité du stockage, ce qui la rend idéale pour les entreprises à la recherche d'une infrastructure de stockage robuste, évolutive et flexible.

Pour en savoir plus, la documentation officielle F5 pour BIG-IP DNS est disponible ici : "lien". Un guide de style classe guidée, fournissant des instructions étape par étape sur un exemple de configuration, est également disponible. "ici".

Configuration SNMP Datalog

Par Aron Klein

Configurez Datalog pour collecter les mesures snmp et les traps StorageGRID.

Configurer Datalog

Datalog est une solution de surveillance qui fournit des mesures, des visualisations et des alertes. La configuration suivante a été implémentée avec l'agent linux version 7.43.1 sur un hôte Ubuntu 22.04.1 déployé localement sur le système StorageGRID.

Fichiers de profil Datadog et de déroutement générés à partir du fichier MIB StorageGRID

Datadog fournit une méthode de conversion des fichiers MIB de produit en fichiers de référence Datadog requis pour mapper les messages SNMP.

Ce fichier yaml StorageGRID pour le mappage de résolution des interruptions Datadog généré suivant l'instruction trouvée "ici". + placez ce fichier dans /etc/datadog-agent/conf.d/snmp.d/traps_db/ +

- "Téléchargez le fichier yaml d'interruption" +
  - **somme de contrôle md5** 42e27e4210719945a46172b98c379517 +
  - **sha256 checksum** d0fe5c8e6ca3c902d054f85f8554b70a85f928cba8b7c76391d356f05d2cf73b6887 +

Ce fichier yaml de profil StorageGRID pour le mappage de metrics Datadog généré suivant l'instruction trouvée "ici". + placez ce fichier dans /etc/datadog-agent/conf.d/snmp.d/profiles/ +

- "Téléchargez le fichier yaml de profil" +
  - **somme de contrôle md5** 72bb7784f4801adda4e0c3ea77df19aa +
  - **sha256 checksum** b6b7fadd33063422a8bb8e39b3ead8ab38349ee0229926eadc85f0087b8cee +

Configuration du datalog SNMP pour les métriques

La configuration de SNMP pour les mesures peut être gérée de deux manières. Vous pouvez configurer la détection automatique en fournissant une plage d'adresses réseau contenant le(s) système(s) StorageGRID ou en définissant les adresses IP des périphériques individuels. L'emplacement de la configuration est différent en fonction de la décision prise. La découverte automatique est définie dans le fichier yaml de l'agent de données. Les définitions explicites de périphériques sont configurées dans le fichier yaml de configuration snmp. Vous trouverez ci-dessous des exemples de chacun d'eux pour le même système StorageGRID.

Découverte automatique

configuration située dans /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
```

Périphériques individuels

/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'
```

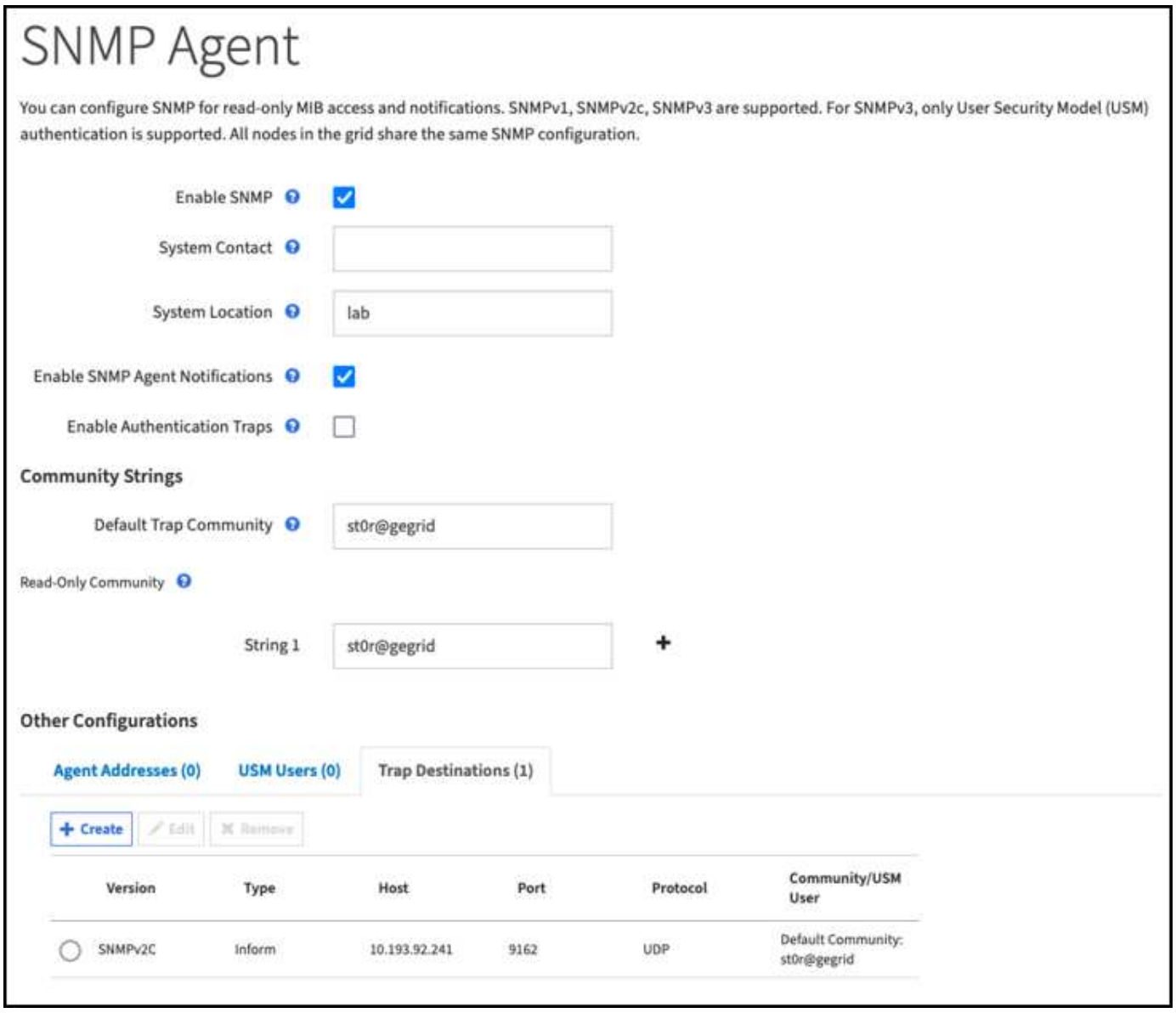
Configuration SNMP pour les interruptions

La configuration des traps SNMP est définie dans le fichier de configuration de datadog yaml /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
```

Exemple de configuration SNMP StorageGRID

L'agent SNMP de votre système StorageGRID se trouve sous l'onglet de configuration, colonne surveillance. Activez SNMP et entrez les informations souhaitées. Si vous souhaitez configurer des interruptions, sélectionnez « destinations des interruptions » et créez une destination pour l'hôte de l'agent Datadog contenant la configuration des interruptions.



Utilisez rclone pour migrer, DÉPLACER et SUPPRIMER des objets sur StorageGRID

Par Siegfried Hepp et Aron Klein

Rclone est un outil de ligne de commande et un client gratuits pour les opérations S3. Vous pouvez utiliser rclone pour migrer, copier et supprimer des données d'objet sur StorageGRID. rclone permet de supprimer des compartiments même s'ils ne sont pas vides, grâce à la fonction de « purge » comme illustré ci-dessous.

Installer et configurer rclone

Pour installer rclone sur un poste de travail ou un serveur, téléchargez-le depuis "rclone.org".

Étapes de configuration initiale

1. Créez le fichier de configuration rclone en exécutant le script de configuration ou en créant manuellement le fichier.
2. Dans cet exemple, j'utilise sgdemo pour le nom du terminal StorageGRID S3 distant dans la configuration rclone.
   a. Créez le fichier de configuration ~/.config/rclone/rclone.conf

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

   b. Exécutez la configuration rclone

rclone config

```
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
```

Exemples de commandes de base

- **Créer un compartiment :**

  `rclone mkdir remote:bucket`

  ```
  # rclone mkdir sgdemo:test01
  ```

  Utilisez --no-check-certificate si vous devez ignorer les certificats SSL.

- **Liste de tous les compartiments:**

```
rclone lsd remote:
```

```
# rclone lsd sgdemo :
```

- **Liste des objets dans un compartiment spécifique :**

```
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
```

- **Supprimer un compartiment :**

```
rclone rmdir remote:bucket
```

```
# rclone rmdir sgdemo:test02
```

- **Mettre un objet:**

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

```
# rclone copy ~/test/testfile.txt sgdemo:test01
```

- **Obtenir un objet:**

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

```
# Rclone copy sgdemo:test01/testfile.txt ~/test/testfileS3.txt
```

- **Supprimer un objet:**

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

```
# rclone delete sgdemo:test01/testfile.txt
```

- **Migrer des objets dans un compartiment**

```
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
```

Utilisez --Progress ou -P pour afficher la progression de la tâche. Sinon, il n'y a pas de sortie.

- **Supprimer un compartiment et tout le contenu de l'objet**

```
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
```

Bonnes pratiques de déploiement de StorageGRID avec Veeam Backup and Replication

Par Oliver Haensel et Aron Klein

Ce guide se concentre sur la configuration de NetApp StorageGRID et en partie de Veeam Backup and Replication. Ce livre blanc s'adresse aux administrateurs du stockage et du réseau qui connaissent bien les systèmes Linux et sont chargés de la maintenance ou de l'implémentation d'un système NetApp StorageGRID en association avec Veeam Backup and Replication.

Présentation

Les administrateurs du stockage cherchent à gérer la croissance de leurs données grâce à des solutions qui répondent à leurs besoins en termes de disponibilité, de restauration rapide, d'évolutivité et d'automatisation des règles de conservation des données à long terme. Ces solutions doivent également offrir une protection contre les pertes et les attaques malveillantes. Ensemble, Veeam et NetApp ont créé une solution de protection des données combinant Veeam Backup & Recovery avec NetApp StorageGRID pour le stockage objet sur site.

Veeam et NetApp StorageGRID proposent une solution simple d'utilisation qui s'associent pour répondre aux exigences liées à la croissance rapide des données et à l'augmentation des réglementations à travers le monde. Le stockage objet basé dans le cloud est réputé pour sa résilience, son évolutivité, ses fonctionnalités opérationnelles et sa rentabilité, qui en font un choix naturel comme cible pour vos sauvegardes. Ce document fournit des conseils et des recommandations pour la configuration de votre solution de sauvegarde Veeam et de votre système StorageGRID.

La charge de travail d'objets de Veeam crée un grand nombre d'opérations simultanées de PUT, DELETE et LIST pour les petits objets. L'activation de l'immuabilité ajoute au nombre de demandes dans le magasin d'objets pour définir la conservation et répertorier les versions. Le processus d'une tâche de sauvegarde comprend l'écriture d'objets pour la modification quotidienne. Une fois les nouvelles écritures terminées, la tâche supprime tous les objets basés sur la stratégie de rétention de la sauvegarde. La planification des tâches de sauvegarde se chevauchera presque toujours. Ce chevauchement entraînera une grande partie de la fenêtre de sauvegarde comprenant une charge de travail PUT/DELETE 50/50 sur le magasin d'objets. Ajuster dans Veeam le nombre d'opérations simultanées avec le paramètre de slot de tâche, augmenter la taille de l'objet en augmentant la taille du bloc de tâche de sauvegarde, réduire le nombre d'objets dans les demandes de suppression multi-objets, et le choix de la fenêtre de temps maximum pour les tâches à effectuer

optimisera la solution en termes de performances et de coûts.

Assurez-vous de lire la documentation du produit pour "Sauvegarde et réplication Veeam" et "StorageGRID" avant de commencer. Veeam fournit des calculateurs permettant de comprendre le dimensionnement de l'infrastructure Veeam et les exigences de capacité qui doivent être utilisées avant de dimensionner votre solution StorageGRID . Veuillez toujours vérifier les configurations validées par Veeam- NetApp sur le site Web du programme Veeam Ready pour "Objets compatibles Veeam, immuabilité d'objet et référentiel" .

Configuration Veeam

Version recommandée

Il est toujours recommandé de rester à jour et d'appliquer les derniers correctifs pour votre système Veeam Backup & Replication 12 ou 12.1. Nous recommandons actuellement d'installer au moins le correctif P20230718 de Veeam 12.

Configuration du référentiel S3

Un référentiel de sauvegarde scale-out (SOBR) est le Tier de capacité du stockage objet S3. Le Tier de capacité est une extension du référentiel principal, qui permet de prolonger les périodes de conservation des données et de réduire le coût de la solution de stockage. Veeam a la possibilité d'immuabilité avec l'API S3 Object Lock. Veeam 12 peut utiliser plusieurs compartiments dans un référentiel scale-out. StorageGRID n'a pas de limite pour le nombre d'objets ou la capacité d'un compartiment unique. L'utilisation de plusieurs compartiments peut améliorer les performances lors de la sauvegarde de datasets très volumineux où les données de sauvegarde peuvent atteindre plusieurs pétaoctets dans des objets.

La limitation des tâches simultanées peut être nécessaire en fonction du dimensionnement de la solution et des besoins spécifiques. Les paramètres par défaut spécifient un emplacement de tâche de référentiel pour chaque cœur de processeur et pour chaque emplacement de tâche une limite d'emplacement de tâche simultanée de 64. Par exemple, si votre serveur dispose de 2 cœurs de processeur, 128 threads simultanés au total seront utilisés pour le magasin d'objets. Cela inclut les COMMANDES PUT, GET et batch Delete. Il est recommandé de sélectionner une limite conservatrice pour les créneaux de tâches à commencer par et d'ajuster cette valeur une fois que les sauvegardes Veeam ont atteint l'état stable de nouvelles sauvegardes et que les données de sauvegarde expirent. Veuillez vous adresser à votre équipe de gestion de compte NetApp pour dimensionner le système StorageGRID en fonction des délais et des performances souhaités. Il peut être nécessaire de régler le nombre d'emplacements de tâches et la limite des tâches par emplacement pour obtenir la solution optimale.

Configuration de la procédure de sauvegarde

Les tâches de sauvegarde Veeam peuvent être configurées avec plusieurs options de taille de bloc qui doivent être prises en compte avec attention. La taille de bloc par défaut est de 1 Mo. Grâce à l'efficacité du stockage, Veeam assure la compression et la déduplication, ce qui permet de créer des tailles d'objet d'environ 500 Ko pour la sauvegarde complète initiale et des objets de 100 à 200 Ko pour les tâches incrémentielles. Nous pouvons considérablement améliorer les performances et réduire les besoins en matière de magasin d'objets en choisissant une taille de bloc de sauvegarde plus importante. Si la taille de bloc supérieure améliore considérablement les performances du magasin d'objets, elle implique toutefois une augmentation potentielle des besoins en capacité de stockage primaire en raison de la réduction des performances du stockage. Il est recommandé de configurer les tâches de sauvegarde avec une taille de bloc de 4 Mo, ce qui crée des objets d'environ 2 Mo pour les sauvegardes complètes et des objets de 700 Ko à 1 Mo pour les sauvegardes incrémentielles. Les clients peuvent même envisager de configurer des tâches de sauvegarde à l'aide d'une taille de bloc de 8 Mo, qui peut être activée avec l'aide du support Veeam.

La mise en œuvre des sauvegardes immuables utilise le verrouillage objet S3 dans le magasin d'objets.

L'option immuabilité génère un nombre accru de requêtes auprès du magasin d'objets pour obtenir des mises à jour de listes et de conservation des objets.

Lorsque les rétentions de sauvegarde expirent, les procédures de sauvegarde traitent la suppression des objets. Veeam envoie les demandes de suppression au magasin d'objets dans le cadre de requêtes de suppression de plusieurs objets de 1000 objets par demande. Pour les petites solutions, il peut être nécessaire de l'ajuster afin de réduire le nombre d'objets par demande. En outre, si cette valeur est moindre, les demandes de suppression seront réparties de manière plus homogène entre les nœuds du système StorageGRID. Il est recommandé d'utiliser les valeurs du tableau ci-dessous comme point de départ pour la configuration de la limite de suppression de plusieurs objets. Multipliez la valeur du tableau par le nombre de nœuds pour le type d'appliance choisi pour obtenir la valeur du paramètre dans Veeam. Si cette valeur est égale ou supérieure à 1000, il n'est pas nécessaire d'ajuster la valeur par défaut. Si cette valeur doit être ajustée, contactez le support Veeam pour effectuer cette modification.

Modèle de type appliance	S3MultiObjectDeleteLimit par nœud
SG5712	34
SG5760	75
SG6060	200

Pour en savoir plus sur la configuration recommandée en fonction de vos besoins, contactez l'équipe NetApp en charge de votre compte. Les recommandations concernant les paramètres de configuration Veeam incluent :

- Taille du bloc de la tâche de sauvegarde = 4 Mo
- Limite d'emplacement de tâche SOBR = 2-16
- Limite de suppression de plusieurs objets = 34-1000

Configuration StorageGRID

Version recommandée

NetApp StorageGRID 11.9 ou 12.0 avec le dernier correctif sont les versions recommandées pour les déploiements Veeam. Il est toujours recommandé de rester à jour et d'appliquer les derniers correctifs pour votre système StorageGRID .

Configuration de l'équilibreur de charge et du terminal S3

Dans Veeam, le terminal doit être connecté via HTTPS uniquement. Veeam ne prend pas en charge les connexions non chiffrées. Le certificat SSL peut être un certificat auto-signé, une autorité de certification privée de confiance ou une autorité de certification publique de confiance. Pour assurer un accès continu au référentiel S3, il est recommandé d'utiliser au moins deux équilibreurs de charge dans une configuration haute disponibilité. Les équilibreurs de charge peuvent être un service d'équilibrage de charge intégré fourni par StorageGRID, situé sur chaque nœud d'administration et nœud de passerelle ou sur une solution tierce telle que F5, Kemp, HASProxy, Loadbalancer.org, etc L'utilisation d'un équilibreur de charge StorageGRID permet de définir des classificateurs du trafic (règles de QoS) capables de hiérarchiser le workload Veeam ou de limiter Veeam à ne pas affecter les workloads prioritaires sur le système StorageGRID.

Compartiment S3

StorageGRID est un système de stockage multi-locataire sécurisé. Il est recommandé de créer un locataire dédié pour la charge de travail Veeam. Un quota de stockage peut être éventuellement attribué. En tant que

bonne pratique, activez « Utiliser sa propre source d'identité ». Sécurisez l'utilisateur de gestion racine du locataire avec un mot de passe approprié. Veeam Backup 12 nécessite une forte cohérence pour les buckets S3. StorageGRID propose plusieurs options de cohérence configurées au niveau du bucket. Pour les déploiements multisites avec Veeam accédant aux données à partir de plusieurs emplacements, sélectionnez « strong-global ». Si les sauvegardes et restaurations Veeam s'effectuent sur un seul site, le niveau de cohérence doit être défini sur « site fort ». Pour plus d'informations sur les niveaux de cohérence des buckets, veuillez consulter le "documentation" . Pour utiliser StorageGRID pour les sauvegardes d'immuabilité Veeam, S3 Object Lock doit être activé globalement et configuré sur le bucket lors de la création du bucket.

Gestion du cycle de vie

StorageGRID prend en charge la réplication et le code d'effacement pour la protection au niveau objet sur l'ensemble des nœuds et sites StorageGRID. Le codage d'effacement requiert une taille d'objet d'au moins 200 Ko. La taille de bloc par défaut de Veeam de 1 Mo produit des tailles d'objet qui peuvent souvent être inférieures à cette taille minimale recommandée de 200 Ko après les fonctionnalités d'efficacité du stockage de Veeam. Pour les performances de la solution, il est déconseillé d'utiliser un profil de code d'effacement sur plusieurs sites, sauf si la connectivité entre les sites suffit pour ne pas augmenter la latence ou restreindre la bande passante du système StorageGRID. Dans un système StorageGRID multisite, la règle ILM peut être configurée pour stocker une copie unique sur chaque site. Pour une durabilité ultime, une règle pourrait être configurée de manière à stocker une copie codée en effacement sur chaque site. L'implémentation la plus recommandée pour cette charge de travail est l'utilisation de deux copies en local sur les serveurs Veeam Backup.

Supprimer les performances

Veeam fournit un réglage du taux de demande de suppression et une planification du processus de suppression de sauvegarde. Pour optimiser davantage les performances de suppression, vous pouvez désactiver les suppressions synchrones et laisser le scanner ILM gérer la suppression éventuelle des objets.

Étapes pour désactiver les suppressions synchrones

1. Ouvrez le gestionnaire de grille StorageGRID .
2. Dans le coin supérieur droit, sélectionnez le point d'interrogation puis Documentation API.
3. Dans le coin supérieur droit, cliquez sur le lien de la page de documentation de l'API privée.
4. Développer ilm-advanced.
5. Sélectionnez OBTENIR ilm-avancé.
6. Sélectionnez Essayer, puis Exécuter.
7. Vérifiez le résultat de la réponse.

    a. Si les valeurs sont nulles, cela signifie que les valeurs ilm-advanced par défaut sont utilisées.

    b. Si les valeurs ne sont pas nulles, cela signifie que des valeurs avancées ILM personnalisées sont utilisées. Copiez toutes les sorties après « données » :, en commençant par le { jusqu'à l'avant-dernier }.

        i. Enregistrez-le dans un éditeur de texte.

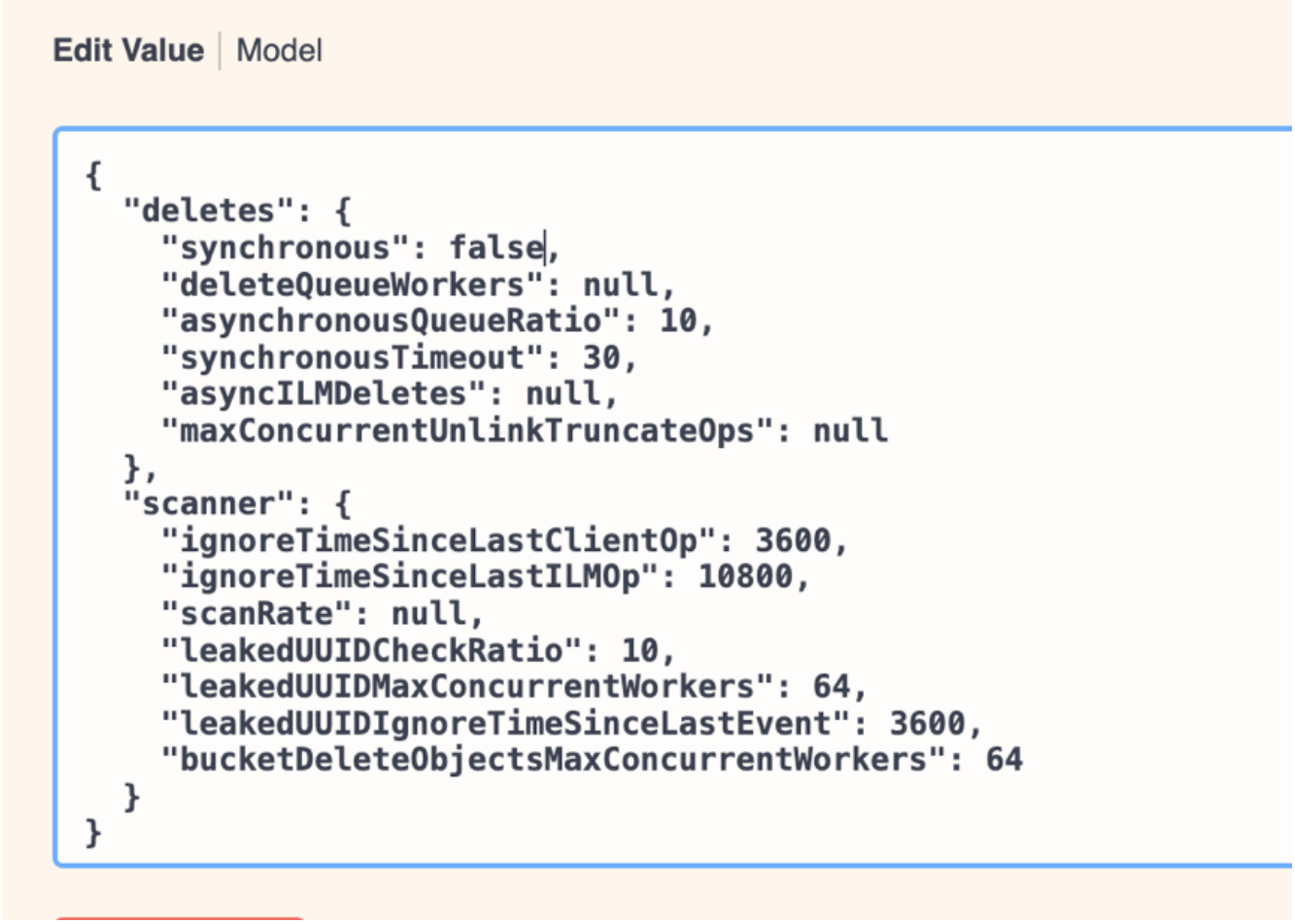
        Exemple de réponse :

Response body


```
{
  "responseTime": "2025-09-19T15:01:28.142Z",
  "status": "success",
  "apiVersion": "4.2",
  "data": {
    "deletes": {
      "synchronous": null,
      "deleteQueueWorkers": null,
      "asynchronousQueueRatio": null,
      "synchronousTimeout": null,
      "asyncILMDeletes": null,
      "maxConcurrentUnlinkTruncateOps": null
    },
    "scanner": {
      "ignoreTimeSinceLastClientOp": null,
      "ignoreTimeSinceLastILMOp": null,
      "scanRate": null,
      "leakedUUIDCheckRatio": null,
      "leakedUUIDMaxConcurrentWorkers": null,
      "leakedUUIDIgnoreTimeSinceLastEvent": null,
      "bucketDeleteObjectsMaxConcurrentWorkers": null
    }
  }
}
```


8. Sélectionnez PUT ilm-advanced.
9. Sélectionnez Essayer pour commencer à modifier le corps de l'API.
    a. Par défaut, le corps de l'API contiendra des valeurs par défaut et non des valeurs personnalisées précédemment configurées. C'est la raison pour laquelle il est TRÈS important d'exécuter les étapes 5 à 7.
10. Si des valeurs non par défaut sont trouvées à l'étape 5 à 7, remplacez le corps de l'API par la sortie enregistrée à l'étape 7. . Sinon, si les valeurs étaient nulles à l'étape 5-7, laissez le corps de l'API tel quel.
11. Ajustez les paramètres suivants dans la zone de corps de l'API :
    a. Définissez la valeur synchrone sur faux.

       Exemple de texte du corps de l'API :

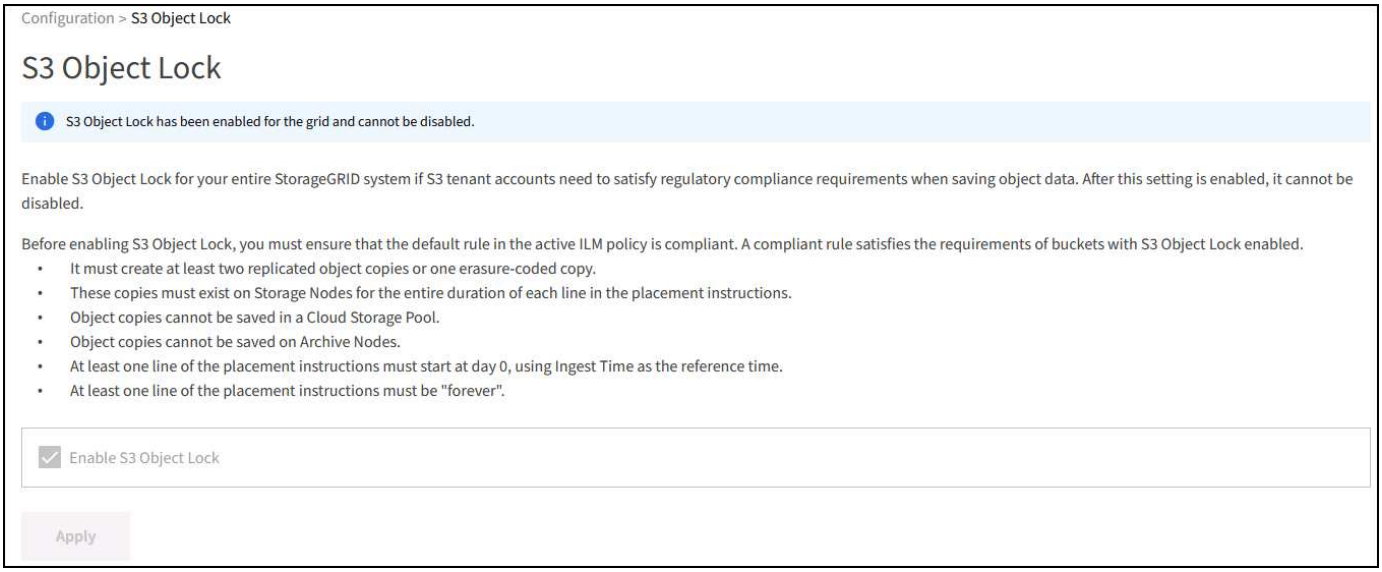


12. Une fois terminé, sélectionnez Exécuter

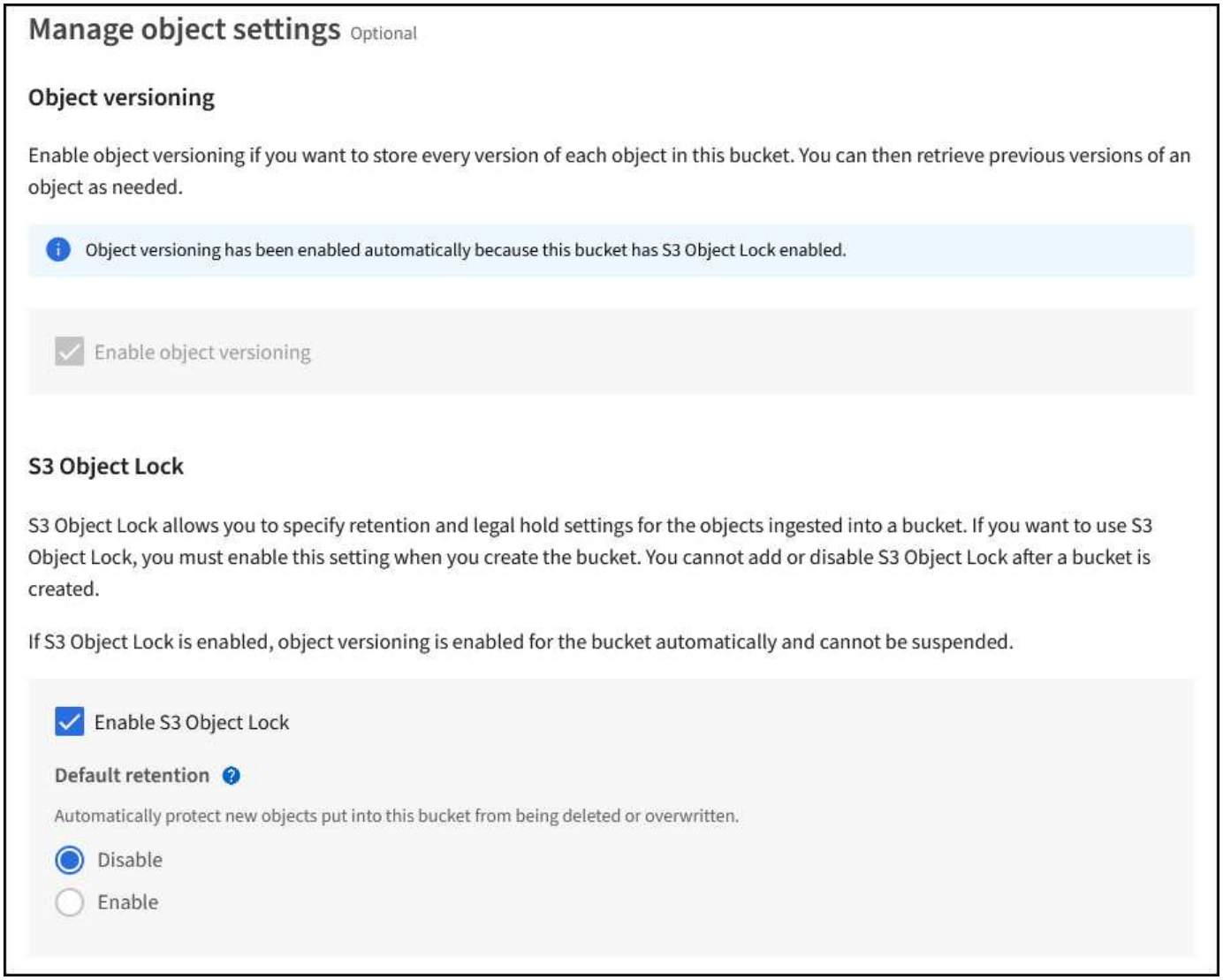
Points clés de la mise en œuvre

StorageGRID

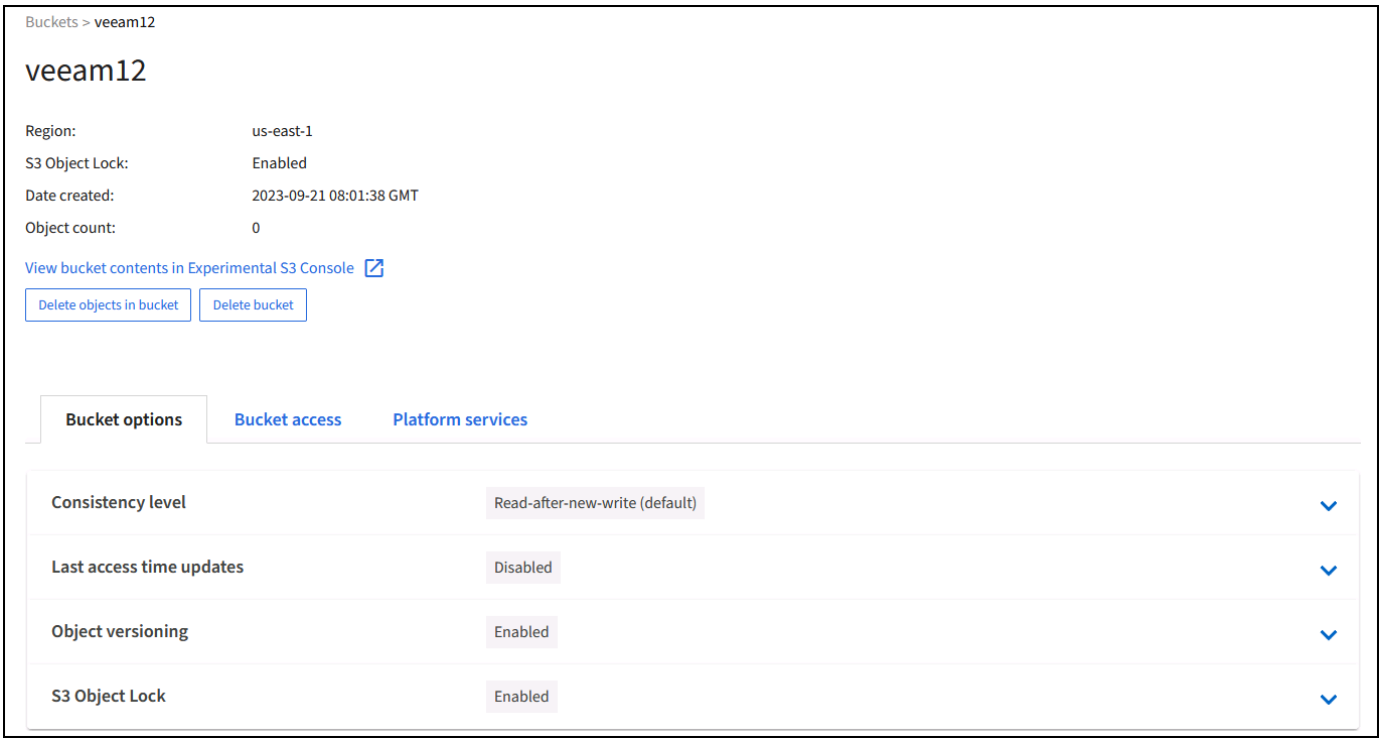
Assurez-vous que le verrouillage des objets est activé sur le système StorageGRID si l'immuabilité est requise. Recherchez l'option dans l'interface de gestion sous Configuration/S3 Object Lock.



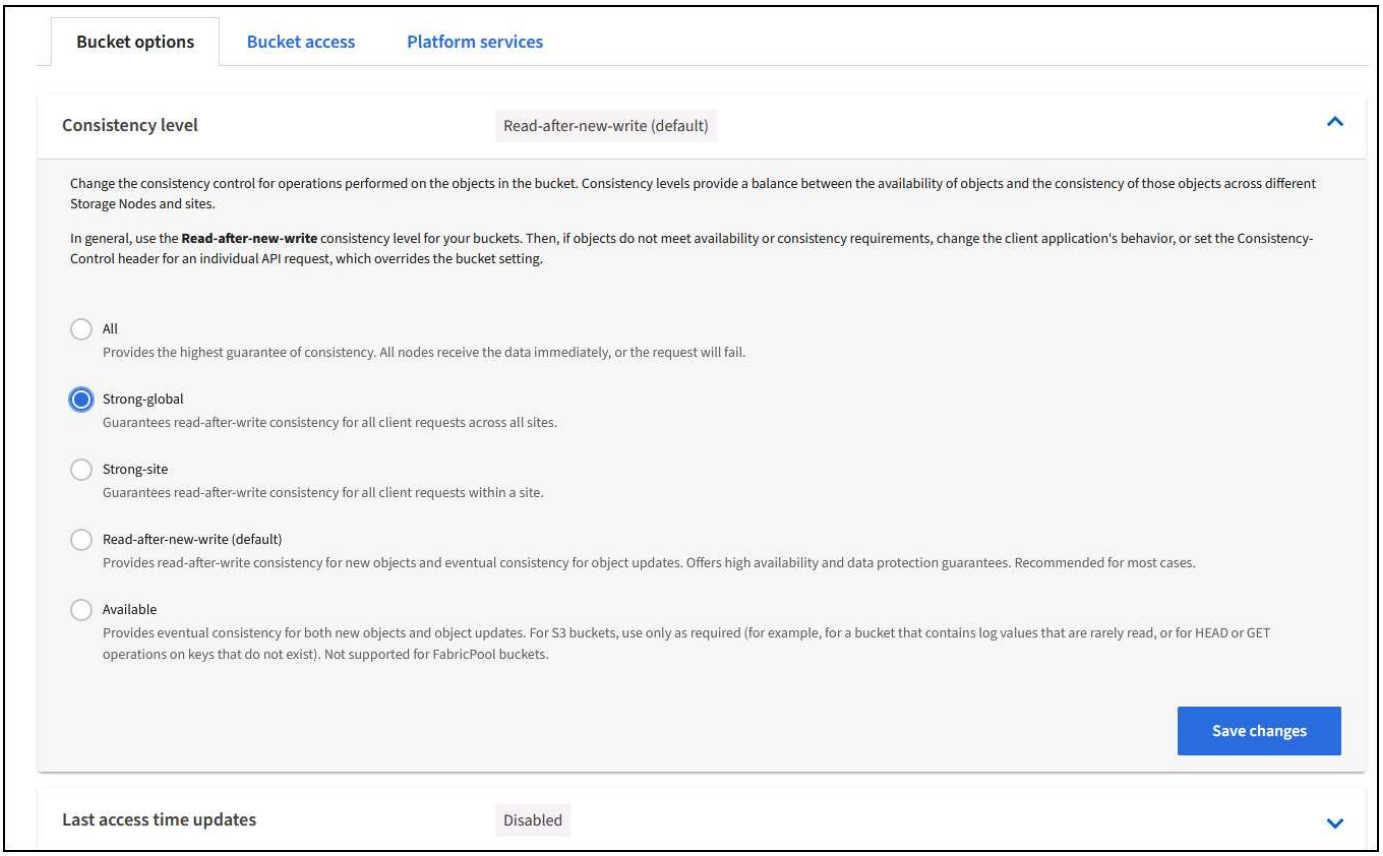
Lors de la création du compartiment, sélectionnez Activer le verrouillage des objets S3 si ce compartiment doit être utilisé pour les sauvegardes sans altération. La gestion des versions de compartiment est alors automatiquement activée. Laissez la conservation par défaut désactivée, car Veeam définit la conservation d'objet de manière explicite. La gestion des versions et le verrouillage objet S3 ne doivent pas être sélectionnés si Veeam ne crée pas de sauvegardes immuables.



Une fois le compartiment créé, accédez à la page de détails du compartiment créé. Sélectionnez le niveau de cohérence.



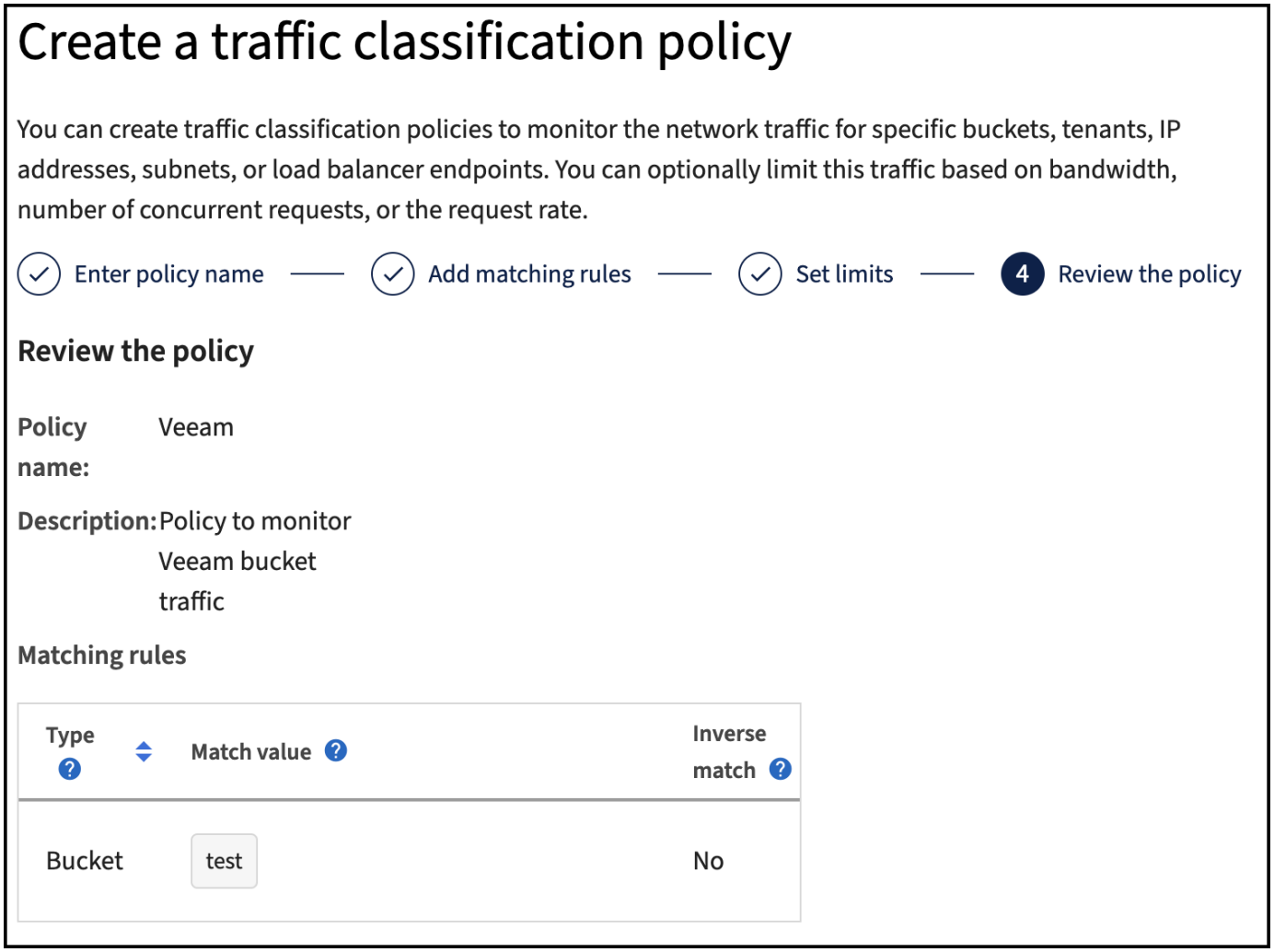
Veeam requiert une cohérence renforcée pour les compartiments S3. Pour les déploiements multi-sites avec Veeam qui accèdent aux données depuis plusieurs sites, sélectionnez « strong-global ». Si les sauvegardes et les restaurations Veeam ont lieu sur un seul site, le niveau de cohérence doit être défini sur « site à forte intensité ». Enregistrez les modifications.



StorageGRID propose un service d’équilibrage de la charge intégré sur chaque nœud d’administration et sur

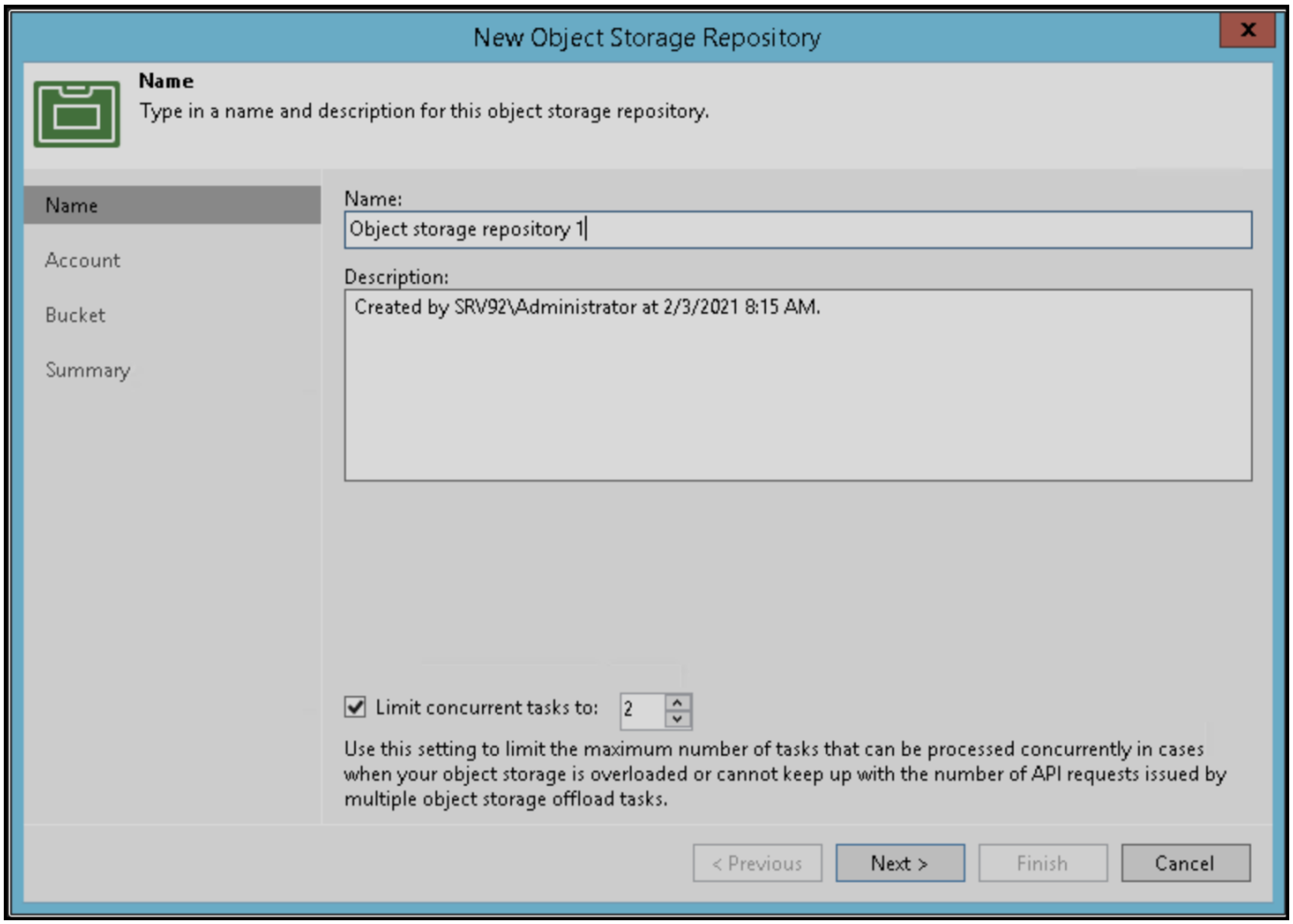
tous les nœuds de passerelle dédiés. L'un des nombreux avantages de l'utilisation de cet équilibreur de charge est la possibilité de configurer des règles de classification du trafic (QoS). Bien qu'elles soient principalement utilisées pour limiter l'impact des applications sur les autres charges de travail client ou pour hiérarchiser une charge de travail sur d'autres, elles fournissent également un bonus de collecte de metrics supplémentaires pour faciliter le contrôle.

Dans l'onglet de configuration, sélectionnez "classification du trafic" et créez une nouvelle stratégie. Attribuez un nom à la règle et sélectionnez le ou les compartiments ou le tenant comme type. Entrez le(s) nom(s) du ou des compartiments ou du tenant. Si la qualité de service est requise, définissez une limite, mais pour la plupart des implémentations, il convient d'ajouter les avantages en termes de surveillance, afin de ne pas fixer de limite.

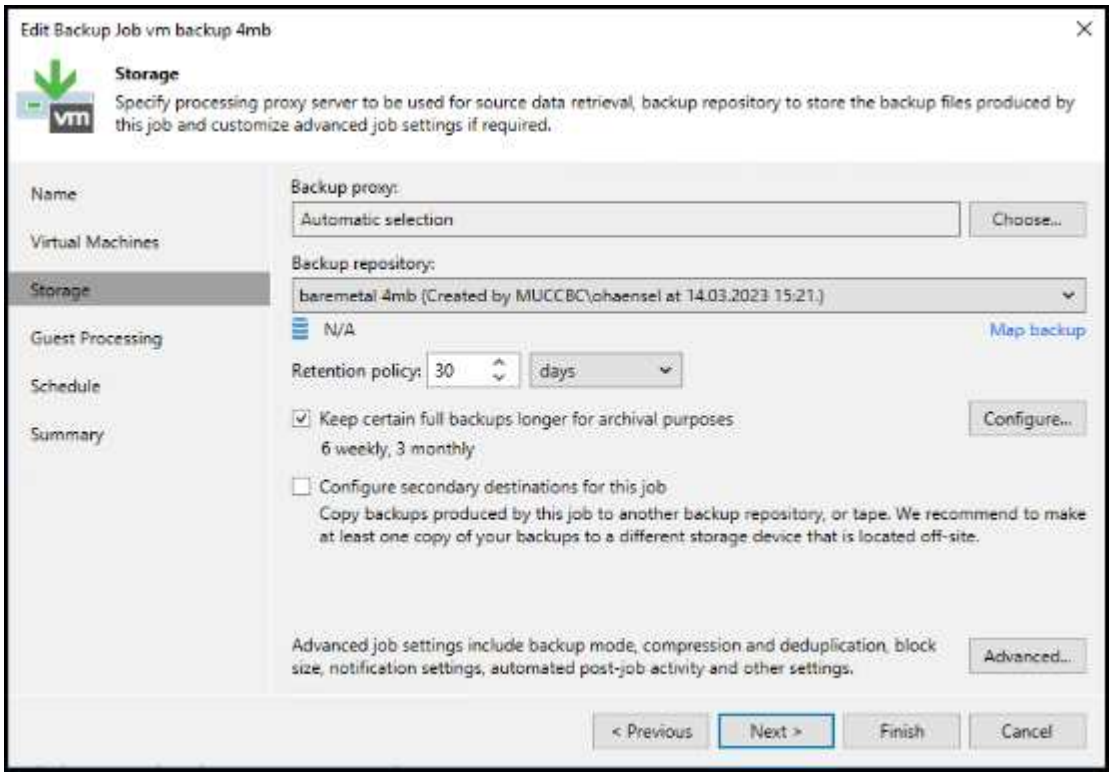


Veeam

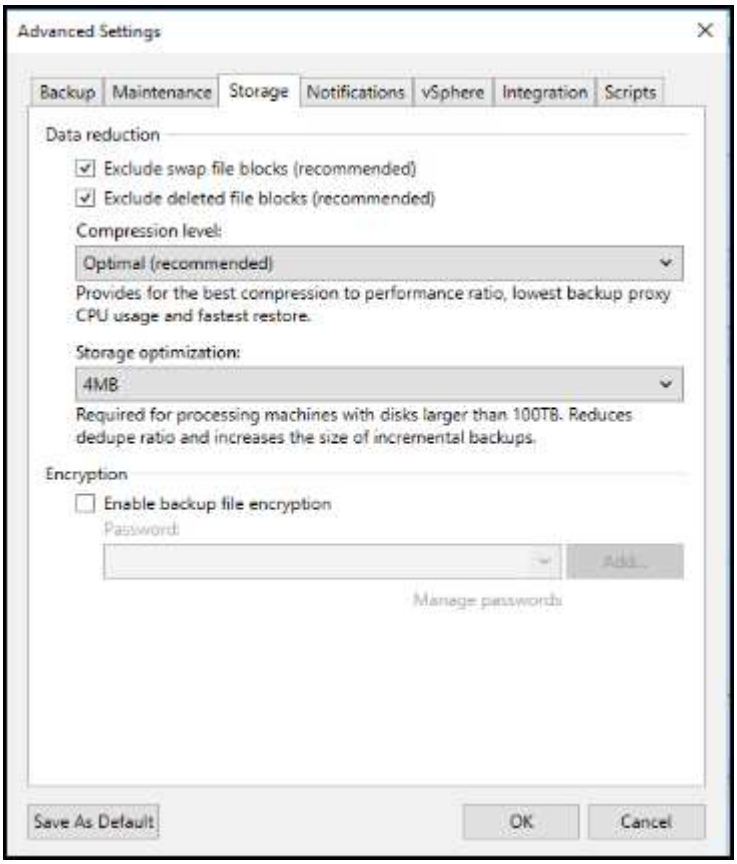
Selon le modèle et la quantité d'appliances StorageGRID, il peut être nécessaire de sélectionner et de configurer une limite au nombre d'opérations simultanées sur le compartiment.



Pour démarrer l'assistant, suivez la documentation Veeam sur la configuration des tâches de sauvegarde dans la console Veeam. Après avoir ajouté des machines virtuelles, sélectionnez le référentiel SOBR.



Cliquez sur Paramètres avancés et définissez les paramètres d'optimisation du stockage sur 4 Mo ou plus. La compression et la déduplication doivent être activées. Modifiez les paramètres invités en fonction de vos besoins et configurez la planification des tâches de sauvegarde.



Surveillance StorageGRID

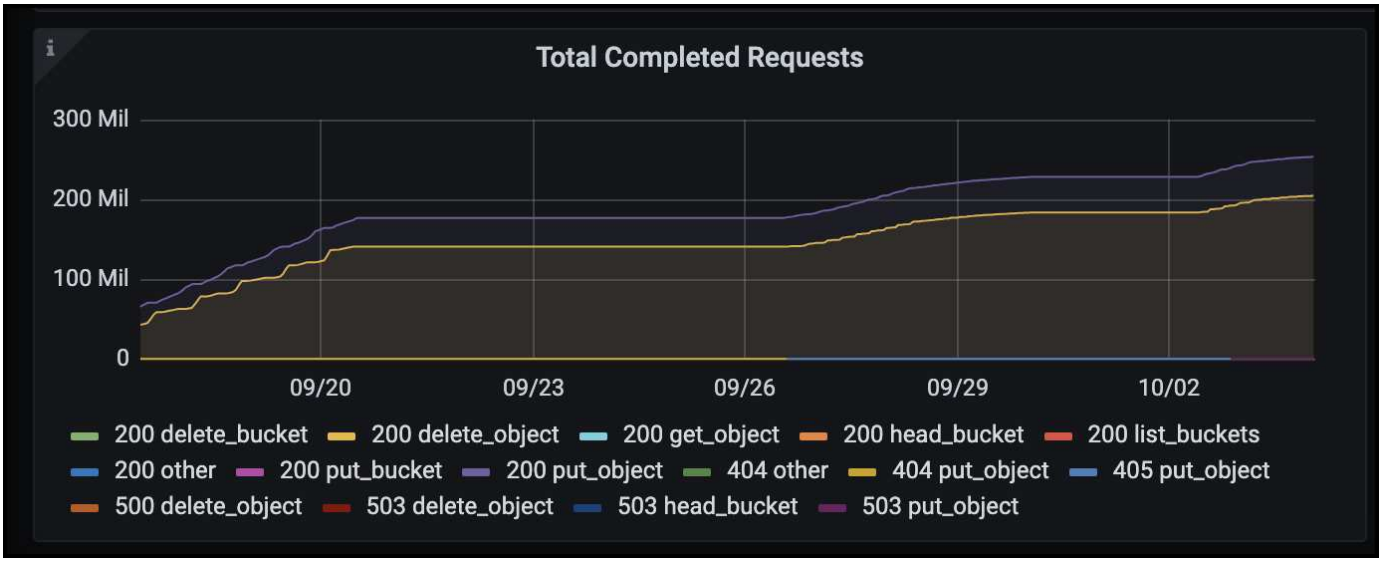
Pour obtenir une vue d'ensemble des performances de Veeam et StorageGRID, vous devez attendre l'expiration du délai de conservation des premières sauvegardes. Jusqu'à présent, la charge de travail Veeam se compose principalement d'opérations PUT et aucune suppression n'a eu lieu. Une fois que les données de sauvegarde arrivent à expiration et que les nettoyages sont en cours, vous pouvez voir l'utilisation cohérente complète du magasin d'objets et ajuster les paramètres dans Veeam, si nécessaire.

StorageGRID fournit des graphiques pratiques pour contrôler le fonctionnement du système, disponibles dans l'onglet support, page Metrics. Les principaux tableaux de bord à examiner seront la vue d'ensemble S3, ILM et la règle de classification du trafic si une règle a été créée. Vous trouverez dans le tableau de bord S3 des informations sur les taux d'opération S3, les latences et les réponses aux demandes.

Les taux S3 et les requêtes actives vous permettent de voir la charge que chaque nœud gère et le nombre total de requêtes par type.

Le graphique durée moyenne indique la durée moyenne de chaque nœud pour chaque type de demande. Il s'agit de la latence moyenne de la demande et peut être un bon indicateur qu'un réglage supplémentaire peut être nécessaire ou que le système StorageGRID peut prendre plus de charge.

Dans le tableau nombre total de demandes terminées, vous pouvez voir les demandes par type et par code de réponse. Si vous voyez des réponses autres que 200 (OK), cela peut indiquer un problème comme le système StorageGRID est fortement chargé et envoie 503 réponses (ralentissement) et un réglage supplémentaire peut être nécessaire, ou le temps est venu d'étendre le système pour augmenter la charge.



Le tableau de bord ILM vous permet de contrôler les performances de suppression de votre système StorageGRID. StorageGRID combine les suppressions synchrones et asynchrones sur chaque nœud afin d'essayer d'optimiser la performance globale de toutes les requêtes.

Dans le cadre d'une règle de classification du trafic, nous pouvons afficher des metrics sur le débit de la demande d'équilibrage de charge, les taux, la durée, ainsi que la taille des objets envoyés et reçus par Veeam.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- "Documentation du produit NetApp StorageGRID"
- "Sauvegarde et réplication Veeam"

Configurez la source de données Dremio avec StorageGRID

Par Angela Cheng

Dremio prend en charge la rareté des sources de données, y compris le stockage objet dans le cloud ou sur site. Vous pouvez configurer Dremio pour qu'il utilise StorageGRID comme source de données de stockage objet.

Configurer la source de données Dremio

Prérequis

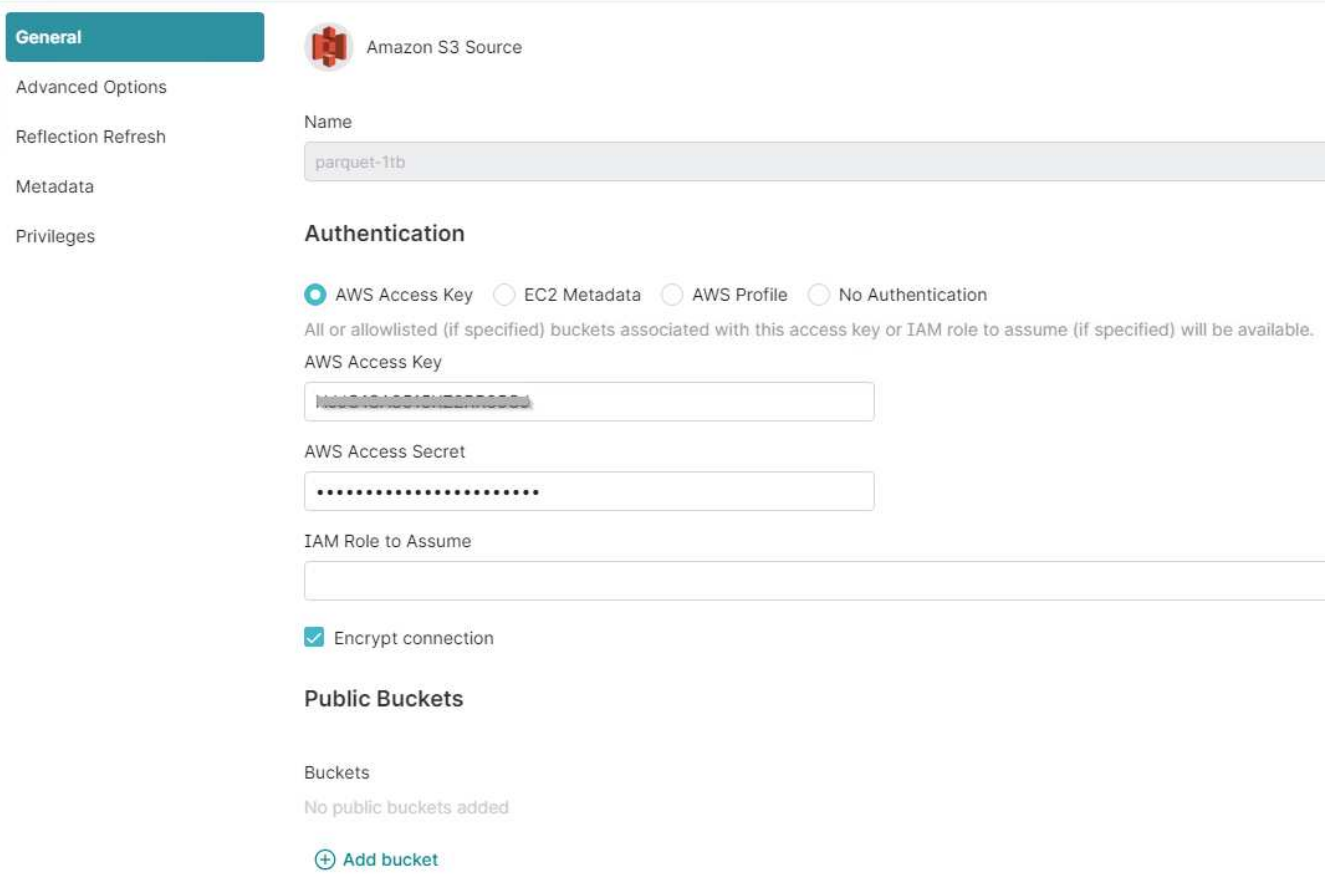
- URL de terminal StorageGRID S3, ID de clé d'accès s3 du locataire et clé d'accès secrète.
- Recommandation de configuration StorageGRID : désactivez la compression (désactivée par défaut). Dremio utilise la plage d'octets GET pour extraire simultanément différentes plages d'octets à partir du même objet pendant la requête. La taille type des demandes de plage d'octets est de 1 Mo. Les objets compressés dégradent les performances GET au niveau de la plage d'octets.

Guide Dremio

"Connexion à Amazon S3 : Configuration du stockage compatible avec S3".

Instructions

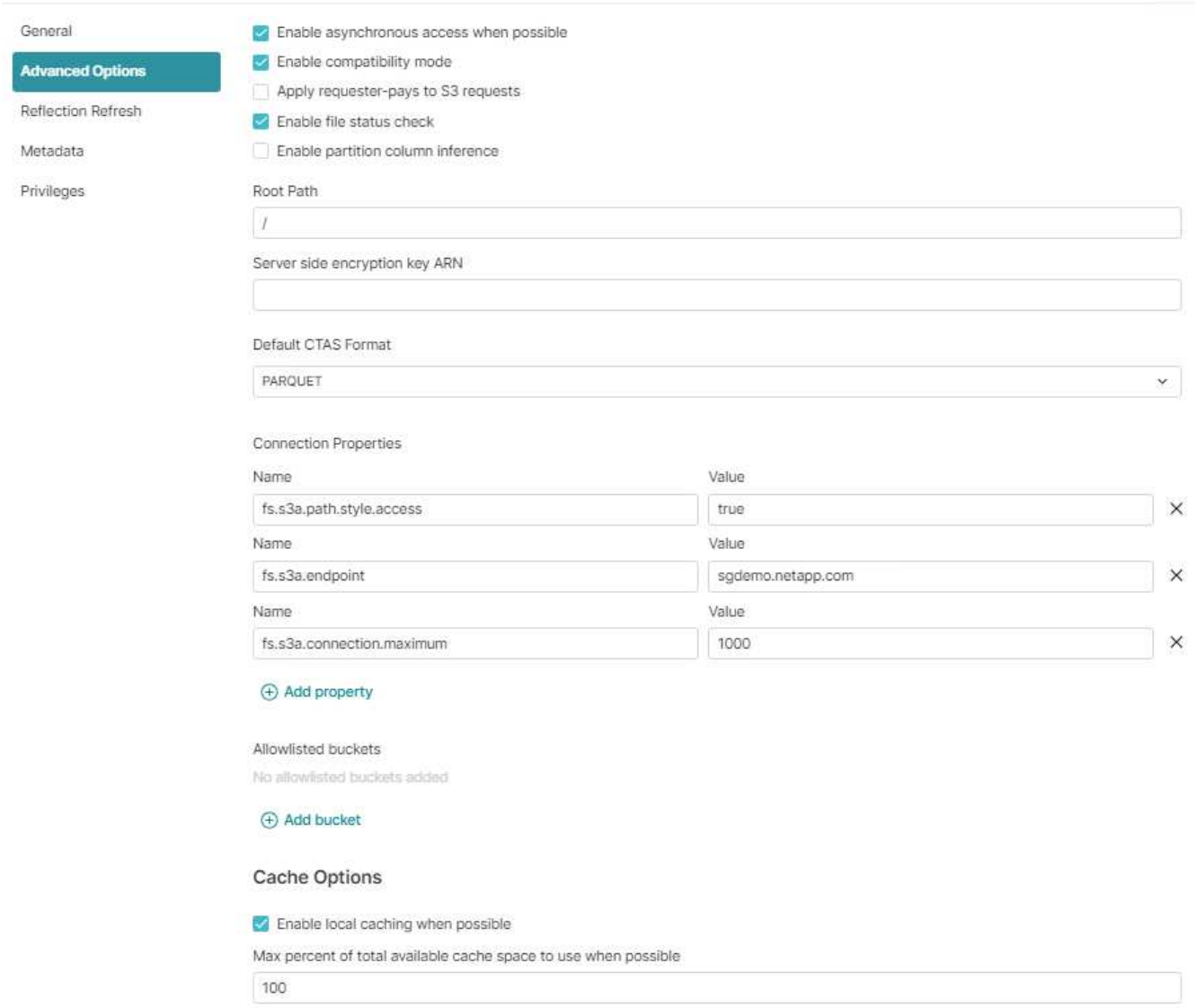
1. Sur la page Datasets Dremio, cliquez sur le signe + pour ajouter une source, sélectionnez 'Amazon S3'.
2. Entrez le nom de cette nouvelle source de données : ID de clé d'accès du locataire StorageGRID S3 et clé d'accès secrète.
3. Cochez la case « crypter la connexion » si vous utilisez https pour la connexion au terminal StorageGRID S3.
   Si vous utilisez un certificat CA auto-signé pour ce noeud final s3, suivez l'instructions du guide Dremio pour ajouter ce certificat CA dans <JAVA_HOME>/jre/lib/Security + du serveur Dremio
   Exemple de capture d'écran



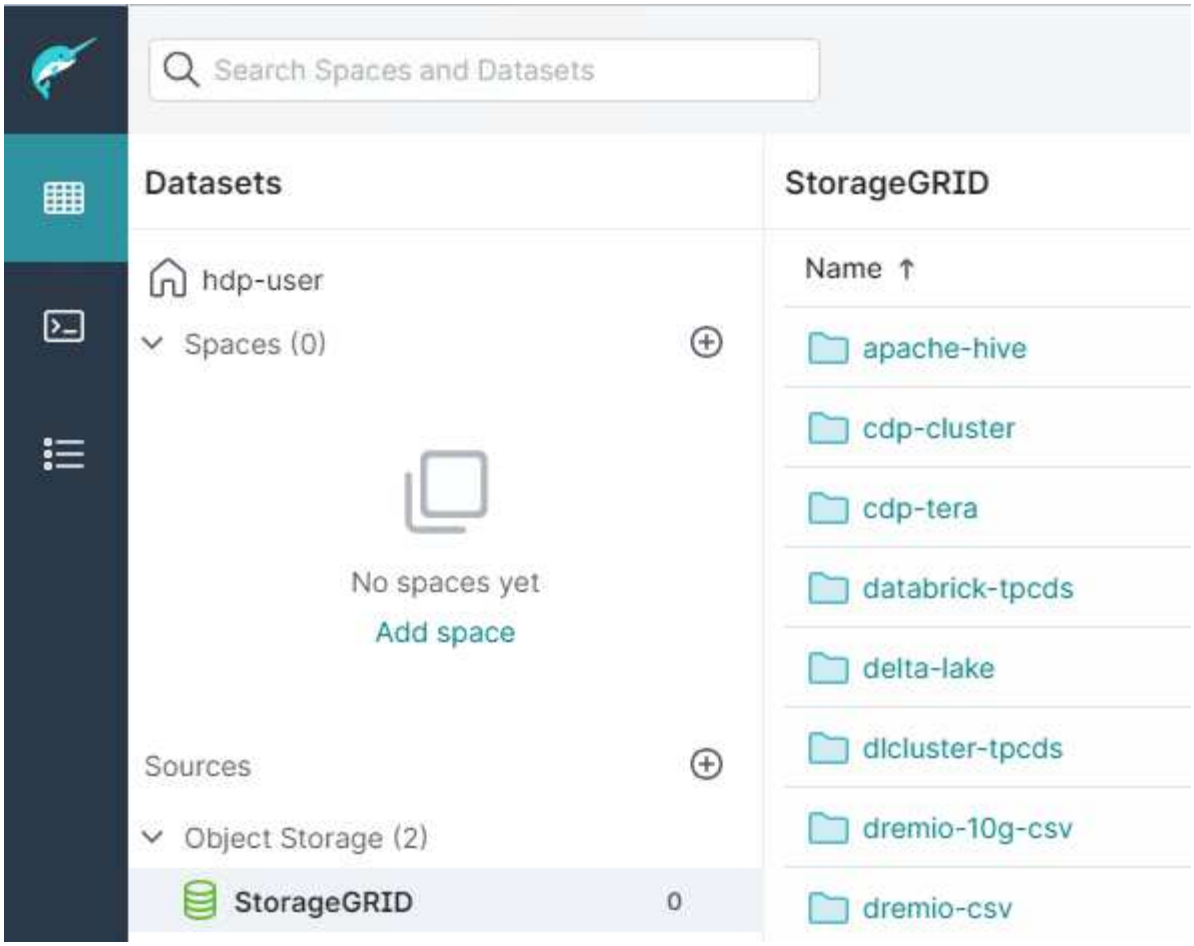
4. Cliquez sur « Options avancées », cochez « Activer le mode de compatibilité ».
5. Sous Propriétés de connexion, cliquez sur + Ajouter des propriétés et ajoutez ces propriétés s3a.
6. fs.s3a.connection.la valeur par défaut maximale est 100. Si vos datasets s3 incluent des fichiers de parquet volumineux comportant au moins 100 colonnes, vous devez entrer une valeur supérieure à 100. Reportez-vous au guide Dremio pour ce réglage.

Nom	Valeur
fs.s3a.endpoint	*<noeud final StorageGRID S3:port>*
fs.s3a.path.style.access	vrai
fs.s3a.connexion.maximum	*<une valeur supérieure à 100>*

Exemple de capture d'écran



7. Configurez les autres options de Dremio en fonction des besoins de votre organisation ou de vos applications.
8. Cliquez sur le bouton Enregistrer pour créer cette nouvelle source de données.
9. Une fois la source de données StorageGRID ajoutée, une liste de rubriques s'affiche dans le panneau de gauche.
   Exemple de capture d'écran



NetApp StorageGRID avec GitLab

Par Angela Cheng

NetApp a testé StorageGRID avec GitLab. Voir l'exemple de configuration GitLab ci-dessous. Reportez-vous à la section "Guide de configuration du stockage objet GitLab" pour plus d'informations.

Exemple de connexion de stockage objet

Pour les installations de package Linux, voici un exemple de `connection` configuration dans le formulaire consolidé. Modifier `/etc/gitlab/gitlab.rb` et ajoutez les lignes suivantes en remplaçant les valeurs souhaitées :

```
# 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'
```

Procédures et exemples d'API

Tester et démontrer les options de cryptage S3 sur StorageGRID

Par Aron Klein

StorageGRID et l'API S3 proposent plusieurs façons de chiffrer vos données au repos. Pour en savoir plus, voir "Étudiez les méthodes de cryptage StorageGRID".

Ce guide présente les méthodes de chiffrement de l'API S3.

Chiffrement côté serveur (SSE)

SSE permet au client de stocker un objet et de le chiffrer à l'aide d'une clé unique gérée par StorageGRID. Lorsque l'objet est demandé, il est décrypté par la clé stockée dans StorageGRID.

Exemple SSE

- PLACER un objet avec SSE

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

- DIRIGEZ l'objet pour vérifier le chiffrement

```
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": {}
}
```

- OBTENIR l'objet

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

Chiffrement côté serveur avec clés fournies par le client (SSE-C)

SSE permet au client de stocker un objet et de le chiffrer à l'aide d'une clé unique fournie par le client avec l'objet. Lorsque l'objet est demandé, la même clé doit être fournie pour décrypter et renvoyer l'objet.

Exemple SSE-C.

- Vous pouvez créer une clé de chiffrement à des fins de test ou de démonstration
  - Créez une clé de chiffrement

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

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

- Placer un objet avec la clé générée

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

- Dirigez l'objet

```
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=="
}
```

Si vous ne fournissez pas la clé de cryptage, vous recevrez une erreur « une erreur s'est produite (404) lors de l'appel de l'opération HeadObject : introuvable ».

- Obtenir l'objet

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

> Si vous ne fournissez pas la clé de cryptage, vous recevrez une erreur "une erreur s'est produite (InvalidRequest) lors de l'appel de l'opération GetObject: L'objet a été stocké à l'aide d'une forme de chiffrement côté serveur. Les paramètres corrects doivent être fournis pour récupérer l'objet. »

Chiffrement côté serveur godet (SSE-S3)

SSE-S3 permet au client de définir un comportement de cryptage par défaut pour tous les objets stockés dans un compartiment. Les objets sont chiffrés avec une clé unique gérée par StorageGRID. À la demande de l'objet, celui-ci est décrypté par la clé stockée dans StorageGRID.

Exemple de godet SSE-S3

- Créez un compartiment et définissez une règle de chiffrement par défaut
  - Créer un nouveau compartiment

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

  - Put bucket Encryption

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

- Placer un objet dans le godet

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

- Dirigez l'objet

```
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": {}
}
```

- OBTENIR l'objet

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

Testez et faites une démonstration du verrouillage d'objet S3 sur StorageGRID

Par Aron Klein

Le verrouillage d'objet fournit un modèle WORM pour éviter que les objets ne soient supprimés ou remplacés. L'implémentation StorageGRID du verrouillage d'objet est une fonctionnalité qui est évaluée afin de respecter les exigences réglementaires, et qui prend en charge le mode de conservation légale et de conformité pour la conservation des objets et les règles de conservation des compartiments par défaut.

Ce guide présente l'API de verrouillage d'objet S3.

Obligation légale

- La mise en attente légale de verrouillage d'objet est un état activé/désactivé simple appliqué à un objet.

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

- Vérifiez-le avec une opération GET.

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

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

- Désactiver la mise en attente légale

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

- Vérifiez-le avec une opération GET.

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

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

Mode de conformité

- La conservation de l'objet s'effectue avec une conservation jusqu'à l'horodatage.

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

- Vérifiez l'état de la rétention

```
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"
    }
}
```

Conservation par défaut

- Définissez la période de conservation en jours et années par rapport à une date de conservation définie avec l'api par objet.

```
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
```

- Vérifiez l'état de la rétention

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

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

- Placer un objet dans le godet

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

- La durée de conservation définie dans le compartiment est convertie en horodatage de conservation sur l'objet.

```
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"
    }
}
```

Test de la suppression d'un objet avec une rétention définie

Le verrouillage d'objet est basé sur la gestion des versions. La conservation est définie sur une version de l'objet. Si une tentative de suppression d'un objet avec une rétention définie et qu'aucune version n'est spécifiée, un marqueur de suppression est créé comme version actuelle de l'objet.

- Supprimez l'objet dont la conservation est définie

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

- Lister les objets dans le compartiment

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

  - Notez que l'objet n'est pas répertorié.
- Répertorier les versions pour voir le marqueur de suppression et la version verrouillée d'origine

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

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

- Supprimer la version verrouillée de l'objet

```
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
```

Stratégies et autorisations dans StorageGRID

Voici des exemples de règles et d'autorisations dans StorageGRID S3.

Structure d'une politique

Dans StorageGRID, les règles de groupe sont identiques aux règles de service S3 de l'utilisateur AWS (IAM).

Les stratégies de groupe sont requises dans StorageGRID. Un utilisateur avec des clés d'accès S3, mais qui n'est pas affecté à un groupe d'utilisateurs, ou affecté à un groupe sans règle lui accordant certaines autorisations, ne pourra accéder à aucune donnée.

Les règles de compartiment et de groupe partagent la plupart des mêmes éléments. Les stratégies sont créées au format json et peuvent être générées à l'aide de "Générateur de règles AWS"

Toutes les règles définissent l'effet, les actions et les ressources. Les règles de compartiment définiront également un principal.

Effet sera soit permettre ou refuser la demande.

Le **principal**

- S'applique uniquement aux politiques de compartiment.
- L'entité de sécurité est le(s) compte(s)/utilisateur(s) auquel(s) les autorisations ont été accordées ou refusées.
- Peut être défini comme :
  - Un caractère générique "+*"

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

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

  - ID de locataire pour tous les utilisateurs d'un locataire (équivalent au compte AWS)

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

  - Utilisateur (local ou fédéré depuis le locataire où réside le compartiment ou un autre locataire de la grille)

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

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

- Un groupe (local ou fédéré depuis le locataire où réside le compartiment ou un autre locataire de la grille).

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

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

Action est l'ensemble des opérations S3 accordées ou refusées aux utilisateurs.

> Pour les stratégies de groupe, l'action s3:ListBucket autorisée est requise pour que les utilisateurs puissent exécuter n'importe quelle action S3.

La ressource **Resource** est le compartiment ou les compartiments auxquels les principaux ont été accordés ou refusés la capacité d'exécuter les actions sur. En option, il peut y avoir une **condition** lorsque l'action de stratégie est valide.

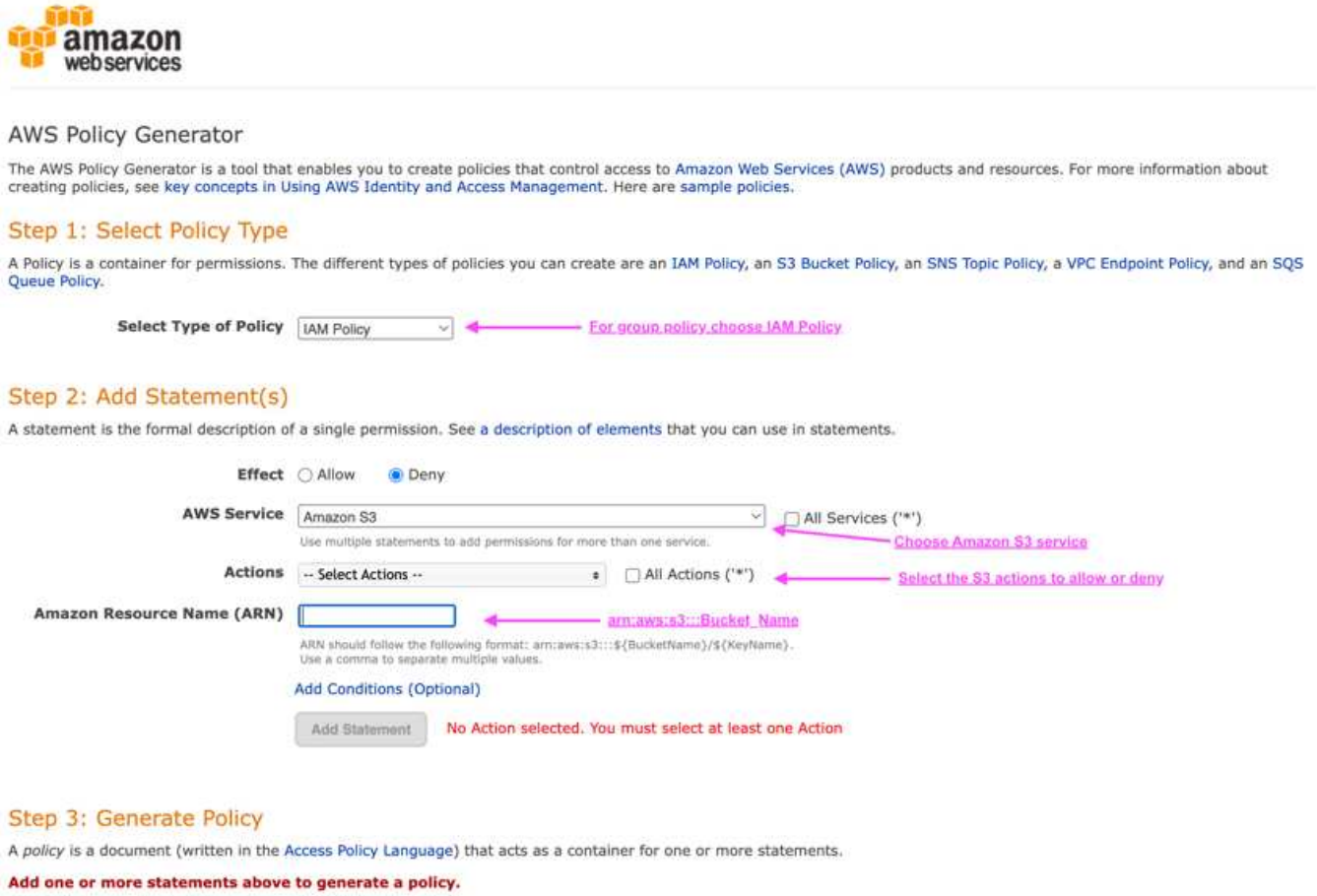
Le format de la politique JSON se présente comme suit :

```
{
  "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/*"
      ],
    }
  ]
}
```

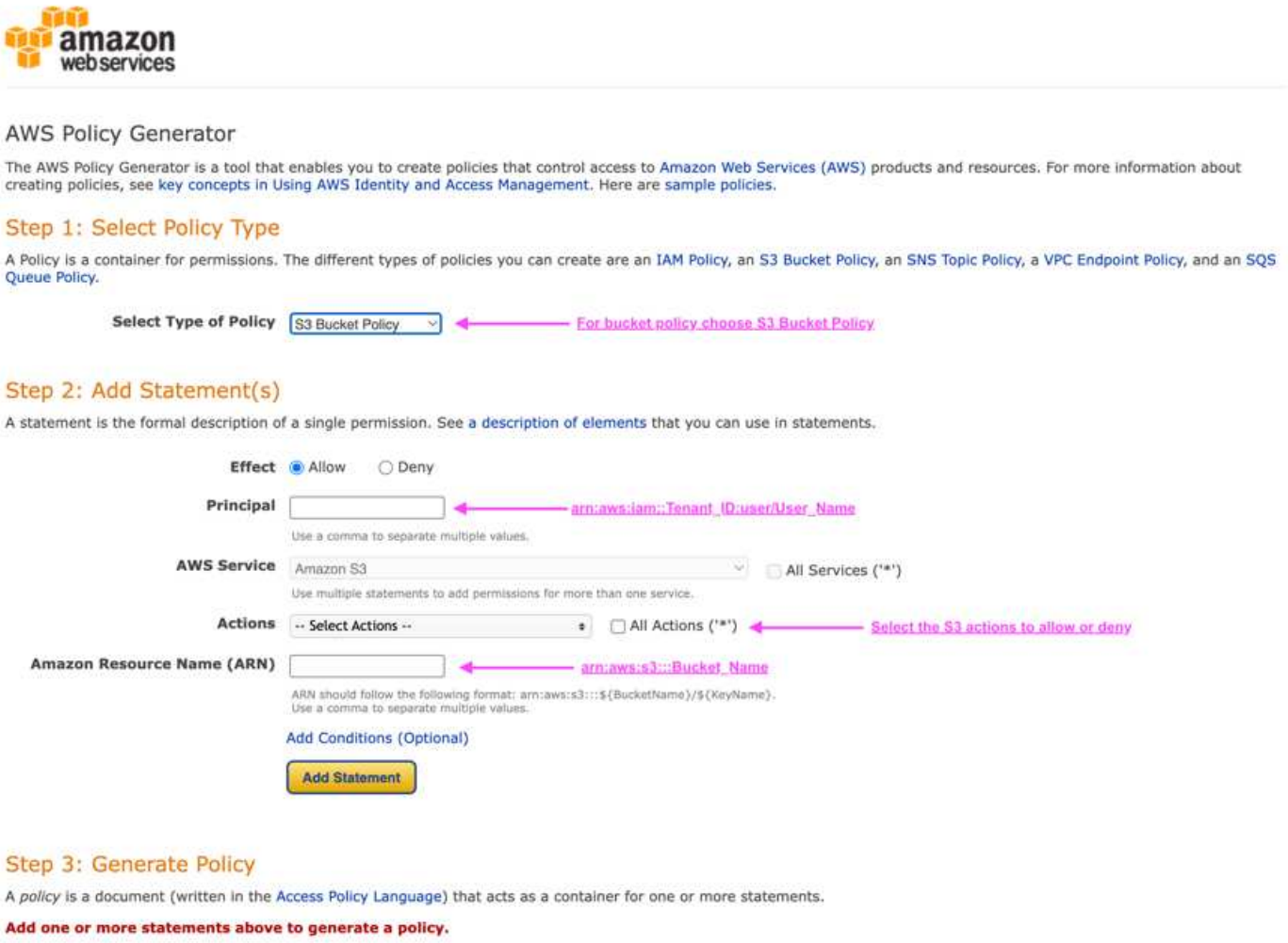
À l'aide du générateur de règles AWS

Le générateur de règles AWS est un excellent outil pour vous aider à obtenir le code json avec le format et les informations que vous essayez d'implémenter.

Pour générer les autorisations d'une stratégie de groupe StorageGRID : * Choisissez la stratégie IAM pour le type de stratégie. * Sélectionnez le bouton pour l'effet désiré - Autoriser ou refuser. Il est recommandé de démarrer vos stratégies avec les autorisations de refus, puis d'ajouter les autorisations d'autorisation * dans la liste déroulante actions, cliquez sur la case en regard du nombre d'actions S3 que vous souhaitez inclure dans cette autorisation ou dans la zone « toutes les actions ». * Tapez les chemins de compartiment dans la zone Amazon Resource Name (ARN). Incluez "arn:aws:s3:::" avant le nom du compartiment. Ex. « arn:aws:s3:::example_bucket »

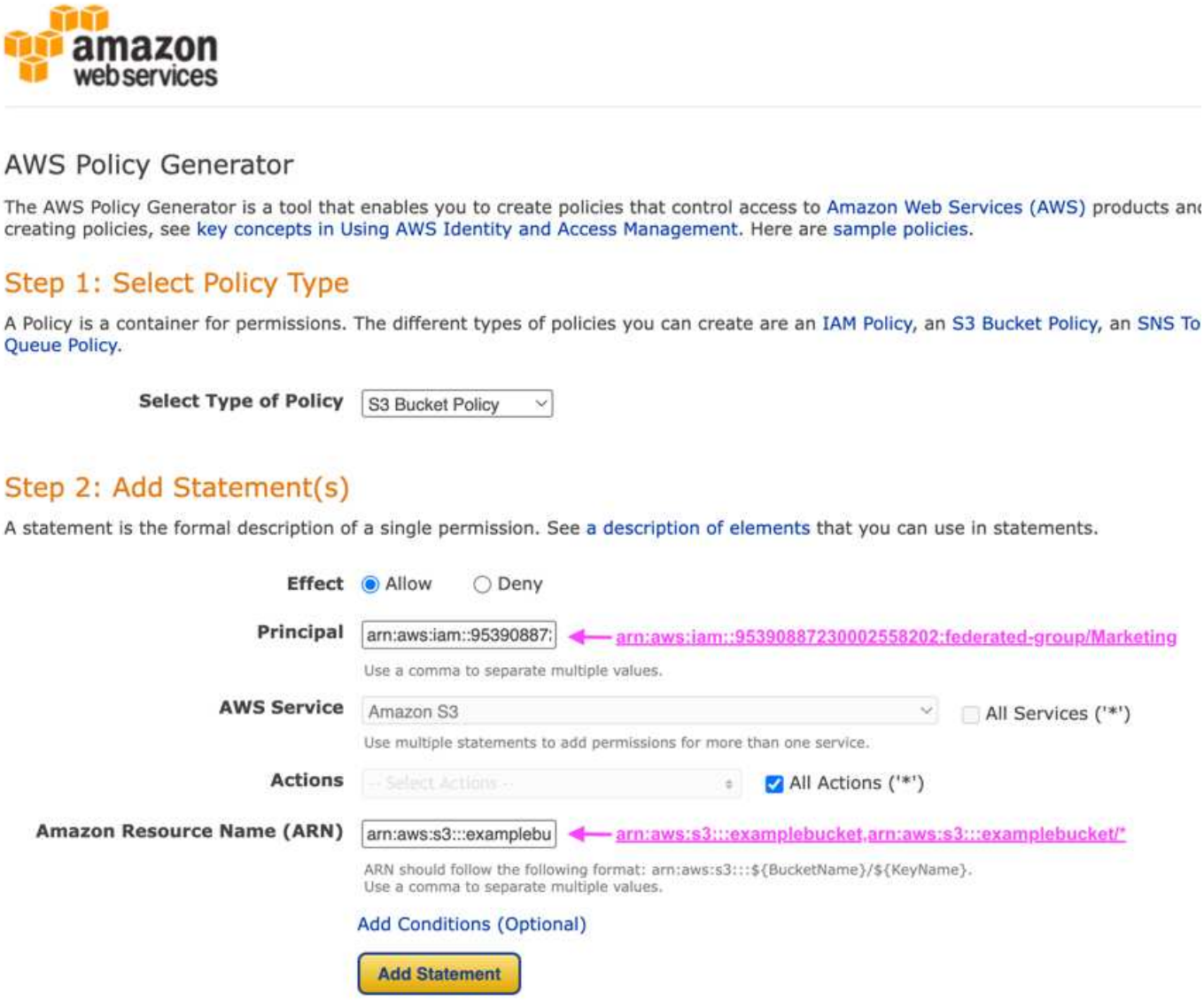


Pour générer les autorisations d'une règle de compartiment : * Choisissez la règle de compartiment S3 pour le type de règle. * Sélectionnez le bouton pour l'effet désiré - Autoriser ou refuser. Il est recommandé de démarrer vos stratégies avec les autorisations refuser, puis d'ajouter le type Autoriser les autorisations * dans les informations sur l'utilisateur ou le groupe pour le principal. * Dans la liste déroulante actions, cliquez sur la case en regard du nombre d'actions S3 que vous souhaitez inclure dans cette autorisation ou de la case « toutes les actions ». * Tapez les chemins de compartiment dans la zone Amazon Resource Name (ARN). Incluez "arn:aws:s3:::" avant le nom du compartiment. Ex. « arn:aws:s3:::example_bucket »



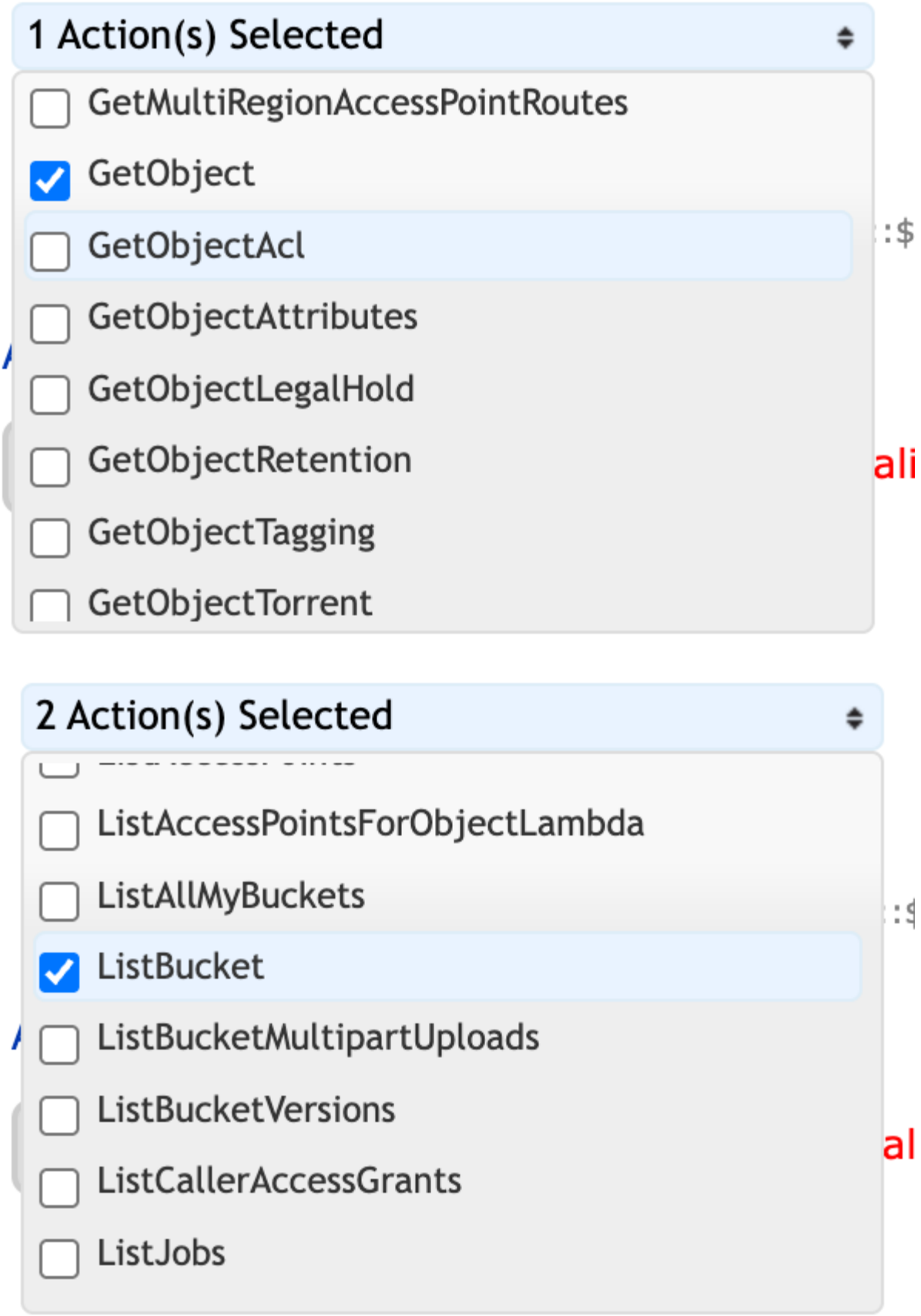
Par exemple, si vous souhaitez générer une stratégie de compartiment pour permettre à tous les utilisateurs d'effectuer des opérations GetObject sur tous les objets du compartiment, alors que seuls les utilisateurs appartenant au groupe « Marketing » du compte spécifié disposent d'un accès complet.

- Sélectionnez S3 Bucket Policy comme type de règle.
- Choisissez l'effet d'autorisation
- Entrez les informations du groupe Marketing - arn:aws:iam::95390887230002558202:Federated-group/Marketing
- Cliquez sur la case « toutes les actions ».
- Entrez les informations relatives au compartiment - arn:aws:s3:::example_bucket,arn:aws:s3:::example_bucket/*



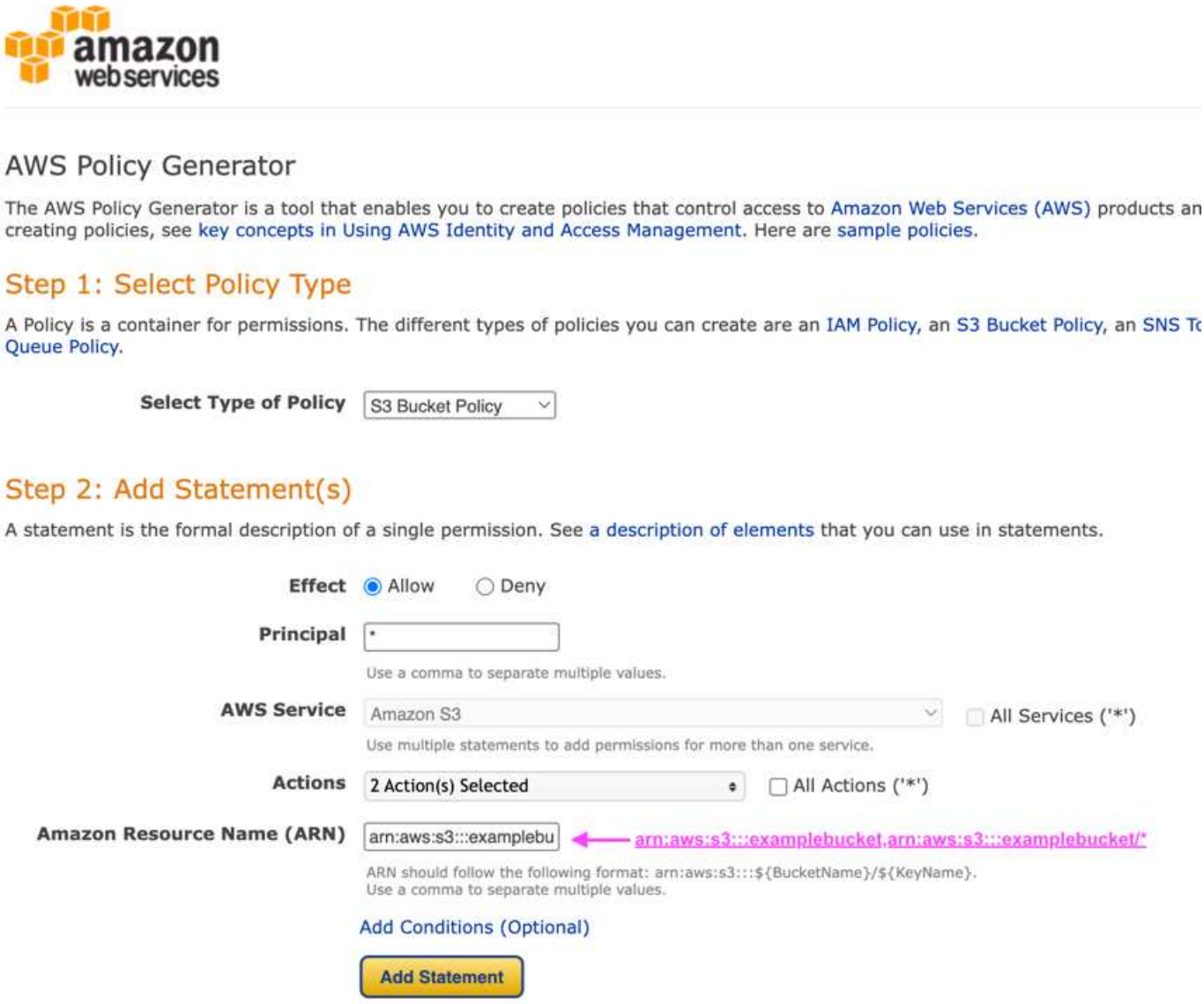
- Cliquez sur le bouton « Ajouter une déclaration »

- Choisissez l'effet d'autorisation
- Entrez l'astérisque +* pour tout le monde
- Cliquez sur la case en regard des actions GetObject et ListBucket »



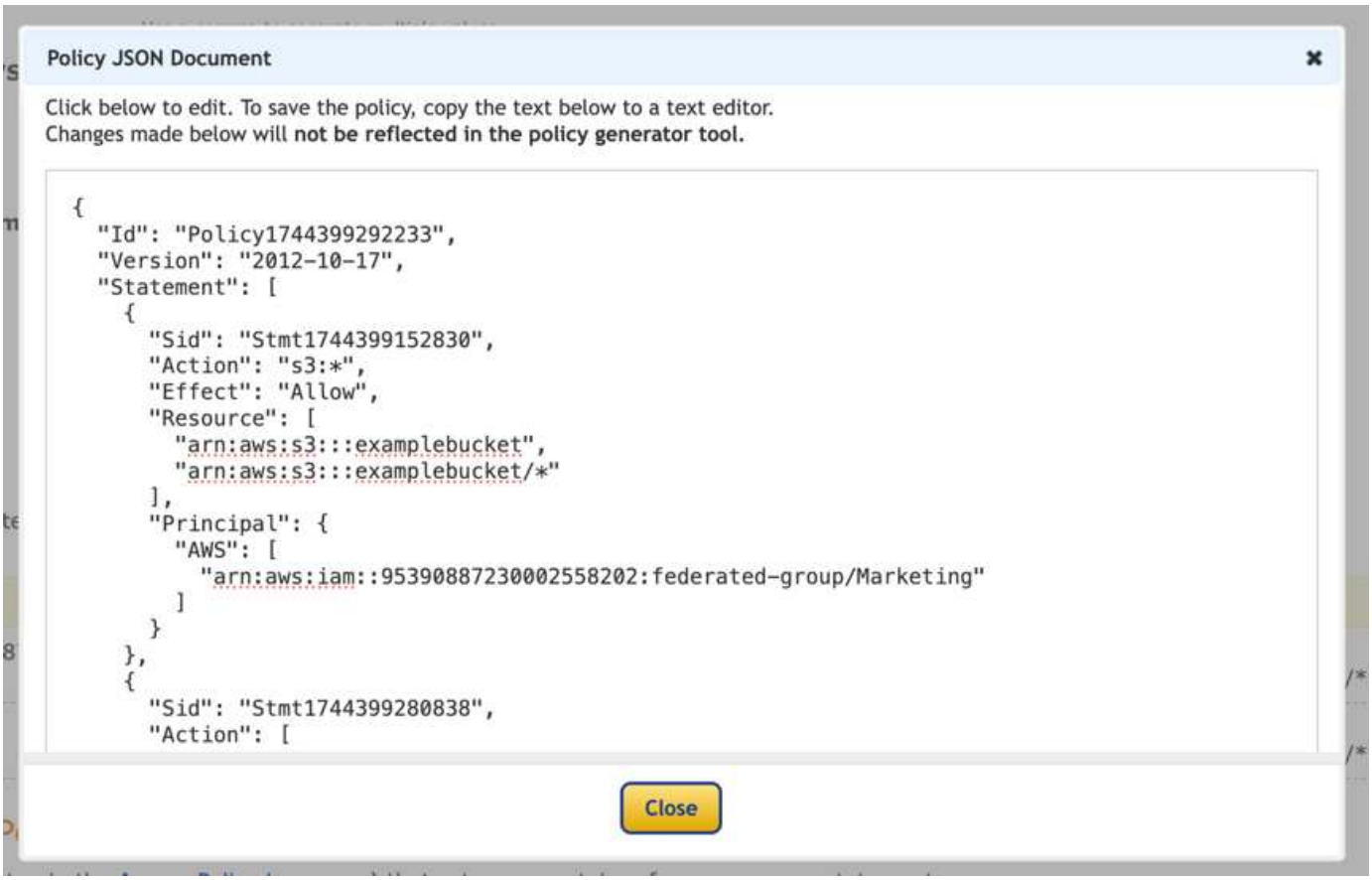
- Entrez les informations relatives au compartiment -

arn:aws:s3:::example_bucket,arn:aws:s3:::example_bucket/*



- Cliquez sur le bouton « Ajouter une déclaration »

- Cliquez sur le bouton « générer une politique » et une fenêtre contextuelle s'affiche avec votre police générée.



- Copiez le texte Json complet qui devrait ressembler à ceci :

```
{
  "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": "*"
    }
  ]
}
```

Ce Json peut être utilisé tel quelle, ou vous pouvez supprimer les lignes ID et version au-dessus de la ligne « Statement » et vous pouvez personnaliser l'ID pour chaque autorisation avec un titre plus significatif pour chaque autorisation ou elles peuvent également être supprimées.

Par exemple :

```
{
  "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": "*"
    }
  ]
}
```

Stratégies de groupe (IAM)

Accès au compartiment de style Home Directory

Cette stratégie de groupe autorise uniquement les utilisateurs à accéder aux objets du compartiment nommé nom d'utilisateur utilisateurs.

```
{
"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}/*"
    }

  ]
}
```

Refuser la création de compartiments de verrouillage d'objet

Cette stratégie de groupe empêche les utilisateurs de créer un compartiment avec le verrouillage d'objet activé sur le compartiment.

> Cette règle n'est pas appliquée dans l'interface utilisateur de StorageGRID et elle n'est appliquée que par l'API S3.

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

Limite de conservation du verrouillage des objets

Cette stratégie de compartiment limite la durée de conservation du verrouillage de l'objet à 10 jours ou moins

```
{
 "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"
      }
    }
   }
  ]
}
```

Empêcher les utilisateurs de supprimer des objets par ID de version

Cette stratégie de groupe empêche les utilisateurs de supprimer des objets multiversion par ID de version

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

Limiter un groupe à un sous-répertoire unique (préfixe) avec accès en lecture seule

Cette règle permet aux membres du groupe d'accéder en lecture seule à un sous-répertoire (préfixe) au sein d'un compartiment. Le nom du compartiment est « Study » et le sous-répertoire est « 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/*"
            ]
        }
    ]
}
```

Règles de compartiment

Restriction du compartiment à un seul utilisateur avec un accès en lecture seule

Cette stratégie permet à un seul utilisateur de disposer d'un accès en lecture seule à un compartiment et d'accéder explicitement à tous les autres utilisateurs. Le regroupement des déclarations de refus en haut de la politique est une bonne pratique pour une évaluation plus rapide.

```
{
    "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/*"
            ]
        }
    ]
}
```

limitez un compartiment à quelques utilisateurs disposant d'un accès en lecture seule.

```
{
    "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/*"
        ]
      }
    ]
}
```

Limitez les suppressions d'objets multiversion par l'utilisateur dans un compartiment

Cette stratégie de compartiment empêche un utilisateur (identifié par l'ID utilisateur « 56622399308951294926 ») de supprimer des objets multiversion par l'ID de version

```
{
  "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"
        ]
      }
    }
  ]
}
```

Cycle de vie du bucket dans StorageGRID

Vous pouvez créer une configuration de cycle de vie S3 afin de contrôler la suppression d'objets spécifiques du système StorageGRID.

Qu'est-ce qu'une configuration de cycle de vie

La configuration du cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle indique quels objets sont affectés et quand ces objets vont expirer (à une date spécifique ou après un certain nombre de jours).

Chaque objet respecte les paramètres de conservation du cycle de vie d'un compartiment S3 ou une règle ILM. Lorsqu'un cycle de vie d'un compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la règle ILM pour les objets correspondant au filtre de cycle de vie du compartiment. Les objets qui ne correspondent pas au filtre de cycle de vie des compartiments utilisent les paramètres de conservation de

la règle ILM. Si un objet correspond à un filtre de cycle de vie de compartiment et qu'aucune action d'expiration n'est explicitement spécifiée, les paramètres de conservation de la règle ILM ne sont pas utilisés et les versions d'objet sont conservées indéfiniment.

Par conséquent, il est possible de supprimer un objet de la grille, même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Ou bien, un objet peut être conservé sur la grille même après l'expiration des instructions de placement ILM pour l'objet.

StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants :

- Expiration : supprimez un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à partir de l'ingestion de l'objet.
- NonactuelVersionExexpiration : supprimez un objet lorsque le nombre de jours spécifié est atteint, à partir de quand l'objet est devenu non courant.
- Filtre (préfixe, étiquette)
- Statut *ID

StorageGRID prend en charge les opérations suivantes des compartiments pour gérer les configurations du cycle de vie :

- DeleteBuckeLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Structure d'une politique de cycle de vie

Comme première étape de la création de la configuration du cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON contient trois règles, comme suit :

1. La **Règle 1** s'applique uniquement aux objets correspondant au préfixe category1/ et dont la valeur key2 est tag2. Le paramètre Expiration spécifie que les objets correspondant au filtre expireront à minuit le 22 août 2020.
2. La **Règle 2** s'applique uniquement aux objets correspondant au préfixe category2/. Le paramètre Expiration spécifie que les objets correspondant au filtre expireront 100 jours après leur ingestion.

   > Les règles spécifiant un nombre de jours sont relatives à l'ingestion de l'objet. Si la date actuelle dépasse la date d'ingestion et le nombre de jours, certains objets peuvent être supprimés du compartiment dès que la configuration de cycle de vie est appliquée.

3. La **Règle 3** s'applique uniquement aux objets correspondant au préfixe category3/. Le paramètre Expiration spécifie que toute version obsolète des objets correspondants expirera 50 jours après sa date d'expiration.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Appliquez la configuration du cycle de vie au compartiment

Après avoir créé le fichier de configuration du cycle de vie, vous l'appliquez à un compartiment en émettant une demande PutBucketLifecycleConfiguration.

Cette requête applique la configuration de cycle de vie du fichier d'exemple aux objets d'un compartiment nommé `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour vérifier qu'une configuration de cycle de vie a été correctement appliquée au compartiment, exécutez une demande GetBucketLifecycleConfiguration. Par exemple :

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Exemples de politiques de cycle de vie pour les buckets standard (non versionnés)

Supprimer les objets après 90 jours

Cas d'utilisation : Cette stratégie est idéale pour gérer les données pertinentes pendant une durée limitée, telles que les fichiers temporaires, les journaux ou les données de traitement intermédiaire. Avantage : Réduisez les coûts de stockage et assurez-vous que le bucket est épuré.

```
{
    "Rules": [
      {
        "ID": "Delete after 90 day rule",
        "Filter": {},
        "Status": "Enabled",
          "Expiration": {
              "Days": 90
        }
      }
    ]
}
```

Exemples de politiques de cycle de vie pour les buckets versionnés

Supprimer les versions non actuelles après 10 jours

Cas d'utilisation : Cette stratégie permet de gérer le stockage des objets de version obsolète, qui peuvent s'accumuler au fil du temps et consommer un espace important. Avantage : Optimisez l'utilisation du stockage

en conservant uniquement la version la plus récente.

```
{
    "Rules": [
            {
        "ID": "NoncurrentVersionExpiration 10 day rule",
        "Filter": {},
        "Status": "Enabled",
          "NoncurrentVersionExpiration": {
              "NoncurrentDays": 10
        }
    }
    ]
}
```

Conserver 5 versions non actuelles

Cas d'utilisation : utile lorsque vous souhaitez conserver un nombre limité de versions précédentes à des fins de récupération ou d'audit. Avantage : conservez suffisamment de versions non actuelles pour garantir un historique et des points de récupération suffisants.

```
{
    "Rules": [
      {
        "ID": "NewerNoncurrentVersions 5 version rule",
        "Filter": {},
        "Status": "Enabled",
        "NoncurrentVersionExpiration": {
            "NewerNoncurrentVersions": 5
        }
    }
    ]
}
```

Supprimer les marqueurs de suppression lorsqu'aucune autre version n'existe

Cas d'utilisation : Cette politique permet de gérer les marqueurs de suppression restants après la suppression de toutes les versions obsolètes, qui peuvent s'accumuler au fil du temps. Avantage : Réduit l'encombrement inutile.

```
{
    "Rules": [
    {
        "ID": "Delete marker cleanup rule",
        "Filter": {},
        "Status": "Enabled",
        "Expiration": {
        "ExpiredObjectDeleteMarker": true
        }
    }
    ]
}
```

Supprimez les versions actuelles après 30 jours, supprimez les versions non actuelles après 60 jours et supprimez les marqueurs de suppression créés par la suppression de la version actuelle une fois qu'aucune autre version n'existe.

Cas d'utilisation : Fournir un cycle de vie complet pour les versions actuelles et obsolètes, y compris les marqueurs de suppression. Avantage : Réduire les coûts de stockage et garantir un bucket épuré tout en conservant suffisamment de points de récupération et d'historique.

```
{
  "Rules": [
    {
      "ID": "Delete current version",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "Days": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 60
      }
    },
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    }
  ]
}
```

supprimez les marqueurs de suppression qui n'ont pas d'autres versions, conservez 4 versions non actuelles et au moins 30 jours d'historique pour les objets avec le préfixe « accounts_ » et conservez 2 versions et au moins 10 jours d'historique pour toutes les autres versions d'objet.

Cas d'utilisation : Fournissez des règles uniques pour des objets spécifiques, en plus d'autres objets, afin de gérer l'intégralité du cycle de vie des versions actuelles et obsolètes, y compris les marqueurs de suppression. Avantage : Réduisez les coûts de stockage et assurez-vous que le bucket est épuré, tout en conservant suffisamment de points de récupération et d'historique pour répondre aux différents besoins des clients.

```
{
  "Rules": [
    {
      "ID": "Markers",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {
        "ExpiredObjectDeleteMarker": true
      }
    },
    {
      "ID": "accounts version retention",
      "Filter": {"Prefix":"account_"},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 4,
        "NoncurrentDays": 30
      }
    },
    {
      "ID": "noncurrent version retention",
      "Filter": {},
      "Status": "Enabled",
      "NoncurrentVersionExpiration": {
        "NewerNoncurrentVersions": 2,
        "NoncurrentDays": 10
      }
    }
  ]
}
```

Conclusion

- Examinez et mettez à jour régulièrement les politiques de cycle de vie et alignez-les sur les objectifs de gestion ILM et de gestion des données.
- Testez les politiques dans un environnement ou un compartiment hors production avant de les appliquer à grande échelle pour vous assurer qu'elles fonctionnent comme prévu
- Utilisez des identifiants descriptifs pour les règles afin de les rendre plus intuitives, car la structure logique peut devenir complexe
- Surveillez l'impact de ces politiques de cycle de vie de bucket sur l'utilisation et les performances du stockage pour effectuer les ajustements nécessaires.

Rapports techniques

Présentation des rapports techniques de StorageGRID

NetApp StorageGRID est une suite de stockage objet Software-defined qui prend en charge un large éventail d'utilisations dans les environnements multiclouds publics, privés et hybrides. StorageGRID offre une prise en charge native de l'API Amazon S3 et propose des innovations de pointe, telles que la gestion automatisée du cycle de vie, pour stocker, sécuriser, protéger et conserver les données non structurées de manière économique sur de longues périodes.

StorageGRID fournit une documentation qui couvre les bonnes pratiques et les recommandations pour plusieurs fonctionnalités et intégrations StorageGRID.

NetApp StorageGRID et l'analytique Big Data

Utilisations de NetApp StorageGRID

La solution de stockage objet NetApp StorageGRID offre évolutivité, disponibilité des données, sécurité et hautes performances. Les entreprises de toutes tailles et de tous secteurs utilisent StorageGRID S3 pour un large éventail d'utilisations. Étudions quelques scénarios types :

Analytique Big Data : StorageGRID S3 est fréquemment utilisé comme data Lake, où les entreprises stockent de grandes quantités de données structurées et non structurées à des fins d'analyse à l'aide d'outils tels que Apache Spark, Splunk Smartstore et Dremio.

Tiering des données : les clients NetApp utilisent la fonctionnalité FabricPool d'ONTAP pour déplacer automatiquement les données entre un niveau local haute performance et StorageGRID. Le Tiering libère un stockage Flash coûteux pour les données actives tout en maintenant les données inactives disponibles dans un stockage objet à faible coût. Cela optimise les performances et les économies.

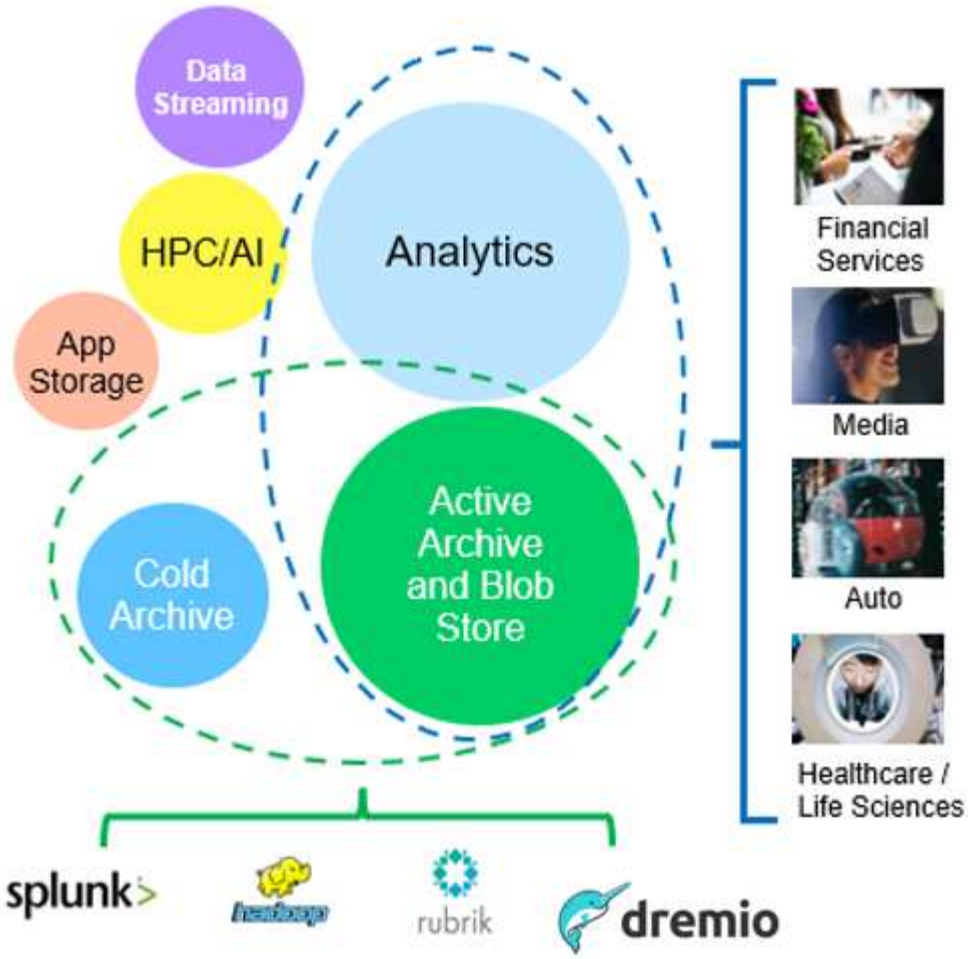
Sauvegarde des données et reprise après incident : les entreprises peuvent utiliser StorageGRID S3 comme une solution fiable et économique pour sauvegarder des données critiques et les restaurer en cas d'incident.

Stockage des données pour les applications : StorageGRID S3 peut être utilisé comme backend de stockage pour les applications, ce qui permet aux développeurs de stocker et de récupérer facilement des fichiers, des images, des vidéos et d'autres types de données.

Diffusion de contenu : StorageGRID S3 peut être utilisé pour stocker et fournir aux utilisateurs du monde entier du contenu statique, des fichiers multimédias et des téléchargements logiciels, en exploitant la répartition géographique et l'espace de noms global de StorageGRID pour une diffusion de contenu rapide et fiable.

Archives de données : StorageGRID offre différents types de stockage et prend en charge la hiérarchisation vers des options de stockage public à faible coût à long terme, en faisant une solution idéale pour l'archivage et la conservation à long terme des données qui doivent être conservées à des fins de conformité ou d'historique.

Cas d'utilisation du stockage objet

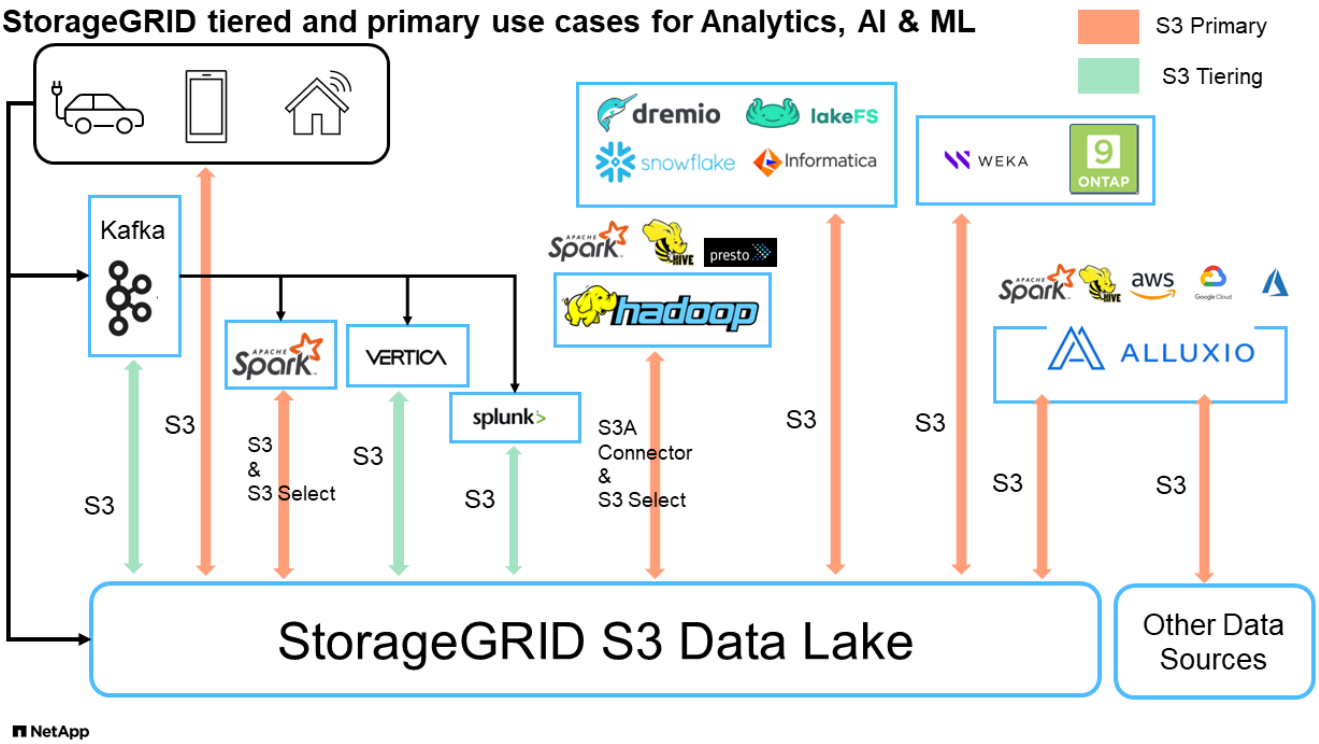


Parmi ces cas d'usage, l'analytique Big Data est l'un des plus utilisés, et son utilisation est en hausse.

Pourquoi choisir StorageGRID pour les data Lakes ?

- Collaboration renforcée : colocation multisite partagée massive avec accès API standard
- Coûts d'exploitation réduits : simplicité opérationnelle d'une seule architecture à autorétablissement
- Évolutivité : contrairement aux solutions Hadoop et d'entrepôt de données classiques, le stockage objet StorageGRID S3 dissocie le stockage des ressources de calcul et de données pour vous permettre de faire évoluer vos besoins de stockage au fur et à mesure de leur croissance.
- Durabilité et fiabilité : StorageGRID garantit une durabilité de 99.999999999 %, ce qui signifie que les données stockées sont hautement résistantes à la perte de données. Il assure également une haute disponibilité, garantissant ainsi un accès permanent aux données.
- Sécurité : StorageGRID offre plusieurs fonctionnalités de sécurité, notamment le chiffrement, les règles de contrôle d'accès, la gestion du cycle de vie des données, le verrouillage d'objets et la gestion des versions pour protéger les données stockées dans des compartiments S3

StorageGRID S3 Data Lakes



Étude comparative des entrepôts de données et des Lakehouses avec le stockage objet S3 : étude comparative

Cet article présente un banc d'essai complet de divers entrepôts de données et écosystèmes de lakehouse utilisant NetApp StorageGRID. L'objectif est de déterminer quel système fonctionne le mieux avec le stockage objet S3. Reportez-vous à cette "Apache Iceberg : guide de référence" section pour en savoir plus sur les architectures datawarehous/lakehouse et le format de table (parquet et Iceberg).

- Outil de référence - TPC-DS - https://www.tpc.org/tpcds/
- Les écosystèmes Big Data
  - Cluster de machines virtuelles, chacune avec 128 G de RAM et 24 vCPU, stockage SSD pour le disque système
  - Hadoop 3.3.5 avec Hive 3.1.3 (1 nœud de nom + 4 nœuds de données)
  - Delta Lake avec Spark 3.2.0 (1 maître + 4 employés) et Hadoop 3.3.5
  - Dremio v25.2 (1 coordinateur + 5 exécuteurs)
  - Trino v438 (1 coordinateur + 5 travailleurs)
  - Starburst v453 (1 coordinateur + 5 travailleurs)
- Stockage objet
  - NetApp® StorageGRID® 11.8 avec 3 x SG6060 + 1 équilibreur de charge SG1000
  - Protection d'objet : 2 copies (le résultat est similaire à EC 2+1)
- Taille de base de données : 1 000 Go
- Le cache a été désactivé dans tous les écosystèmes pour chaque test de requête utilisant le format parquet. Pour le format Iceberg, nous avons comparé le nombre de requêtes GET S3 et le temps total d'interrogation entre les scénarios avec mise en cache désactivée et activée.

TPC-DS comprend 99 requêtes SQL complexes conçues pour l'analyse comparative. Nous avons mesuré le temps total nécessaire à l'exécution des 99 requêtes et réalisé une analyse détaillée en examinant le type et le nombre de requêtes S3. Nos tests ont comparé l'efficacité de deux formats de table courants : parquet et Iceberg.

Résultat de la requête TPC-DS avec le format de table parquet

Écosystème	Ruche	Delta Lake	Dremio	Trino	En étoile
Requêtes TPCDS 99 nombre total de minutes	1084 [1]	55	36	32	28
Répartition des demandes S3	OBTENEZ	1,117,184	2,074,610	3 939 690	1 504 212
1 495 039	observation: Tous les ACCÈS à la gamme	Plage de 80 % de 2 Ko à 2 Mo à partir d'objets de 32 Mo, 50 à 100 requêtes/sec	Plage de 73 % inférieure à 100 Ko pour les objets de 32 Mo, 1000 à 1400 requêtes/sec	90 % plage d'octets de 1 Mo provenant d'objets de 256 Mo, 2500 à 3000 requêtes/sec	Taille GET de la plage : 50 % en dessous de 100 Ko, 16 % autour de 1 Mo, 27 % 2 Mo - 9 Mo, 3500 - 4000 requêtes/sec
Taille GET de la plage : 50 % en dessous de 100 Ko, 16 % autour de 1 Mo, 27 % 2 Mo - 9 Mo, 4000 à 5000 requêtes/sec	Liste des objets	312,053	24,158	120	509
512	TÊTE (objet inexistant)	156,027	12,103	96	0
0	TÊTE (objet existant)	982,126	922,732	0	0
0	Nombre total de demandes	2,567,390	3,033,603	3 939,906	1 504 721

[1] Hive Impossible de compléter la requête numéro 72

Résultat de la requête TPC-DS avec format de table Iceberg

Écosystème	Dremio	Trino	En étoile
Requêtes TPCDS 99 + minutes totales (cache désactivé)	22	28	22
Requêtes TPCDS 99 + minutes totales [2] (mémoire cache activée)	16	28	21,5
Répartition des demandes S3	OBTENIR (cache désactivé)	1 985 922	938 639
931 582	OBTENIR (cache activé)	611 347	30 158
3 281	observation: Tous les ACCÈS à la gamme	Taille GET de plage : 67 % 1 Mo, 15 % 100 Ko, 10 % 500 Ko, 3500 à 4500 requêtes/sec	Taille GET de la plage : 42 % en dessous de 100 Ko, 17 % autour de 1 Mo, 33 % 2 Mo - 9 Mo, 3500 - 4000 requêtes/sec
Taille GET de la plage : 43 % en dessous de 100 Ko, 17 % autour de 1 Mo, 33 % 2 Mo - 9 Mo, 4000 - 5000 requêtes/sec	Liste des objets	1465	0
0	TÊTE (objet inexistant)	1464	0
0	TÊTE (objet existant)	3 702	509
509	Nombre total de requêtes (cache désactivé)	1 992 553	939 148

[2] les performances de Trino/Starburst sont des engorgements dus aux ressources de calcul ; l'ajout de RAM au cluster réduit le temps total de requête.

Comme le montre le premier tableau, Hive est beaucoup plus lente que les autres écosystèmes de maisons de données modernes. Nous avons observé qu'Hive a envoyé un grand nombre de requêtes d'objets de liste S3, qui sont généralement lentes sur toutes les plateformes de stockage objet, en particulier lorsqu'il s'agit de compartiments contenant de nombreux objets. Cela augmente considérablement la durée globale des requêtes. En outre, les écosystèmes de lakehouse modernes peuvent envoyer un grand nombre de requêtes GET en parallèle, allant de 2,000 à 5,000 requêtes par seconde, contre 50 à 100 requêtes par seconde de Hive. La copie de système de fichiers standard de Hive et Hadoop S3A contribue à la lenteur d'Hive lors de l'interaction avec le stockage objet S3.

L'utilisation d'Hadoop (HDFS ou le stockage objet S3) avec Hive ou Spark nécessite une connaissance approfondie de Hadoop et Hive/Spark, ainsi qu'une compréhension des interactions entre les paramètres de chaque service. Ensemble, ils ont plus de 1,000 réglages, dont beaucoup sont liés et ne peuvent pas être modifiés indépendamment. Trouver la combinaison optimale de paramètres et de valeurs nécessite beaucoup de temps et d'efforts.

En comparant les résultats du parquet et de l'Iceberg, nous constatons que le format du tableau est un facteur de performance important. Le format de table Iceberg est plus efficace que le parquet en termes de nombre de requêtes S3, avec 35 à 50 % de demandes en moins par rapport au format parquet.

Les performances de Dremio, Trino ou Starburst sont principalement déterminées par la puissance de calcul du cluster. Bien que les trois utilisent le connecteur S3A pour la connexion de stockage objet S3, ils ne nécessitent pas Hadoop et la plupart des paramètres fs.s3a de Hadoop ne sont pas utilisés par ces systèmes. Cela simplifie le réglage des performances, éliminant ainsi la nécessité d'apprendre et de tester les différents paramètres Hadoop S3A.

À partir de ce résultat du banc d'essai, nous pouvons conclure que le système d'analytique Big Data optimisé pour les workloads S3 constitue un facteur de performance majeur. Les blanchisseurs modernes optimisent l'exécution des requêtes, utilisent efficacement les métadonnées et fournissent un accès transparent aux données S3. Ils offrent ainsi de meilleures performances que Hive avec le stockage S3.

Reportez-vous à cette "page" section pour configurer la source de données Dremio S3 avec StorageGRID.

Cliquez sur les liens ci-dessous pour découvrir comment StorageGRID et Dremio travaillent en collaboration pour fournir une infrastructure de data Lake moderne et efficace, et comment NetApp a migré de Hive + HDFS vers Dremio + StorageGRID pour améliorer considérablement l'efficacité de l'analyse Big Data.

- "Optimisez les performances de vos Big Data avec NetApp StorageGRID"
- "Infrastructure de data Lake moderne, puissante et efficace avec StorageGRID et Dremio"
- "Comment NetApp redéfinit l'expérience client avec l'analytique des produits"

Réglage Hadoop S3A

Par Angela Cheng

Le connecteur Hadoop S3A facilite l'interaction transparente entre les applications Hadoop et le stockage objet S3. Le réglage du connecteur Hadoop S3A est essentiel pour optimiser les performances lorsque vous travaillez avec le stockage objet S3. Avant d'entrer dans les détails d'ajustement, analysons très bien Hadoop et ses composants.

Qu'est-ce que Hadoop ?

Hadoop est une structure open source puissante conçue pour gérer le traitement et le stockage de données à grande échelle. Il permet le stockage distribué et le traitement parallèle sur des clusters d'ordinateurs.

Ces trois composants sont les suivants :

- **Hadoop HDFS (Hadoop Distributed File System)** : gère le stockage, décode les données en blocs et les distribue entre les nœuds.
- **Hadoop MapReduce** : responsable du traitement des données en divisant les tâches en petits blocs et en les exécutant en parallèle.
- **FIL Hadoop (encore un autre négociateur de ressources):** "Gère les ressources et planifie les tâches de manière efficace"

Connecteur HDFS et S3A Hadoop

HDFS est un composant essentiel de l'écosystème Hadoop, qui joue un rôle essentiel dans l'efficacité du traitement des Big Data. HDFS assure un stockage et une gestion fiables. Elle assure un traitement parallèle

et un stockage des données optimisé, ce qui accélère l'accès aux données et leur analyse.

Dans le traitement du Big Data, HDFS se distingue par son excellente tolérance aux pannes pour le stockage de datasets volumineux. Pour cela, il s'agit de la réplication des données. Il peut stocker et gérer d'importants volumes de données structurées et non structurées dans un environnement de data warehouse. De plus, il s'intègre en toute transparence aux principales structures de traitement des Big Data, comme Apache Spark, Hive, Pig et Flink, pour un traitement des données évolutif et efficace. Il est compatible avec les systèmes d'exploitation Unix (Linux), ce qui en fait un choix idéal pour les entreprises qui préfèrent utiliser des environnements Linux pour leur traitement Big Data.

Comme le volume de données s'est accru au fil du temps, l'approche consistant à ajouter de nouvelles machines au cluster Hadoop avec leurs propres ressources de calcul et de stockage s'avère inefficace. L'évolutivité linéaire engendre des défis pour utiliser les ressources efficacement et gérer l'infrastructure.

Pour relever ces défis, le connecteur Hadoop S3A offre des E/S haute performance par rapport au stockage objet S3. L'implémentation d'un workflow Hadoop avec S3A vous permet d'exploiter le stockage objet en tant que référentiel de données et de séparer les ressources de calcul et de stockage. Vous pouvez ainsi faire évoluer indépendamment les ressources de calcul et de stockage. Grâce à la dissociation du calcul et du stockage, vous pouvez également dédier la bonne quantité de ressources pour vos tâches de calcul et fournir la capacité requise en fonction de la taille de votre jeu de données. Par conséquent, vous pouvez réduire votre TCO global pour les workflows Hadoop.

Réglage du connecteur S3A Hadoop

S3 se comporte différemment de HDFS et certaines tentatives de préservation de l'apparence d'un système de fichiers ne sont pas totalement optimales. Des ajustements/tests/tests rigoureux sont nécessaires pour optimiser l'utilisation des ressources S3.

Les options Hadoop présentées dans ce document sont basées sur Hadoop 3.3.5, voir "Hadoop 3.3.5 core-site.xml" pour toutes les options disponibles.

Remarque – la valeur par défaut de certains paramètres Hadoop fs.s3a est différente dans chaque version de Hadoop. Vérifiez la valeur par défaut spécifique à votre version Hadoop actuelle. Si ces paramètres ne sont pas spécifiés dans Hadoop core-site.xml, la valeur par défaut sera utilisée. Vous pouvez remplacer la valeur au moment de l'exécution à l'aide des options de configuration Spark ou Hive.

Vous devez accéder à cette page "Page Apache Hadoop" pour comprendre chaque option fs.s3a. Si possible, testez-les dans un cluster Hadoop non productif pour trouver les valeurs optimales.

Vous devriez lire "Optimisation des performances lors de l'utilisation du connecteur S3A" pour obtenir d'autres recommandations de réglage.

Examinons quelques points clés à prendre en compte :

1. Compression des données

N'activez pas la compression StorageGRID. La plupart des systèmes Big Data utilisent l'option GET de plage d'octets au lieu de récupérer l'objet entier. L'utilisation de la plage d'octets GET avec des objets compressés dégrade considérablement les performances GET.

2. S3A committers

En général, le Comitter Magic s3a est recommandé. Se reporter à ceci "Page des options de renvoi S3A courantes" pour mieux comprendre le comitter magique et ses paramètres s3a associés.

Magic Committer :

Le Magic Committer s'appuie spécifiquement sur S3Guard pour offrir des listes de répertoires cohérentes sur le magasin d'objets S3.

Avec S3 cohérent (ce qui est désormais le cas), le Magic Committer peut être utilisé en toute sécurité avec n'importe quel compartiment S3.

Choix et expérimentation :

Selon votre cas d'utilisation, vous pouvez choisir entre la variable de transfert (qui s'appuie sur un système de fichiers HDFS de cluster) et la variable Magic Committer.

Testez les deux pour déterminer celle qui convient le mieux à votre workload et à vos besoins.

En résumé, les committers S3A constituent une solution au défi fondamental de l'engagement de sortie cohérent, haute performance et fiable pour S3. Leur conception interne garantit un transfert de données efficace tout en préservant l'intégrité des données.

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. Threads, tailles de pool de connexions et taille de bloc

- Chaque client **S3A** interagissant avec un seul compartiment dispose de son propre pool dédié de connexions HTTP 1.1 ouvertes et de threads pour les opérations de téléchargement et de copie.
- "Vous pouvez régler la taille de ces pools de manière à trouver un équilibre entre les performances et l'utilisation de la mémoire/des threads".
- Lors du téléchargement de données vers S3, elles sont divisées en blocs. La taille de bloc par défaut est de 32 Mo. Vous pouvez personnaliser cette valeur en définissant la propriété fs.s3a.block.size.
- Des blocs plus volumineux peuvent améliorer les performances lors du chargement de données volumineuses en réduisant la surcharge liée à la gestion des pièces à part multiple lors du téléchargement. La valeur recommandée est de 256 Mo ou plus pour les jeux de données volumineux.

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. Téléchargement partitionné

s3a committers **toujours** utiliser MPU (téléchargement partitionné) pour charger des données dans le compartiment s3. Ceci est nécessaire pour permettre : l'échec de tâche, l'exécution spéculative des tâches et les abandons de travail avant la validation. Voici quelques spécifications clés relatives aux téléchargements partitionnés :

- Taille maximale des objets : 5 Tio (téraoctets).
- Nombre maximum de pièces par téléchargement: 10,000.
- Numéros de pièce : compris entre 1 et 10,000 (inclus).
- Taille de la pièce : entre 5 Mio et 5 Gio. En particulier, il n'existe pas de limite de taille minimale pour la dernière partie de votre téléchargement partitionné.

L'utilisation d'une taille de pièce plus petite pour les téléchargements partitionnés S3 présente à la fois des avantages et des inconvénients.

Avantages :

- Récupération rapide à partir des problèmes réseau : lorsque vous chargez des pièces plus petites, l'impact du redémarrage d'un téléchargement échoué en raison d'une erreur réseau est réduit. Si une pièce

échoue, il vous suffit de télécharger à nouveau cette pièce spécifique plutôt que l'objet entier.

- Meilleure parallélisation : plus de pièces peuvent être téléchargées en parallèle, ce qui permet de tirer parti du multithreading ou des connexions simultanées. Cette parallélisation améliore les performances, en particulier pour les fichiers volumineux.

Désavantage :

- Surcharge réseau : une taille de pièce plus petite signifie plus de parties à télécharger, chaque partie nécessite sa propre requête HTTP. Le nombre de requêtes HTTP augmente la charge de lancement et de traitement des requêtes individuelles. La gestion d'un grand nombre de petites pièces peut avoir un impact sur les performances.
- Complexité : la gestion de la commande, le suivi des pièces et la garantie de la réussite des téléchargements peuvent s'avérer fastidieux. Si le téléchargement doit être abandonné, tous les articles déjà téléchargés doivent être suivis et purgés.

Pour Hadoop, la taille de pièce de 256 Mo ou plus est recommandée pour fs.s3a.multipart.size. Définissez toujours la valeur fs.s3a.mutipart.threshold sur 2 x fs.s3a.multipart.size. Par exemple, si fs.s3a.multipart.size = 256M, fs.s3a.mutlipart.threshold doit être de 512M.

Utiliser une taille de pièce plus grande pour un jeu de données volumineux. Il est important de choisir une taille de pièce qui équilibre ces facteurs en fonction de votre cas d'utilisation et des conditions réseau spécifiques.

Un téléchargement partitionné est un "processus en trois étapes":

1. Le téléchargement est lancé, StorageGRID renvoie un ID de téléchargement
2. Les parties d'objet sont chargées à l'aide de l'ID de téléchargement
3. Une fois toutes les parties d'objet chargées, envoie une demande de téléchargement partitionné complète avec upload-ID StorageGRID construit l'objet à partir des pièces téléchargées, et le client peut accéder à l'objet.

Si la demande complète de téléchargement partitionné n'est pas envoyée correctement, les pièces restent dans StorageGRID et ne créeront aucun objet. Cela se produit lorsque les travaux sont interrompus, en échec ou abandonnés. Les pièces restent dans la grille jusqu'à ce que le téléchargement partitionné soit terminé ou abandonné ou que StorageGRID purge ces pièces si 15 jours se sont écoulés depuis le lancement du téléchargement. S'il y a beaucoup (quelques centaines de milliers à plusieurs millions) de téléchargements partitionnés en cours dans un compartiment, lorsque Hadoop envoie des « téléchargements partiaux-listes » (cette requête ne filtre pas par identifiant de téléchargement), la demande peut prendre un certain temps ou finir par se terminer. Vous pouvez envisager de définir fs.s3a.mutipart.purge sur TRUE avec une valeur fs.s3a.multipart.purge.age appropriée (par exemple, 5 à 7 jours, n'utilisez pas la valeur par défaut de 86400, c'est-à-dire 1 jour). Ou faites appel au support NetApp pour étudier la situation.

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. Mémoire tampon pour écrire les données en mémoire

Pour améliorer les performances, vous pouvez mettre en mémoire tampon l'écriture des données en mémoire avant de les télécharger dans S3. Cela permet de réduire le nombre d'écritures de petite taille et d'améliorer l'efficacité.

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

N’oubliez pas que S3 et HDFS fonctionnent différemment. Des ajustements/tests/expériences minutieux sont nécessaires pour utiliser de manière optimale les ressources S3.

Tr-4871 : configurez StorageGRID pour la sauvegarde et la restauration avec CommVault

Sauvegardez et restaurez les données à l’aide de StorageGRID et de CommVault

CommVault et NetApp se sont associés pour créer une solution commune de protection des données qui combine le logiciel CommVault Complete Backup and Recovery pour NetApp et le logiciel NetApp StorageGRID pour le stockage cloud. CommVault Complete Backup and Recovery et NetApp StorageGRID proposent des solutions uniques et faciles à utiliser qui s’associent pour répondre aux exigences de croissance rapide des données et à celles de réglementations toujours plus strictes à travers le monde.

De nombreuses entreprises souhaitent migrer leur stockage dans le cloud, faire évoluer leurs systèmes et automatiser leurs règles de conservation des données à long terme. Réputé pour sa résilience, son évolutivité, ses avantages opérationnels et ses économies, le stockage objet basé dans le cloud en fait un choix naturel comme cible pour votre sauvegarde. CommVault et NetApp ont certifié conjointement leur solution combinée en 2014. Depuis, ils ont développé une intégration plus étroite entre leurs deux solutions. Des clients de tous types dans le monde ont adopté la solution combinée CommVault Complete Backup and Recovery and StorageGRID.

À propos de CommVault et StorageGRID

Le logiciel CommVault Complete Backup and Recovery est une solution haute performance de gestion des données et des informations intégrée, conçue dès le départ sur une plateforme unique et dotée d’une base de code unifiée. Toutes ses fonctions partagent des technologies back-end, offrant ainsi les avantages et avantages inégalés d’une approche entièrement intégrée de protection, de gestion et d’accès à vos données. Le logiciel contient des modules pour protéger, archiver, analyser, répliquer et rechercher vos données. Les modules partagent un ensemble commun de services back-end et de fonctionnalités avancées qui interagissent en toute transparence les uns avec les autres. Cette solution aborde tous les aspects de la gestion des données dans votre entreprise, tout en offrant une évolutivité illimitée et un contrôle sans précédent des données et des informations.

NetApp StorageGRID, en tant que Tier cloud CommVault, est une solution de stockage objet de cloud hybride d’entreprise. Vous pouvez le déployer sur de nombreux sites, que ce soit sur une appliance dédiée ou en tant que déploiement Software-defined. StorageGRID vous permet d’établir des règles de gestion des données qui déterminent le mode de stockage et de protection des données. StorageGRID collecte les informations dont vous avez besoin pour développer et appliquer des règles. Il examine un large éventail de caractéristiques et de besoins, y compris les performances, la durabilité, la disponibilité, l’emplacement géographique, longévité et coût. Elles sont intégralement conservées et protégées lors de leur déplacement entre différents sites et au fur et à mesure du vieillissement.

Le moteur de règles intelligent StorageGRID vous aide à choisir l’une des options suivantes :

- Utiliser le code d’effacement pour sauvegarder les données sur plusieurs sites à des fins de résilience.
- Pour copier des objets vers des sites distants afin de minimiser la latence et le coût du WAN.

Lorsque StorageGRID stocke un objet, vous y accédez en tant qu’objet unique, quel que soit son emplacement et le nombre de copies existantes. Ce comportement est crucial pour la reprise d’activité, car grâce à lui, même si une copie de sauvegarde de vos données est corrompue, StorageGRID peut restaurer

vos données.

La conservation des données de sauvegarde dans votre stockage primaire peut s'avérer coûteuse. Avec NetApp StorageGRID, vous libérez de l'espace sur votre stockage primaire en migrant les données de sauvegarde inactives vers StorageGRID, tout en bénéficiant des nombreuses fonctionnalités de StorageGRID. La valeur des données de sauvegarde évolue au fil du temps, tout comme le coût de leur stockage. StorageGRID réduit le coût du stockage primaire tout en augmentant la durabilité des données.

Fonctionnalités clés

Principales fonctionnalités de la plateforme logicielle CommVault :

- Une solution complète de protection des données prenant en charge tous les principaux systèmes d'exploitation, applications et bases de données sur des serveurs virtuels et physiques, des systèmes NAS, des infrastructures cloud et des appareils mobiles.
- Gestion simplifiée via une console unique : vous pouvez afficher, gérer et accéder à toutes les fonctions, à toutes les données et à toutes les informations de l'entreprise.
- Plusieurs méthodes de protection, notamment la sauvegarde et l'archivage des données, la gestion de snapshots, la réplication des données et l'indexation du contenu à des fins d'e-Discovery.
- Gestion du stockage efficace grâce à la déduplication pour le stockage sur disque et cloud.
- Intégration aux baies de stockage NetApp telles que AFF, FAS, NetApp HCI et E-Series et aux systèmes de stockage scale-out NetApp SolidFire®. Intégration également au logiciel NetApp Cloud Volumes ONTAP pour automatiser la création de copies NetApp Snapshot™ indexées sur les applications, sur l'ensemble du portefeuille de stockage NetApp.
- Une gestion complète de l'infrastructure virtuelle qui prend en charge les principaux hyperviseurs virtuels sur site et plateformes d'hyperscaler de cloud public.
- Des fonctionnalités de sécurité avancées pour limiter l'accès aux données stratégiques, fournir des fonctionnalités de gestion granulaire et fournir aux utilisateurs Active Directory un accès Single Sign-on.
- Une gestion des données basée sur des règles qui vous permet de gérer vos données en fonction de vos besoins et non de votre emplacement physique.
- Une expérience utilisateur de pointe qui permet à vos utilisateurs de protéger, de rechercher et de restaurer leurs propres données.
- L'automatisation par API vous permet d'utiliser des outils tiers tels que vRealize Automation ou Service Now pour gérer vos opérations de protection et de récupération des données.

Pour plus de détails sur les charges de travail prises en charge, consultez "Technologies prises en charge par CommVault".

Options de sauvegarde

Lorsque vous implémentez le logiciel CommVault Complete Backup and Recovery avec le stockage cloud, vous disposez de deux options de sauvegarde :

- Sauvegarde sur une cible de disque primaire et sauvegarde également une copie auxiliaire sur un stockage cloud.
- Sauvegarde dans le cloud en tant que cible principale.

Auparavant, le stockage cloud ou objet était considéré comme trop faible pour être utilisé pour la sauvegarde principale. L'utilisation d'une cible de disque primaire a permis aux clients d'accélérer les processus de sauvegarde et de restauration, et de conserver une copie auxiliaire dans le cloud en tant que sauvegarde à

froid. StorageGRID est la nouvelle génération de stockage objet. StorageGRID offre des performances élevées et un débit massif, ainsi que des performances et une flexibilité bien supérieures à celles des autres fournisseurs de stockage objet.

Le tableau suivant répertorie les avantages de chaque option de sauvegarde avec StorageGRID :

	Sauvegarde principale sur disque et copie auxiliaire sur StorageGRID	**Sauvegarde principale vers StorageGRID**
Performance	Délai de restauration le plus rapide, via un montage en direct ou une restauration en direct : idéal pour les workloads de niveau 0/niveau 1.	Ne peut pas être utilisé pour les opérations de montage en direct ou de restauration en direct. Idéal pour les opérations de restauration en streaming et pour la conservation à long terme.
Architecture de déploiement	Utilisation de la technologie 100 % Flash ou d'un disque mécanique comme premier palier d'atterrissage de sauvegarde. StorageGRID est utilisé comme Tier secondaire.	Simplifie le déploiement en utilisant StorageGRID comme cible de sauvegarde complète.
Fonctionnalités avancées (restauration en direct)	Pris en charge	Non pris en charge

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation StorageGRID 11.9 + https://docs.netapp.com/us-en/storagegrid-119/
- Documentation produit NetApp https://docs.netapp.com
- Documentation CommVault https://documentation.commvault.com/2024/essential/index.html

Présentation de la solution testée

La solution testée combine les solutions CommVault et NetApp pour offrir une solution commune puissante.

Configuration de la solution

Dans la configuration de laboratoire, l'environnement StorageGRID se composait de quatre appliances NetApp StorageGRID SG5712, d'un nœud d'administration principal virtuel et d'un nœud de passerelle virtuelle. L'appliance SG5712 est l'option d'entrée de gamme, une configuration de base. Le choix d'appliances plus performantes, telles que NetApp StorageGRID SG5760 ou SG6060, peut considérablement améliorer les performances. Consultez votre architecte de solutions NetApp StorageGRID pour obtenir de l'aide sur le dimensionnement.

Pour sa règle de protection des données, StorageGRID utilise une règle de gestion du cycle de vie intégrée afin de gérer et de protéger les données. Les règles ILM sont évaluées dans une règle de haut en bas. Nous avons implémenté la politique ILM présentée dans le tableau suivant :

Règle ILM	Qualificatifs	Comportement d'ingestion
Code d'effacement 2+1	Objets de plus de 200 Ko	Équilibré
2 copies	Tous les objets	Double allocation

La règle ILM 2 Copy est la règle par défaut. La règle Erasure Coding 2+1 a été appliquée pour ce test à tout objet de 200 Ko ou plus. La règle par défaut a été appliquée aux objets inférieurs à 200 Ko. L'application des règles de cette manière est une bonne pratique StorageGRID.

Pour obtenir des informations techniques sur cet environnement de test, consultez la section conception de la solution et meilleures pratiques du "Protection des données scale-out NetApp avec CommVault" rapport technique.

Spécifications matérielles de la baie StorageGRID

Le tableau suivant décrit le matériel NetApp StorageGRID utilisé dans ce test. L'appliance StorageGRID SG5712 avec mise en réseau 10 Gbits/s est l'option d'entrée de gamme et représente une configuration de base. Éventuellement, le SG5712 peut être configuré pour une mise en réseau de 25 Gbit/s.

Sous-jacent	Quantité	Disque	Capacité exploitable	Le réseau
Appliances StorageGRID SG5712	4	48 x 4 To (disque dur SAS secondaire)	136 TO	10 Gbit/s

Le choix d'options d'appliance hautes performances, telles que les appliances NetApp StorageGRID SG5760, SG6060 et 100 % Flash SGF6112 peut apporter des avantages significatifs en matière de performance. Consultez votre architecte de solutions NetApp StorageGRID pour obtenir de l'aide sur le dimensionnement.

Configuration logicielle requise pour CommVault et StorageGRID

Les tableaux suivants répertorient les logiciels requis pour les logiciels CommVault et NetApp StorageGRID installés sur le logiciel VMware à des fins de test. Quatre gestionnaires de transmission de données MediaAgent et un serveur CommServe ont été installés. Lors du test, une mise en réseau de 10 Gbits/s a été mise en œuvre pour l'infrastructure VMware. Le tableau suivant

Le tableau suivant répertorie la configuration système totale requise pour le logiciel CommVault :

Composant	Quantité	Datastore	Taille	Total	Nombre total d'IOPS requises
Serveur CommServe	1	OS	500 GO	500 GO	s/o
		SQL	500 GO	500 GO	s/o

Composant	Quantité	Datastore	Taille	Total	Nombre total d'IOPS requises
MediaAgent	4	Processeur virtuel (vCPU)	16	64	s/o
		RAM	128 GO	512	s/o
		OS	500 GO	2 TO	s/o
		Cache d'index	2 TO	8 TO	200+
		DDB	2 TO	8 TO	200 000 000 K

Dans l'environnement de test, un nœud d'administration principal virtuel et un nœud de passerelle virtuelle ont été déployés sur VMware sur une baie de stockage NetApp E-Series E2812. Chaque nœud se trouvait sur un serveur distinct avec les exigences minimales relatives à l'environnement de production décrites dans le tableau suivant :

Le tableau suivant répertorie les conditions requises pour les nœuds d'administration virtuelle et les nœuds de passerelle StorageGRID :

Type de nœud	Quantité	VCPU	RAM	Stockage
Nœud de passerelle	1	8	24 GO	LUN de 100 Gb pour le système d'exploitation
Nœud d'administration	1	8	24 GO	LUN de 100 Gb pour le système d'exploitation LUN de 200 Go pour les tables de nœuds d'administration LUN de 200 Go pour le journal d'audit du nœud d'administration

Conseils sur le dimensionnement de StorageGRID

Pour en savoir plus sur le dimensionnement de votre environnement, consultez vos spécialistes de la protection des données NetApp. Les spécialistes de la protection des données NetApp peuvent utiliser le calculateur de stockage de sauvegarde total CommVault pour estimer les exigences de l'infrastructure de sauvegarde. Cet outil requiert un accès au CommVault Partner Portal. Inscrivez-vous pour y accéder, si nécessaire.

Entrées de dimensionnement CommVault

Les tâches suivantes peuvent être utilisées pour effectuer la découverte du dimensionnement de la solution de protection des données :

- Identifiez les charges de travail du système ou des applications/bases de données et la capacité frontale correspondante (en téraoctets [To]) à protéger.
- Identifiez le workload de machines virtuelles/fichiers et une capacité front-end similaire (To) à protéger.
- Identifier les exigences de conservation à court et à long terme.
- Identifier le taux de modification quotidien en % pour les datasets/workloads identifiés
- Identification de la croissance des données prévue au cours des 12, 24 et 36 prochains mois
- Définissez les objectifs RTO et RPO pour la protection et la restauration des données en fonction des besoins de l'entreprise.

Lorsque ces informations sont disponibles, le dimensionnement de l'infrastructure de sauvegarde peut être effectué, ce qui entraîne la répartition des capacités de stockage requises.

Conseils sur le dimensionnement de StorageGRID

Avant d'effectuer le dimensionnement NetApp StorageGRID, tenez compte des aspects suivants de votre charge de travail :

- Capacité exploitable
- Mode WORM
- Taille moyenne des objets
- Exigences en matière de performances
- Règle ILM appliquée

La capacité utilisable doit tenir compte de la taille de la charge de travail de sauvegarde que vous avez basculée vers StorageGRID et du calendrier de conservation.

Le mode WORM sera-t-il activé ou non ? Une fois WORM activé dans CommVault, le verrouillage d'objet est configuré sur StorageGRID. Cela augmente la capacité de stockage objet requise. La capacité requise varie en fonction de la durée de conservation et du nombre de modifications d'objet apportées à chaque sauvegarde.

La taille moyenne d'objet est un paramètre d'entrée qui facilite le dimensionnement des performances dans un environnement StorageGRID. La taille moyenne des objets utilisés pour une charge de travail CommVault dépend du type de sauvegarde.

Le tableau suivant répertorie la taille moyenne des objets par type de sauvegarde et décrit ce que le processus de restauration lit à partir du magasin d'objets :

Type de sauvegarde	Taille moyenne de l'objet	Restaurer le comportement
Effectuer une copie auxiliaire dans StorageGRID	32 MO	Lecture complète de l'objet 32 Mo

Type de sauvegarde	Taille moyenne de l'objet	Restaurer le comportement
Orienter la sauvegarde vers StorageGRID (déduplication activée)	8 MO	Lecture aléatoire 1 Mo
Dirigez la sauvegarde vers StorageGRID (déduplication désactivée)	32 MO	Lecture complète de l'objet 32 Mo

En outre, la compréhension de vos besoins en performances pour les sauvegardes complètes et les sauvegardes incrémentielles vous aide à déterminer le dimensionnement des nœuds de stockage StorageGRID. Les méthodes de protection des données de la règle de gestion du cycle de vie des informations (ILM) de StorageGRID déterminent la capacité requise pour stocker les sauvegardes CommVault et affectent le dimensionnement de la grille.

La réplication ILM de StorageGRID est l'un des deux mécanismes utilisés par StorageGRID pour stocker les données en mode objet. Lorsque StorageGRID attribue des objets à une règle ILM de réplication des données, le système crée des copies exactes des données des objets et les stocke sur des nœuds de stockage.

Le codage d'effacement est la deuxième méthode utilisée par StorageGRID pour stocker les données d'objet. Lorsque StorageGRID attribue des objets à une règle ILM configurée pour créer des copies avec code d'effacement, elle coupe les données en mode objet en fragments de données. Il calcule ensuite des fragments de parité supplémentaires et stocke chaque fragment sur un nœud de stockage différent. Lorsqu'un objet est accédé, il est réassemblé à l'aide des fragments stockés. En cas de corruption ou de perte d'un fragment de données ou de parité, l'algorithme de code d'effacement peut recréer ce fragment à l'aide d'un sous-ensemble des fragments de données et de parité restants.

Les deux mécanismes nécessitent différentes quantités de stockage, comme le démontrent ces exemples :

- Si vous stockez deux copies répliquées, la surcharge de stockage double.
- Si vous stockez une copie avec code d'effacement 2+1, votre surconsommation de stockage est multipliée par 1.5.

Pour la solution testée, un déploiement StorageGRID d'entrée de gamme sur un seul site a été utilisé :

- Nœud d'administration : machine virtuelle VMware (VM)
- Équilibreur de charge : VMware VM
- Nœuds de stockage : 4 x SG5712 avec disques de 4 To
- Nœud d'administration principal et nœud de passerelle : machines virtuelles VMware avec des exigences minimales en termes de charge de travail de production

StorageGRID prend également en charge les équilibreurs de charge tiers.

StorageGRID est généralement déployé sur deux sites ou plus, avec des règles de protection des données qui répliquent les données afin d'éviter les défaillances au niveau des nœuds et des sites. En sauvegardant vos données sur StorageGRID, elles sont protégées par plusieurs copies ou par un code d'effacement qui sépare et réassemble les données de manière fiable à l'aide d'un algorithme.

Vous pouvez utiliser l'outil de dimensionnement "Fusion" pour dimensionner votre grille.

Évolutivité

Pour étendre un système NetApp StorageGRID, il est possible d'ajouter du stockage aux nœuds de stockage, d'ajouter de nouveaux nœuds grid à un site déjà en place ou d'ajouter un nouveau site de data Center. Les expansions ne nécessitent aucune interruption du fonctionnement du système.
StorageGRID fait évoluer les performances en utilisant soit des nœuds de performance plus élevée pour les nœuds de stockage, soit l'appliance physique qui exécute l'équilibreur de charge et les nœuds d'administration, soit en ajoutant simplement des nœuds supplémentaires.

Pour plus d'informations sur l'extension du système StorageGRID, reportez-vous àla section "Guide d'extension StorageGRID 11.9".

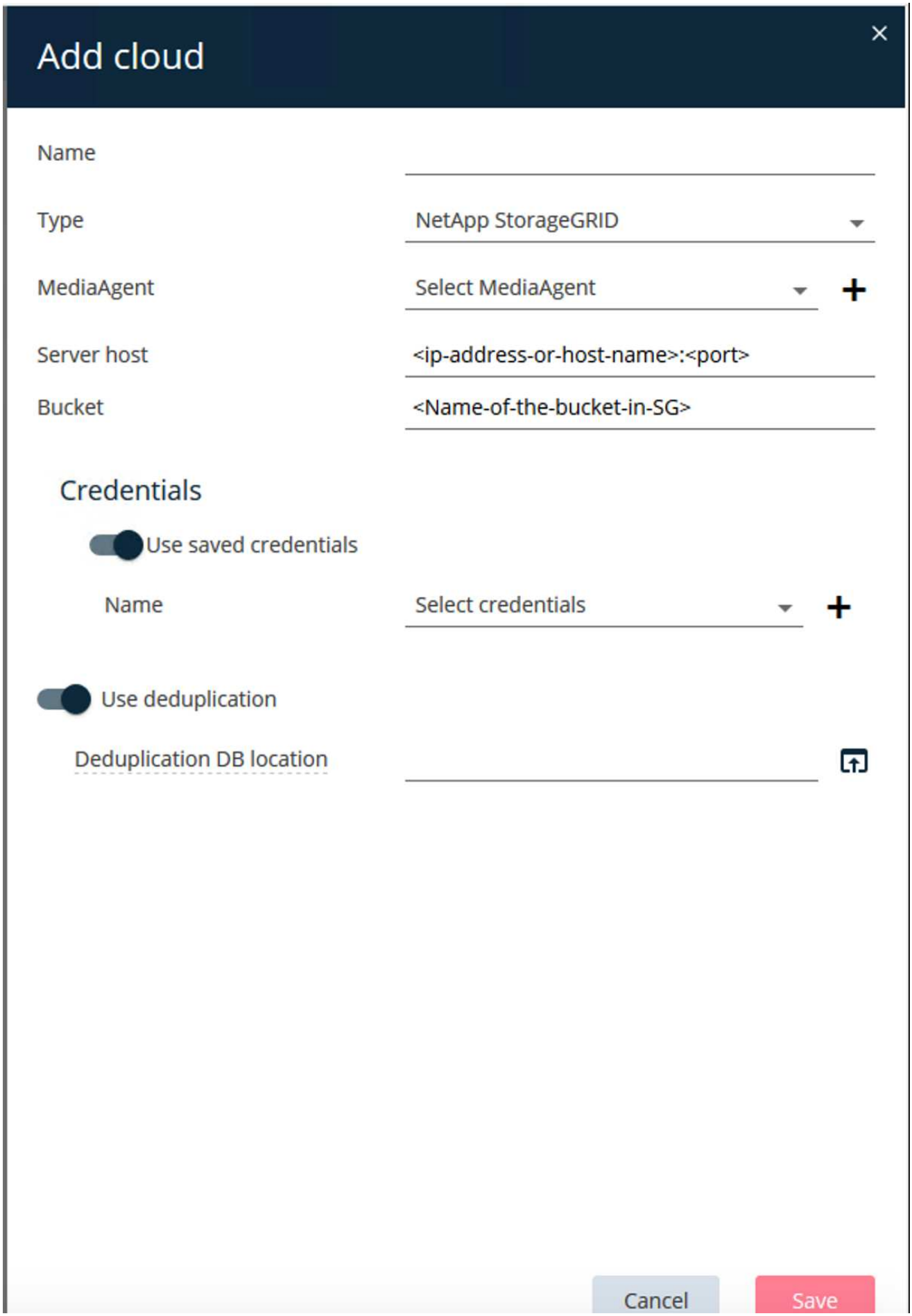
Exécutez une tâche de protection des données

Pour configurer StorageGRID avec CommVault Complete Backup and Recovery pour NetApp, les étapes suivantes ont été effectuées pour ajouter StorageGRID en tant que bibliothèque cloud dans le logiciel CommVault.

Étape 1 : configurer CommVault avec StorageGRID

Étapes

1. Connectez-vous au Centre de commande CommVault. Dans le panneau de gauche, cliquez sur stockage > Cloud > Ajouter pour afficher la boîte de dialogue Ajouter un nuage et y répondre :


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. Sous Type, sélectionnez NetApp StorageGRID.
3. Pour MediaAgent, sélectionnez tous les éléments associés à la bibliothèque cloud.
4. Pour hôte serveur, entrez l'adresse IP ou le nom d'hôte du noeud final StorageGRID et le numéro de port.

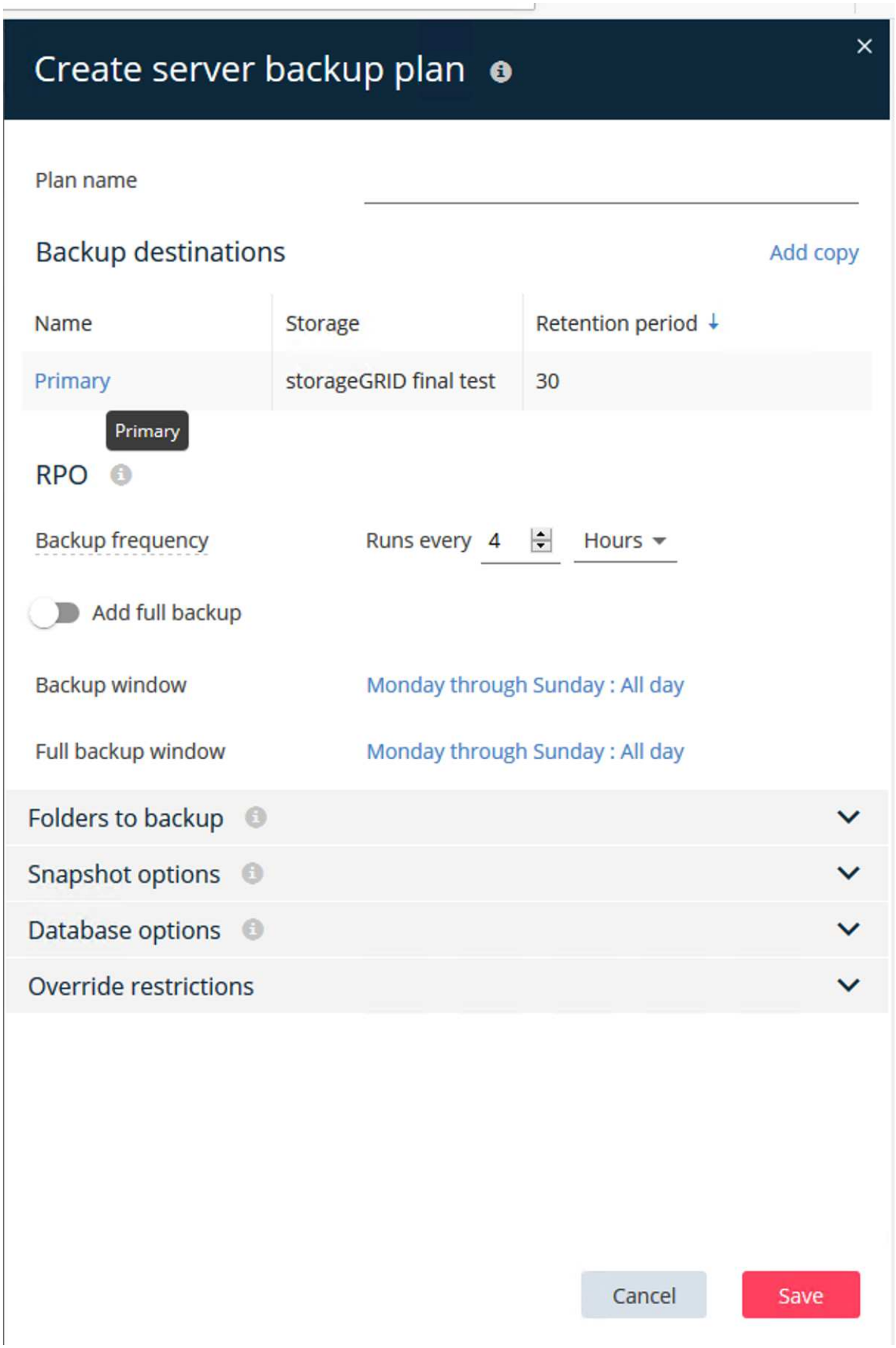
   Suivez les étapes de la documentation StorageGRID sur "comment configurer un terminal d'équilibrage de charge (port)". Assurez-vous que vous disposez d'un port HTTPS avec un certificat auto-signé et que vous disposez de l'adresse IP ou du nom de domaine du noeud final StorageGRID.

5. Si vous souhaitez utiliser la déduplication, activez cette option et indiquez le chemin d'accès à l'emplacement de la base de données de déduplication.
6. Cliquez sur Enregistrer.

Étape 2 : créez un plan de sauvegarde avec StorageGRID comme cible principale

Étapes

1. Dans le panneau de gauche, sélectionnez gérer > plans pour afficher la boîte de dialogue Créer un plan de sauvegarde du serveur et y répondre.

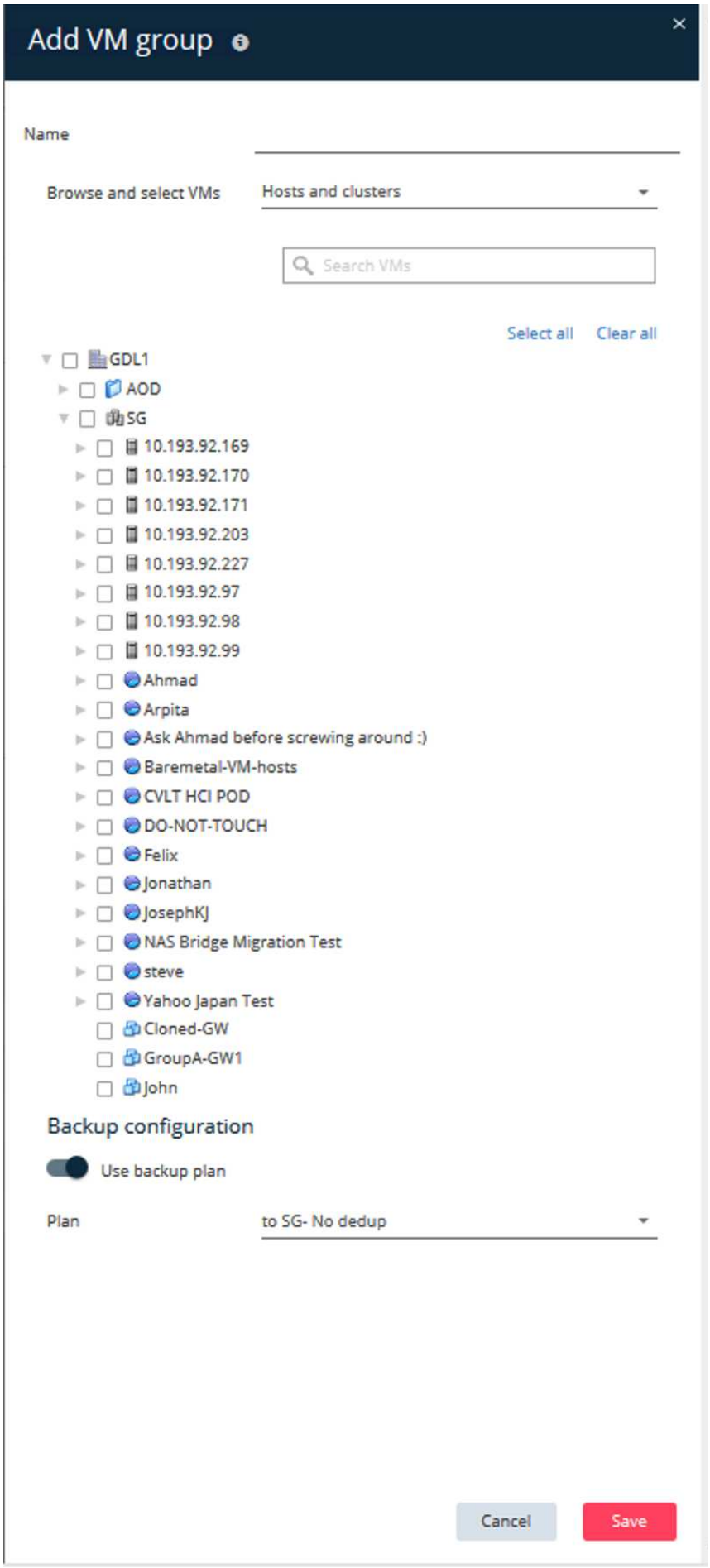

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to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

2. Entrez un nom de plan.
3. Sélectionnez la destination de sauvegarde du stockage StorageGRID simple Storage Service (S3) que vous avez créée précédemment.
4. Saisissez la période de conservation des sauvegardes et l'objectif de point de récupération (RPO) souhaités.
5. Cliquez sur Enregistrer.

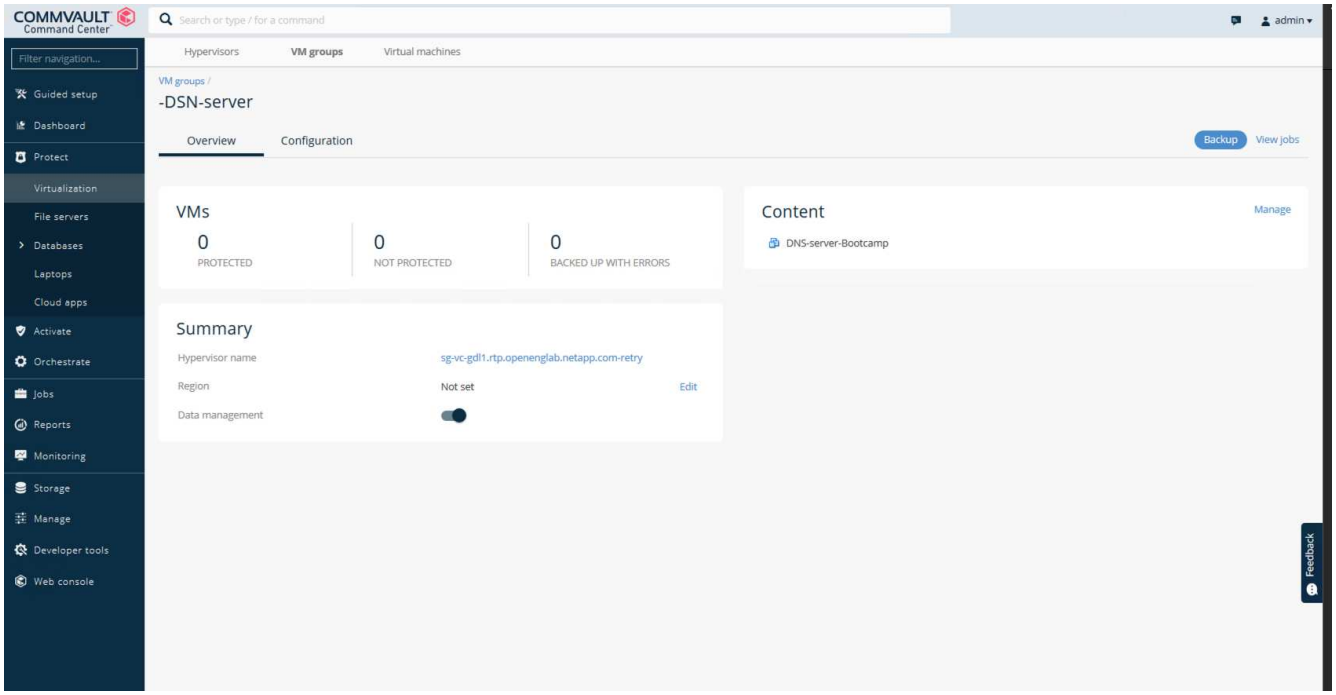
Étape 3 : démarrez une tâche de sauvegarde pour protéger vos workloads

Étapes

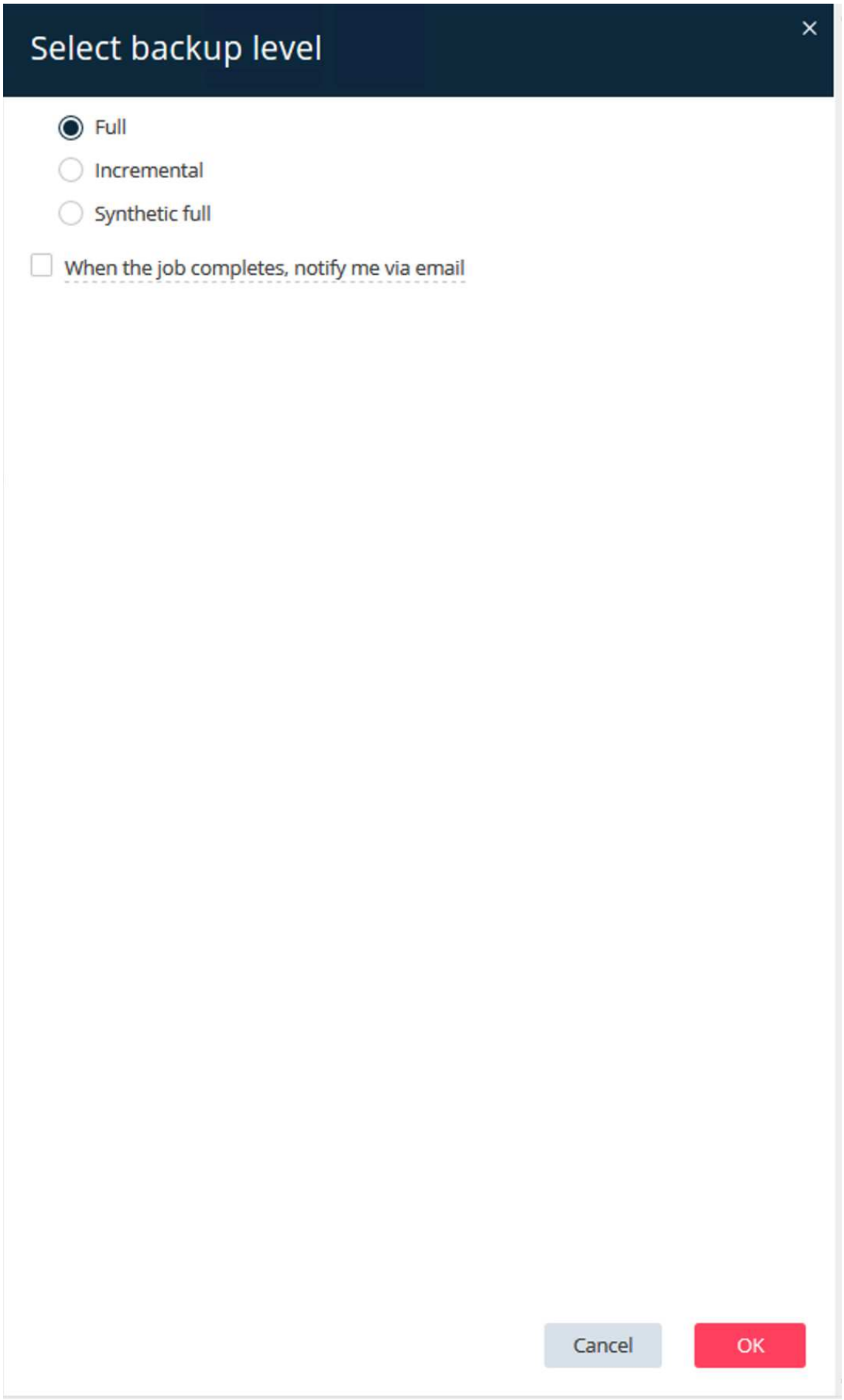
1. Dans CommVault Command Center, accédez à protection > virtualisation.
2. Ajoutez un hyperviseur VMware vCenter Server.
3. Cliquez sur l'hyperviseur que vous venez d'ajouter.
4. Cliquez sur Ajouter un groupe de machines virtuelles pour répondre à la boîte de dialogue Ajouter un groupe de machines virtuelles afin de voir l'environnement vCenter que vous prévoyez de protéger.


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

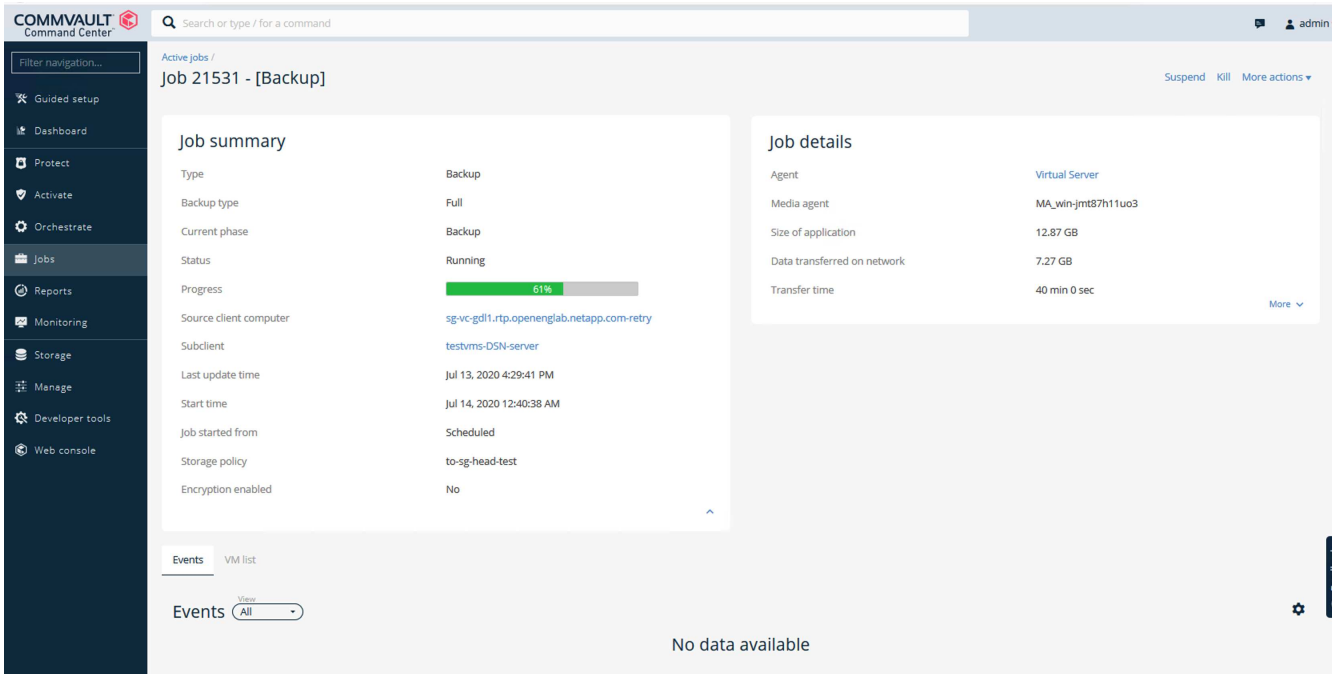
5. Sélectionnez un datastore, une machine virtuelle ou un ensemble de machines virtuelles, puis entrez son nom.
6. Sélectionnez le plan de sauvegarde que vous avez créé dans la tâche précédente.
7. Cliquez sur Enregistrer pour afficher le groupe de machines virtuelles que vous avez créé.
8. Dans le coin supérieur droit de la fenêtre VM group, sélectionnez Backup :



9. Sélectionnez Full comme niveau de sauvegarde, (facultatif) demandez un e-mail lorsque la sauvegarde est terminée, puis cliquez sur OK pour lancer votre tâche de sauvegarde :


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

10. Accédez à la page de résumé du travail pour afficher les mesures du travail :



Passez en revue les tests de performances de base

Lors de l'opération copie auxiliaire, quatre MediaAgents CommVault ont sauvegardé des données sur un système NetApp AFF A300 et une copie auxiliaire a été créée sur NetApp StorageGRID. Pour plus d'informations sur l'environnement de configuration de test, consultez la section conception de la solution et meilleures pratiques du "Protection des données scale-out NetApp avec CommVault" rapport technique.

Les tests ont été réalisés avec 100 machines virtuelles et 1000 machines virtuelles, les deux tests portant sur 50/50 combinaisons de machines virtuelles Windows et CentOS. Le tableau suivant présente les résultats de nos tests de performances de base :

Fonctionnement	Vitesse de secours	Vitesse de restauration
Copie aux	2 To/heure	1.27 To/heure
Direct vers et depuis l'objet (déduplication activée)	2.2 To/heure	1.22 To/heure

Pour tester les performances de suppression des données, 2.5 millions d'objets ont été supprimés. Comme le montrent les Figures 2 et 3, l'exécution de la suppression s'est terminée en moins de 3 heures et a libéré plus de 80 To d'espace. La séquence de suppression a démarré à 10:30 AM.

Figure 1 : suppression de 2.5 millions (80 To) d'objets en moins de 3 heures.

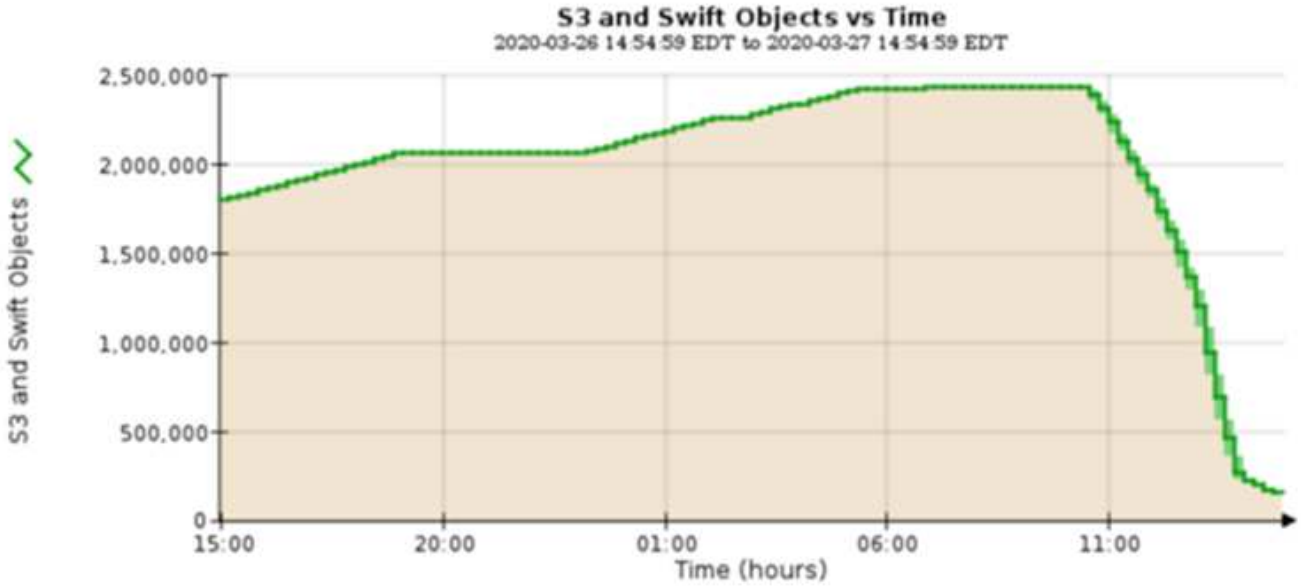
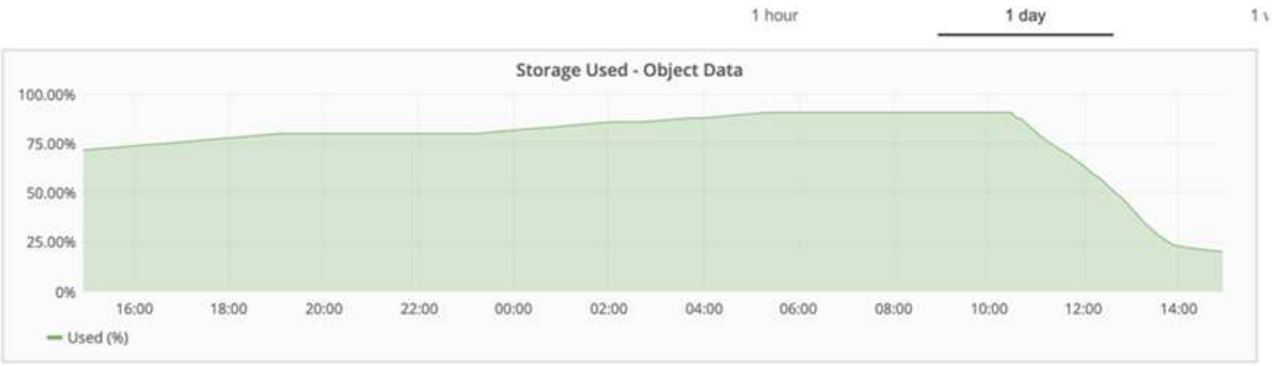


Figure 2 : libération de 80 To de stockage en moins de 3 heures.



Recommandation de niveau de cohérence des compartiments

NetApp StorageGRID permet à l'utilisateur final de sélectionner le niveau de cohérence des opérations effectuées sur les objets dans des compartiments simple Storage Service (S3).

CommVault MediaAgents sont les Data Movers d'un environnement CommVault. Dans la plupart des cas, les MediaAgents sont configurés pour écrire localement sur un site StorageGRID principal. Pour cette raison, un niveau de cohérence élevé est recommandé au sein d'un site primaire local. Lorsque vous définissez un niveau de cohérence sur les compartiments CommVault créés dans StorageGRID, veillez à respecter les consignes suivantes.

Si vous disposez d'une version de CommVault antérieure à 11.0.0 - Service Pack 16, envisagez de mettre à niveau CommVault vers la version la plus récente. Si ce n'est pas une option, assurez-vous de suivre les directives pour votre version.

- Versions CommVault antérieures à 11.0.0 - Service Pack 16.* dans les versions antérieures à 11.0.0 - Service Pack 16, CommVault effectue des opérations S3 HEAD et GET sur des objets inexistants dans le cadre du processus de restauration et de nettoyage. Définissez le niveau de cohérence du compartiment sur site forte pour atteindre un niveau de cohérence optimal pour les sauvegardes CommVault vers

StorageGRID.

- CommVault versions 11.0.0 - Service Pack 16 et ultérieures.* dans les versions 11.0.0 - Service Pack 16 et ultérieures, le nombre d'opérations S3 HEAD et GET effectuées sur des objets inexistants est réduit. Définissez le niveau de cohérence du compartiment par défaut sur lecture après nouvelle écriture afin d'assurer une cohérence élevée dans l'environnement CommVault et StorageGRID.

Tr-4626 : équilibreurs de charge

Utilisez des équilibreurs de charge tiers avec StorageGRID

En savoir plus sur le rôle d'équilibreurs de charge globaux ou tiers dans des systèmes de stockage objet tels que StorageGRID.

Conseils généraux pour la mise en œuvre de NetApp® StorageGRID® avec des équilibreurs de charge tiers.

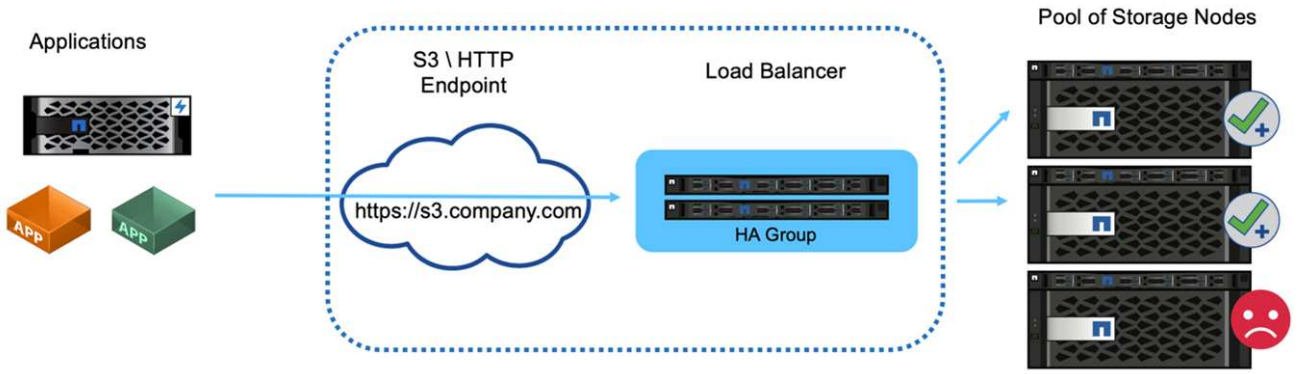
Le stockage objet est synonyme de stockage cloud et, comme vous le feriez, les applications qui exploitent le stockage cloud utilisent une adresse URL. Derrière cette URL simple, StorageGRID peut faire évoluer la capacité, les performances et la durabilité dans un seul site ou sur des sites dispersés géographiquement. L'équilibreur de charge constitue le principal facteur de simplicité.

L'objectif de ce document est d'informer les clients StorageGRID des options d'équilibreur de charge et de fournir des conseils généraux sur la configuration d'équilibreurs de charge tiers.

Principes de base de l'équilibreur de charge

Les équilibreurs de charge sont un composant essentiel d'un système de stockage objet haute performance tel que StorageGRID. StorageGRID est constitué de plusieurs nœuds de stockage, chacun pouvant présenter l'intégralité de l'espace de noms simple Storage Service (S3) d'une instance StorageGRID donnée. Les équilibreurs de charge créent un terminal extrêmement disponible derrière lequel nous pouvons placer les nœuds StorageGRID. StorageGRID est unique en son genre parmi les systèmes de stockage objet compatibles avec S3, dans la mesure où il fournit son propre équilibreur de charge, mais il prend également en charge des équilibreurs de charge tiers ou à usage générique tels que F5, Citrix NetScaler, HA Proxy, NGINX, etc.

La figure suivante utilise l'exemple URL/ nom de domaine complet (FQDN) « s3.company.com". L'équilibreur de charge crée une adresse IP virtuelle (VIP) qui résout le nom de domaine complet via DNS, puis dirige toutes les requêtes des applications vers un pool de nœuds StorageGRID. L'équilibreur de charge vérifie l'état de chaque nœud et établit uniquement les connexions aux nœuds sains.



La figure présente l'équilibreur de charge fourni par StorageGRID, mais le concept est le même pour les équilibreurs de charge tiers. Les applications établissent une session HTTP à l'aide du VIP sur l'équilibreur de

charge et le trafic passe par l'équilibreur de charge aux nœuds de stockage. Par défaut, l'ensemble du trafic, de l'application à l'équilibreur de charge et de l'équilibreur de charge au nœud de stockage, est chiffré via HTTPS. HTTP est une option prise en charge.

Équilibreurs de charge locaux et globaux

Il existe deux types d'équilibreurs de charge :

- **Gestionnaires locaux du trafic (LTM)**. Répartit les connexions sur un pool de nœuds dans un seul site.
- **Equilibreur de charge de service global (GSLB)**. Répartit les connexions sur plusieurs sites, assurant ainsi un équilibrage de charge efficace pour les équilibreurs de charge LTM. Considérez un GSLB comme un serveur DNS intelligent. Lorsqu'un client demande une URL de point de terminaison StorageGRID, le GSLB la résout au VIP d'un LTM en fonction de sa disponibilité ou d'autres facteurs (par exemple, quel site peut fournir une latence plus faible à l'application). Bien qu'un LTM soit toujours requis, un GSLB est facultatif selon le nombre de sites StorageGRID et les exigences de vos applications.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Considérations relatives à la conception de l'équilibreur de charge StorageGRID f5 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load NetApp StorageGRID d'équilibrage https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp—NetApp StorageGRID d'équilibrage de charge https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Utiliser les équilibreurs de charge StorageGRID

Découvrez le rôle d'un équilibreur de charge de nœud de passerelle StorageGRID .

Conseils généraux pour la mise en œuvre des nœuds de passerelle NetApp® StorageGRID®.

Équilibreur de charge des nœuds de passerelle StorageGRID par rapport à un équilibreur de charge tiers

En effet, StorageGRID est une fonctionnalité exclusive des fournisseurs de stockage objet compatibles avec S3, car elle offre un équilibreur de charge natif disponible en tant qu'appliance, VM ou conteneur dédiés. L'équilibreur de charge fourni par StorageGRID est également appelé nœud de passerelle.

Pour les clients qui ne possèdent pas encore d'équilibreur de charge, comme F5, Citrix, etc., l'implémentation d'un équilibreur de charge tiers peut s'avérer très complexe. L'équilibreur de charge StorageGRID simplifie considérablement les opérations d'équilibrage de charge.

Le nœud de passerelle est un équilibreur de charge haute performance, extrêmement disponible et haute performance. Les clients peuvent choisir d'implémenter le nœud de passerelle, l'équilibreur de charge tiers, ou même les deux, dans le même grid. Le nœud de passerelle est un gestionnaire de trafic local par rapport à un GSLB.

L’équilibreur de charge StorageGRID offre les avantages suivants :

- **Simplicité**. Configuration automatique des pools de ressources, vérifications de l’état, correctifs et maintenance, le tout géré par StorageGRID.
- **Performance**. L’équilibreur de charge StorageGRID est dédié à StorageGRID, peut fournir une mise en cache hautes performances et vous n’êtes pas en concurrence avec d’autres applications pour la bande passante.
- **Coût**. Les versions de machine virtuelle et de conteneur sont fournies sans frais supplémentaires.
- **Classifications de trafic**. La fonctionnalité Advanced Traffic Classification permet d’appliquer des règles de QoS spécifiques à StorageGRID ainsi qu’une analyse des workloads.
- **Futures fonctionnalités spécifiques à StorageGRID**. StorageGRID va continuer à optimiser et à ajouter des fonctionnalités innovantes à l’équilibreur de charge dans les prochaines versions.

En tant que nœud intégré de StorageGRID, le gestionnaire de trafic local a la possibilité d’utiliser des contrôles de santé avancés pour distribuer les demandes en fonction de l’état de santé, de la charge et de la disponibilité des ressources du nœud de stockage. De plus, il a la capacité de répartir la charge sur plusieurs sites lorsque les coûts de liaison StorageGRID sont définis sur « 0 » entre les sites. Dans le cas où les nœuds de stockage ne sont pas disponibles mais que le nœud de passerelle est disponible sur un site, la charge sera automatiquement dirigée vers un autre site de la grille.

La fonctionnalité de mise en cache de l’équilibreur de charge du nœud de passerelle est destinée à fournir une amélioration substantielle des performances pour certaines charges de travail (telles que la formation de l’IA) qui relisent un ensemble de données plusieurs fois dans le cadre du traitement de ces données. Les nœuds de passerelle de mise en cache peuvent également être déployés physiquement loin du reste de la grille, ce qui permet de meilleures performances et une utilisation réduite du réseau WAN dans certaines charges de travail. Le cache fonctionne en mode de lecture arrière où les écritures ne sont pas mises en cache et ne modifient pas l’état du cache. Chaque nœud de passerelle de mise en cache fonctionne indépendamment de tout autre nœud de passerelle de mise en cache.

Pour plus de détails sur le déploiement du nœud de passerelle StorageGRID , consultez le "Documentation StorageGRID" .

Découvrez comment implémenter des certificats SSL pour HTTPS dans StorageGRID

Comprendre l’importance et les étapes de la mise en œuvre des certificats SSL dans StorageGRID.

Si vous utilisez HTTPS, vous devez disposer d’un certificat SSL (Secure Sockets Layer). Le protocole SSL identifie les clients et les noeuds finaux et les valide comme étant approuvés. SSL assure également le cryptage du trafic. Le certificat SSL doit être approuvé par les clients. Pour ce faire, le certificat SSL peut provenir d’une autorité de certification (CA) de confiance mondiale, telle que DigiCert, d’une autorité de certification privée exécutée dans votre infrastructure ou d’un certificat auto-signé généré par l’hôte.

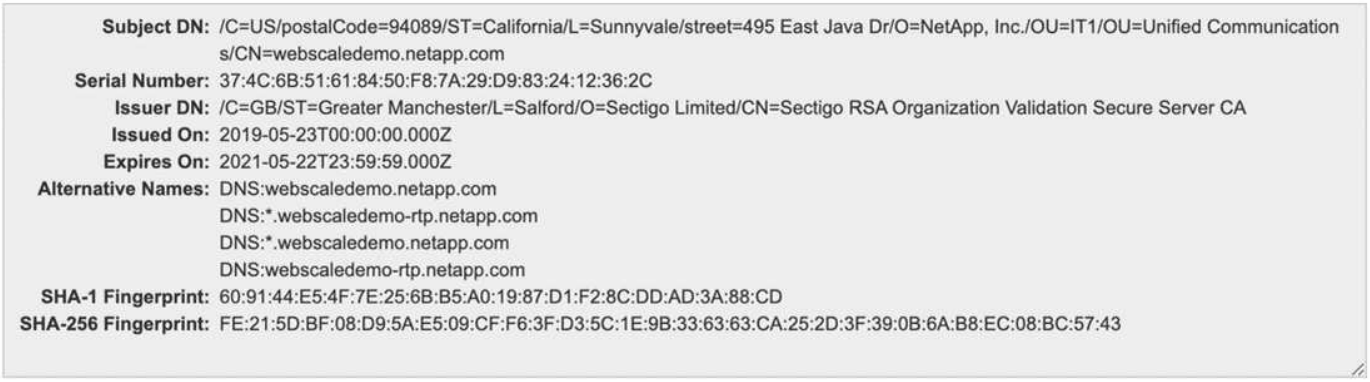
L’utilisation d’un certificat d’autorité de certification approuvée à l’échelle mondiale est la méthode recommandée, car aucune action supplémentaire côté client n’est requise. Le certificat est chargé dans l’équilibreur de charge ou StorageGRID, et les clients font confiance et se connectent au terminal.

L’utilisation d’une autorité de certification privée nécessite l’ajout de la racine et de tous les certificats subordonnés au client. Le processus d’approbation d’un certificat d’autorité de certification privée peut varier en fonction du système d’exploitation et des applications du client. Par exemple, dans ONTAP for FabricPool, vous devez télécharger individuellement chaque certificat de la chaîne (certificat racine, certificat subordonné,

certificat de point final) sur le cluster ONTAP.

L'utilisation d'un certificat auto-signé exige que le client ait confiance dans le certificat fourni sans aucune autorité de certification pour vérifier l'authenticité. Certaines applications peuvent ne pas accepter de certificats auto-signés et ne pas pouvoir ignorer la vérification.

Le placement du certificat SSL dans le chemin StorageGRID de l'équilibreur de charge du client dépend de l'emplacement où vous avez besoin de la terminaison SSL. Vous pouvez configurer un équilibreur de charge comme point d'extrémité pour le client, puis le chiffrer à nouveau ou le chiffrer à chaud avec un nouveau certificat SSL pour l'équilibreur de charge vers la connexion StorageGRID. Ou vous pouvez passer par le trafic et laisser StorageGRID être le point de terminaison SSL. Si l'équilibreur de charge est le noeud final de terminaison SSL, le certificat est installé sur l'équilibreur de charge et contient le nom du sujet pour le nom DNS/l'URL et tout autre nom URL/DNS pour lequel un client est configuré pour se connecter à la cible StorageGRID via l'équilibreur de charge, y compris les noms de caractères génériques. Si l'équilibreur de charge est configuré pour l'intercommunication, le certificat SSL doit être installé dans StorageGRID. Encore une fois, le certificat doit contenir le nom de l'objet du nom DNS/URL, ainsi que tous les autres noms URL/DNS pour lesquels un client est configuré pour se connecter à la cible StorageGRID via l'équilibreur de charge, y compris les noms de caractères génériques. Il n'est pas nécessaire d'inclure les noms de nœud de stockage individuel sur le certificat, mais uniquement les URL de point final.



Configurez un équilibreur de charge tiers fiable dans StorageGRID

Découvrez comment configurer un équilibreur de charge tiers fiable dans StorageGRID.

Si vous utilisez un ou plusieurs équilibreurs de charge de couche 7 externes et une règle de compartiment S3 ou de groupe basée sur IP, StorageGRID doit déterminer l'adresse IP de l'expéditeur réel. Pour ce faire, il examine l'en-tête X-Forided-for (XFF), qui est inséré dans la demande par l'équilibreur de charge. Étant donné que l'en-tête XFF peut facilement être usurpé dans les requêtes envoyées directement aux nœuds de stockage, StorageGRID doit confirmer que chaque demande est routée par un équilibreur de charge de niveau 7 approuvé. Si StorageGRID ne peut pas faire confiance à la source de la demande, il ignore l'en-tête XFF. Une API de gestion du grid permet de configurer une liste d'équilibreurs de charge externes de couche 7 approuvés. Cette nouvelle API est privée et est susceptible d'être modifiée dans les prochaines versions d'StorageGRID. Pour obtenir les informations les plus récentes, consultez l'article de la base de connaissances, "Comment configurer StorageGRID pour qu'il fonctionne avec des équilibreurs de charge tiers de couche 7".

En savoir plus sur les équilibreurs de charge du gestionnaire de trafic local

Explorez les conseils pour les équilibreurs de charge du gestionnaire de trafic local et déterminez la configuration optimale.

Vous trouverez ci-dessous des conseils généraux pour la configuration d'équilibreurs de charge tiers. Déterminez avec votre administrateur d'équilibreur de charge la configuration optimale pour votre environnement.

Créez un groupe de ressources de nœuds de stockage

Regroupez les nœuds de stockage StorageGRID dans un pool de ressources ou un groupe de services (la terminologie peut varier en fonction des équilibreurs de charge). Les nœuds de stockage StorageGRID présentent l'API S3 sur les ports suivants :

- HTTPS S3 : 18082
- S3 HTTP : 18084

La plupart des clients choisissent de présenter les API sur le serveur virtuel via les ports HTTPS et HTTP standard (443 et 80).

> Chaque site StorageGRID requiert une valeur par défaut de trois nœuds de stockage, deux d'entre eux devant être sains.

Vérification de l'état

Les équilibreurs de charge tiers ont besoin d'une méthode pour déterminer l'état de santé de chaque nœud et son éligibilité à la réception du trafic. NetApp recommande la méthode HTTP `OPTIONS` pour effectuer la vérification de l'état. L'équilibreur de charge envoie des requêtes HTTP `OPTIONS` à chaque nœud de stockage et attend une `200` réponse d'état.

Si aucun nœud de stockage ne fournit `200` de réponse, ce nœud ne peut pas traiter les demandes de stockage. Les exigences de vos applications et de votre entreprise doivent déterminer le délai d'attente de ces vérifications et les actions que votre équilibreur de charge prend.

Par exemple, si trois des quatre nœuds de stockage du data Center 1 sont en panne, vous pouvez diriger l'ensemble du trafic vers le data Center 2.

L'intervalle d'interrogation recommandé est d'une fois par seconde, marquant le nœud hors ligne après trois échecs de vérification.

Exemple de vérification de l'état S3

Dans l'exemple suivant, nous envoyons `OPTIONS` et vérifions pour `200 OK`. Nous l'utilisons `OPTIONS` car Amazon S3) ne prend pas en charge les requêtes non autorisées.

```
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
```

Vérifications de l'état des fichiers ou des contenus

En général, NetApp ne recommande pas de vérifications de l'état des systèmes basées sur des fichiers. En général, un petit fichier —`healthcheck.htm`, par exemple, est créé dans un compartiment avec une règle en lecture seule. Ce fichier est ensuite récupéré et évalué par l'équilibreur de charge. Cette approche présente plusieurs inconvénients :

- **Dépendant d'un seul compte.** Si le compte propriétaire du fichier est désactivé, le bilan de santé échoue et aucune demande de stockage n'est traitée.
- **Règles de protection des données.** Par défaut, le schéma de protection des données est une approche à deux copies. Dans ce scénario, si les deux nœuds de stockage hébergeant le fichier de vérification de l'état sont indisponibles, la vérification de l'état échoue et les demandes de stockage ne sont pas envoyées aux nœuds de stockage sains, ce qui rend la grille hors ligne.
- **Bloat du journal d'audit.** L'équilibreur de charge extrait le fichier de chaque nœud de stockage toutes les X minutes, créant ainsi de nombreuses entrées de journal d'audit.
- **Ressource intensive.** L'extraction du fichier de vérification de l'état de santé de chaque nœud toutes les quelques secondes consomme des ressources de réseau et de grille.

Si un contrôle de l'état basé sur le contenu est nécessaire, utilisez un locataire dédié avec un compartiment S3 dédié.

Persistance de la session

La persistance de session, ou persistance, fait référence à la durée pendant laquelle une session HTTP donnée est autorisée à persister. Par défaut, les sessions sont supprimées par les nœuds de stockage au bout de 10 minutes. Une persistance plus longue peut améliorer les performances, car les applications n'ont pas besoin de rétablir leurs sessions pour chaque action. Cependant, garder ces sessions ouvertes consomme des ressources. Si vous déterminez que votre charge de travail sera avantageuse, vous pouvez réduire la

persistance des sessions sur un équilibreur de charge tiers.

Adressage virtuel de type hébergé

La méthode par défaut d'AWS S3 est désormais de type hébergement virtuel. StorageGRID et de nombreuses applications prennent toujours en charge le style de chemin, mais il est recommandé d'implémenter la prise en charge de type hébergement virtuel. Les demandes de type hébergement virtuel disposent du compartiment dans le nom de l'hôte.

Pour prendre en charge le style hébergé virtuel, procédez comme suit :

- Prend en charge les recherches DNS génériques : *.s3.company.com
- Utilisez un certificat SSL avec des noms alt d'objet pour prendre en charge le caractère générique : *.s3.company.com certains clients ont exprimé des préoccupations de sécurité concernant l'utilisation de certificats génériques. StorageGRID continue de prendre en charge l'accès de type chemin, tout comme les applications clés telles que FabricPool. Ceci étant dit, certains appels de l'API S3 échouent ou se comportent de manière incorrecte sans prise en charge hébergée virtuelle.

Terminaison SSL

La terminaison SSL présente des avantages en termes de sécurité sur les équilibreurs de charge tiers. Si l'équilibreur de charge est compromis, le grid est compartimenté.

Trois configurations sont prises en charge :

- **Pass-through SSL.** Le certificat SSL est installé sur StorageGRID en tant que certificat de serveur personnalisé.
- **Terminaison et re-cryptage SSL (recommandé).** Cela peut être bénéfique si vous effectuez déjà la gestion des certificats SSL sur l'équilibreur de charge plutôt que d'installer le certificat SSL sur StorageGRID. Cette configuration offre l'avantage de sécurité supplémentaire de limiter la surface d'attaque à l'équilibreur de charge.
- **Terminaison SSL avec HTTP.** Dans cette configuration, SSL est interrompu sur l'équilibreur de charge tiers et la communication entre l'équilibreur de charge et StorageGRID n'est pas chiffrée pour tirer parti du déchargement SSL (avec les bibliothèques SSL intégrées dans les processeurs modernes, cela présente un avantage limité).

Configuration de passage

Si vous préférez configurer votre équilibreur de charge pour le transfert, vous devez installer le certificat sur StorageGRID. Accédez au **Configuration › certificats de serveur › noeuds finaux du service API de stockage objet certificat de serveur**.

Visibilité IP du client source

StorageGRID 11.4 a introduit le concept d'équilibreur de charge tiers fiable. Pour transférer l'adresse IP de l'application client vers StorageGRID, vous devez configurer cette fonction. Pour plus d'informations, voir "Comment configurer StorageGRID pour qu'il fonctionne avec des équilibreurs de charge tiers de couche 7."

Pour activer l'en-tête XFF pour afficher l'adresse IP de l'application client, procédez comme suit :

Étapes

1. Enregistrez l'adresse IP du client dans le journal d'audit.

2. Utilisez `aws:SourceIp` un compartiment S3 ou une règle de groupe.

Stratégies d'équilibrage de charge

La plupart des solutions d'équilibrage de charge offrent plusieurs stratégies d'équilibrage de charge. Les stratégies courantes sont les suivantes :

- **Robin rond.** Une solution universelle, mais avec peu de nœuds et de grands transferts obstruant les nœuds uniques.
- **Connexion minimale.** Convient parfaitement aux charges de travail mixtes et de petite taille qui offrent une distribution égale des connexions à tous les nœuds.

Le choix de l'algorithme devient moins important, car le nombre de nœuds de stockage est de plus en plus important.

Chemin d'accès aux données

Les données transitent par les équilibreurs de charge du gestionnaire de trafic local. StorageGRID ne prend pas en charge le routage direct de serveur (DSR).

Vérification de la distribution des connexions

Pour vérifier que votre méthode répartit la charge uniformément entre les nœuds de stockage, vérifiez les sessions établies sur chaque nœud d'un site donné :

- **Méthode UI.** Aller au **support › Metrics › S3 Overview › LDR HTTP sessions**
- **API métriques.** Utilisation `storagegrid_http_sessions_incoming_currently_established`

Découvrez quelques utilisations des configurations StorageGRID

Explorez les quelques cas d'utilisation des configurations StorageGRID mises en œuvre par les clients et PAR NetApp IT.

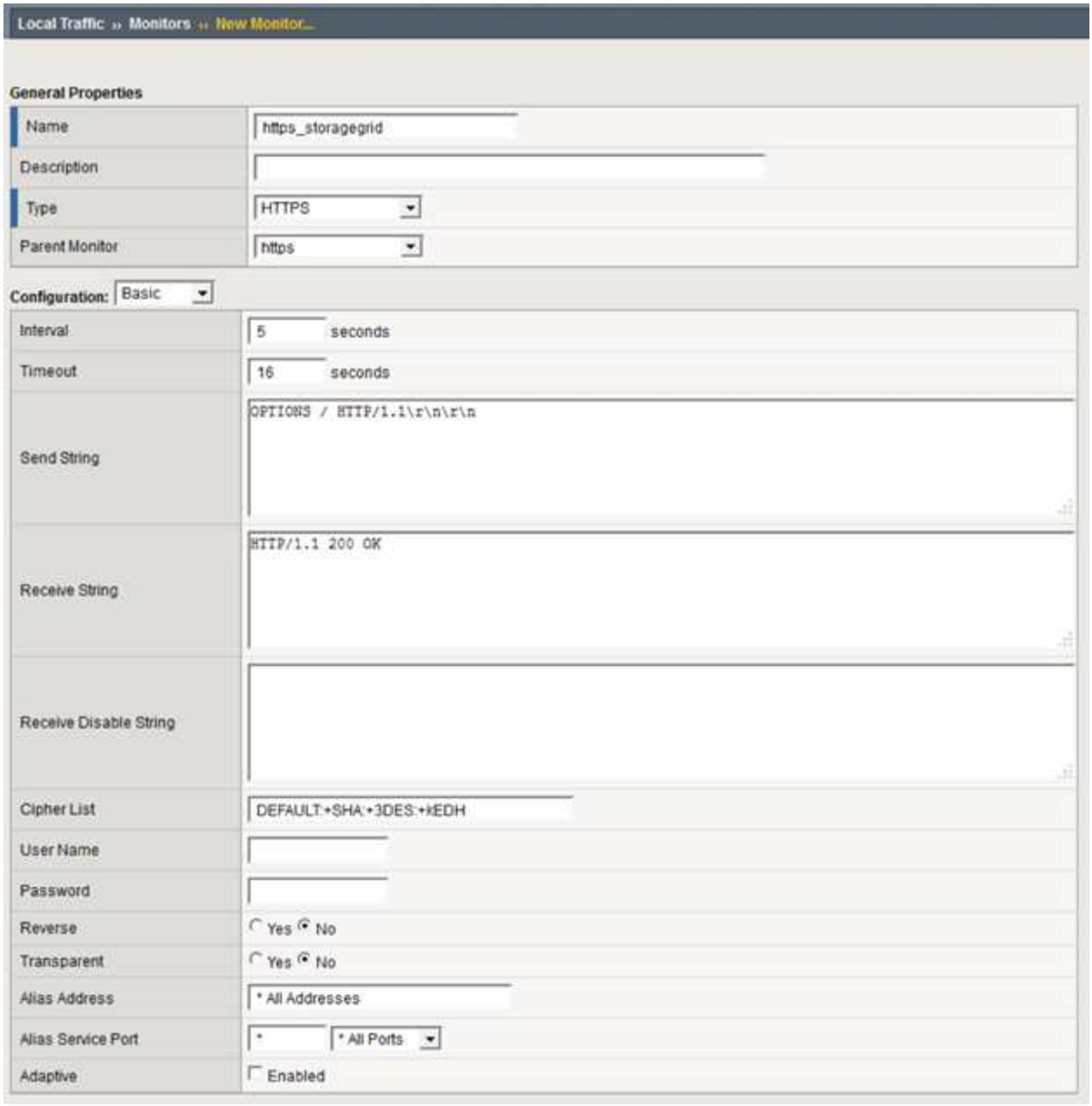
Les exemples suivants illustrent les configurations mises en œuvre par les clients StorageGRID, y compris NetApp IT.

Contrôle DE l'état du gestionnaire du trafic local BIG-IP de F5 pour le compartiment S3

Pour configurer le moniteur de vérification de l'état du gestionnaire de trafic local BIG-IP F5, procédez comme suit :

Étapes

1. Créer un nouveau moniteur.
   a. Dans le champ Type, entrez `HTTPS`.
   b. Configurez l'intervalle et le délai d'attente comme vous le souhaitez.
   c. Dans le champ Envoyer chaîne, entrez `OPTIONS / HTTP/1.1\r\n\r\n`. \r\n sont des retours chariot ; les différentes versions du logiciel BIG-IP nécessitent zéro, un ou deux ensembles de séquences \r\n. Pour plus d'informations, voir https://support.f5.com/csp/article/K10655.
   d. Dans le champ chaîne de réception, entrez : `HTTP/1.1 200 OK`.



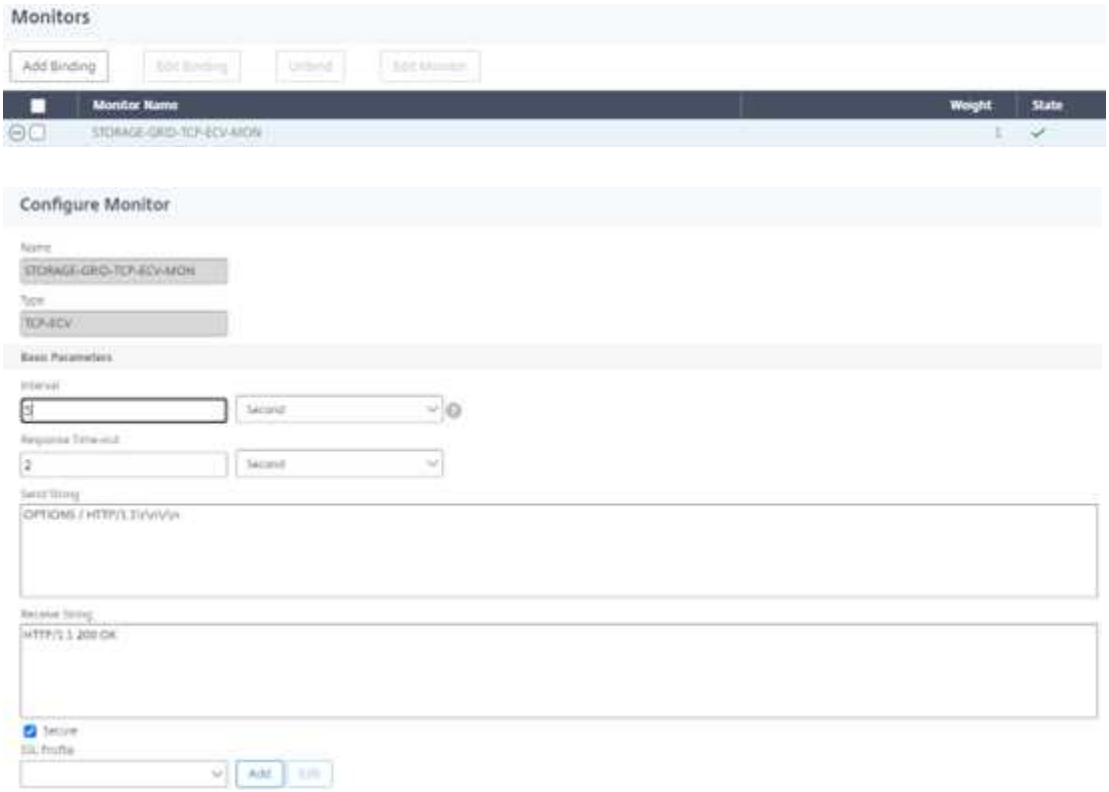
2. Dans Créer un pool, créez un pool pour chaque port requis.
   a. Attribuez le contrôle de l'état que vous avez créé à l'étape précédente.
   b. Sélectionnez une méthode d'équilibrage de charge.
   c. Sélectionnez le port de service : 18082 (S3).
   d. Ajouter des nœuds.

Citrix NetScaler

Citrix NetScaler crée un serveur virtuel pour le terminal de stockage et fait référence aux nœuds de stockage StorageGRID en tant que serveurs d'applications, qui sont ensuite regroupés dans des services.

Utilisez le moniteur de vérification de l'état de santé HTTPS-ECV pour créer un moniteur personnalisé afin d'effectuer le contrôle de l'état de santé recommandé en utilisant les OPTIONS demande et réception `200`. HTTP-ECV est configuré avec une chaîne d'envoi et valide une chaîne de réception.

Pour plus d'informations, consultez la documentation Citrix, "Exemple de configuration pour le moniteur de vérification de l'état HTTP-ECV".



Loadbalancer.org

Loadbalancer.org a réalisé ses propres tests d'intégration avec StorageGRID et dispose d'un guide de configuration complet : https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp a réalisé ses propres tests d'intégration avec StorageGRID et dispose d'un guide de configuration complet : https://kemptechnologies.com/solutions/netapp/.

HABProxy

Configurez HANProxy pour utiliser la demande d'OPTIONS et vérifiez la réponse d'état 200 pour le contrôle d'intégrité dans haproxy.cfg. Vous pouvez remplacer le port de liaison de l'interface frontale par un autre port, tel que 443.

Voici un exemple de terminaison SSL sur HASProxy :

```
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
```

Voici un exemple de 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
```

Pour obtenir des exemples complets de configurations pour StorageGRID, reportez-vous à la section "Exemples de configuration HANProxy" sur GitHub.

Valider la connexion SSL dans StorageGRID

Apprenez à valider la connexion SSL dans StorageGRID.

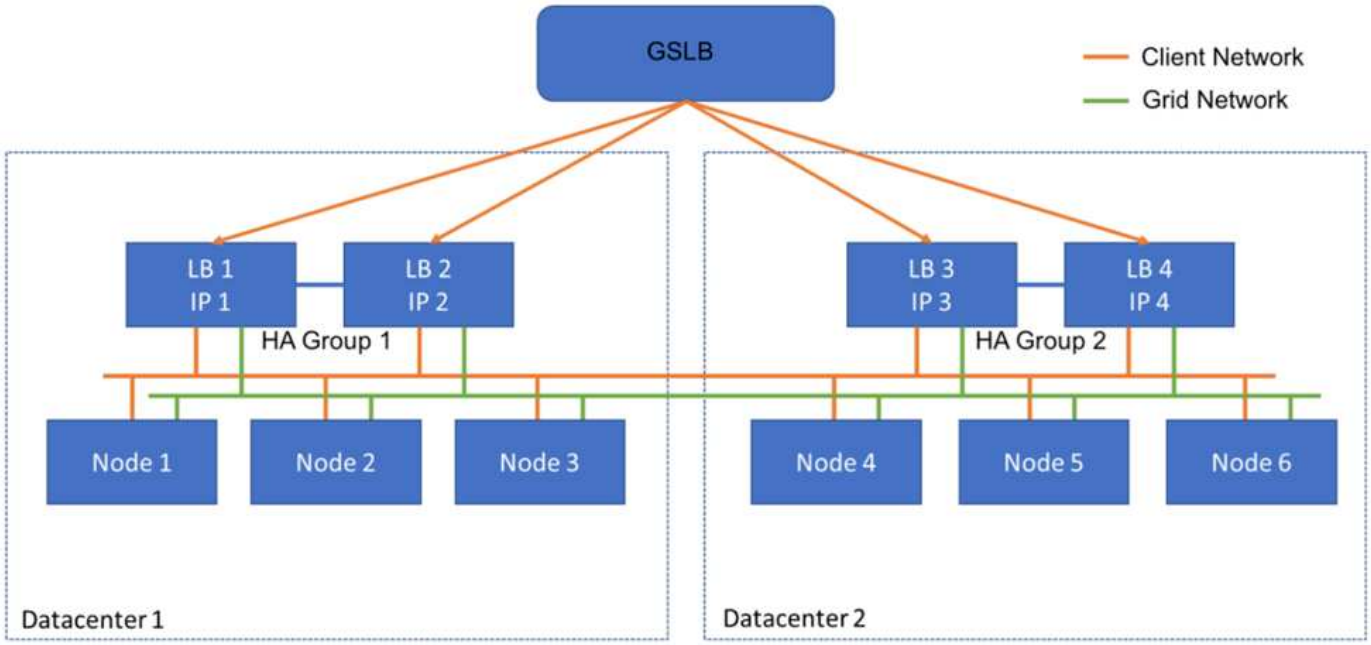
Une fois votre équilibreur de charge configuré, vous devez valider la connexion à l'aide d'outils tels que OpenSSL et l'interface de ligne de commande AWS. D'autres applications, telles que le navigateur S3, peuvent ignorer les erreurs de configuration SSL.

Comprendre les exigences globales d'équilibrage de charge pour StorageGRID

Explorez les considérations et exigences de conception pour l'équilibrage global de la charge dans StorageGRID.

L'équilibrage global de la charge nécessite l'intégration à DNS pour assurer un routage intelligent sur plusieurs sites StorageGRID. Cette fonction ne relève pas du domaine StorageGRID et doit être fournie par une solution tierce, telle que les produits d'équilibrage de charge mentionnés précédemment et/ou une solution de contrôle du trafic DNS telle qu'Infoblox. Cet équilibrage de charge de niveau supérieur assure le routage intelligent vers

le site de destination le plus proche dans l'espace de noms, ainsi que la détection des pannes et la redirection vers le site suivant dans l'espace de noms. Une implémentation GSLB type consiste en un GSLB de niveau supérieur avec des pools de site contenant des équilibreurs de charge site-local. Les équilibreurs de charge de site contiennent des pools de nœuds de stockage sur site local. Cela peut inclure une combinaison d'équilibreurs de charge tiers pour les fonctions GSLB et de StorageGRID fournissant l'équilibrage de charge site-local, ou une combinaison de tiers. Un grand nombre de tiers évoqués précédemment peuvent fournir à la fois un équilibrage de charge GSLB et site-local.



Tr-4645 : fonctions de sécurité

Sécurisation des données et des métadonnées StorageGRID dans un magasin d'objets

Découvrez les fonctions de sécurité intégrées à la solution de stockage objet StorageGRID.

Il s'agit d'un aperçu des nombreuses fonctionnalités de sécurité de NetApp® StorageGRID®, couvrant l'accès aux données, les objets et les métadonnées, l'accès administratif et la sécurité de la plate-forme. Il a été mis à jour pour inclure les dernières fonctionnalités publiées avec StorageGRID 12.0.

La sécurité fait partie intégrante de la solution de stockage objet NetApp StorageGRID. La sécurité est particulièrement importante, car de nombreux types de données riches bien adaptées au stockage objet sont également sensibles, soumises aux réglementations et à la conformité. À mesure que les fonctionnalités StorageGRID continuent d'évoluer, le logiciel met à disposition de nombreuses fonctionnalités de sécurité précieuses pour protéger la stratégie de sécurité de l'entreprise et aider l'entreprise à respecter les bonnes pratiques du secteur.

Cet article présente un aperçu des nombreuses fonctionnalités de sécurité de StorageGRID 12.0, divisées en cinq catégories :

- Sécurité de l'accès aux données
- Fonctionnalités de sécurité des objets et des métadonnées

- Fonctions de sécurité de l'administration
- Fonctions de sécurité de la plate-forme
- Intégration au cloud

Ce document est destiné à être une fiche technique de sécurité : il ne détaille pas comment configurer le système pour prendre en charge les fonctionnalités de sécurité énumérées qui ne sont pas configurées par défaut. Le "Guide de renforcement de la StorageGRID" est disponible sur le site officiel "Documentation StorageGRID" page.

Outre les fonctionnalités décrites dans ce rapport, StorageGRID suit le "Politique de notification et de réponse aux vulnérabilités de sécurité des produits NetApp". Les vulnérabilités signalées sont vérifiées et une réponse est apportée conformément au processus de réponse aux incidents de sécurité du produit.

NetApp StorageGRID fournit des fonctionnalités de sécurité avancées pour les cas d'utilisation très exigeants du stockage objet.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- NetApp StorageGRID : évaluation de la conformité SEC 17a-4(f), FINRA 4511(c) et CFTC 1.31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Certification cryptographique du NetApp StorageGRID NIST FIPS 140-3 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- Certification d'entropie NetApp StorageGRID NIST SP 800-90B https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- Certification Critères communs du Centre canadien de cybersécurité pour NetApp StorageGRID https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- Page de documentation de StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Termes et acronymes

Cette section fournit des définitions de la terminologie utilisée dans le document.

Terme ou acronyme	Définition
S3	Simple Storage Service.
Client	Application pouvant interagir avec StorageGRID via le protocole S3 d'accès aux données ou le protocole HTTP de gestion.
Administrateur des locataires	Administrateur du compte locataire StorageGRID
Utilisateur locataire	Utilisateur d'un compte de locataire StorageGRID
TLS	Sécurité de la couche de transport
ILM	Gestion du cycle de vie des informations
RÉSEAU LOCAL	Réseau local
Administrateur du grid	Administrateur du système StorageGRID

Terme ou acronyme	Définition
Grille	Le système StorageGRID
Godet	Un conteneur pour les objets stockés dans S3
LDAP	Protocole d’accès à l’annuaire simplifié
SEC	Securities and Exchange Commission; réglemente les membres de change, les courtiers ou les courtiers
FINRA	Autorité de réglementation du secteur financier ; diffère des exigences de format et de support de la règle SEC 17a-4(f)
CFTC	Commissions sur les opérations à terme sur les matières premières; réglemente les opérations à terme sur les matières premières
NIST	Institut national des normes et de la technologie

Sécurité de l’accès aux données

Découvrez les fonctionnalités de sécurité d’accès aux données de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
TLS (transport Layer Security) configurable	TLS établit un protocole de liaison pour la communication entre un client et un nœud de passerelle StorageGRID, un nœud de stockage ou un point d'extrémité d'équilibreur de charge. StorageGRID prend en charge les suites de chiffrement suivantes pour 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 TLS v1.2 et 1.3 pris en charge. SSLv3, TLS v1.1 et les versions antérieures ne sont pas pris en charge.	Permet à un client et à StorageGRID de s'identifier et de s'authentifier mutuellement et de communiquer avec confidentialité et intégrité des données. Garantit l'utilisation d'une version TLS récente. Les chiffrements sont désormais configurables sous les paramètres de configuration/sécurité	—

Fonction	Fonction	Impact	Conformité réglementaire
Certificat de serveur configurable (noeud final Load Balancer)	Les administrateurs du grid peuvent configurer les noeuds finaux Load Balancer pour générer ou utiliser un certificat de serveur.	Permet l'utilisation de certificats numériques signés par leur autorité de certification approuvée standard pour authentifier les opérations d'API d'objet entre la grille et le client par point final Load Balancer.	—
Certificat de serveur configurable (terminal API)	Les administrateurs du grid peuvent configurer de manière centralisée tous les terminaux de l'API StorageGRID pour qu'ils utilisent un certificat de serveur signé par l'autorité de certification de confiance de leur entreprise.	Permet l'utilisation de certificats numériques signés par leur autorité de certification standard de confiance pour authentifier les opérations de l'API objet entre un client et la grille.	—

Fonction	Fonction	Impact	Conformité réglementaire
Colocation	StorageGRID prend en charge plusieurs locataires par grille ; chaque locataire dispose de son propre espace de noms. Un locataire utilise le protocole S3. Par défaut, l'accès aux compartiments/conteneurs et aux objets est limité aux utilisateurs au sein du compte. Les locataires peuvent avoir un utilisateur (par exemple, un déploiement d'entreprise, dans lequel chaque utilisateur a son propre compte) ou plusieurs utilisateurs (par exemple, un déploiement de fournisseur de services, dans lequel chaque compte est une entreprise et un client du fournisseur de services). Les utilisateurs peuvent être locaux ou fédérés. Les utilisateurs fédérés sont définis par Active Directory ou LDAP (Lightweight Directory Access Protocol). StorageGRID fournit un tableau de bord par locataire, dans lequel les utilisateurs se connectent à l'aide de leurs informations d'identification de compte locales ou fédérées. Les utilisateurs peuvent accéder à des rapports visualisés sur l'utilisation des locataires par rapport au quota attribué par l'administrateur de la grille, y compris des informations d'utilisation dans les données et objets stockés par compartiments. Les utilisateurs disposant d'autorisations administratives peuvent effectuer des tâches d'administration système au niveau du locataire, telles que la gestion des utilisateurs et des groupes et des clés d'accès.	Permet aux administrateurs StorageGRID d'héberger les données de plusieurs locataires tout en isolant l'accès des locataires et d'établir l'identité des utilisateurs en fédérant les utilisateurs avec un fournisseur d'identité externe, tel qu'Active Directory ou LDAP.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Non-répudiation des identifiants d'accès	Chaque opération S3 est identifiée et consignée à l'aide d'un compte de locataire, d'un utilisateur et d'une clé d'accès uniques.	Permet aux administrateurs du grid d'établir les actions d'API exécutées par des individus.	—
Accès anonyme désactivé	Par défaut, l'accès anonyme est désactivé pour les comptes S3. Un demandeur doit disposer d'un droit d'accès valide pour qu'un utilisateur valide du compte de tenant puisse accéder aux compartiments, conteneurs ou objets du compte. L'accès anonyme aux compartiments ou objets S3 peut être activé avec une règle IAM explicite.	Permet aux administrateurs de Grid de désactiver ou de contrôler l'accès anonyme aux compartiments/conteneurs et objets.	—
Conformité WORM	Conçu pour répondre aux exigences de la règle SEC 17a-4(f) et validé par Cohasset. Les clients peuvent assurer la conformité au niveau du compartiment. La conservation peut être étendue, mais jamais réduite. Les règles de gestion du cycle de vie des informations (ILM) appliquent des niveaux minimaux de protection des données.	Permet aux locataires qui ont des exigences réglementaires en matière de conservation des données d'activer la protection WORM sur les objets stockés et les métadonnées d'objet.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
VER	Les administrateurs du grid peuvent activer le mode WORM au niveau de la grille en activant l'option Désactiver la modification du client, qui empêche les clients d'écraser ou de supprimer des objets ou des métadonnées d'objet dans tous les comptes de locataires. Les administrateurs de locataires S3 peuvent également activer le mode WORM par locataire, compartiment ou préfixe d'objet en spécifiant une règle IAM qui inclut l'autorisation S3 : PutOverwriteObject personnalisée pour le remplacement d'objets et de métadonnées.	Permet aux administrateurs du grid et aux locataires de contrôler la protection WORM sur les objets stockés et les métadonnées d'objet.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Gestion des clés de cryptage du serveur hôte KM	Les administrateurs du grid peuvent configurer un ou plusieurs serveurs de gestion externe des clés (KMS) dans Grid Manager afin que les clés de chiffrement soient attribuées aux services StorageGRID et aux appliances de stockage. Chaque serveur hôte KMS ou cluster de serveurs hôtes KMS utilise le protocole KMIP (Key Management Interoperability Protocol) pour fournir une clé de chiffrement aux nœuds de l'appliance sur le site StorageGRID associé.	Vous pouvez chiffrer les données au repos. Une fois les volumes de l'appliance chiffrés, vous ne pouvez pas accéder aux données de l'appliance sauf si le nœud peut communiquer avec le serveur hôte KMS.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Basculement automatique	StorageGRID fournit une redondance intégrée et un basculement automatisé. L'accès aux comptes de locataires, aux compartiments et aux objets peut continuer même en cas de pannes multiples, depuis des disques ou des nœuds jusqu'à des sites entiers. StorageGRID est conscient des ressources et redirige automatiquement les requêtes vers les nœuds disponibles et les emplacements de données. Les sites StorageGRID peuvent même fonctionner en mode iskattered. En cas de panne de réseau étendu, un site est déconnecté du reste du système, les lectures et écritures peuvent continuer avec les ressources locales, et la réplication reprend automatiquement lorsque le réseau WAN est restauré.	Permet aux administrateurs du grid de répondre aux exigences de disponibilité, aux contrats de niveau de service et aux autres obligations contractuelles et de mettre en œuvre des plans de continuité de l'activité.	—
Fonctions de sécurité d'accès aux données spécifiques à S3	Signature AWS version 2 et version 4	La signature des requêtes d'API permet d'authentifier les opérations de l'API S3. Amazon prend en charge deux versions de Signature version 2 et version 4. Le processus de signature vérifie l'identité du demandeur, protège les données en transit et les protège contre les attaques de relecture potentielles.	S'aligne sur la recommandation AWS pour Signature version 4 et permet une rétrocompatibilité avec les anciennes applications avec Signature version 2.

Fonction	Fonction	Impact	Conformité réglementaire
—	Verrouillage d'objet S3	La fonctionnalité de verrouillage objet S3 d'StorageGRID est une solution de protection objet équivalente au verrouillage objet S3 dans Amazon S3.	Permet aux locataires de créer des compartiments avec S3 Object Lock activé pour se conformer aux réglementations exigeant la conservation de certains objets pendant une durée fixe ou indéfiniment.
Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)	Stockage sécurisé des identifiants S3	Les clés d'accès S3 sont stockées dans un format protégé par une fonction de hachage des mots de passe (SHA-2).	Permet le stockage sécurisé des clés d'accès par une combinaison de longueur de clé (un nombre généré de manière aléatoire de 10^{31}) et d'un algorithme de hachage de mot de passe.
—	Clés d'accès S3 limitées dans le temps	Lorsque vous créez une clé d'accès S3 pour un utilisateur, les clients peuvent définir une date et une heure d'expiration sur la clé d'accès.	Permet aux administrateurs du grid de provisionner des clés d'accès S3 temporaires.
—	Plusieurs clés d'accès par compte d'utilisateur	StorageGRID permet de créer plusieurs clés d'accès et de les activer simultanément pour un compte utilisateur. Chaque action d'API étant consignée avec un compte utilisateur de locataire et une clé d'accès, la non-répudiation est préservée même si plusieurs clés sont actives.	Permet aux clients de faire pivoter les clés d'accès sans interruption et à chaque client d'avoir sa propre clé, décourageant ainsi le partage des clés entre les clients.

Fonction	Fonction	Impact	Conformité réglementaire
—	Règle d’accès IAM S3	StorageGRID prend en charge les règles IAM S3, ce qui permet aux administrateurs du grid de spécifier le contrôle d’accès granulaire par locataire, compartiment ou préfixe d’objet. StorageGRID prend également en charge les conditions et les variables des règles IAM, ce qui permet des règles de contrôle d’accès plus dynamiques.	Permet aux administrateurs de Grid de spécifier le contrôle d’accès par groupes d’utilisateurs pour l’ensemble du tenant ; permet également aux utilisateurs locataires de spécifier le contrôle d’accès pour leurs propres compartiments et objets.
—	API du service de jeton de sécurité S3 AssumeRole	StorageGRID prend en charge l’API S3 STS AssumeRole pour fournir des informations d’identification de sécurité temporaires (ID de clé d’accès, clé d’accès secrète, jeton de session) avec des autorisations réduites et une durée limitée. Les stratégies de session en ligne permettant de restreindre davantage les autorisations pendant la session sont prises en charge dans le cadre de l’API AssumeRole.	Permet aux administrateurs locataires de fournir un accès temporaire sécurisé aux données de l’objet.

Fonction	Fonction	Impact	Conformité réglementaire
—	Service de notification simple	StorageGRID prend en charge l'envoi de notifications lors de l'accès aux objets. Les types d'événements suivants sont pris en charge : • s3 : Objet créé : • s3:ObjetCréé:Mettre • s3 : Objet créé : Publication • s3:ObjetCréé:Copier • s3 : Objet créé : Téléchargement multi-parties complet • s3 : Objet supprimé : • s3:ObjectRemoved:Supprimer • s3 : Objet supprimé : Supprimer le marqueur créé • s3 : Restauration d'objet : Publication	Permet aux administrateurs locataires de surveiller l'accès aux objets
—	Chiffrement côté serveur avec clés gérées par StorageGRID (SSE)	StorageGRID prend en charge SSE, ce qui permet une protection mutualisée des données au repos avec des clés de chiffrement gérées par StorageGRID.	Permet aux locataires de chiffrer les objets. Une clé de chiffrement est requise pour écrire et récupérer ces objets.
Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)	Chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)	StorageGRID prend en charge SSE-C, ce qui permet une protection mutualisée des données au repos avec des clés de chiffrement gérées par le client. Bien que StorageGRID gère toutes les opérations de chiffrement et de déchiffrement d'objets, avec SSE-C, le client doit gérer les clés de cryptage lui-même.	Permet aux clients de chiffrer les objets avec des clés qu'ils contrôlent. Une clé de chiffrement est requise pour écrire et récupérer ces objets.

Sécurité des objets et des métadonnées

Explorez les fonctionnalités de sécurité des objets et des métadonnées de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Advanced Encryption Standard (AES) - chiffrement d'objets côté serveur	StorageGRID assure le chiffrement des objets côté serveur basé sur AES 128 et AES 256. Les administrateurs du grid peuvent activer le chiffrement comme paramètre global par défaut. StorageGRID prend également en charge l'en-tête de chiffrement S3 x-amz côté serveur pour activer ou désactiver le chiffrement par objet. Lorsque cette option est activée, les objets sont chiffrés lorsqu'ils sont stockés ou en transit entre des nœuds de grid.	Stockage et transmission sécurisés d'objets, indépendamment du matériel de stockage sous-jacent.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Gestion intégrée des clés	Lorsque le chiffrement est activé, chaque objet est chiffré avec une clé symétrique unique générée de manière aléatoire, stockée dans StorageGRID sans accès externe.	Permet le chiffrement des objets sans gestion externe des clés.	
Disques de chiffrement conformes à la norme FIPS (Federal information Processing Standard) 140-2	Les appliances StorageGRID SG5812, SG5860, SG6160 et SGF6024 offrent la possibilité d'utiliser des disques de chiffrement conformes à la norme FIPS 140-2. Les clés de chiffrement des disques peuvent être gérées par un serveur KMIP externe.	Stockage sécurisé des données, métadonnées et objets du système. Le chiffrement logiciel des objets StorageGRID sécurise le stockage et la transmission des objets.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Cryptage conforme à la norme FIPS (Federal Information Processing Standard) 140-3 pour les nœuds	Les appliances StorageGRID SG5812, SG5860, SG6160, SGF6112, SG1100 et SG110 offrent l'option de chiffrement de nœud conforme à la norme FIPS 140-3. Les clés de chiffrement des nœuds sont gérées par un serveur KMIP externe.	Stockage sécurisé des données, métadonnées et objets du système. Le chiffrement logiciel des objets StorageGRID sécurise le stockage et la transmission des objets.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Analyse de l'intégrité en arrière-plan et auto-rétablissement	StorageGRID utilise un mécanisme d'interverrouillage de hachages, de checksums et de vérifications de la redondance cyclique (CRC) au niveau de l'objet et des sous-objets pour se protéger contre l'incohérence, la falsification ou la modification des données, aussi bien lorsque les objets sont en stockage qu'en transit. StorageGRID détecte automatiquement les objets corrompus et falsifiés et les remplace, tout en mettant en quarantaine les données modifiées et en alertant l'administrateur.	Permet aux administrateurs du grid de respecter les SLA, les réglementations et autres obligations en matière de durabilité des données. Aide les clients à détecter les ransomwares ou les virus qui tentent de chiffrer, d'altérer ou de modifier des données.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Placement et conservation des objets basés sur des règles	StorageGRID permet aux administrateurs du grid de configurer des règles ILM, qui spécifient la conservation, le placement, la protection, la transition et l'expiration des objets. Les administrateurs du grid peuvent configurer StorageGRID pour filtrer les objets en fonction de leurs métadonnées et appliquer des règles à différents niveaux de granularité, notamment à l'échelle du grid, du locataire, du compartiment, du préfixe de clé et des paires clé-valeur de métadonnées définies par l'utilisateur. StorageGRID permet de s'assurer que les objets sont stockés conformément aux règles ILM tout au long de leur cycle de vie, à moins qu'ils ne soient explicitement supprimés par le client.	Renforce le placement, la protection et la conservation des données. Aide les clients à respecter les SLA en matière de durabilité, de disponibilité et de performance.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Analyse des métadonnées en arrière-plan	StorageGRID analyse régulièrement les métadonnées d'objet en arrière-plan pour appliquer des modifications au placement ou à la protection des données d'objet, comme spécifié par la règle ILM.	Permet de détecter les objets corrompus.	
Cohérence ajustable	Les locataires peuvent sélectionner des niveaux de cohérence au niveau du compartiment pour s'assurer que les ressources, telles que la connectivité multisite, sont disponibles.	Offre la possibilité d'effectuer des écritures dans la grille uniquement lorsqu'un nombre requis de sites ou de ressources est disponible.	

Fonctions de sécurité de l'administration

Découvrez les fonctions de sécurité d'administration de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Certificat de serveur (interface de gestion Grid)	Les administrateurs du grid peuvent configurer l'interface de gestion Grid pour utiliser un certificat de serveur signé par l'autorité de certification approuvée de leur organisation.	Permet l'utilisation de certificats numériques signés par leur autorité de certification standard et approuvée pour authentifier l'accès à l'interface utilisateur de gestion et à l'API entre un client de gestion et la grille.	—
Authentification utilisateur administrative	Les utilisateurs administratifs sont authentifiés à l'aide du nom d'utilisateur et du mot de passe. Les utilisateurs et groupes administratifs peuvent être locaux ou fédérés, importés depuis Active Directory ou LDAP du client. Les mots de passe des comptes locaux sont stockés dans un format protégé par bcrypt ; les mots de passe de ligne de commande sont stockés dans un format protégé par SHA-2.	Authentifie l'accès administratif à l'interface utilisateur de gestion et aux API.	—

Fonction	Fonction	Impact	Conformité réglementaire
Prise en charge SAML	StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme SAML 2.0 (Security assertion Markup Language 2.0). Lorsque l'authentification SSO est activée, tous les utilisateurs doivent être authentifiés par un fournisseur d'identités externe avant d'accéder au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.	Niveaux de sécurité supplémentaires pour les administrateurs du grid et des locataires tels que SSO et l'authentification multifacteur (MFA)	NIST SP800-63
Contrôle granulaire des autorisations	Les administrateurs du grid peuvent attribuer des autorisations aux rôles et attribuer des rôles à des groupes d'utilisateurs administratifs, ce qui permet d'appliquer les tâches que les clients administratifs sont autorisés à effectuer à l'aide de l'interface utilisateur de gestion et des API.	Permet aux administrateurs de Grid de gérer le contrôle d'accès pour les utilisateurs et les groupes d'administration.	—

Fonction	Fonction	Impact	Conformité réglementaire
Journalisation des audits distribués	StorageGRID offre une infrastructure intégrée de journalisation des audits distribuée et évolutive pour des centaines de nœuds répartis sur un maximum de 16 sites. Les nœuds logiciels StorageGRID génèrent des messages d'audit, qui sont transmis via un système de relais d'audit redondant et finalement capturés dans un ou plusieurs référentiels de journaux d'audit. Les messages d'audit capturent les événements au niveau objet, tels que les opérations de l'API S3 initiées par le client, les événements de cycle de vie des objets par ILM, les vérifications de l'état des objets en arrière-plan et les modifications de configuration effectuées à partir de l'interface utilisateur de gestion ou des API. Les journaux d'audit peuvent être exportés par Syslog, ce qui permet aux messages d'audit d'être exploités par des outils tels que Splunk et ELK. Il existe quatre types de messages d'audit : • Messages d'audit système • Messages d'audit du stockage objet • Messages d'audit du protocole HTTP • Messages d'audit de gestion Les journaux d'audit peuvent être stockés dans un compartiment S3 pour une conservation à long terme et un accès aux applications.	Fournit aux administrateurs du grid un service d'audit évolutif et éprouvé qui leur permet d'exploiter les données d'audit pour divers objectifs. Tels que la résolution de problèmes, l'audit des performances des SLA, les opérations d'API d'accès aux données du client et les modifications de la configuration de la gestion.	—

Fonction	Fonction	Impact	Conformité réglementaire
Audit du système	Les messages d'audit du système capturent les événements liés au système, tels que l'état des nœuds de grid, la détection d'objets corrompus, les objets validés à tous les emplacements spécifiés conformément à la règle ILM et la progression des tâches de maintenance à l'échelle du système (tâches de grid).	Aide les clients à résoudre les problèmes liés aux systèmes et apporte une preuve que les objets sont stockés conformément à leur SLA. Les SLA sont implémentés par les règles ILM de StorageGRID et sont protégés contre l'intégrité.	—
Audit du stockage objet	Les messages d'audit du stockage objet capturent les transactions de l'API objet et les événements liés au cycle de vie. Ces événements incluent le stockage objet et la récupération, les transferts de nœuds grid à nœud grid et les vérifications.	Aide les clients à vérifier la progression des données dans le système et si les SLA, spécifiés dans la ILM de StorageGRID, sont livrés.	—
Audit du protocole HTTP	Les messages d'audit du protocole HTTP capturent les interactions du protocole HTTP liées aux applications clientes et aux nœuds StorageGRID. En outre, les clients peuvent capturer des en-têtes de requête HTTP spécifiques (tels que X-retransmis-for et les métadonnées utilisateur [x-amz-meta-*]) dans l'audit.	Aide les clients à auditer les opérations d'API d'accès aux données entre les clients et StorageGRID et à tracer une action sur un compte utilisateur individuel et une clé d'accès. Ils peuvent également connecter les métadonnées utilisateur à des fins d'audit et utiliser des outils de recherche de journaux, tels que Splunk ou ELK, pour rechercher des métadonnées objet.	—
Audit de gestion	Les messages d'audit de gestion consignent les demandes des utilisateurs administrateurs dans l'interface de gestion (Grid Management interface) ou les API. Chaque requête qui n'est pas une requête GET ou HEAD à l'API consigne une réponse avec le nom d'utilisateur, l'IP et le type de requête à l'API.	Aide les administrateurs Grid à établir un enregistrement des modifications de configuration système effectuées par l'utilisateur à partir de quelle adresse IP source et de quelle adresse IP de destination à quel moment.	—

Fonction	Fonction	Impact	Conformité réglementaire
Prise en charge de TLS 1.3 pour l'interface de gestion et l'accès aux API	TLS établit un protocole de poignée de main pour la communication entre un client admin et un nœud admin StorageGRID.	Permet à un client administratif et à StorageGRID de s'identifier et de s'authentifier mutuellement et de communiquer avec confidentialité et intégrité des données.	—
SNMPv3 pour surveillance StorageGRID	SNMPv3 fournit la sécurité en offrant à la fois une authentification forte et un cryptage des données pour la confidentialité. Avec v3, les unités de données de protocole sont chiffrées à l'aide de CBC-DES pour son protocole de chiffrement. L'authentification utilisateur de la personne qui a envoyé l'unité de données de protocole est fournie par le protocole d'authentification HMAC-SHA ou HMAC-MD5. SNMPv2 et v1 sont toujours pris en charge.	Permet aux administrateurs de la grille de surveiller le système StorageGRID en activant un agent SNMP sur le nœud d'administration.	—
Certificats client pour l'exportation des metrics Prometheus	Les administrateurs du grid peuvent télécharger ou générer des certificats clients qui peuvent être utilisés pour fournir un accès sécurisé et authentifié à la base de données StorageGRID Prometheus.	Les administrateurs du grid peuvent utiliser des certificats client pour surveiller StorageGRID en externe à l'aide d'applications telles que Grafana.	—

Fonctions de sécurité de la plate-forme

Découvrez les fonctionnalités de sécurité de la plate-forme dans StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Infrastructure de clé publique (PKI) interne, certificats de nœud et TLS	StorageGRID utilise une PKI interne et des certificats de nœud pour authentifier et crypter les communications internœuds. La communication internœud est sécurisée par TLS.	Permet de sécuriser le trafic système sur le LAN ou le WAN, en particulier dans un déploiement multisite.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Pare-feu de nœud	StorageGRID configure automatiquement les tables IP et les règles de pare-feu pour contrôler le trafic réseau entrant et sortant, ainsi que pour fermer les ports inutilisés.	Protection du système StorageGRID, des données et des métadonnées contre le trafic réseau non sollicité.	—
Durcicement du système d'exploitation	Le système d'exploitation de base des appliances physiques et des nœuds virtuels StorageGRID est renforcé ; les logiciels non liés sont supprimés.	Permet de minimiser les surfaces d'attaque potentielles.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Mises à jour périodiques de la plate-forme et des logiciels	StorageGRID fournit régulièrement des versions logicielles, notamment des systèmes d'exploitation, des binaires d'applications et des mises à jour logicielles.	Ils permettent de maintenir le système StorageGRID à jour avec les logiciels et les binaires d'applications les plus récents.	—
Connexion racine désactivée via SSH (Secure Shell)	La connexion root via SSH est désactivée sur tous les nœuds StorageGRID. L'accès SSH utilise l'authentification par certificat.	Aide les clients à se protéger contre les éventuels problèmes de piratage à distance des mots de passe de la connexion racine.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Synchronisation temporelle automatisée	StorageGRID synchronise automatiquement les horloges système de chaque nœud avec plusieurs serveurs NTP (External Time Network Time Protocol). Au moins quatre serveurs NTP de Stratum 3 ou version ultérieure sont requis.	Garantit la même référence de temps sur tous les nœuds.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Réseaux séparés pour le trafic client, administrateur et grid interne	Les nœuds logiciels et les appliances matérielles StorageGRID prennent en charge plusieurs interfaces réseau physiques et virtuelles, de sorte que les clients peuvent séparer le trafic client, d'administration et le trafic réseau interne sur différents réseaux.	Permettez aux administrateurs du grid de séparer le trafic réseau interne et externe et de fournir le trafic sur les réseaux avec différents SLA.	—
Plusieurs interfaces VLAN (Virtual LAN)	StorageGRID prend en charge la configuration des interfaces VLAN sur vos réseaux client et grid StorageGRID.	Permettez aux administrateurs de Grid de partitionner et d'isoler le trafic des applications pour plus de sécurité, de flexibilité et de performances.	
Réseau client non fiable	L'interface réseau client non fiable accepte les connexions entrantes uniquement sur les ports qui ont été explicitement configurés comme des noeuds finaux d'équilibrage de charge.	Garantit que les interfaces exposées à des réseaux non fiables sont sécurisées.	—
Pare-feu configurable	Gérez les ports ouverts et fermés pour les réseaux Admin, Grid et client.	Autoriser les administrateurs du grid à contrôler l'accès aux ports et à gérer l'accès aux périphériques approuvés aux ports.	
Comportement SSH amélioré	désactiver SSH par défaut avant l'installation. Dans l'état par défaut, l'accès SSH n'est activé que sur l'adresse des ports de gestion locaux. Les mots de passe des utilisateurs administrateur et root sont définis sur le numéro de série du contrôleur de calcul de l'appliance. La connexion n'est autorisée que sur la console série et la console graphique (BMC KVM). SSH sur n'importe quel port réseau est désactivé.	Améliore la protection de l'accès au réseau.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Chiffrement de nœud	Dans le cadre de la nouvelle fonction de chiffrement du serveur hôte KMS, un nouveau paramètre de chiffrement de nœud est ajouté au programme d'installation de l'appliance StorageGRID.	Ce paramètre doit être activé pendant la phase de configuration matérielle de l'installation de l'appliance.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Intégration au cloud

Découvrez comment StorageGRID s'intègre aux services cloud.

Fonction	Fonction	Impact
Analyse antivirus basée sur les notifications	Notifications d'événements de support des services de plateforme StorageGRID. Les notifications d'événements peuvent être utilisées avec des services de cloud computing externes pour déclencher des flux de travail d'analyse antivirus sur les données.	Permet aux administrateurs de locataires de déclencher l'analyse antivirus des données à l'aide de services de cloud computing externes.

Tr-4921 : défense contre les ransomware

Protégez les objets StorageGRID S3 contre les attaques par ransomware

Découvrez les attaques par ransomware et comment protéger vos données grâce aux bonnes pratiques de sécurité de StorageGRID.

Le nombre d'attaques par ransomware est en hausse Ce document fournit quelques recommandations sur la protection des données d'objet sur StorageGRID.

Les ransomware représentent aujourd'hui le danger omniprésent dans les data centers. Les ransomwares ont été conçus pour chiffrer les données et les rendre inutilisables par des utilisateurs et des applications qui en dépendent. La protection commence par les défenses habituelles : une mise en réseau renforcée et de solides pratiques de sécurité des utilisateurs. Nous devons ensuite appliquer les pratiques de sécurité de l'accès aux données.

Les ransomwares sont l'une des plus grandes menaces de sécurité. L'équipe NetApp StorageGRID travaille avec nos clients pour garder une longueur d'avance sur ces menaces. Le verrouillage d'objets et la gestion des versions vous permettent de vous protéger contre les modifications indésirables et de restaurer votre système suite à des attaques malveillantes. La sécurité des données est une entreprise multiniveaux, dans laquelle le stockage objet n'est qu'une partie de votre data Center.

Meilleures pratiques StorageGRID

Pour StorageGRID, les bonnes pratiques en matière de sécurité doivent inclure l'utilisation du protocole HTTPS avec des certificats signés pour la gestion et l'accès aux objets. Créez des comptes utilisateur dédiés

aux applications et aux particuliers et n'utilisez pas les comptes root des locataires pour l'accès aux applications ou aux données utilisateur. En d'autres termes, suivez le principe du privilège minimum. Utilisez des groupes de sécurité avec des règles de gestion des identités et des accès (IAM) définies pour régir les droits d'utilisateur et les comptes d'accès spécifiques aux applications et aux utilisateurs. Une fois ces mesures mises en place, vous devez vous assurer que vos données sont protégées. Dans le cas de simple Storage Service (S3), lorsque les objets sont modifiés pour les chiffrer, il est remplacé par l'objet d'origine.

Méthodes de défense

Le mécanisme principal de protection contre les ransomwares dans l'API S3 consiste à mettre en œuvre le verrouillage objet. Toutes les applications ne sont pas compatibles avec le verrouillage d'objet. Il existe donc deux autres options pour protéger vos objets décrites dans ce rapport : la réplication vers un autre compartiment avec la gestion des versions activée et la gestion des versions avec les règles IAM.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

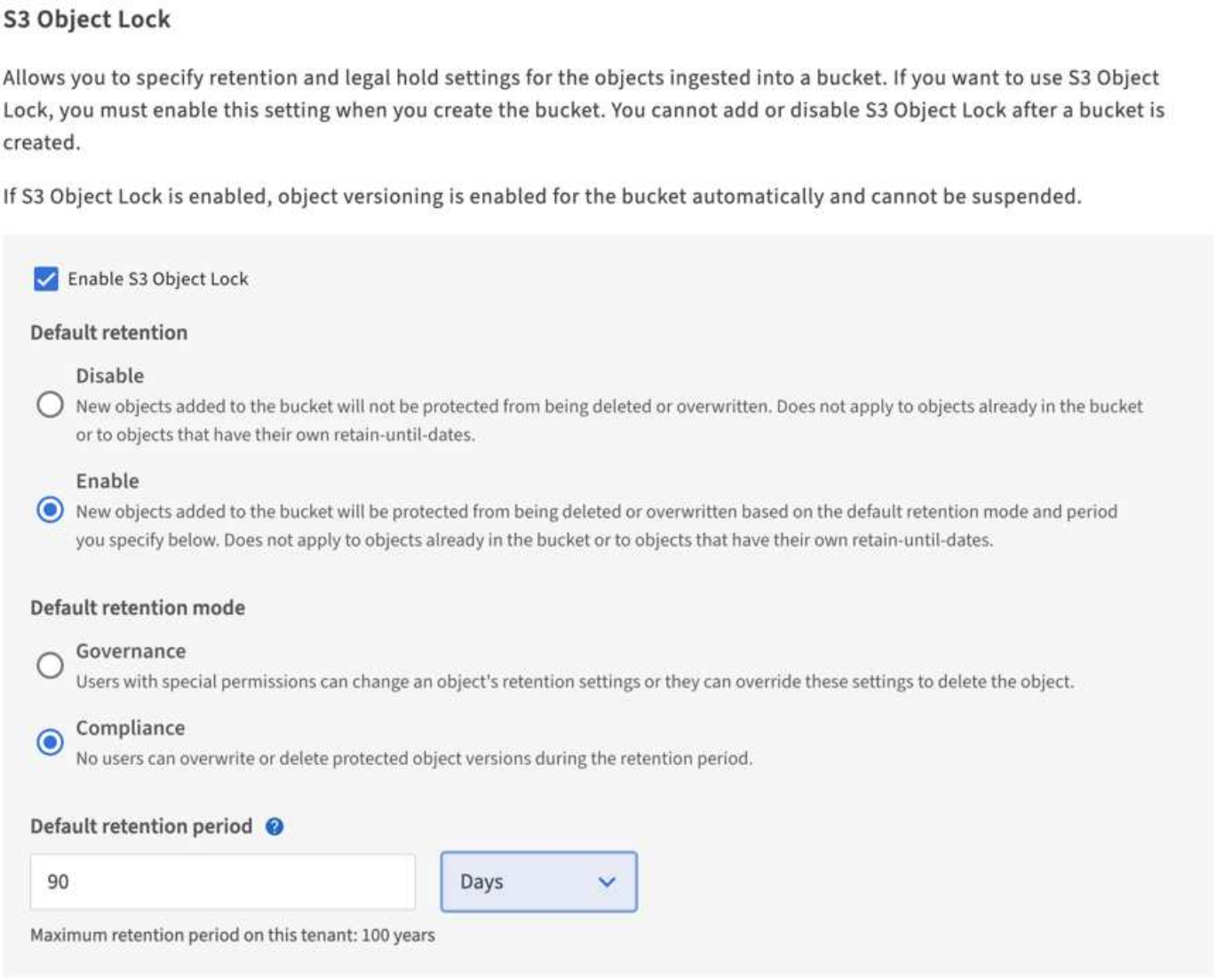
- Centre de documentation NetApp StorageGRIDhttps://docs.netapp.com/us-en/storagegrid/[]
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Protégez vos données contre les ransomwares à l'aide d'un verrouillage objet

Découvrez comment le verrouillage d'objets dans StorageGRID fournit un modèle WORM pour empêcher la suppression ou le remplacement des données, et comment il répond aux exigences réglementaires.

Le verrouillage des objets fournit un modèle WORM qui empêche la suppression ou l'écrasement d'objets. L'implémentation du verrouillage objet par StorageGRID "Cohasset évalué" permet de respecter les exigences réglementaires et prend en charge la conservation à des fins juridiques, le mode de conformité et le mode de gouvernance pour la conservation des objets ainsi que les règles de conservation des compartiments par défaut. Vous devez activer le verrouillage d'objet dans le cadre de la création de compartiment et de la gestion des versions. Une version spécifique d'un objet est verrouillée, et si aucun ID de version n'est défini, la rétention est placée sur la version actuelle de l'objet. Si la conservation de la version actuelle est configurée et qu'une tentative de suppression, de modification ou d'écrasement de l'objet est effectuée, une nouvelle version est créée avec un marqueur de suppression ou la nouvelle révision de l'objet comme version actuelle, et la version verrouillée est conservée comme une version non actuelle. Pour les applications qui ne sont pas encore compatibles, vous pouvez toujours utiliser le verrouillage objet et une configuration de conservation par défaut placée sur le compartiment. Une fois la configuration définie, une conservation d'objet est appliquée à chaque nouvel objet placé dans le compartiment. Cela fonctionne tant que l'application est configurée pour ne pas supprimer ou écraser les objets avant que la durée de conservation ne soit écoulée.

Lors de la création d'un bucket dans l'interface utilisateur de gestion des locataires, vous pouvez activer le verrouillage des objets et configurer un mode de conservation par défaut et une période de conservation. Une fois configuré, cela définira une rétention de verrouillage d'objet minimale sur chaque objet ingéré dans ce bucket.



Voici quelques exemples d'utilisation de l'API de verrouillage d'objet :

La mise en attente légale du verrouillage d'objet est un état activé/désactivé simple appliqué à un objet.

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

La définition de l'état de mise en attente légale ne renvoie aucune valeur si elle a réussi, de sorte qu'elle peut être vérifiée à l'aide d'une opération GET.

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

Pour désactiver la mise en attente légale, appliquez le statut 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"
    }
}
```

La définition de la conservation d'objet s'effectue à l'aide d'un horodatage de conservation jusqu'à.

```
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
```

Encore une fois, il n'y a pas de valeur renvoyée en cas de réussite, vous pouvez donc vérifier l'état de conservation de la même manière avec un appel 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"
    }
```

Le fait de conserver une conservation par défaut dans un compartiment activé pour le verrouillage d'objet applique une période de conservation en jours et en années.

```
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
```

Comme pour la plupart de ces opérations, aucune réponse n'est renvoyée en cas de succès. Par conséquent, nous pouvons effectuer une OPÉRATION GET pour que la configuration puisse être vérifiée.

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

Vous pouvez ensuite placer un objet dans le compartiment avec la configuration de conservation appliquée.

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

L'opération PUT renvoie une réponse.

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

Sur l'objet de conservation, la durée de conservation définie dans le compartiment de l'exemple précédent est convertie en horodatage de conservation de l'objet.

```
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"
    }
}
```

Protection contre les ransomwares à l'aide d'un compartiment répliqué avec gestion des versions

Découvrez comment répliquer des objets vers un compartiment secondaire à l'aide de StorageGRID CloudMirror.

Les applications et les charges de travail ne seront pas toutes compatibles avec le verrouillage en mode objet. Une autre option consiste à répliquer les objets vers un compartiment secondaire dans la même grille (de préférence un locataire différent avec accès limité) ou tout autre terminal S3 avec le service de plateforme

StorageGRID, CloudMirror.

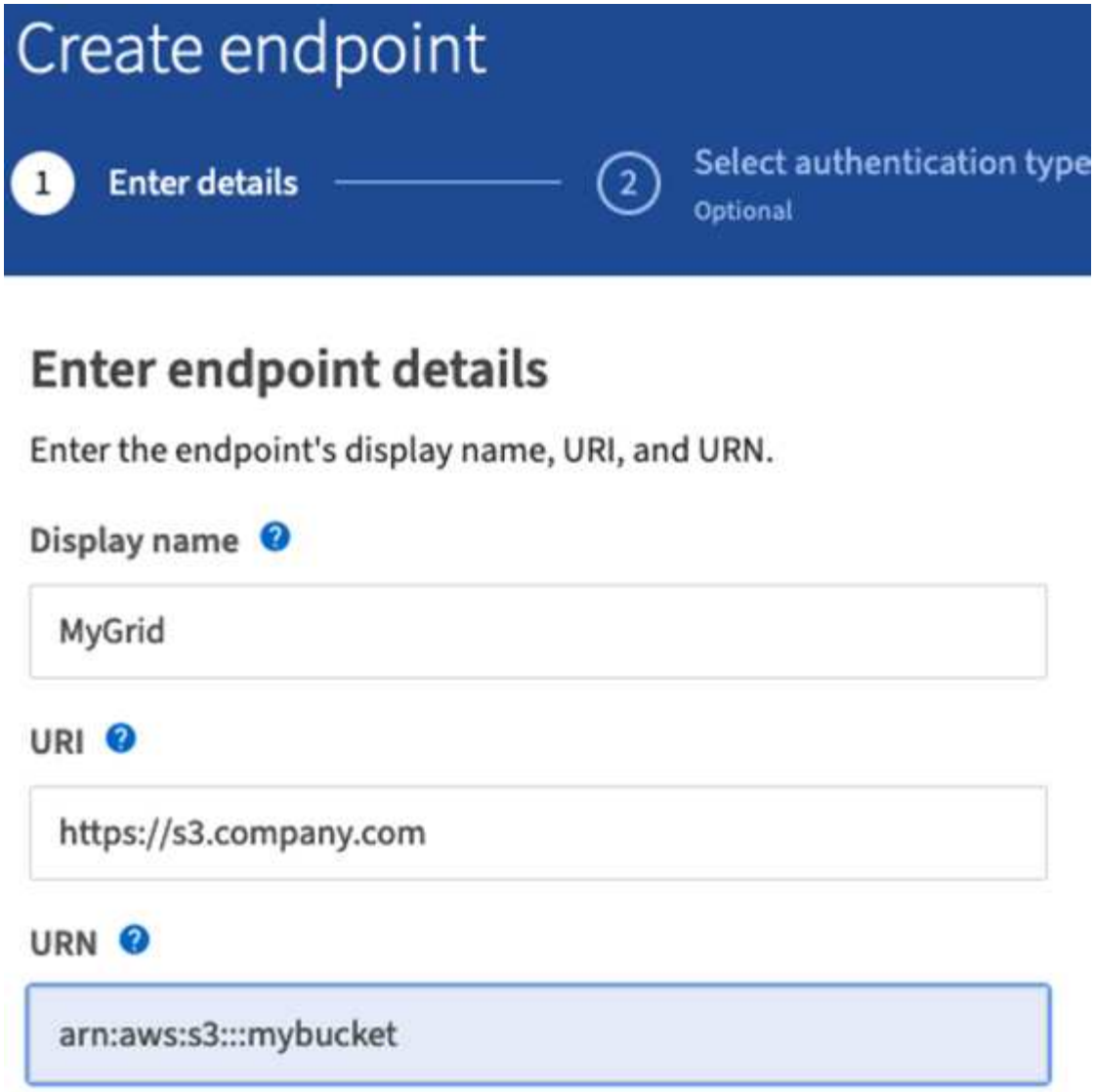
StorageGRID CloudMirror est un composant de StorageGRID qui peut être configuré pour répliquer les objets d'un compartiment vers une destination définie lors de leur ingestion dans le compartiment source et ne réplique pas les suppressions. Comme CloudMirror est un composant intégré de StorageGRID, il ne peut pas être désactivé ou manipulé par une attaque basée sur l'API S3. Vous pouvez configurer ce compartiment répliqué avec la gestion des versions activée. Dans ce scénario, vous avez besoin d'un nettoyage automatisé des anciennes versions du compartiment répliqué qui peuvent être jetées en toute sécurité. Pour cela, vous pouvez utiliser le moteur de règles ILM de StorageGRID. Créez des règles pour gérer le placement des objets en fonction d'une période non actuelle pendant plusieurs jours, suffisamment pour avoir identifié et récupéré une attaque.

L'un des inconvénients de cette approche est qu'elle consomme plus de stockage en conservant une seconde copie complète du compartiment et plusieurs versions des objets pendant un certain temps. En outre, les objets qui ont été supprimés intentionnellement du compartiment principal doivent être supprimés manuellement du compartiment répliqué. Il existe d'autres options de réplication en dehors du produit, telles que NetApp CloudSync, qui peuvent répliquer les suppressions pour une solution similaire. Un autre inconvénient est que la gestion des versions du compartiment secondaire est activée et que le verrouillage d'objet n'est pas activé, c'est qu'il existe un certain nombre de comptes privilégiés qui peuvent être utilisés pour causer des dommages à l'emplacement secondaire. L'avantage est qu'il doit s'agir d'un compte unique pour ce terminal ou ce compartiment locataire, et le compromis n'inclut probablement pas l'accès aux comptes sur l'emplacement principal, et inversement.

Une fois les compartiments source et destination créés et la destination configurée avec la gestion des versions, vous pouvez configurer et activer la réplication comme suit :

Étapes

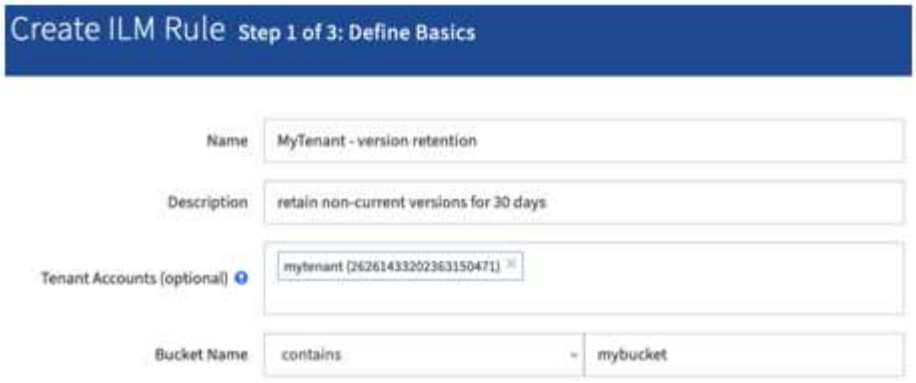
1. Pour configurer CloudMirror, créez un terminal de services de plateforme pour la destination S3.

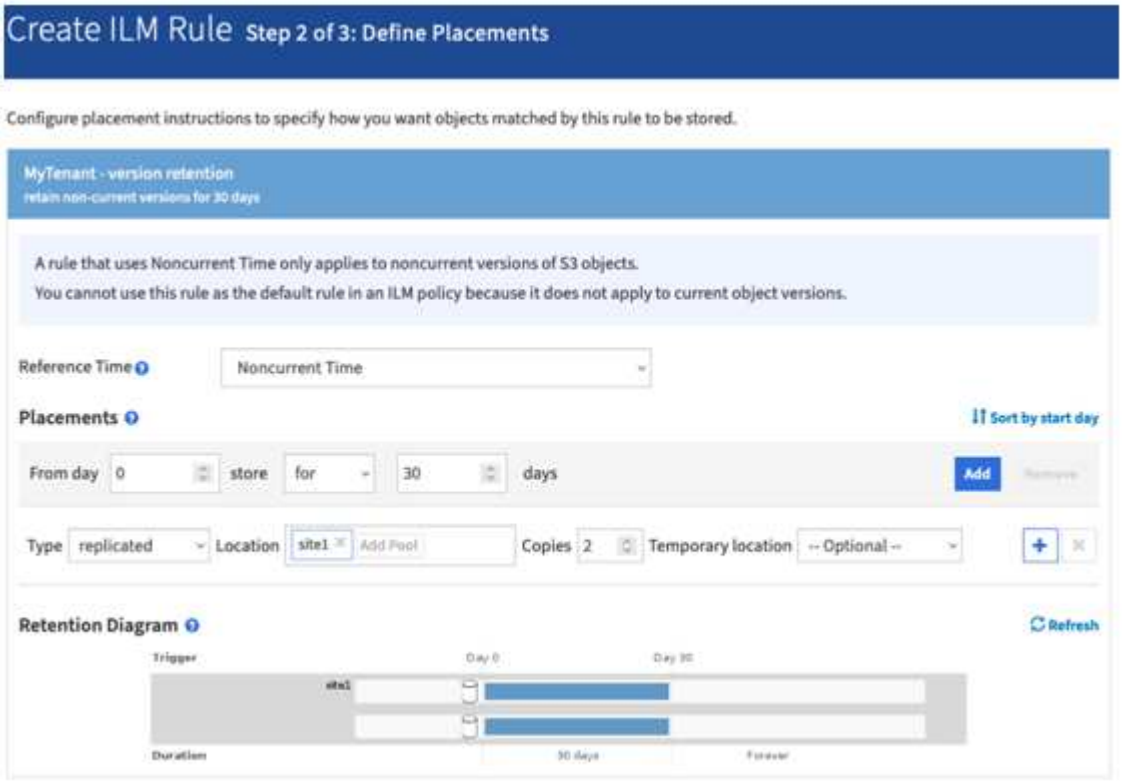


2. Sur le compartiment source, configurez la réplication pour utiliser le terminal configuré.

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

3. Créez des règles ILM pour gérer le placement du stockage et la gestion de la durée du stockage des versions. Dans cet exemple, les versions non actuelles des objets à stocker sont configurées.





Il y a deux copies sur le site 1 pendant 30 jours. Vous configurez également les règles de la version actuelle des objets en fonction de l'utilisation de l'heure d'ingestion comme heure de référence dans la règle ILM pour correspondre à la durée de stockage du compartiment source. Le placement de stockage des versions d'objets peut être codé par effacement ou répliqué.

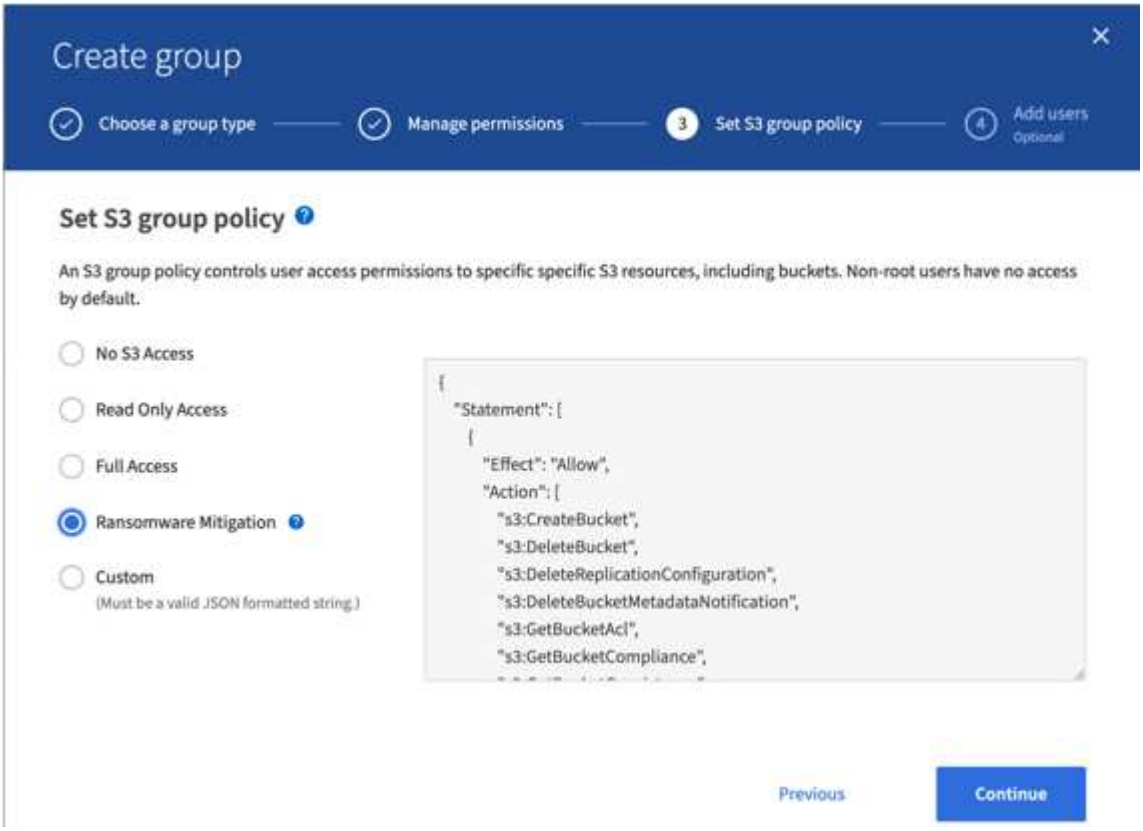
Défense anti-ransomware à l'aide du contrôle des versions avec une politique IAM de protection

Découvrez comment protéger vos données en activant la gestion des versions dans le compartiment et en implémentant les règles IAM sur les groupes de sécurité des utilisateurs dans StorageGRID.

Une méthode pour protéger vos données sans verrouillage objet ou réplication consiste à activer la gestion des versions sur le compartiment et à mettre en œuvre des règles IAM sur les groupes de sécurité utilisateur afin de limiter la capacité des utilisateurs à gérer des versions des objets. En cas d'attaque, de nouvelles

versions incorrectes des données sont créées en tant que version actuelle, et la version la plus récente non-actuelle est la sécurité des données. Les comptes compromis pour accéder aux données n'ont pas accès à supprimer ni à modifier la version non actuelle qui les protège pour des opérations de restauration ultérieures. Comme dans le scénario précédent, les règles ILM gèrent la conservation des versions non actuelles avec la durée de votre choix. L'inconvénient est qu'il existe toujours la possibilité de comptes privilégiés pour une attaque de mauvais acteurs, mais tous les comptes de service d'application et les utilisateurs doivent être configurés avec un accès plus restrictif. La stratégie de groupe restrictif doit explicitement autoriser chaque action que vous souhaitez que les utilisateurs ou l'application soient capables et refuser explicitement toute action dont vous ne voulez pas qu'ils soient capables. NetApp ne recommande pas l'utilisation d'une autorisation générique car une nouvelle action pourrait être introduite à l'avenir et vous voudrez contrôler si elle est autorisée ou refusée. Pour cette solution, la liste de refus doit inclure DeleteObjectVersion, PutBucketPolicy, DeleteBuckePolicy, PutLifecycleConfiguration et PutBucketVersioning afin de protéger la configuration de gestion des versions du compartiment et de l'objet des modifications utilisateur ou programmatiques.

Dans StorageGRID, l'option de stratégie de groupe S3 « Atténuation des ransomwares » facilite la mise en œuvre de cette solution. Lors de la création d'un groupe d'utilisateurs dans le locataire, après avoir sélectionné les autorisations du groupe, vous pouvez voir cette politique facultative.



Voici le contenu de la stratégie de groupe qui inclut la plupart des opérations disponibles explicitement autorisées et le minimum requis refusé.

```
{
    "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:::*"
        }
    ]
}
```

Enquête et correction des ransomwares

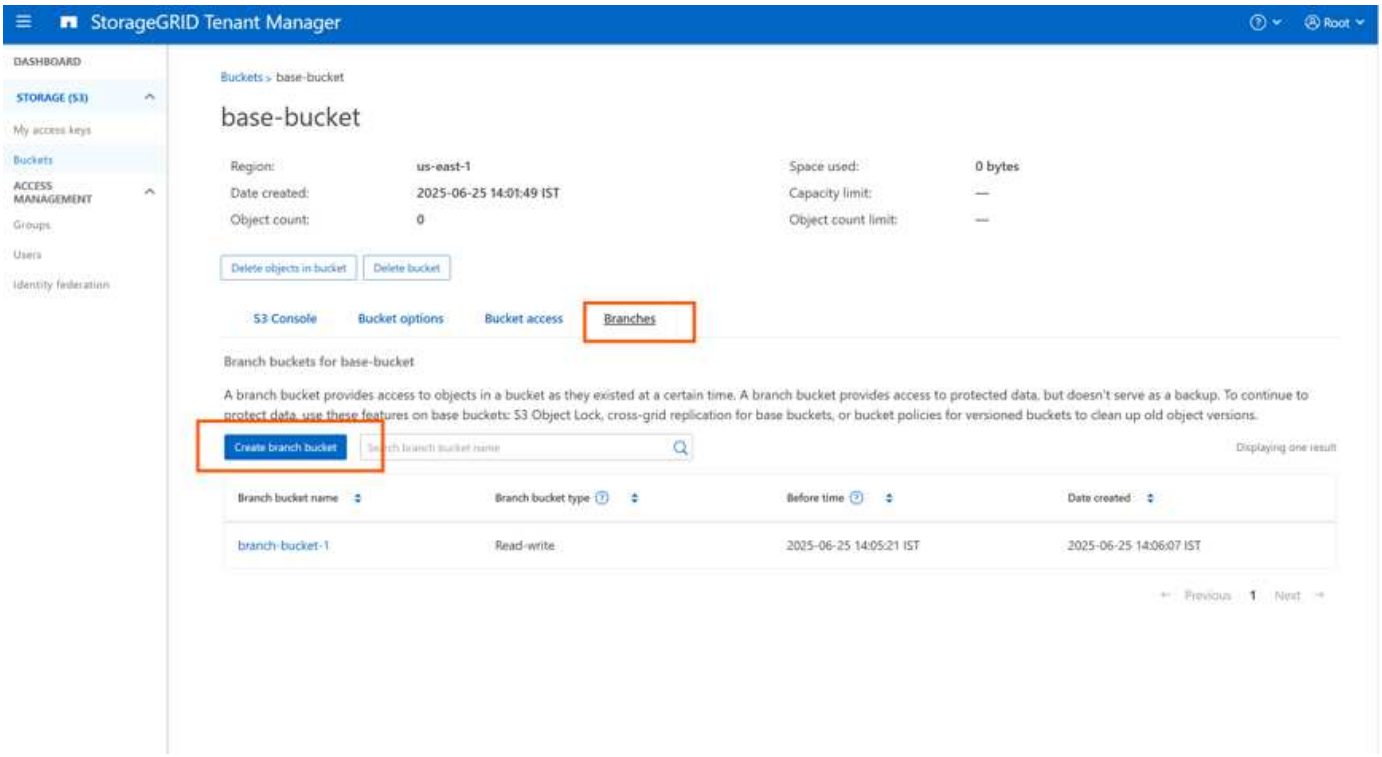
Découvrez comment enquêter et corriger les buckets après une éventuelle attaque de ransomware avec StorageGRID.

Dans StorageGRID 12.0, la nouvelle fonctionnalité de compartiment de branche a été ajoutée pour étendre l'utilité du contrôle de version pour la défense contre les ransomwares. Un bucket de branche fournit un accès aux objets d'un bucket tels qu'ils existaient à un certain moment, à condition qu'ils existent toujours dans le bucket. Les buckets de branches ne peuvent être créés que pour les buckets de base compatibles avec le contrôle de version.

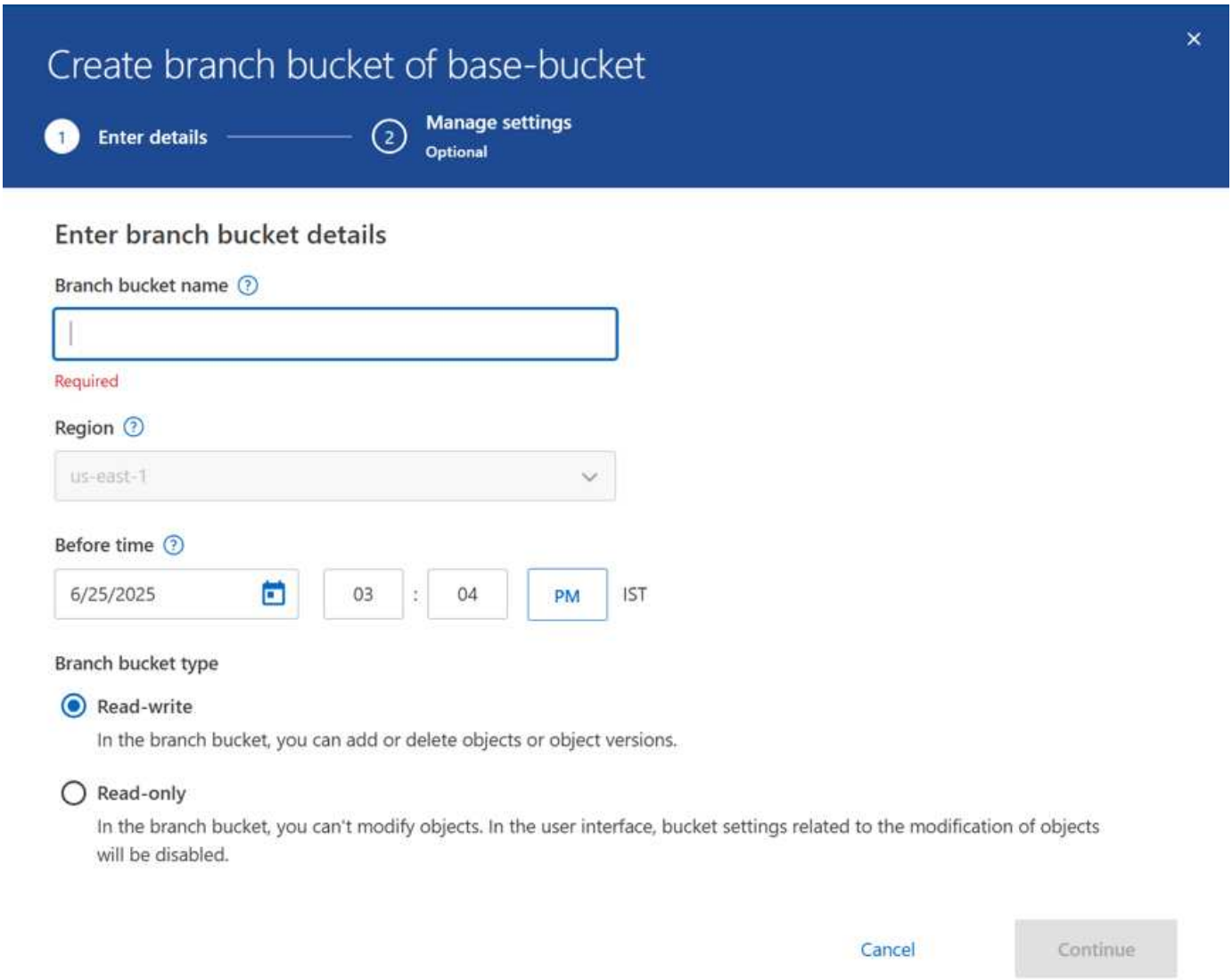
Cela signifie que si vous suspectez qu'une attaque de ransomware a eu lieu, vous pouvez créer un bucket de branche en lecture/écriture ou en lecture seule contenant tous les objets et versions qui existaient avant l'heure de l'attaque initiale. Vous pouvez utiliser ce bucket de branche pour comparer le contenu du bucket de base afin de déterminer quels objets ont changé et si le changement faisait partie de l'attaque ou non. Vous pouvez également utiliser un bucket de branche pour poursuivre les opérations client à l'aide de la branche propre tout en enquêtant sur l'attaque.

Création d'un bucket de branches

- Accédez à la page des détails du bucket de base et à l'onglet Branches pour créer un bucket de branche.



- Une fois le bouton Créer un bucket de branche cliqué, une fenêtre contextuelle s’ouvre avec les détails préremplis de la région associée au bucket de base.
- indiquez le nom du bucket de branche, avant l’heure, et sélectionnez le type de bucket de branche à créer.



Tr-4765 : StorageGRID du moniteur

Introduction à la surveillance StorageGRID

Découvrez comment contrôler votre système StorageGRID à l'aide d'applications externes telles que Splunk.

La surveillance efficace du stockage objet NetApp StorageGRID permet aux administrateurs de répondre rapidement aux problèmes urgents et d'ajouter de manière proactive des ressources pour gérer la croissance des workloads. Ce rapport fournit des conseils généraux sur la façon de surveiller les mesures clés et d'exploiter les applications de surveillance externes. Il est destiné à compléter le guide de surveillance et de dépannage existant.

Un déploiement NetApp StorageGRID se compose généralement de plusieurs sites et de nombreux nœuds qui créent un système de stockage objet distribué et tolérant aux pannes. Dans un système de stockage distribué et résilient tel que StorageGRID, il est normal que des conditions d'erreur existent alors que la grille continue de fonctionner normalement. En tant qu'administrateur, le défi consiste à comprendre le seuil auquel les conditions d'erreur (telles que les nœuds en panne) constituent un problème qui doit être immédiatement résolu par rapport aux informations à analyser. En analysant les données d'StorageGRID, vous pouvez

analyser votre charge de travail et prendre des décisions avisées, notamment concernant l'ajout de ressources.

StorageGRID fournit une excellente documentation qui analyse le sujet de la surveillance. Ce rapport part du principe que vous connaissez StorageGRID et que vous avez consulté la documentation correspondante. Au lieu de répéter ces informations, nous nous référons à la documentation produit tout au long de ce guide. La documentation des produits StorageGRID est disponible en ligne et au format PDF.

L'objectif de ce document est de compléter la documentation produit et de découvrir comment contrôler votre système StorageGRID à l'aide d'applications externes, telles que Splunk.

Sources de données

Pour réussir la surveillance de NetApp StorageGRID, il est important de savoir où collecter des données sur l'état et les opérations de votre système StorageGRID.

- **Interface utilisateur Web et tableau de bord.** Le gestionnaire de grille StorageGRID présente une vue de haut niveau des informations que vous, en tant qu'administrateur, devez voir dans une présentation logique. En tant qu'administrateur, vous pouvez également approfondir les informations de niveau de service pour le dépannage et la collecte des journaux.
- **Journaux d'audit.** StorageGRID conserve des journaux d'audit granulaires des actions des locataires telles que LA COMMANDE PUT, GET et DELETE. Vous pouvez également suivre le cycle de vie d'un objet de l'ingestion à l'application des règles de gestion des données.
- **API métriques.** Les API de l'interface utilisateur sont sous-jacentes à l'interface GMI de StorageGRID. Cette approche vous permet d'extraire des données à l'aide d'outils externes de surveillance et d'analyse.

Où trouver des informations complémentaires

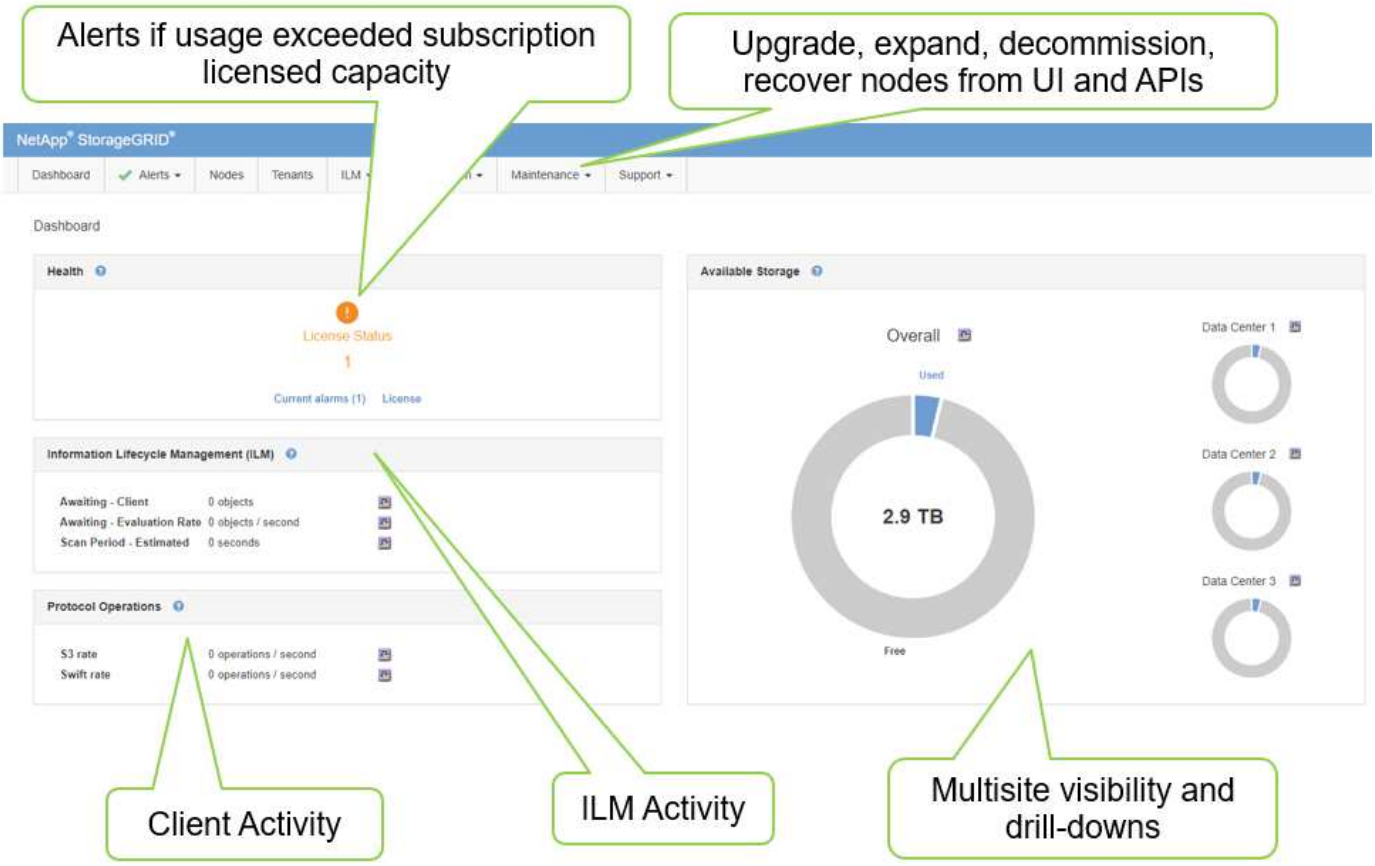
Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/
- NetApp StorageGRID application pour Splunk https://splunkbase.splunk.com/app/3898/#/details

Utilisez le tableau de bord GMI pour surveiller StorageGRID

Le tableau de bord de l'interface de gestion Grid (GMI) de StorageGRID offre une vue centralisée de l'infrastructure StorageGRID. Vous pouvez ainsi surveiller l'état, les performances et la capacité de l'ensemble du grid.

Utilisez le tableau de bord GMI pour examiner chaque composant central de la grille.



Informations à surveiller régulièrement

Une version précédente de ce rapport technique énuméré les mesures à vérifier périodiquement par rapport aux tendances. Cette information est maintenant incluse dans le "Guide de surveillance et de dépannage".

Surveiller le stockage

Dans une version précédente de ce rapport technique, nous liseous où surveiller les mesures importantes, telles que l'espace de stockage objet, l'espace de métadonnées, les ressources réseau, etc. Cette information est maintenant incluse dans le "Guide de surveillance et de dépannage".

Utilisez les alertes pour surveiller StorageGRID

Découvrez comment utiliser le système d'alertes de StorageGRID pour surveiller les problèmes, gérer les alertes personnalisées et étendre les notifications d'alertes via SNMP ou par e-mail.

Les alertes fournissent des informations critiques qui vous permettent de surveiller les divers événements et conditions de votre système StorageGRID.

Le système d'alertes est conçu pour être le principal outil de surveillance des problèmes susceptibles de survenir dans votre système StorageGRID. Le système d'alertes se concentre sur les problèmes exploitables du système et propose une interface simple d'utilisation.

Nous fournissons un ensemble de règles d'alerte par défaut qui visent à faciliter la surveillance et le dépannage de votre système. Vous pouvez davantage gérer les alertes en créant des alertes personnalisées, en modifiant ou en désactivant les alertes par défaut et en désactivant les notifications d'alerte.

Les alertes sont également extensibles via SNMP ou la notification par e-mail.

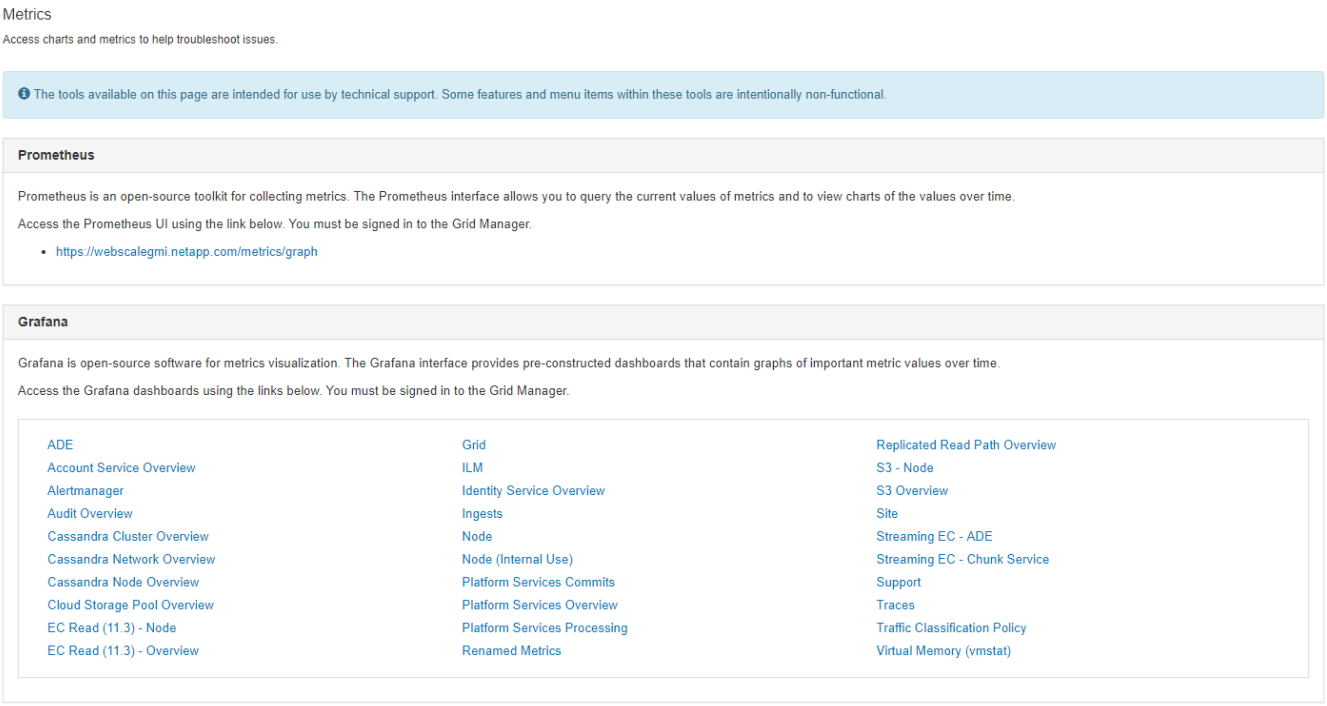
Pour plus d'informations sur les alertes, reportez-vous à la "documentation produit" page disponible en ligne et au format PDF.

Surveillance avancée dans StorageGRID

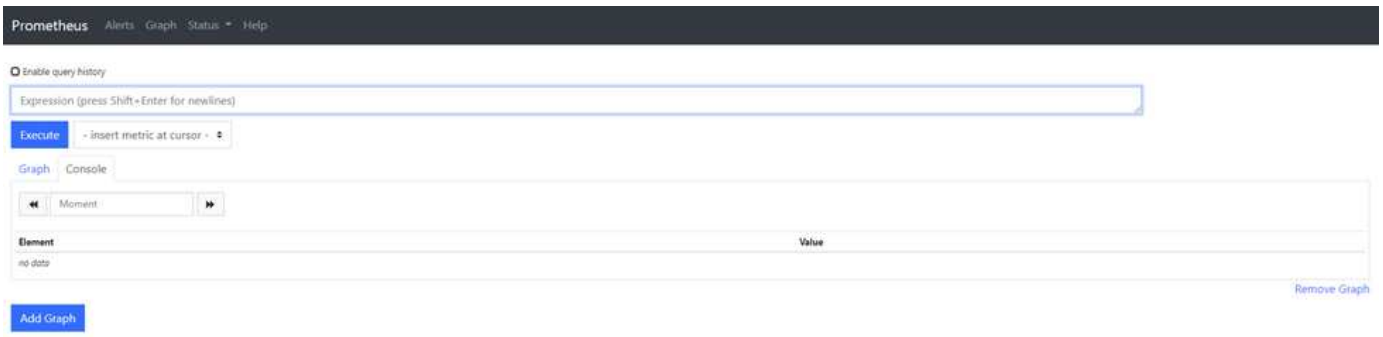
Découvrez comment accéder à des metrics et les exporter pour résoudre vos problèmes.

Affichage des API de metrics via une requête Prometheus

Prometheus est un logiciel open source qui collecte des metrics. Pour accéder au Prometheus intégré de StorageGRID via l'interface GMI, accédez au **support › Metrics**.



Vous pouvez également accéder directement au lien.



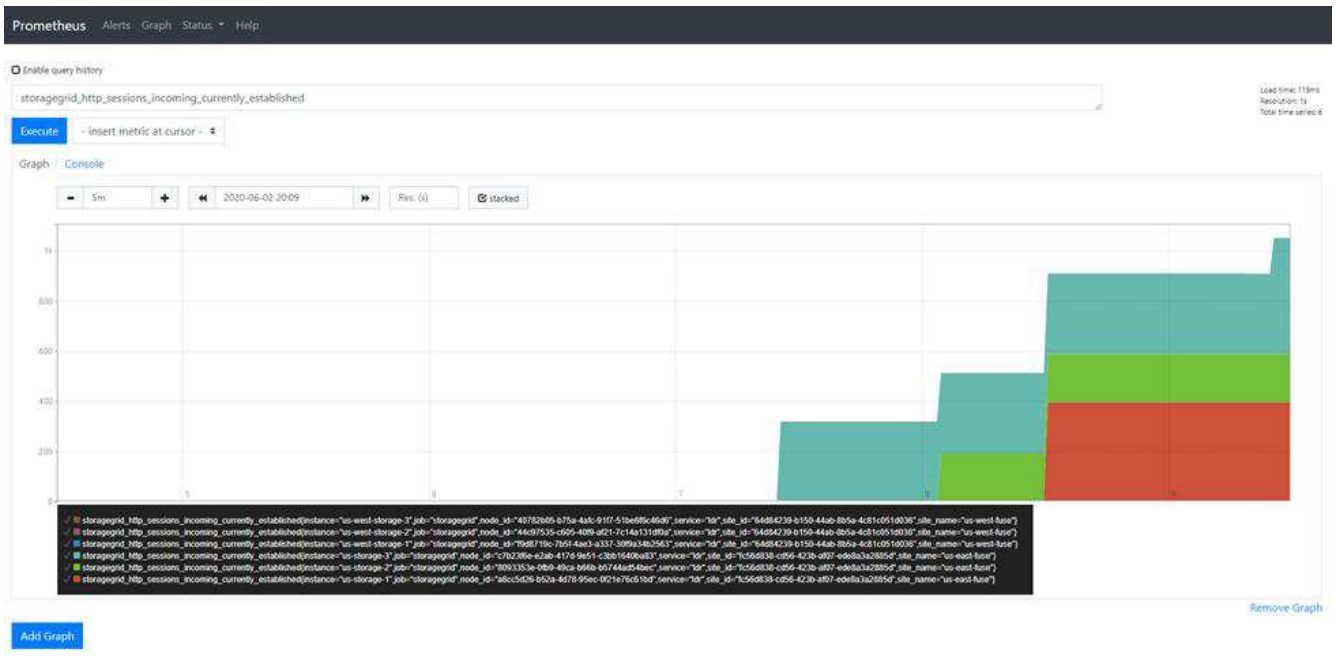
Avec cette vue, vous pouvez accéder à l'interface Prometheus. Ensuite, vous pouvez effectuer des recherches

parmi les mesures disponibles et même tester des requêtes.

Pour effectuer une requête URL Prometheus, procédez comme suit :

Étapes

1. Commencez à taper dans la zone de texte de la requête. Au fur et à mesure que vous tapez, les indicateurs sont répertoriés. À nos fins, seuls les metrics commençant par StorageGRID et Node sont importants.
2. Pour afficher le nombre de sessions HTTP pour chaque nœud, tapez `storagegrid_http` et sélectionnez `storagegrid_http_sessions_incoming_currently_established`. Cliquez sur Exécuter et affichez les informations au format graphique ou console.



Les requêtes et les graphiques que vous créez via cette URL ne persistent pas. Les requêtes complexes consomment des ressources sur le nœud d'administration. NetApp vous recommande d'utiliser cette vue pour explorer les metrics disponibles.

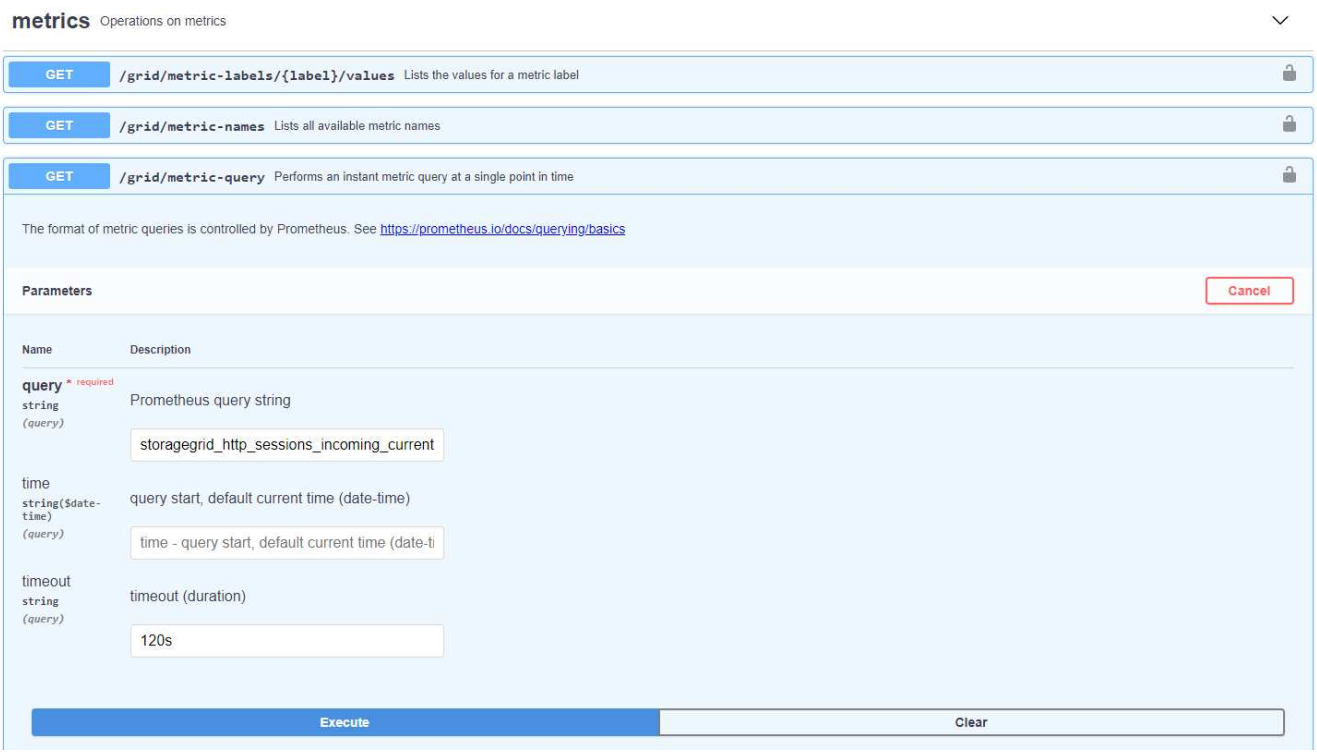
Il n'est pas recommandé de s'interfacer directement avec notre instance Prometheus, car cela nécessite l'ouverture de ports supplémentaires. L'accès aux metrics via notre API est la méthode recommandée et sécurisée.

Exportez les metrics via l'API

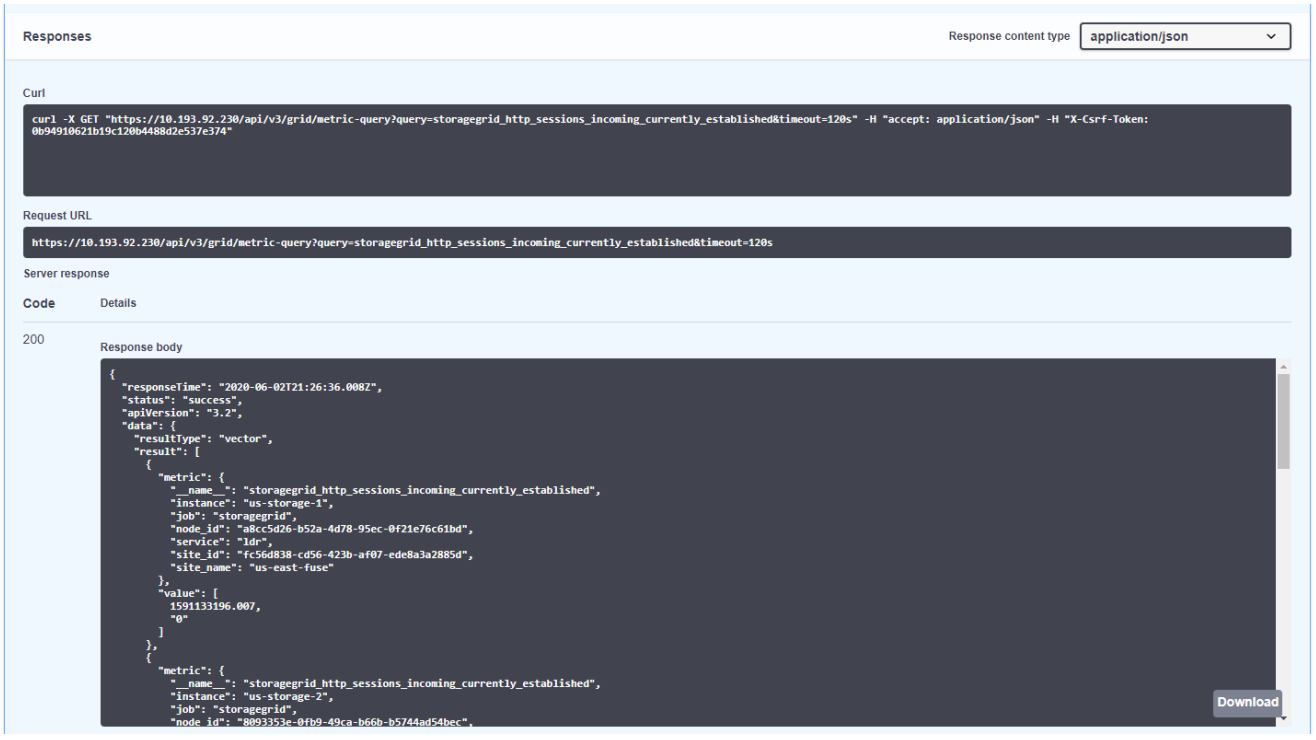
Vous pouvez également accéder aux mêmes données via l'API de gestion StorageGRID.

Pour exporter des metrics via l'API, effectuez la procédure suivante :

1. Dans l'interface GMI, sélectionnez **aide › Documentation API**.
2. Faites défiler jusqu'à Metrics et sélectionnez GET /grid/Metric-query.



La réponse inclut les mêmes informations que celles que vous pouvez obtenir via une requête URL Prometheus. Vous pouvez à nouveau voir le nombre de sessions HTTP actuellement établies sur chaque nœud de stockage. Vous pouvez également télécharger la réponse au format JSON pour plus de lisibilité. La figure suivante présente des exemples de réponses à des requêtes Prometheus.



L’avantage de l’utilisation de l’API est qu’elle vous permet d’effectuer des requêtes authentifiées

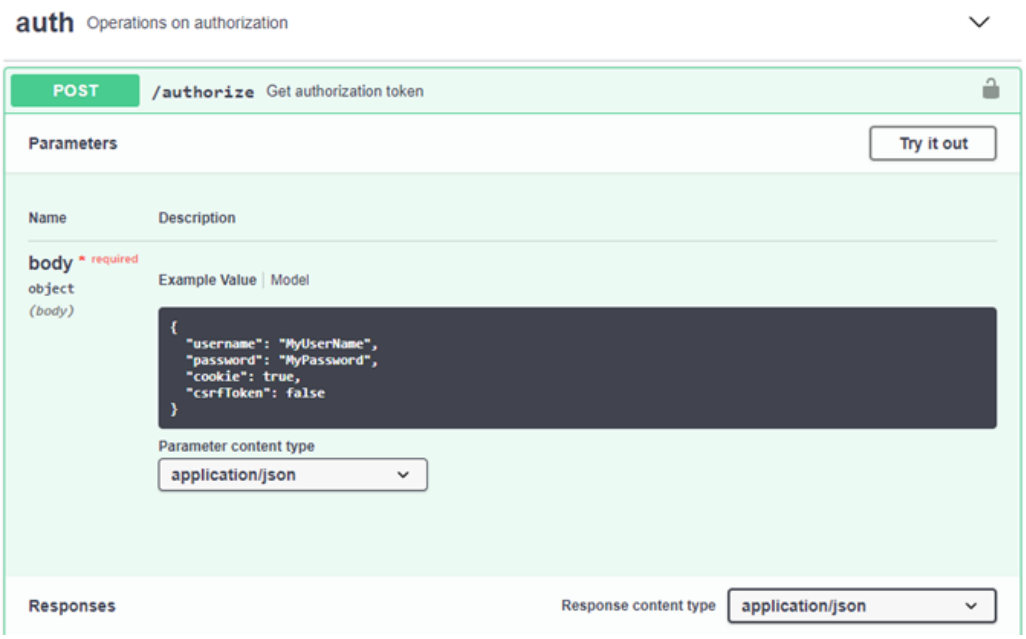
Accédez aux metrics à l'aide de CURL dans StorageGRID

Découvrez comment accéder aux metrics via l'interface de ligne de commandes en utilisant curl.

Pour effectuer cette opération, vous devez d'abord obtenir un jeton d'autorisation. Pour demander un jeton, procédez comme suit :

Étapes

1. Dans l'interface GMI, sélectionnez **aide › Documentation API**.
2. Faites défiler jusqu'à Auth pour rechercher des opérations sur l'autorisation. La capture d'écran suivante montre les paramètres de la méthode POST.



3. Cliquez sur essayer et modifiez le corps avec votre nom d'utilisateur et votre mot de passe GMI.
4. Cliquez sur Exécuter.
5. Copiez la commande curl fournie dans la section curl et collez-la dans une fenêtre de terminal. La commande se présente comme suit :

```
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
```

> Si votre mot de passe GMI contient des caractères spéciaux, n'oubliez pas d'utiliser \ pour échapper à des caractères spéciaux. Par exemple, remplacez ! avec \!

6. Après avoir exécuté la commande curl précédente, le résultat vous donne un jeton d'autorisation comme dans l'exemple suivant :

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

Vous pouvez désormais utiliser la chaîne de tokens d'autorisation pour accéder aux métriques via curl. Le processus d'accès aux mesures est similaire aux étapes de la section "Surveillance avancée dans StorageGRID". Cependant, à des fins de démonstration, nous montrons un exemple avec /grid/Metric-labels/{label}/values sélectionnées dans la catégorie Metrics.

7. Par exemple, la commande curl suivante avec le jeton d'autorisation précédent répertorie les noms de sites dans 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"
```

La commande CURL génère la sortie suivante :

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

Affichez les metrics à l'aide du tableau de bord Grafana dans StorageGRID

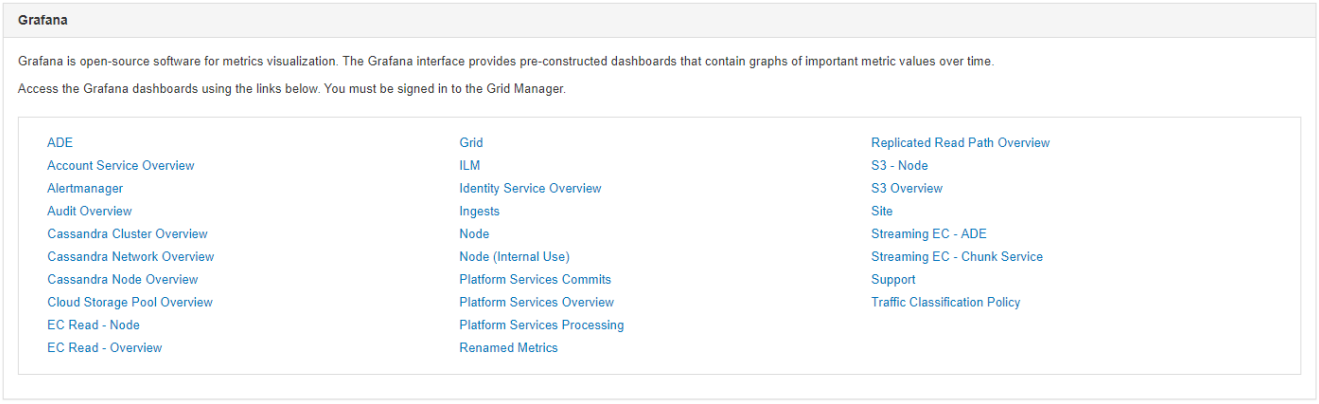
Découvrez comment utiliser l'interface Grafana pour visualiser et surveiller vos données StorageGRID.

Grafana est un logiciel open source pour la visualisation des mesures. Par défaut, nous disposons de tableaux de bord préconstruits qui fournissent des informations utiles et puissantes sur votre système StorageGRID.

Ces tableaux de bord préconstruits sont non seulement utiles pour la surveillance, mais aussi pour le dépannage d'un problème. Certains sont destinés à être utilisés par le support technique. Par exemple, pour afficher les mesures d'un nœud de stockage, procédez comme suit.

Étapes

1. Dans l'interface GMI, **support › Metrics**.
2. Dans la section Grafana, sélectionnez le tableau de bord Node.



3. Dans Grafana, définissez les hôtes sur le nœud sur lequel vous souhaitez afficher les mesures. Dans ce cas, un nœud de stockage est sélectionné. Plus d'informations sont fournies que les captures d'écran suivantes.

Utilisez les stratégies de classification du trafic dans StorageGRID

Découvrez comment configurer et configurer des règles de classification du trafic pour gérer et optimiser le trafic réseau dans StorageGRID.

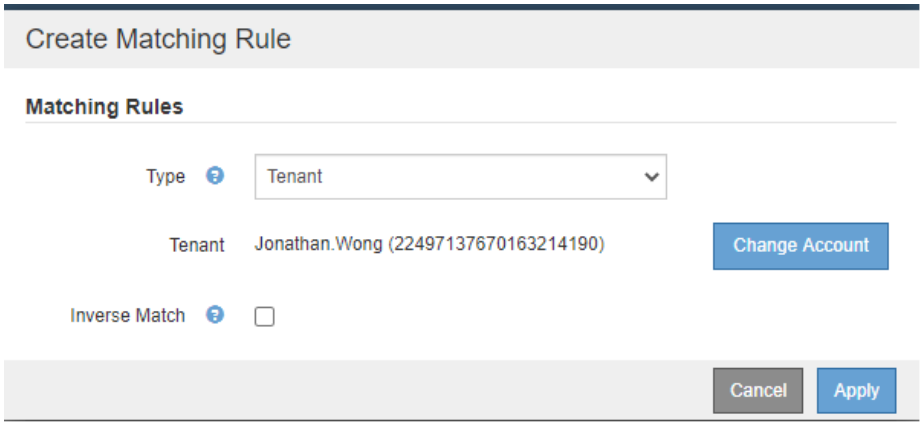
Les règles de classification du trafic fournissent une méthode de surveillance et/ou de limitation du trafic basée sur un locataire, un compartiments, des sous-réseaux IP ou des terminaux d'équilibrage de charge spécifiques. La connectivité réseau et la bande passante sont des mesures particulièrement importantes pour StorageGRID.

Pour configurer une stratégie de classification de trafic, procédez comme suit :

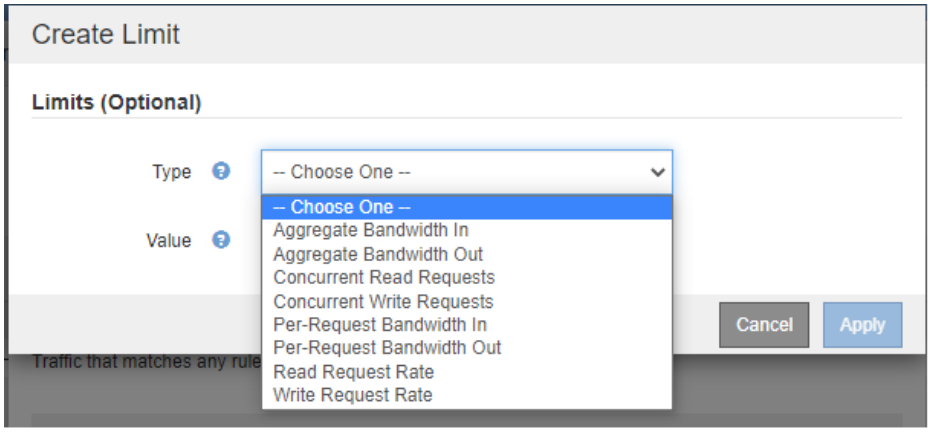
Étapes

1. Dans l'interface GMI, accédez au **Configuration › Paramètres système › Classification du trafic**.
2. Cliquez sur Créer +

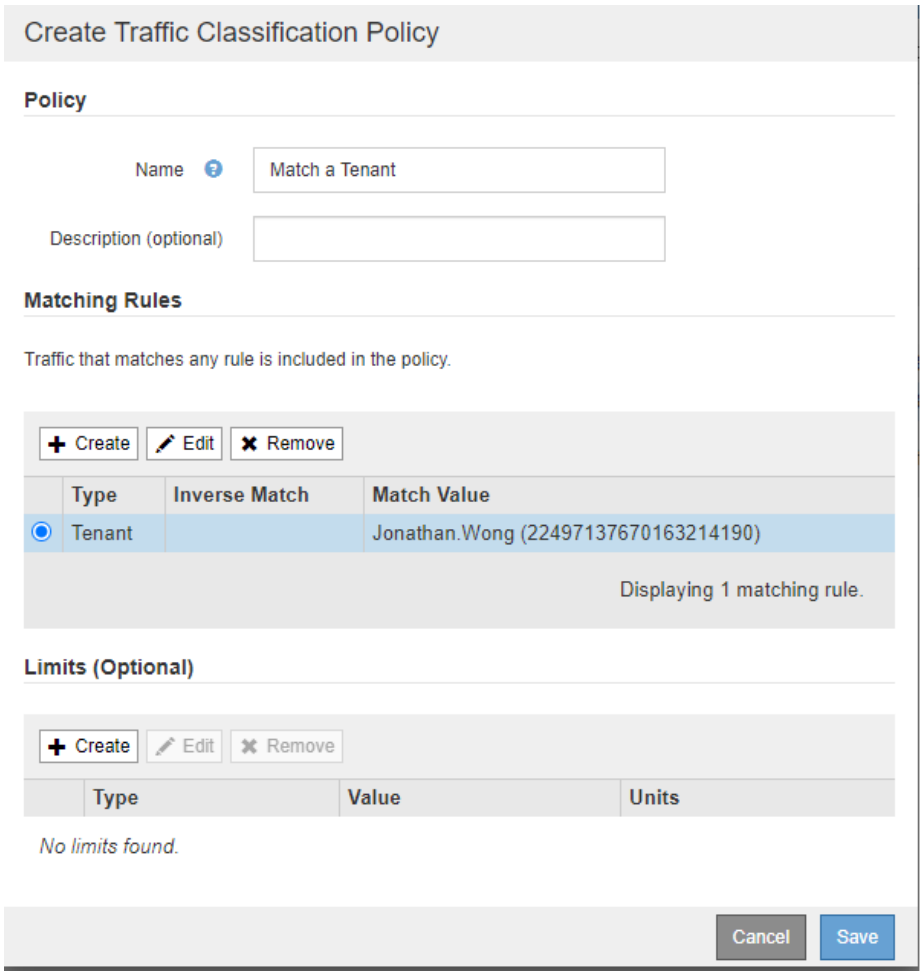
3. Entrez un nom et une description pour votre police.
4. Créez une règle correspondante.



5. Définissez une limite (facultatif).



6. Enregistrez votre police



Pour afficher les mesures associées à votre stratégie de classification de trafic, sélectionnez votre stratégie et cliquez sur métriques. Un tableau de bord Grafana est généré et affiche des informations telles que le trafic des demandes Load Balancer et la durée moyenne des demandes.

Utilisez les journaux d'audit pour surveiller StorageGRID

Découvrez comment utiliser le journal d'audit StorageGRID pour obtenir des informations détaillées sur les activités des locataires et du grid et comment exploiter des outils tels que Splunk pour l'analyse des journaux.

Le journal des audits StorageGRID vous permet de collecter des informations détaillées sur les activités du locataire et du grid. Le journal des audits peut être exposé à des fins d'analytique via le protocole NFS. Pour obtenir des instructions détaillées sur l'exportation du journal d'audit, reportez-vous au Guide de l'administrateur.

Une fois l'audit exporté, vous pouvez utiliser des outils d'analyse des journaux tels que Splunk ou Logstash + Elasticsearch pour comprendre l'activité des locataires ou créer des rapports détaillés de facturation et de facturation interne.

Des informations détaillées sur les messages d'audit sont disponibles dans la documentation StorageGRID. Voir "Messages d'audit".

Utilisez l'application StorageGRID pour Splunk

En savoir plus sur l'application NetApp StorageGRID pour Splunk qui permet de surveiller et d'analyser votre environnement StorageGRID au sein de la plateforme Splunk.

Splunk est une plateforme logicielle qui importe et indexe les données machine pour offrir de puissantes fonctionnalités de recherche et d'analyse. L'application NetApp StorageGRID est un complément pour Splunk qui importe et enrichit les données à partir de StorageGRID.

Vous trouverez des instructions sur l'installation, la mise à niveau et la configuration du module complémentaire StorageGRID à l'adresse suivante : https://splunkbase.splunk.com/app/3895/#/details

Tr-4882 : installation d'une grille métallique StorageGRID

Introduction à l'installation de StorageGRID

Découvrez comment installer StorageGRID sur des hôtes bare Metal.

Le TR-4882 fournit un ensemble d'instructions pratiques et détaillées qui produit une installation de travail de NetApp StorageGRID. L'installation peut se faire soit sur des serveurs bare Metal, soit sur des machines virtuelles exécutées sur Red Hat Enterprise Linux (RHEL). L'approche consiste à effectuer une installation « optiniée » de six services conteneurisés StorageGRID sur trois machines physiques (ou virtuelles) dans une disposition et une configuration de stockage suggérées. Certains clients peuvent comprendre plus facilement le processus de déploiement en suivant l'exemple de déploiement présenté dans ce rapport technique.

Pour une compréhension plus approfondie de StorageGRID et du processus d'installation, consultez [StorageGRID d'installation, de https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html mise à niveau et de correctif] dans la documentation du produit.

Avant de commencer votre déploiement, examinons les exigences de calcul, de stockage et de réseau du logiciel NetApp StorageGRID. StorageGRID s'exécute en tant que service conteneurisé dans Podman ou Docker. Dans ce modèle, certaines exigences font référence au système d'exploitation hôte (le système d'exploitation qui héberge Docker et exécute le logiciel StorageGRID). En outre, certaines ressources sont allouées directement aux conteneurs Docker s'exécutant au sein de chaque hôte. Dans ce déploiement, afin

d'optimiser l'utilisation du matériel, nous déployons deux services par hôte physique. Pour plus d'informations, passez à la section suivante, "Conditions préalables à l'installation de StorageGRID".

Les étapes décrites dans ce rapport technique permettent d'effectuer une installation StorageGRID fonctionnelle sur six hôtes bare Metal. Vous disposez désormais d'une grille et d'un réseau client qui fonctionnent, ce qui est utile dans la plupart des scénarios de test.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce rapport technique, consultez les ressources de documentation suivantes :

- Centre de documentation NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/
- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Conditions préalables à l'installation de StorageGRID

Découvrez les besoins en ressources de calcul, de stockage, de réseau, docker et de nœuds pour déployer StorageGRID.

Exigences de calcul

Le tableau ci-dessous répertorie les ressources minimales requises pour chaque type de nœud StorageGRID. Il s'agit des ressources minimales requises pour les nœuds StorageGRID.

Type de nœud	Cœurs de processeurs	RAM
Admin	8	24 GO
Stockage	8	24 GO
Passerelle	8	24 GO

En outre, chaque hôte Docker physique doit disposer d'un minimum de 16 Go de RAM pour fonctionner correctement. Ainsi, par exemple, pour héberger deux des services décrits dans le tableau ensemble sur un hôte Docker physique, effectuez le calcul suivant :

24 + 24 + 16 = 64 Go de RAM et 8 + 8 = 16 cœurs

Comme nombre de serveurs modernes dépassent ces exigences, nous combinons six services (conteneurs StorageGRID) en trois serveurs physiques.

Configuration réseau requise

Les trois types de trafic StorageGRID sont les suivants :

- **Trafic de grille (requis).** Trafic StorageGRID interne qui circule entre tous les nœuds de la grille.
- **Trafic Admin (facultatif).** Trafic utilisé pour l'administration et la maintenance du système.
- **Trafic client (facultatif).** Le trafic qui circule entre les applications client externes et la grille, y compris toutes les demandes de stockage objet des clients S3 et Swift.

Vous pouvez configurer jusqu'à trois réseaux à utiliser avec le système StorageGRID. Chaque type de réseau

doit se trouver sur un sous-réseau distinct sans chevauchement. Si tous les nœuds se trouvent sur le même sous-réseau, aucune adresse de passerelle n'est requise.

Pour cette évaluation, nous allons déployer sur deux réseaux, qui contiennent la grille et le trafic client. Il est possible d'ajouter un réseau d'administration plus tard pour servir cette fonction supplémentaire.

Il est très important de mapper les réseaux de manière cohérente aux interfaces sur tous les hôtes. Par exemple, s'il existe deux interfaces sur chaque nœud, sen192 et en224, elles doivent toutes être mappées sur le même réseau ou VLAN sur tous les hôtes. Dans cette installation, le programme d'installation les mappe dans les conteneurs Docker comme eth0@if2 et eth2@if3 (car le bouclage est if1 à l'intérieur du conteneur). Il est donc très important d'avoir un modèle cohérent.

Remarque sur la mise en réseau Docker

StorageGRID utilise la mise en réseau différemment de certaines implémentations de conteneurs Docker. Il n'utilise pas la mise en réseau fournie par Docker (ou Kubernetes ou Swarm). StorageGRID génère alors le conteneur sous la forme --net=none, de sorte que Docker ne fait rien pour le mettre en réseau. Une fois le conteneur généré par le service StorageGRID, un nouveau périphérique macvlan est créé à partir de l'interface définie dans le fichier de configuration du nœud. Ce périphérique a une nouvelle adresse MAC et agit comme un périphérique réseau distinct qui peut recevoir des paquets de l'interface physique. Le périphérique macvlan est alors déplacé dans l'espace de noms du conteneur et renommé eth0, eth1 ou eth2 à l'intérieur du conteneur. À ce stade, le périphérique réseau n'est plus visible dans le système d'exploitation hôte. Dans notre exemple, le dispositif réseau Grid est eth0 à l'intérieur des conteneurs Docker et le réseau client est eth2. Si nous disposions d'un réseau d'administration, le dispositif serait eth1 dans le conteneur.

> La nouvelle adresse MAC du périphérique réseau de conteneur peut nécessiter l'activation du mode promiscuous dans certains environnements réseau et virtuels. Ce mode permet au périphérique physique de recevoir et d'envoyer des paquets pour les adresses MAC qui diffèrent de l'adresse MAC physique connue. si vous exécutez VMware vSphere, vous devez accepter le mode promiscuité, les modifications d'adresse MAC et les transmissions forgées dans les groupes de ports qui serviront le trafic StorageGRID lors de l'exécution de RHEL. Ubuntu ou Debian fonctionne sans ces changements dans la plupart des circonstances.

Conditions de stockage

Les nœuds nécessitent chacun des périphériques de disque SAN ou locaux de la taille indiquée dans le tableau suivant.

> Les chiffres indiqués dans le tableau correspondent à chaque type de service StorageGRID, et non à la grille entière ou à chaque hôte physique. En fonction des choix de déploiement, nous calculerons les nombres pour chaque hôte physique dans , plus loin dans "Configuration et configuration requise de l'hôte physique"ce document. les chemins ou systèmes de fichiers marqués d'un astérisque seront créés dans le conteneur StorageGRID lui-même par l'installateur. L'administrateur n'a pas besoin de créer manuellement une configuration ou un système de fichiers, mais les hôtes ont besoin de périphériques en mode bloc pour répondre à ces exigences. En d'autres termes, le périphérique de bloc doit apparaître à l'aide de la commande, mais il ne doit `lsblk` pas être formaté ou monté dans le système d'exploitation hôte.

Type de nœud	Objectif de LUN	Nombre de LUN	Taille minimale de la LUN	Système de fichiers manuel requis	Entrée de configuration de nœud suggérée
Tout	Espace système du nœud d'administration `/var/local` (SSD utile ici)	Un pour chaque nœud d'administration	90 GO	Non	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`
Tous les nœuds	Pool de stockage Docker au `/var/lib/docker for container pool`	Un pour chaque hôte (physique ou machine virtuelle)	100 Go par conteneur	Oui – etx4	Na : formatez et montez en tant que système de fichiers hôte (non mappé dans le conteneur)
Admin	Journaux d'audit de nœud d'administration (données système dans le conteneur d'administration) `/var/local/audit/export`	Un pour chaque nœud d'administration	200 GO	Non	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
Admin	Tables de nœuds d'administration (données système dans le conteneur d'administration) `/var/local/mysql_ibdata`	Un pour chaque nœud d'administration	200 GO	Non	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
Nœuds de stockage	Stockage objet (dispositifs en mode bloc `/var/local/rangedb0`) (SSD utile ici) `/var/local/rangedb1` `/var/local/rangedb2`	Trois pour chaque conteneur de stockage	4,000 GO	Non	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

Dans cet exemple, les tailles de disques indiquées dans le tableau suivant sont requises par type de conteneur. Les exigences par hôte physique sont décrites dans "Configuration et configuration requise de l'hôte physique", plus loin dans ce document.

Tailles de disques par type de conteneur

Conteneur d'administration

Nom	Taille (Gio)
Docker-Store	100 (par conteneur)
ADM-OS	90
SMA-Vérification	200
ADM-MySQL	200

Conteneur de stockage

Nom	Taille (Gio)
Docker-Store	100 (par conteneur)
SN-OS	90
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

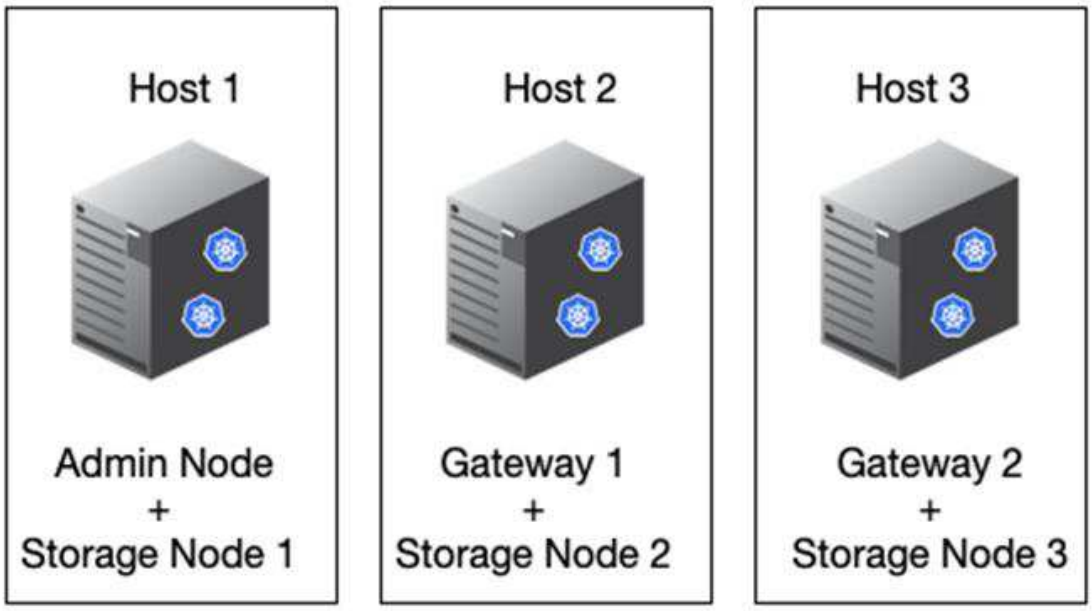
Conteneur de passerelle

Nom	Taille (Gio)
Docker-Store	100 (par conteneur)
/var/local	90

Configuration et configuration requise de l’hôte physique

En combinant les exigences de calcul et de réseau indiquées dans le tableau ci-dessus, vous pouvez obtenir un ensemble de matériel de base requis pour cette installation de trois serveurs physiques (ou virtuels) avec 16 cœurs, 64 Go de RAM et deux interfaces réseau. Si un débit plus élevé est souhaité, il est possible de lier deux interfaces ou plus sur la grille ou le réseau client et d’utiliser une interface marquée VLAN telle que bond0.520 dans le fichier de configuration du nœud. Si vous attendez des charges de travail plus intenses, il vaut mieux augmenter la mémoire pour l’hôte et les conteneurs.

Comme illustré dans la figure ci-dessous, ces serveurs hébergent six conteneurs Docker, deux par hôte. La RAM est calculée en fournissant 24 Go par conteneur et 16 Go pour le système d’exploitation hôte lui-même.



La mémoire RAM totale requise par hôte physique (ou machine virtuelle) est de 24 x 2 + 16 = 64 Go. Les tableaux suivants répertorient le stockage sur disque requis pour les hôtes 1, 2 et 3.

Hôte 1	**Taille (Gio)**
Docker Store	`/var/lib/docker` (Système de fichiers)
200 (100 x 2)	**Conteneur Admin**
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
Conteneur de stockage	SN-OS `/var/local` (périphérique)
90	Rangedb-0 (périphérique)
4096	Rangedb-1 (périphérique)
4096	Rangedb-2 (dispositif)

Hôte 2	**Taille (Gio)**
Docker Store	`/var/lib/docker` (Partagé)
200 (100 x 2)	**Conteneur passerelle**
GW-OS */`var/local`	100

Hôte 2	Taille (Gio)
Conteneur de stockage	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Hôte 3	Taille (Gio)
Docker Store	/var/lib/docker (Partagé)
200 (100 x 2)	**Conteneur passerelle**
*/var/local	100
Conteneur de stockage	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Le Docker Store a été calculé en autorisant 100 Go par /var/local (par conteneur) x deux conteneurs = 200 Go.

Préparation des nœuds

Pour préparer l'installation initiale de StorageGRID, installez d'abord RHEL version 9.2 et activez SSH. Configurez les interfaces réseau, le protocole NTP (Network Time Protocol), le DNS et le nom d'hôte conformément aux bonnes pratiques. Vous avez besoin d'au moins une interface réseau activée sur le réseau en grille et une autre pour le réseau client. Si vous utilisez une interface marquée VLAN, configurez-la comme indiqué dans les exemples ci-dessous. Sinon, une simple configuration d'interface réseau standard suffit.

Si vous devez utiliser une balise VLAN sur l'interface réseau de la grille, votre configuration doit avoir deux fichiers /etc/sysconfig/network-scripts/ au format suivant :

```
# 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
```

Cet exemple suppose que votre périphérique réseau physique pour le réseau de grille est enp67s0. Il pourrait également être un dispositif lié tel que bond0. Que vous utilisiez la liaison ou une interface réseau standard, vous devez utiliser l'interface marquée VLAN dans votre fichier de configuration de nœud si votre port réseau n'a pas de VLAN par défaut ou si le VLAN par défaut n'est pas associé au réseau de grille. Le conteneur StorageGRID lui-même ne débalise pas les trames Ethernet, il doit donc être géré par le système d'exploitation parent.

Configuration du stockage en option avec iSCSI

Si vous n'utilisez pas de stockage iSCSI, vous devez vous assurer que host1, host2 et host3 contiennent des périphériques de bloc de taille suffisante pour répondre à leurs besoins. Reportez-vous à la section pour connaître les exigences en matière de stockage pour "Tailles de disques par type de conteneur" les hôtes 1, 2 et 3.

Pour configurer le stockage avec iSCSI, procédez comme suit :

Étapes

1. Si vous utilisez un stockage iSCSI externe tel que le logiciel de gestion des données NetApp E-Series ou NetApp ONTAP®, installez les packages suivants :

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

2. Recherchez l'ID d'initiateur sur chaque hôte.

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

3. En utilisant le nom d'initiateur de l'étape 2, mappez les LUN de votre périphérique de stockage (du nombre et de la taille indiqués dans le "Conditions de stockage" tableau) sur chaque nœud de stockage.

4. Identifiez les LUN créées avec et connectez-vous à ces LUN `iscsiadm` .

```
# 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.
```

Pour plus de détails, consultez le "Création d'un initiateur iSCSI" portail des clients Red Hat.

5. Pour afficher les chemins d'accès multiples et les WWID de LUN associés, exécutez la commande suivante :

```
# multipath -ll
```

Si vous n'utilisez pas iSCSI avec des périphériques à chemins d'accès multiples, montez simplement votre périphérique à l'aide d'un nom de chemin unique qui persistera à modifier et à redémarrer le périphérique.

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

L'utilisation de `/dev/sdx` noms de périphériques peut entraîner des problèmes ultérieurement si des périphériques sont supprimés ou ajoutés. si vous utilisez des périphériques multivoies, modifiez le `/etc/multipath.conf` fichier pour utiliser les alias comme suit.

Ces périphériques peuvent être présents ou non sur tous les nœuds, selon la disposition.

```
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
}
}
```

Avant d'installer Docker sur votre système d'exploitation hôte, formatez et montez le support de LUN ou de disque `/var/lib/docker`. Les autres LUN sont définies dans le fichier de configuration du nœud et utilisées directement par les conteneurs StorageGRID. C'est-à-dire qu'ils n'apparaissent pas dans le système d'exploitation hôte ; ils apparaissent dans les conteneurs eux-mêmes et ces systèmes de fichiers sont gérés par le programme d'installation.

Si vous utilisez une LUN avec support iSCSI, placez un élément similaire à la ligne suivante dans votre fichier

fstab. Comme indiqué, les autres LUN n'ont pas besoin d'être montées dans le système d'exploitation hôte, mais doivent apparaître comme périphériques de bloc disponibles.

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

Préparation de l'installation de Docker

Pour préparer l'installation de Docker, procédez comme suit :

Étapes

1. Créez un système de fichiers sur le volume de stockage Docker sur les trois hôtes.

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

   Si vous utilisez des périphériques iSCSI avec chemins d'accès multiples, utilisez `/dev/mapper/Docker-Store`.

2. Créer le point de montage du volume de stockage Docker :

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

3. Ajoutez une entrée similaire pour docker-Storage-volume-device à `/etc/fstab`.

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

   L'option suivante `_netdev` est recommandée uniquement si vous utilisez un périphérique iSCSI. Si vous utilisez un périphérique de bloc local `_netdev` n'est pas nécessaire et `defaults` est recommandé.

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

4. Montez le nouveau système de fichiers et affichez l'utilisation du disque.

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

5. Désactivez l'échange et désactivez-le pour des raisons de performances.

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

6. Pour conserver les paramètres, supprimez toutes les entrées de swap de /etc/fstab telles que :

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

> Si vous ne désactivez pas ces fichiers, les performances peuvent être considérablement réduites.

7. Effectuez un redémarrage test de votre nœud pour vous assurer que le `/var/lib/docker` volume est persistant et que tous les périphériques de disque sont retournés.

Installez Docker pour StorageGRID

Découvrez comment installer Docker pour StorageGRID.

Pour installer Docker, procédez comme suit :

Étapes

1. Configurez yum repo pour Docker.

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

2. Installez les packages nécessaires.

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

3. Démarrez Docker.

```
sudo systemctl start docker
```

4. Tester Docker.

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

5. Assurez-vous que Docker s'exécute au démarrage du système.

```
sudo systemctl enable docker
```

Préparez les fichiers de configuration des nœuds pour StorageGRID

Découvrez comment préparer les fichiers de configuration des nœuds pour StorageGRID.

À un niveau élevé, le processus de configuration des nœuds comprend les étapes suivantes :

Étapes

1. Créez le `/etc/storagegrid/nodes` répertoire sur tous les hôtes.

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

2. Créez les fichiers nécessaires par hôte physique pour correspondre à la disposition du type de conteneur/nœud. Dans cet exemple, nous avons créé deux fichiers par hôte physique sur chaque machine hôte.

> Le nom du fichier définit le nom réel du nœud pour l'installation. Par exemple, `dc1-adm1.conf` devient un nœud nommé `dc1-adm1`.

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

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

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

Préparation des fichiers de configuration du nœud

Les exemples suivants utilisent le `/dev/disk/by-path` format. Vous pouvez vérifier les chemins d'accès corrects en exécutant les commandes suivantes :

```
[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
```

Et ces commandes :

```
[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
```

Exemple pour le nœud d'administration principal

Exemple de nom de fichier :

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

Exemple de contenu de fichier :

> Les chemins de disque peuvent suivre les exemples ci-dessous ou utiliser `/dev/mapper/alias` la dénomination de style. N'utilisez pas de noms de périphériques de blocage tels que `/dev/sdb` , car ils peuvent changer au redémarrage et causer des dommages importants à votre grille.

```
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
```

Exemple de nœud de stockage

Exemple de nom de fichier :

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

Exemple de contenu de fichier :

```
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
```

Exemple de nœud de passerelle

Exemple de nom de fichier :

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

Exemple de contenu de fichier :

```
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
```

Installez les dépendances et les packages StorageGRID

Découvrez comment installer les packages et les dépendances StorageGRID.

Pour installer les dépendances et les packages StorageGRID, exécutez les commandes suivantes :

```
[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
```

Validez les fichiers de configuration StorageGRID

Découvrez comment valider le contenu des fichiers de configuration pour StorageGRID.

Après avoir créé les fichiers de configuration dans `/etc/storagegrid/nodes` pour chacun de vos nœuds StorageGRID, vous devez valider le contenu de ces fichiers.

Pour valider le contenu des fichiers de configuration, exécutez la commande suivante sur chaque hôte :

```
sudo storagegrid node validate all
```

Si les fichiers sont corrects, le résultat indique RÉUSSI pour chaque fichier de configuration :

```
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
```

Si les fichiers de configuration sont incorrects, les problèmes sont affichés comme AVERTISSEMENT et ERREUR. Si des erreurs de configuration sont détectées, vous devez les corriger avant de poursuivre l'installation.

```
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
```

Démarrez le service d'hôte StorageGRID

Découvrez comment démarrer le service hôte StorageGRID.

Pour démarrer les nœuds StorageGRID et vous assurer qu'ils redémarrent après un redémarrage de l'hôte, vous devez activer et démarrer le service hôte StorageGRID.

Pour démarrer le service hôte StorageGRID, procédez comme suit.

Étapes

1. Exécutez les commandes suivantes sur chaque hôte :

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

> Le processus de démarrage peut prendre un certain temps lors de l'exécution initiale.

2. Exécutez la commande suivante pour vérifier que le déploiement se déroule :

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

3. Pour tout nœud qui renvoie un état de `Not-Running` ou `Stopped`, exécutez la commande suivante :

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

   Par exemple, dans le résultat suivant, vous démarriez le `dc1-adm1` nœud :

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

4. Si vous avez précédemment activé et démarré le service hôte StorageGRID (ou si vous n'êtes pas sûr que le service a été activé et démarré), exécutez également la commande suivante :

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

Configurez le gestionnaire de grille dans StorageGRID

Découvrez comment configurer le Gestionnaire de grille dans StorageGRID sur le nœud d'administration principal.

Terminez l'installation en configurant le système StorageGRID à partir de l'interface utilisateur du Gestionnaire

de grille sur le nœud d'administration principal.

Étapes générales

La configuration de la grille et la fin de l'installation impliquent les tâches suivantes :

Étapes

1. Accédez à Grid Manager
2. "Spécifier les informations de licence StorageGRID"
3. "Ajouter des sites à StorageGRID"
4. "Spécifiez les sous-réseaux de réseau de grille"
5. "Approuver les nœuds de la grille en attente"
6. "Spécifiez les informations du serveur NTP"
7. "Spécifiez les informations relatives au serveur système du nom de domaine"
8. "Spécifiez les mots de passe système StorageGRID"
9. "Vérifiez votre configuration et terminez l'installation"

Accédez à Grid Manager

Utilisez le Gestionnaire de grille pour définir toutes les informations requises pour configurer votre système StorageGRID.

Avant de commencer, le nœud d'administration principal doit être déployé et avoir terminé la séquence de démarrage initiale.

Pour utiliser Grid Manager pour définir des informations, procédez comme suit.

Étapes

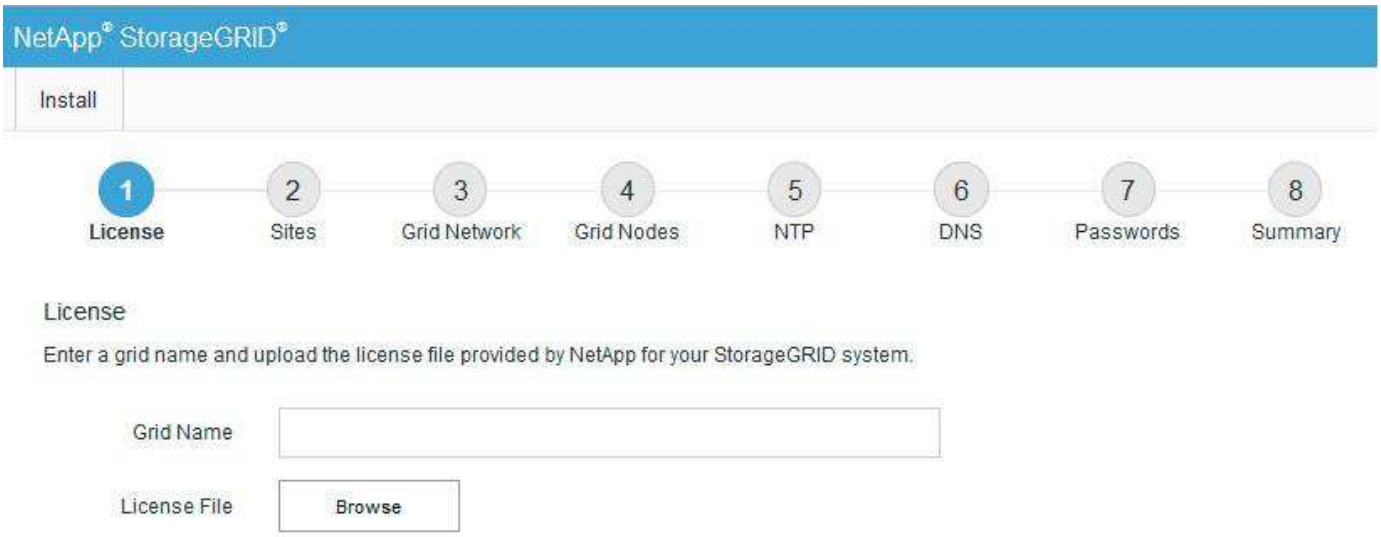
1. Accédez à Grid Manager à l'adresse suivante :

   ```
   https://primary_admin_node_grid_ip
   ```

   Vous pouvez également accéder à Grid Manager sur le port 8443.

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

2. Cliquez sur installer un système StorageGRID. La page utilisée pour configurer une grille StorageGRID s'affiche.



Ajoutez les détails de la licence StorageGRID

Découvrez comment télécharger le fichier de licence StorageGRID.

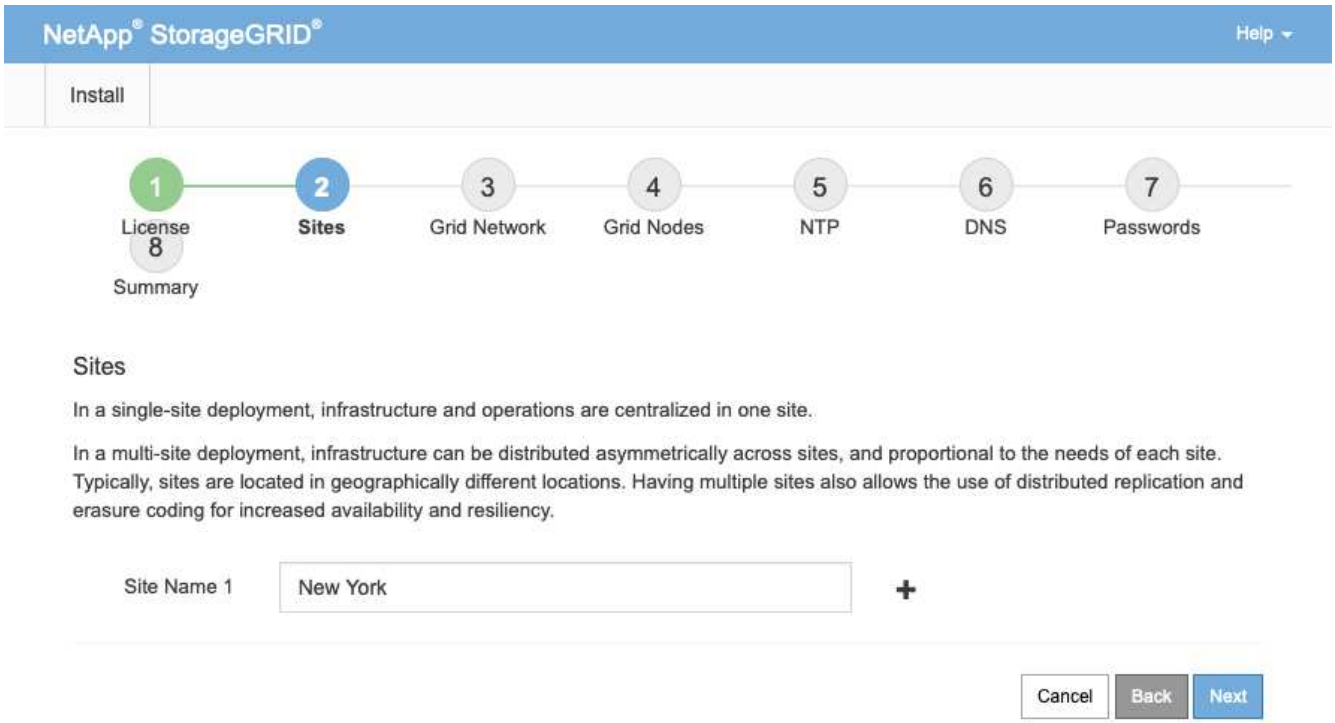
Vous devez indiquer le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Pour spécifier les informations de licence StorageGRID, procédez comme suit :

Étapes

1. Sur la page Licence, dans le champ Nom de la grille, entrez un nom pour votre système StorageGRID. Après l'installation, le nom s'affiche en tant que premier niveau dans l'arborescence de la topologie de la grille.
2. Cliquez sur Parcourir, localisez le fichier de licence NetApp (`NLF-unique-id.txt`), puis cliquez sur Ouvrir. Le fichier de licence est validé et le numéro de série et la capacité de stockage sous licence s'affichent.

> ⓘ L'archive d'installation de StorageGRID inclut une licence gratuite qui ne fournit aucun droit d'assistance pour le produit. Vous pouvez effectuer une mise à jour vers une licence offrant une assistance après l'installation.



3. Cliquez sur Suivant.

Ajouter des sites à StorageGRID

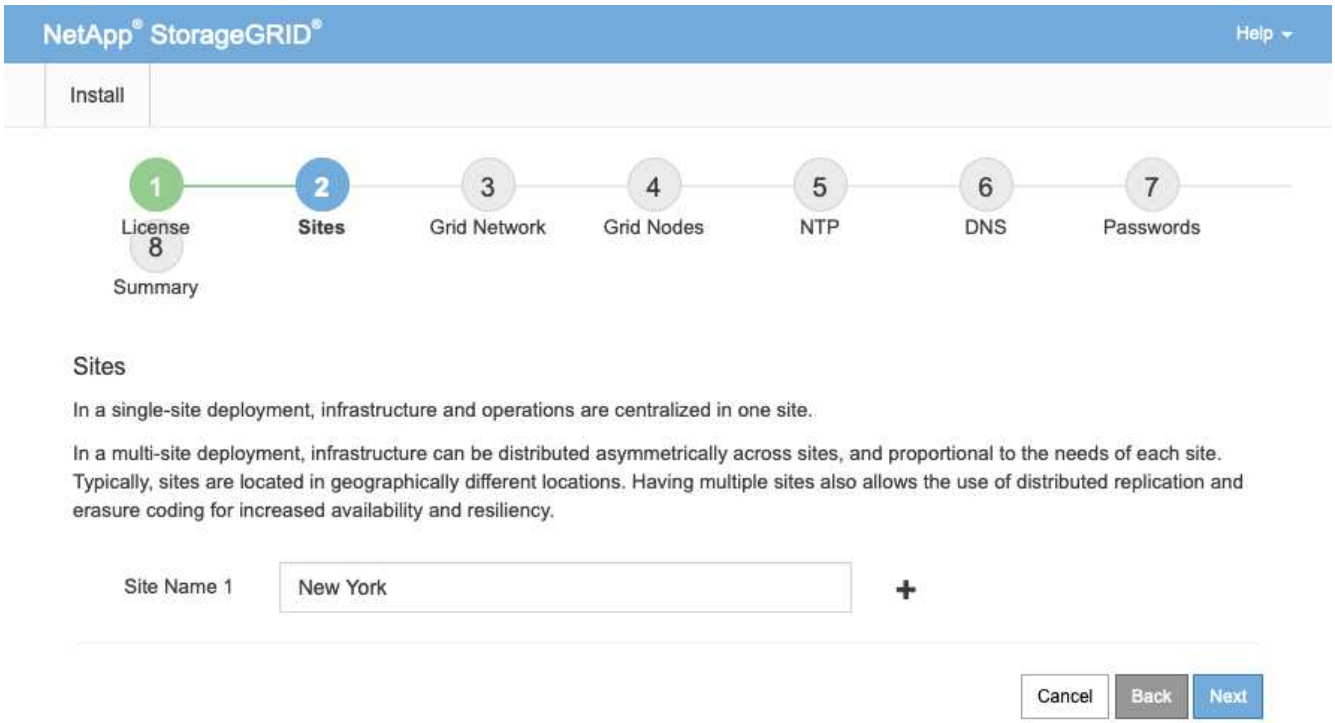
Découvrez comment ajouter des sites à StorageGRID afin d'améliorer la fiabilité et la capacité de stockage.

Lorsque vous installez StorageGRID, vous devez créer au moins un site. Vous pouvez créer des sites supplémentaires pour augmenter la fiabilité et la capacité de stockage de votre système StorageGRID.

Pour ajouter des sites, procédez comme suit :

Étapes

1. Sur la page sites, entrez le nom du site.
2. Pour ajouter des sites supplémentaires, cliquez sur le signe plus en regard de la dernière entrée de site et entrez le nom dans la zone de texte Nouveau nom de site. Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.



3. Cliquez sur Suivant.

Spécifiez les sous-réseaux de réseau de grille pour StorageGRID

Découvrez comment configurer les sous-réseaux réseau de la grille pour StorageGRID.

Vous devez spécifier les sous-réseaux utilisés sur le réseau de la grille.

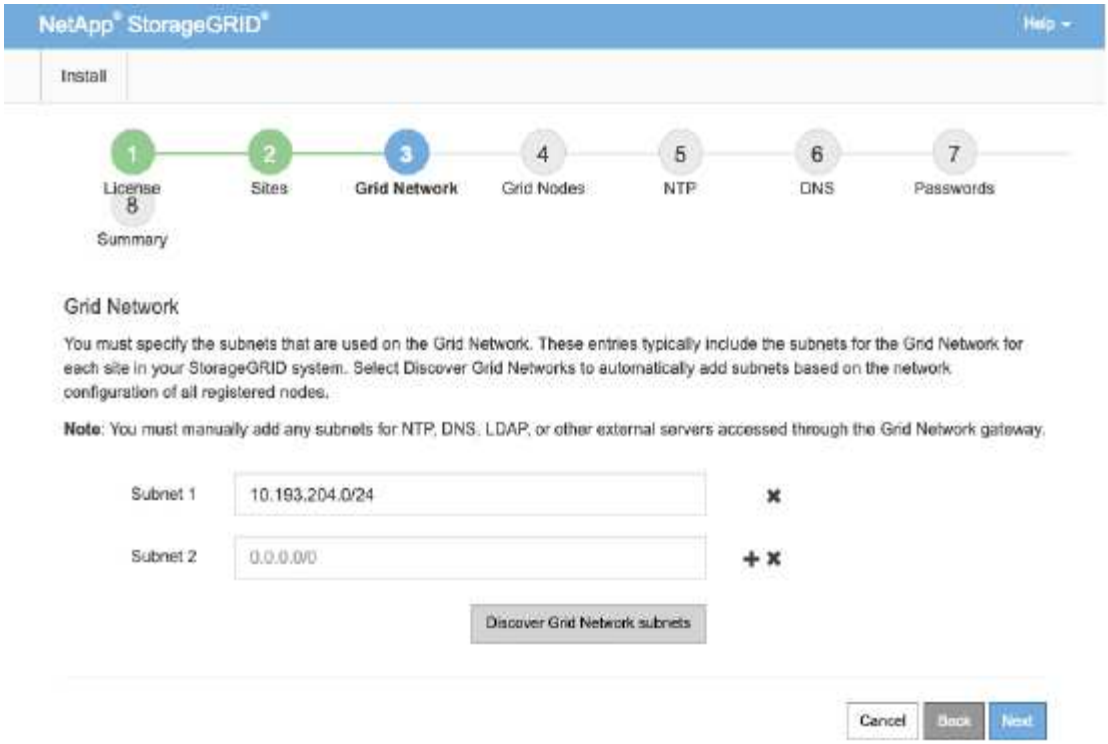
Les entrées de sous-réseau incluent les sous-réseaux du réseau de grille pour chaque site de votre système StorageGRID, en plus des sous-réseaux qui doivent être accessibles via le réseau de grille (par exemple, les sous-réseaux hébergeant vos serveurs NTP).

Si vous avez plusieurs sous-réseaux de grille, la passerelle de réseau de grille est requise. Tous les sous-réseaux de la grille spécifiés doivent être accessibles via cette passerelle.

Pour spécifier des sous-réseaux de réseau de grille, procédez comme suit :

Étapes

1. Dans la zone de texte sous-réseau 1, spécifiez l'adresse réseau CIDR d'au moins un réseau de grille.
2. Cliquez sur le signe plus à côté de la dernière entrée pour ajouter une entrée réseau supplémentaire. Si vous avez déjà déployé au moins un nœud, cliquez sur détecter les sous-réseaux de réseaux de grille pour remplir automatiquement la liste de sous-réseaux de réseau de grille avec les sous-réseaux signalés par les nœuds de grille qui ont été enregistrés avec Grid Manager.



3. Cliquez sur Suivant.

Approuver les nœuds grid pour StorageGRID

Découvrez comment vérifier et approuver tous les nœuds de grille en attente qui rejoignent le système StorageGRID.

Vous devez approuver chaque nœud de grille avant de rejoindre le système StorageGRID.

> Avant de commencer, tous les nœuds de grid des appliances virtuelles et StorageGRID doivent être déployés.

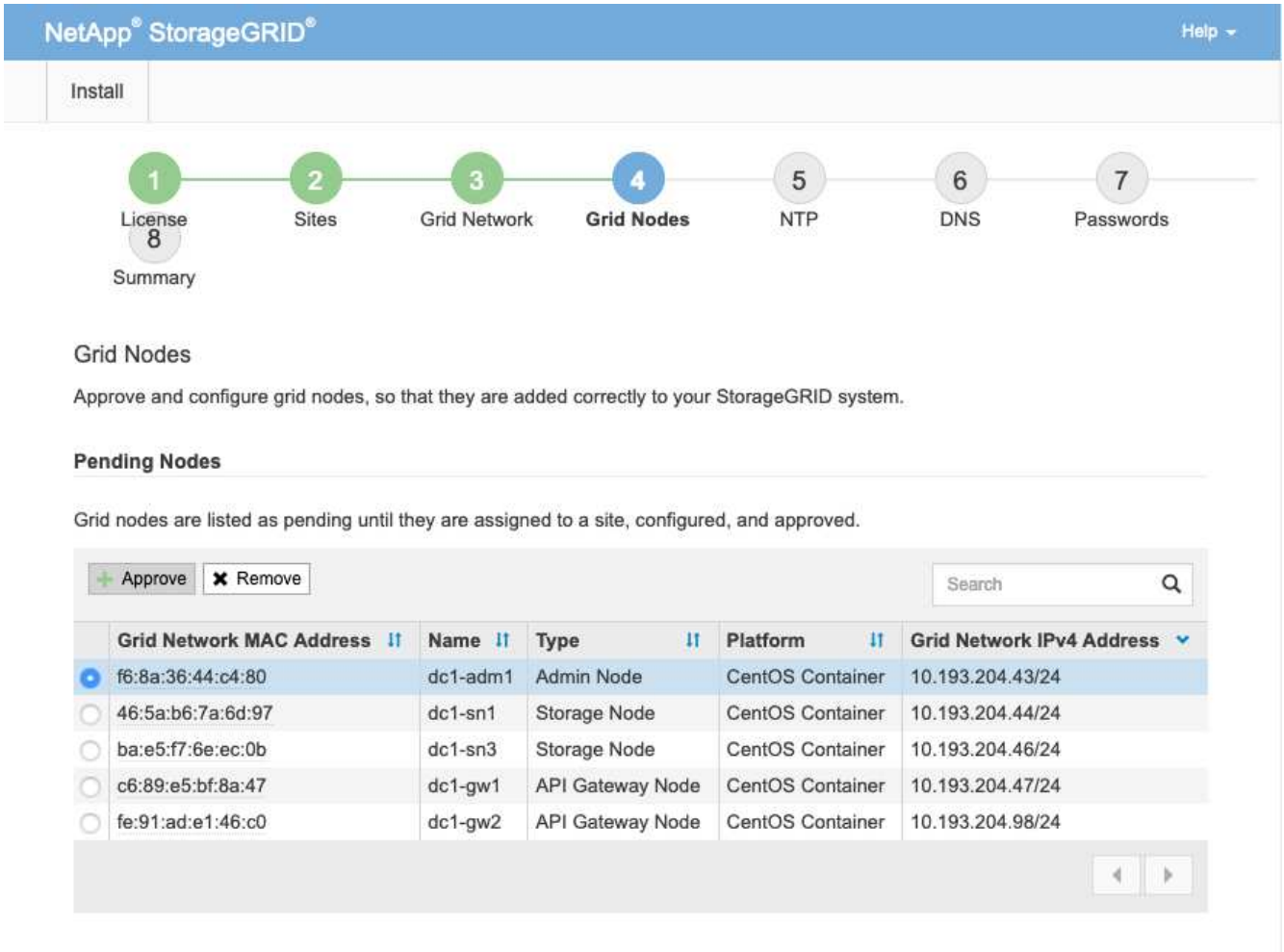
Pour approuver des nœuds de grille en attente, procédez comme suit :

Étapes

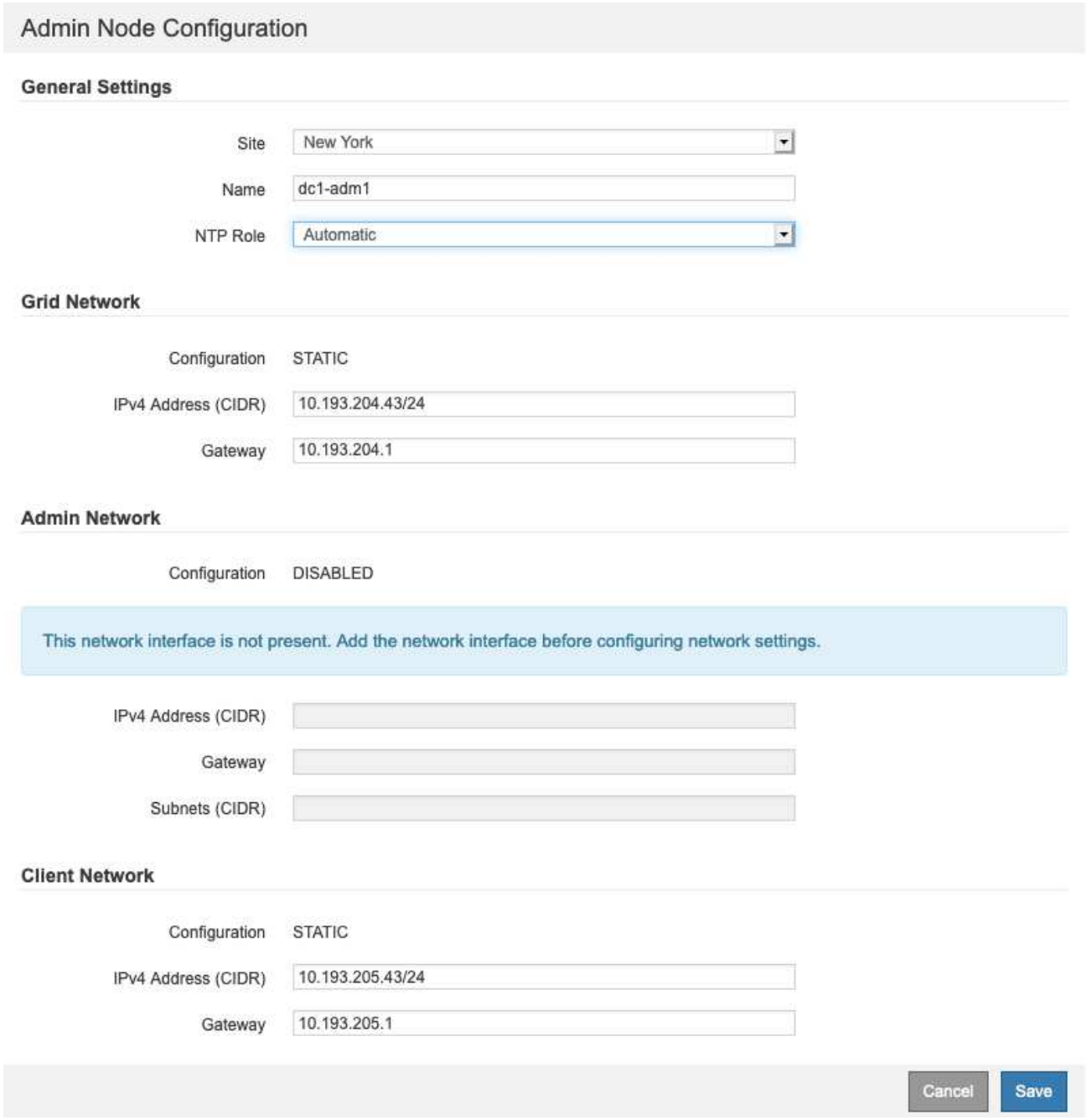
1. Consultez la liste nœuds en attente et vérifiez qu'elle affiche tous les nœuds de grille que vous avez déployés.

   > Si un nœud de grid n'est pas inclus, vérifiez qu'il a été déployé correctement.

2. Cliquez sur le bouton radio en regard d'un nœud en attente que vous souhaitez approuver.



3. Cliquez sur approuver.
4. Dans Paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire.



— **site** : le nom système du site pour ce noeud de grille.

— **Nom** : le nom d'hôte qui sera affecté au nœud, et le nom qui sera affiché dans Grid Manager. Le nom par défaut est celui que vous avez spécifié lors du déploiement du nœud, mais vous pouvez le modifier en fonction de vos besoins.

— **NTP role** : le rôle NTP du nœud de grille. Les options sont automatique, principal et client. La sélection de l'option automatique affecte le rôle principal aux nœuds d'administration, aux nœuds de stockage avec des services ADC (administrative Domain Controller), aux nœuds de passerelle et à tous les nœuds de grille qui ont des adresses IP non statiques. Le rôle client est attribué à tous les autres nœuds de la grille.

Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

— **Service ADC (noeuds de stockage uniquement)** : sélectionnez automatique pour permettre au système de déterminer si le noeud nécessite le service ADC. Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau. Au moins trois nœuds de stockage sur chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans réseau Grid, modifiez les paramètres des propriétés suivantes si nécessaire :

— **adresse IPv4 (CIDR)** : adresse réseau CIDR de l'interface réseau de la grille (eth0 à l'intérieur du conteneur). Par exemple `192.168.1.234/24`, .

— **passerelle** : la passerelle réseau de la grille. Par exemple `192.168.0.1`, .

S'il existe plusieurs sous-réseaux de grille, la passerelle est requise.

Si vous avez sélectionné DHCP pour la configuration réseau de la grille et que vous modifiez la valeur ici, la nouvelle valeur est configurée comme une adresse statique sur le nœud. Assurez-vous que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

6. Pour configurer le réseau d'administration pour le nœud de grille, ajoutez ou mettez à jour les paramètres de la section réseau d'administration si nécessaire.

Entrez les sous-réseaux de destination des routes de cette interface dans la zone de texte Subnet (CIDR). S'il existe plusieurs sous-réseaux d'administration, la passerelle d'administration est requise.

Si vous avez sélectionné DHCP pour la configuration réseau d'administration et que vous modifiez la valeur ici, la nouvelle valeur est configurée comme une adresse statique sur le nœud. Assurez-vous que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

Appareils : pour une appliance StorageGRID, si le réseau d'administration n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé › redémarrer**. Le redémarrage peut prendre plusieurs minutes.
b. Sélectionnez **configurer la mise en réseau › Configuration de la liaison** et activez les réseaux appropriés.
c. Sélectionnez **configurer la mise en réseau › Configuration IP** et configurez les réseaux activés.
d. Revenez à la page d'accueil et cliquez sur Démarrer l'installation.
e. Dans Grid Manager : si le nœud est répertorié dans le tableau nœuds approuvés, réinitialisez-le.
f. Supprimez le nœud du tableau nœuds en attente.

g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà contenir les informations que vous avez fournies sur la page de configuration IP. Pour plus d'informations, reportez-vous aux instructions d'installation et d'entretien de votre modèle d'appareil.

7. Si vous souhaitez configurer le réseau client pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section réseau client si nécessaire. Si le réseau client est configuré, la passerelle est requise et devient la passerelle par défaut du noeud après l'installation.

   Appareils : pour une appliance StorageGRID, si le réseau client n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé › redémarrer**. Le redémarrage peut prendre plusieurs minutes.

   b. Sélectionnez **configurer la mise en réseau › Configuration de la liaison** et activez les réseaux appropriés.

   c. Sélectionnez **configurer la mise en réseau › Configuration IP** et configurez les réseaux activés.

   d. Revenez à la page d'accueil et cliquez sur Démarrer l'installation.

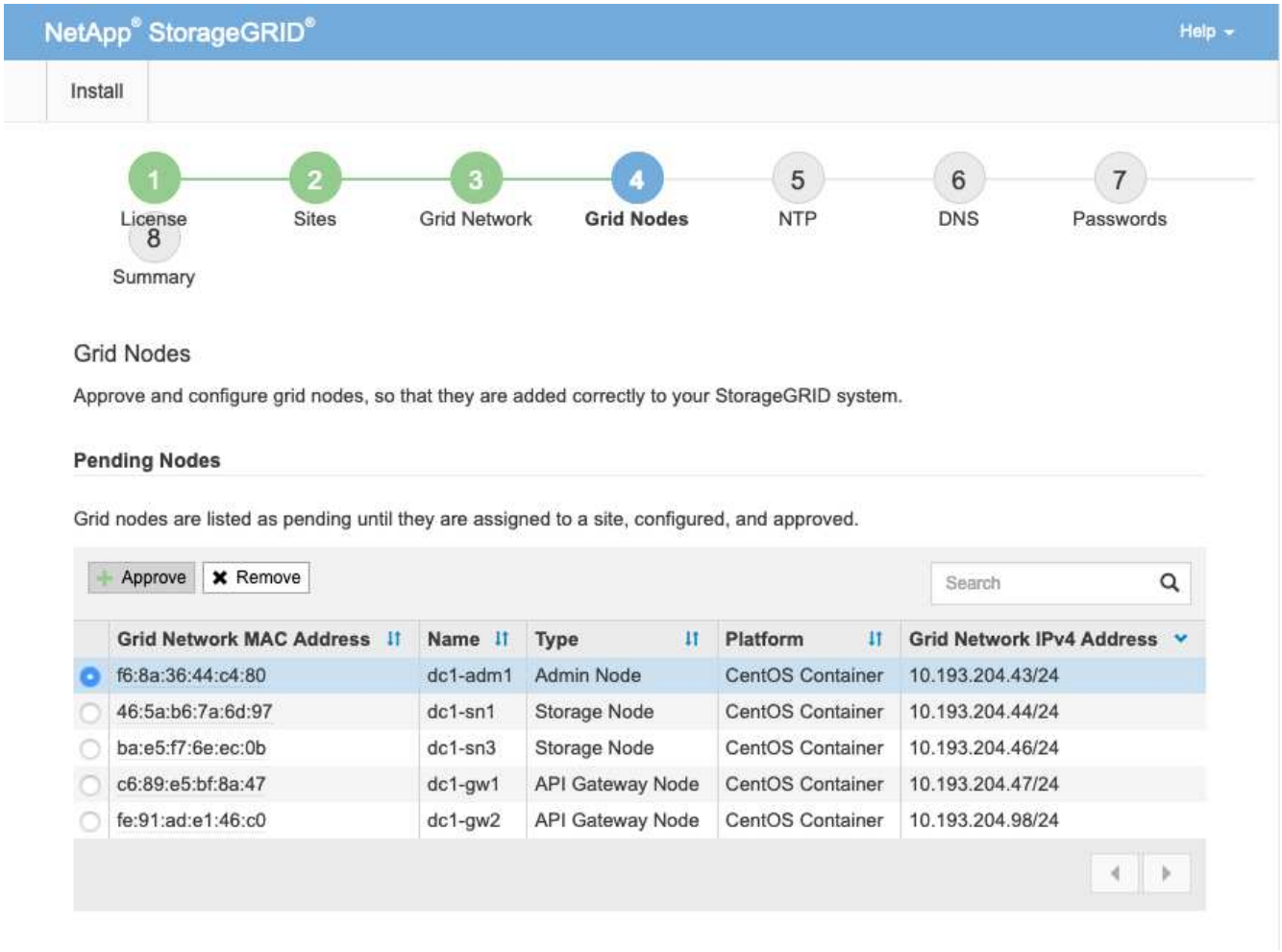
   e. Dans Grid Manager : si le nœud est répertorié dans le tableau nœuds approuvés, réinitialisez-le.

   f. Supprimez le nœud du tableau nœuds en attente.

   g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

   h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà contenir les informations que vous avez fournies sur la page de configuration IP. Pour plus d'informations, reportez-vous aux instructions d'installation et de maintenance de votre appareil.

8. Cliquez sur Enregistrer. L'entrée de nœud de la grille passe à la liste nœuds approuvés.



9. Répétez les étapes 1 à 1-8 pour chaque nœud de grille en attente que vous souhaitez approuver.

   Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir à cette page à tout moment avant de cliquer sur installer sur la page Résumé. Pour modifier les propriétés d'un nœud de grille approuvé, cliquez sur son bouton radio, puis cliquez sur Modifier.

10. Lorsque vous avez fini d'approuver les nœuds de la grille, cliquez sur Suivant.

Spécifiez les détails du serveur NTP pour StorageGRID

Découvrez comment spécifier les informations de configuration NTP de votre système StorageGRID afin que les opérations effectuées sur des serveurs distincts puissent être synchronisées.

Pour éviter les problèmes de décalage horaire, vous devez spécifier quatre références de serveur NTP externe de Stratum 3 ou supérieur.

> Lorsque vous spécifiez la source NTP externe pour une installation StorageGRID au niveau de la production, n'utilisez pas le service Windows Time (W32Time) sur une version de Windows antérieure à Windows Server 2016. Sur les versions antérieures de Windows, le service horaire n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements exigeants tels que StorageGRID.

Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué les rôles

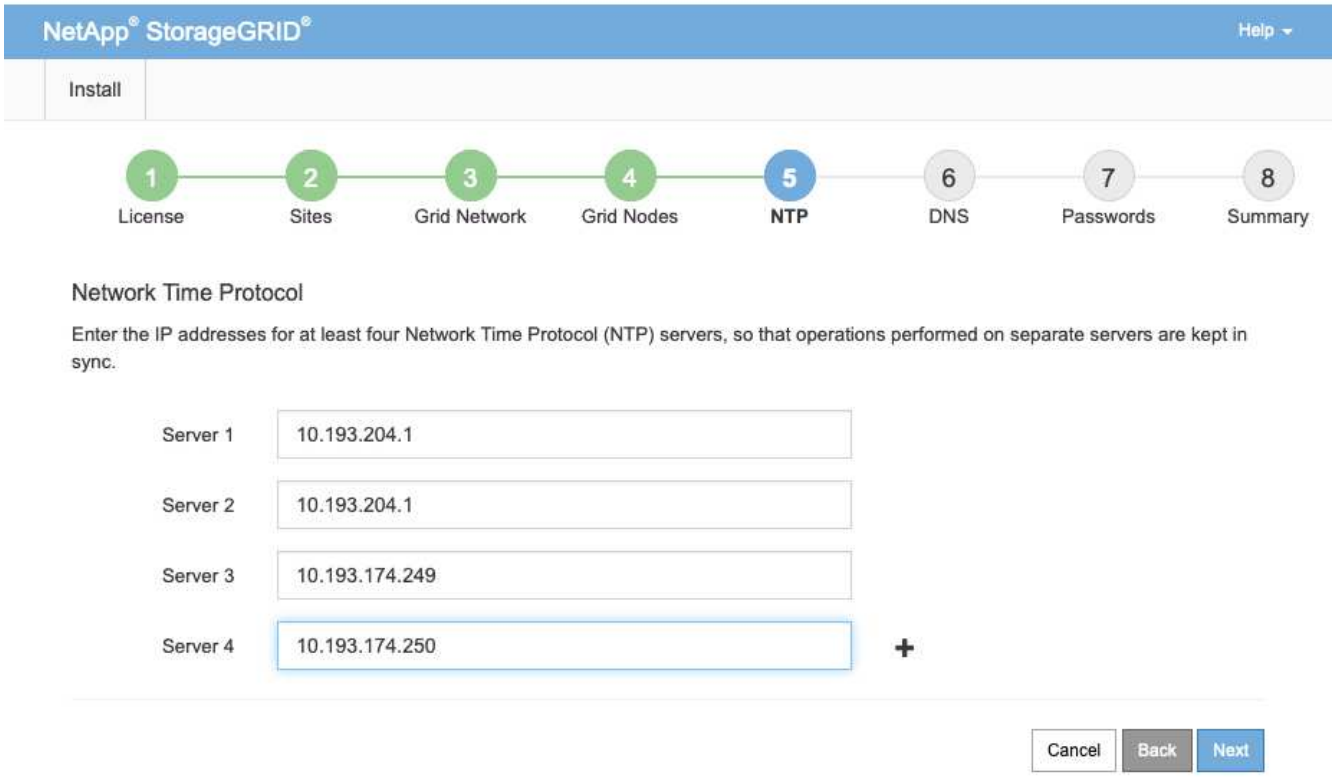
NTP principaux.

> Le réseau client n'est pas activé suffisamment tôt dans le processus d'installation pour être la seule source de serveurs NTP. Assurez-vous qu'au moins un serveur NTP peut être atteint sur le réseau de grille ou le réseau d'administration.

Pour spécifier les informations du serveur NTP, procédez comme suit :

Étapes

1. Dans les zones de texte serveur 1 à serveur 4, spécifiez les adresses IP d'au moins quatre serveurs NTP.
2. Si nécessaire, cliquez sur le signe plus en regard de la dernière entrée pour ajouter d'autres entrées de serveur.



3. Cliquez sur Suivant.

Spécifiez les détails du serveur DNS pour StorageGRID

Découvrez comment configurer le serveur DNS pour StorageGRID.

Vous devez spécifier les informations DNS de votre système StorageGRID pour pouvoir accéder aux serveurs externes en utilisant des noms d'hôte au lieu d'adresses IP.

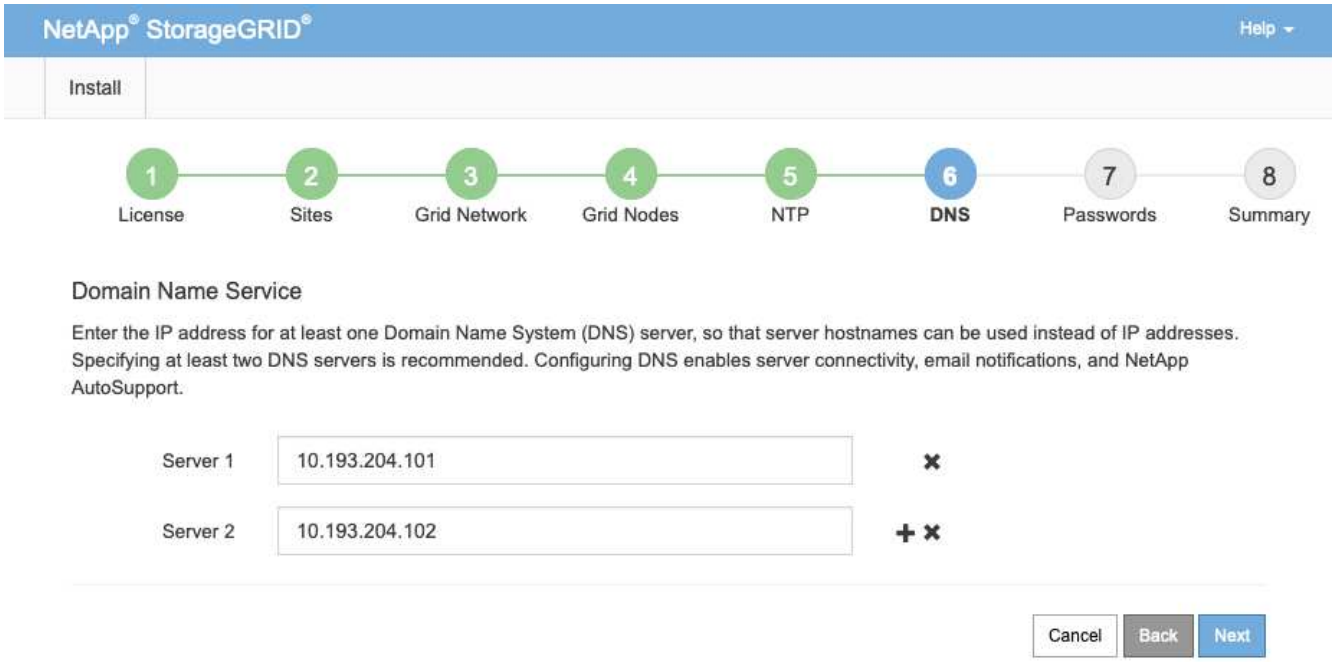
La spécification des informations du serveur DNS vous permet d'utiliser des noms d'hôte de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et les messages NetApp AutoSupport®. NetApp recommande de spécifier au moins deux serveurs DNS.

Vous devez sélectionner des serveurs DNS auxquels chaque site peut accéder localement en cas d'isatterissage du réseau.

Pour spécifier des informations sur le serveur DNS, procédez comme suit :

Étapes

1. Dans la zone de texte serveur 1, spécifiez l'adresse IP d'un serveur DNS.
2. Si nécessaire, cliquez sur le signe plus en regard de la dernière entrée pour ajouter d'autres serveurs.



3. Cliquez sur Suivant.

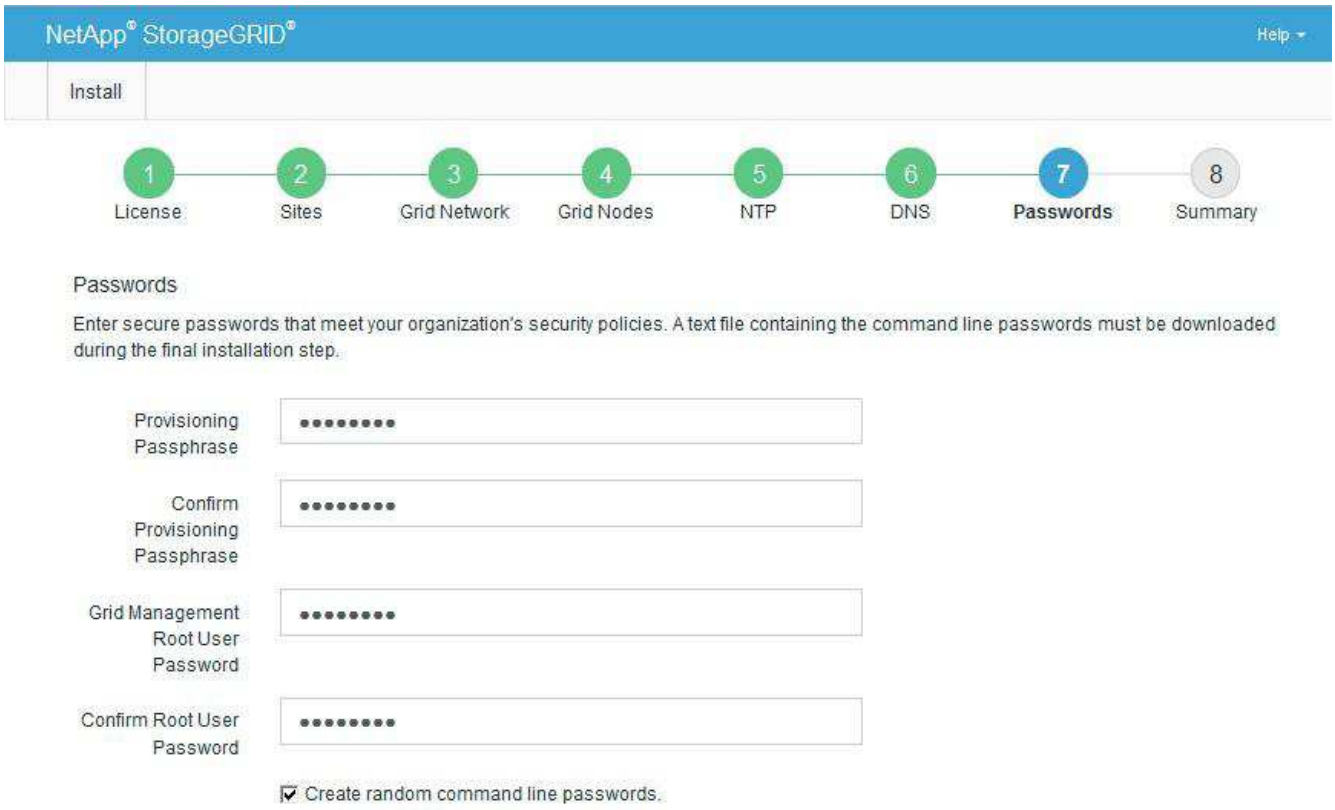
Spécifiez les mots de passe système pour StorageGRID

Découvrez comment sécuriser votre système StorageGRID en définissant la phrase de passe de provisioning et le mot de passe utilisateur root de gestion de grille.

Pour saisir les mots de passe à utiliser pour sécuriser votre système StorageGRID, procédez comme suit :

Étapes

1. Dans Provisioning Passphrase (phrase de passe de provisionnement), saisissez la phrase de passe de provisionnement qui sera requise pour modifier la topologie de la grille de votre système StorageGRID. Vous devez enregistrer ce mot de passe en lieu sûr.
2. Dans confirmer la phrase de passe de provisionnement, saisissez à nouveau la phrase de passe de provisionnement.
3. Dans le champ Grid Management Root User Password, entrez le mot de passe à utiliser pour accéder à Grid Manager en tant qu'utilisateur root.
4. Dans confirmer le mot de passe de l'utilisateur racine, entrez à nouveau le mot de passe du gestionnaire de grille.



5. Si vous installez une grille à des fins de démonstration de faisabilité ou de démonstration, désélectionnez l'option Créer des mots de passe de ligne de commande aléatoires.

   Pour les déploiements en production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Désélectionnez l'option Créer des mots de passe de ligne de commande aléatoires uniquement pour les grilles de démonstration si vous souhaitez utiliser des mots de passe par défaut pour accéder aux nœuds de grille à partir de la ligne de commande à l'aide du compte root ou admin.

   > Lorsque vous cliquez sur installer dans la page Résumé , vous êtes invité à télécharger le fichier du progiciel de récupération (`sgws-recovery-packageid-revision.zip`. Vous devez télécharger ce fichier pour terminer l'installation. Les mots de passe permettant d'accéder au système sont stockés dans le `Passwords.txt` fichier, contenu dans le fichier du progiciel de récupération.

6. Cliquez sur Suivant.

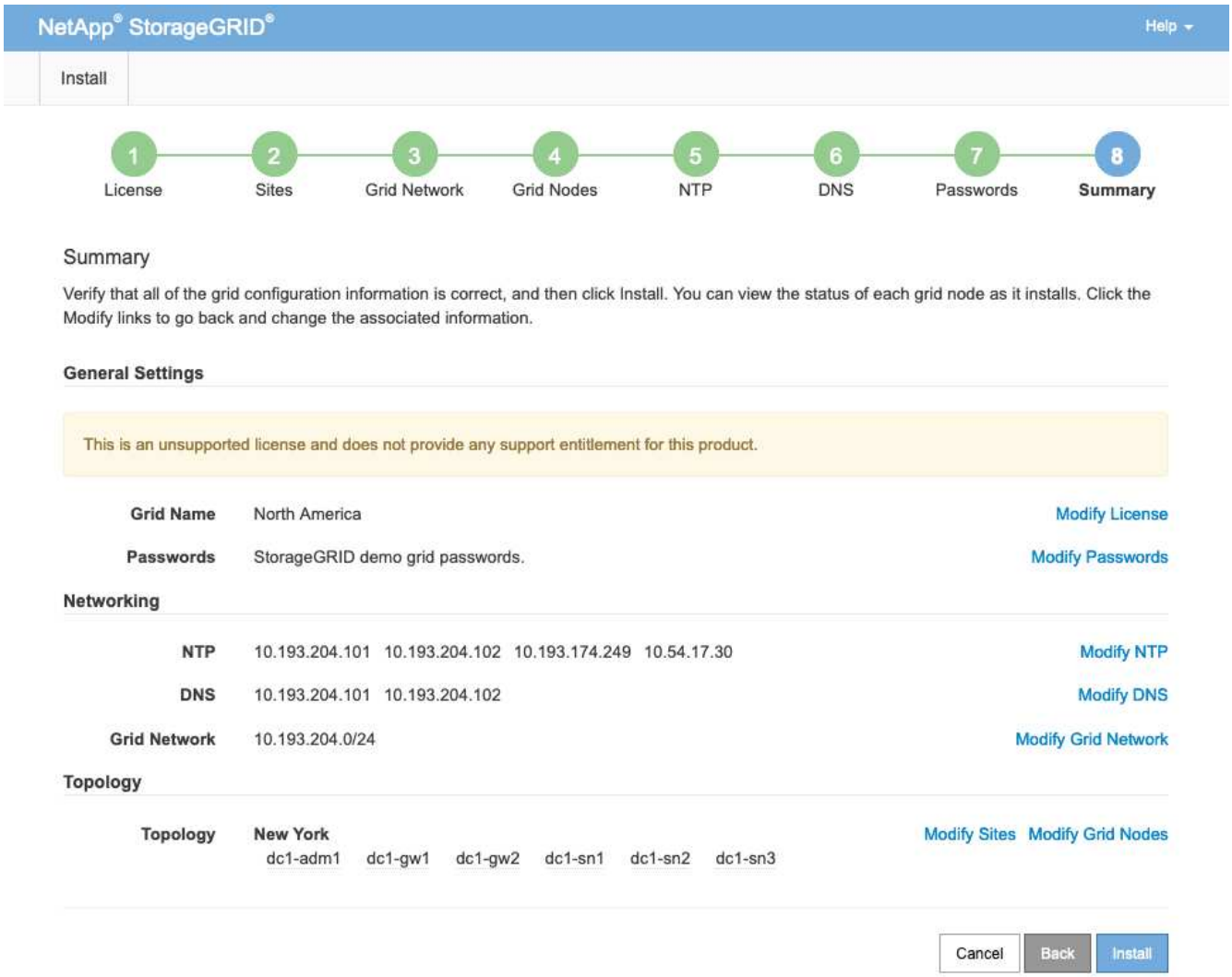
Vérifiez la configuration et terminez l'installation de StorageGRID

Découvrez comment valider les informations de configuration du grid et terminer le processus d'installation de StorageGRID.

Pour vous assurer que l'installation se termine correctement, lisez attentivement les informations de configuration que vous avez saisies. Effectuez la procédure suivante.

Étapes

1. Afficher la page Résumé.



2. Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier de la page Résumé pour revenir en arrière et corriger les erreurs.
3. Cliquez sur installation.

> Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud passe du réseau grid au réseau client lorsque vous cliquez sur installer. En cas de perte de connectivité, assurez-vous que vous accédez au nœud d'administration principal via un sous-réseau accessible. Pour plus d'informations, reportez-vous à la section « installation et provisionnement réseau ».

4. Cliquez sur Télécharger le pack de récupération.

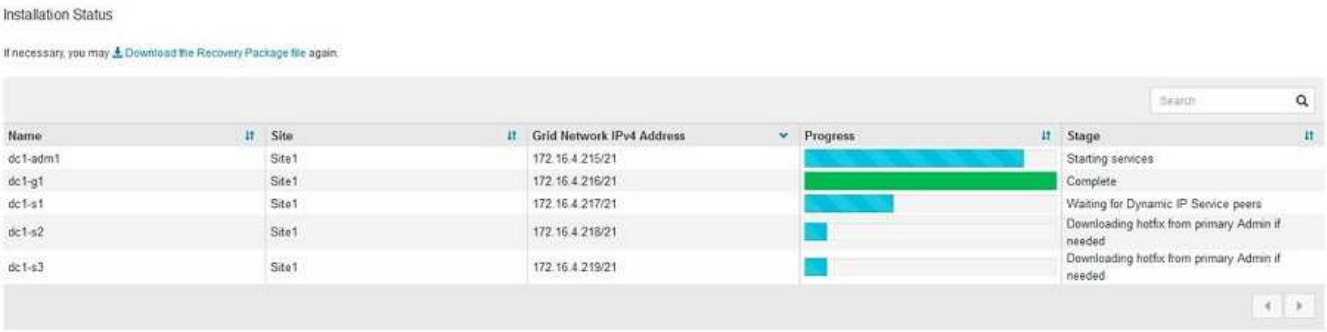
   Lorsque l'installation progresse jusqu'au point où la topologie de la grille est définie, vous êtes invité à télécharger le fichier du progiciel de récupération (`.zip`) et à confirmer que vous pouvez accéder au contenu de ce fichier. Vous devez télécharger le fichier du package de récupération pour pouvoir récupérer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de grille.

   Vérifiez que vous pouvez extraire le contenu du `.zip` fichier, puis l'enregistrer dans deux emplacements sécurisés et séparés.

Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

5. Sélectionnez l'option J'ai téléchargé et vérifié le fichier de package de récupération, puis cliquez sur Suivant.

Si l'installation est toujours en cours, la page État de l'installation s'ouvre. Cette page indique la progression de l'installation pour chaque nœud de la grille.



Lorsque l'étape complète est atteinte pour tous les nœuds de grille, la page de connexion de Grid Manager s'ouvre.

6. Connectez-vous à Grid Manager en tant qu'utilisateur root avec le mot de passe que vous avez spécifié lors de l'installation.

Mettez à niveau les nœuds bare-Metal dans StorageGRID

En savoir plus sur le processus de mise à niveau des nœuds bare-Metal dans StorageGRID.

Le processus de mise à niveau des nœuds bare-Metal est différent de celui des appliances et des nœuds VMware. Avant d'effectuer une mise à niveau d'un nœud bare-Metal, vous devez d'abord mettre à niveau les fichiers RPM sur tous les hôtes avant d'exécuter la mise à niveau via l'interface graphique.

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

Vous pouvez maintenant procéder à la mise à niveau du logiciel via l'interface graphique.

Tr-4907 : configurer StorageGRID avec veritas Enterprise Vault

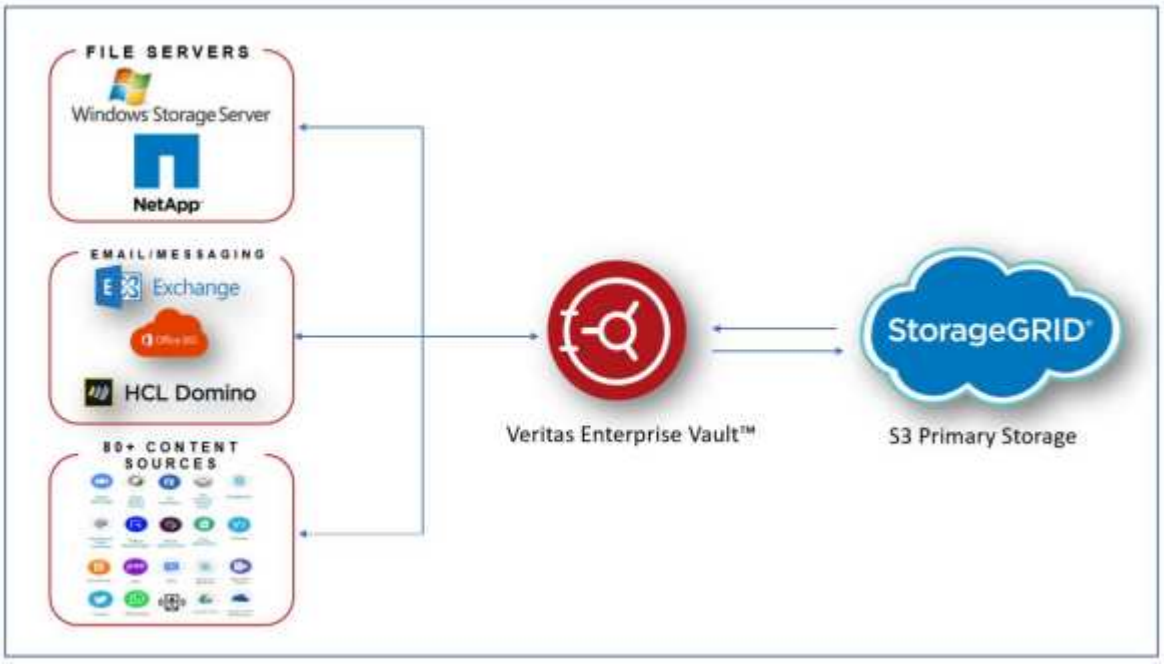
Introduction à la configuration de StorageGRID pour le basculement de site

Découvrez comment veritas Enterprise Vault utilise StorageGRID comme cible de stockage primaire pour la reprise après incident.

Ce guide de configuration fournit les étapes de configuration de NetApp® StorageGRID® en tant que cible de stockage principale avec veritas Enterprise Vault. Elle décrit également comment configurer StorageGRID pour un basculement de site dans un scénario de reprise d'activité.

Architecture de référence

StorageGRID fournit une cible de sauvegarde dans le cloud sur site compatible avec S3 pour veritas Enterprise Vault. La figure suivante illustre l'architecture de veritas Enterprise Vault et StorageGRID.



Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Centre de documentation NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-118/
- Accompagnement NetApp StorageGRID https://docs.netapp.com/us-en/storagegrid-enable/

- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Configurer StorageGRID et veritas Enterprise Vault

Découvrez comment implémenter des configurations de base pour StorageGRID 11.5 ou version ultérieure et veritas Enterprise Vault 14.1 ou version ultérieure.

Ce guide de configuration est basé sur StorageGRID 11.5 et Enterprise Vault 14.1. Pour le stockage en mode WORM (Write Once, Read Many) avec le verrouillage des objets S3, StorageGRID 11.6 et Enterprise Vault 14.2.2 ont été utilisés. Pour plus d'informations sur ces instructions, rendez-vous sur la "Documentation StorageGRID" page ou contactez un expert StorageGRID.

Conditions requises pour configurer StorageGRID et veritas Enterprise Vault

- Avant de configurer StorageGRID avec veritas Enterprise Vault, vérifiez les conditions préalables suivantes :

> Pour le stockage WORM (verrouillage objet), StorageGRID 11.6 ou version supérieure est requis.

- veritas Enterprise Vault 14.1 ou version ultérieure est installé.

> Pour le stockage WORM (Object Lock), Enterprise Vault version 14.2.2 ou supérieure est requis.

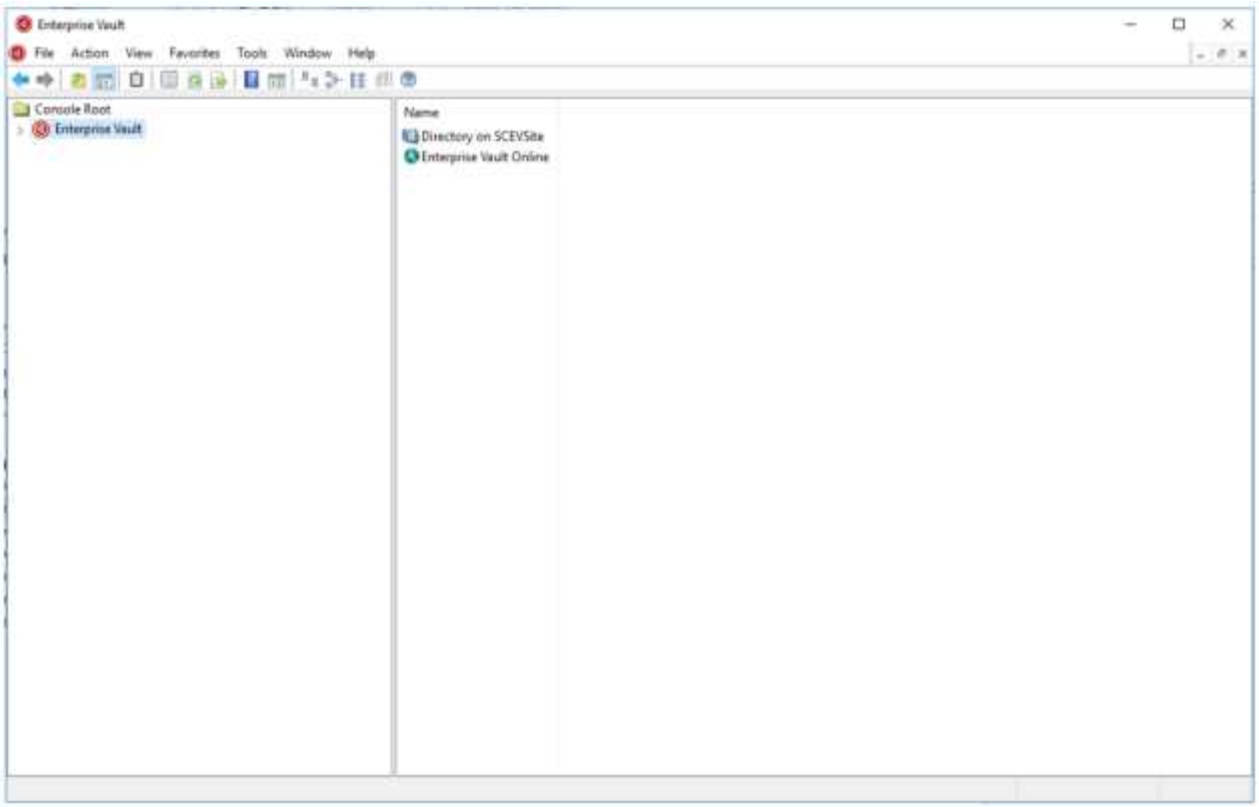
- Des groupes de magasins de coffre-fort et un magasin de coffre-fort ont été créés. Pour plus d'informations, reportez-vous au Guide d'administration de veritas Enterprise Vault.
- Un locataire StorageGRID, une clé d'accès, une clé secrète et un compartiment ont été créés.
- Un noeud final de l'équilibreur de charge StorageGRID a été créé (HTTP ou HTTPS).
- Si vous utilisez un certificat auto-signé, ajoutez le certificat CA auto-signé StorageGRID aux serveurs de coffre-fort d'entreprise. Pour plus d'informations, voir "Article de la base de connaissances veritas".
- Mettez à jour et appliquez le dernier fichier de configuration du coffre-fort d'entreprise pour activer les solutions de stockage prises en charge telles que NetApp StorageGRID. Pour plus d'informations, voir "Article de la base de connaissances veritas".

Configurez StorageGRID avec veritas Enterprise Vault

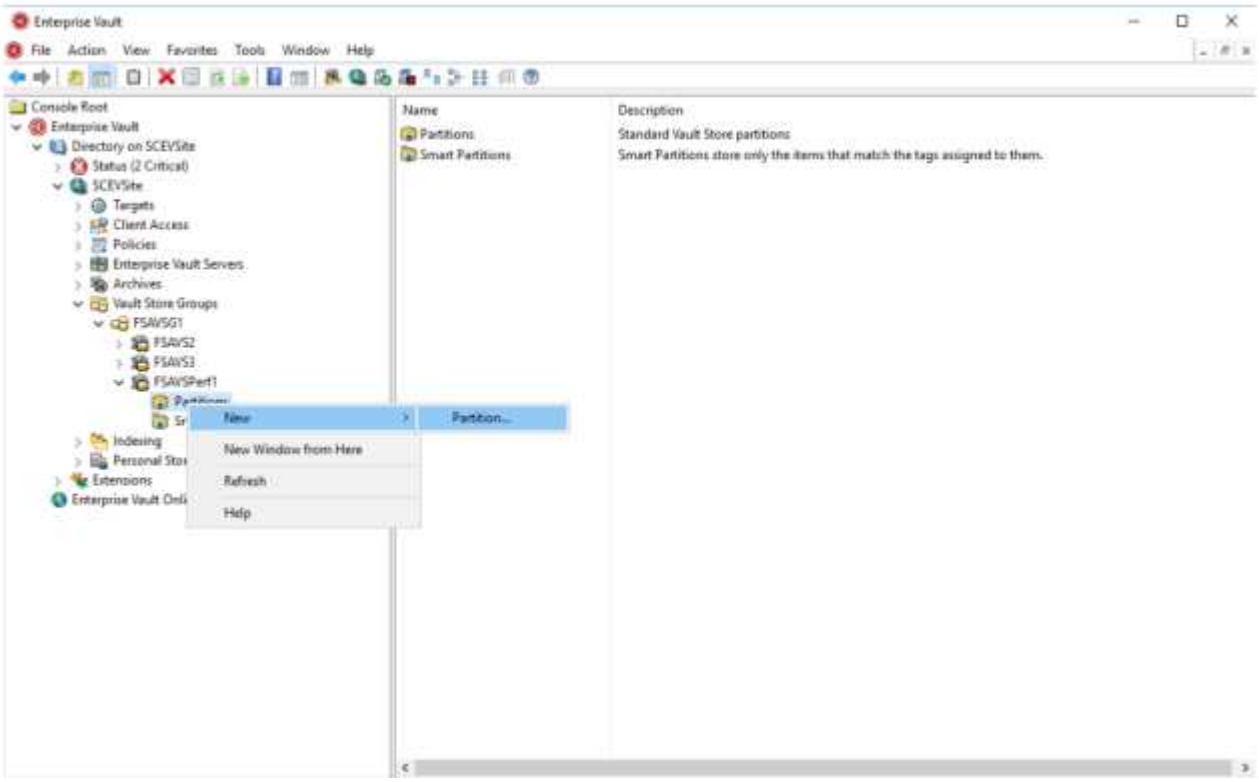
Pour configurer StorageGRID avec veritas Enterprise Vault, procédez comme suit :

Étapes

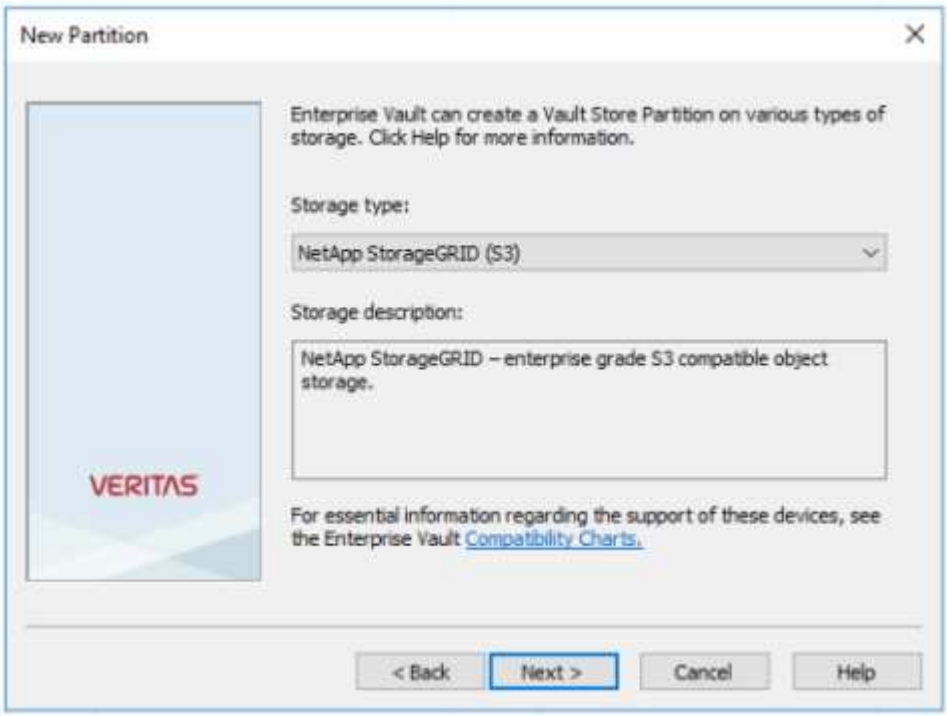
1. Lancez la console Enterprise Vault Administration.



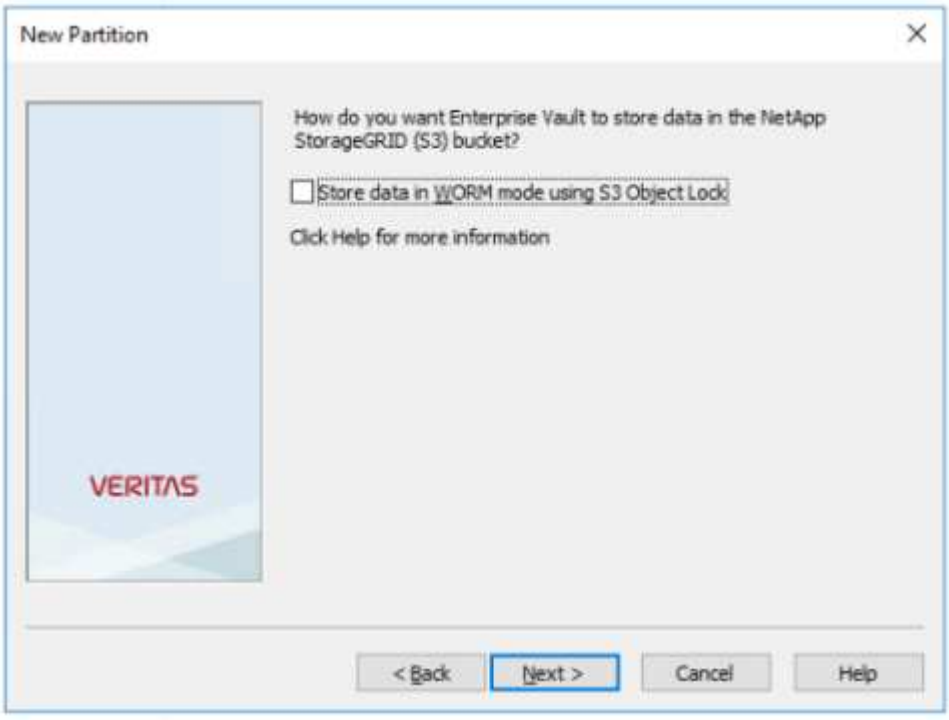
2. Créez une nouvelle partition de magasin de coffre-fort dans le magasin de coffre-fort approprié. Développez le dossier groupes du magasin Vault, puis le magasin de coffre-fort approprié. Cliquez avec le bouton droit de la souris sur partition et sélectionnez **New › partition**.



3. Suivez l’assistant de création de nouvelle partition. Dans le menu déroulant Type de stockage, sélectionnez NetApp StorageGRID (S3). Cliquez sur Suivant.

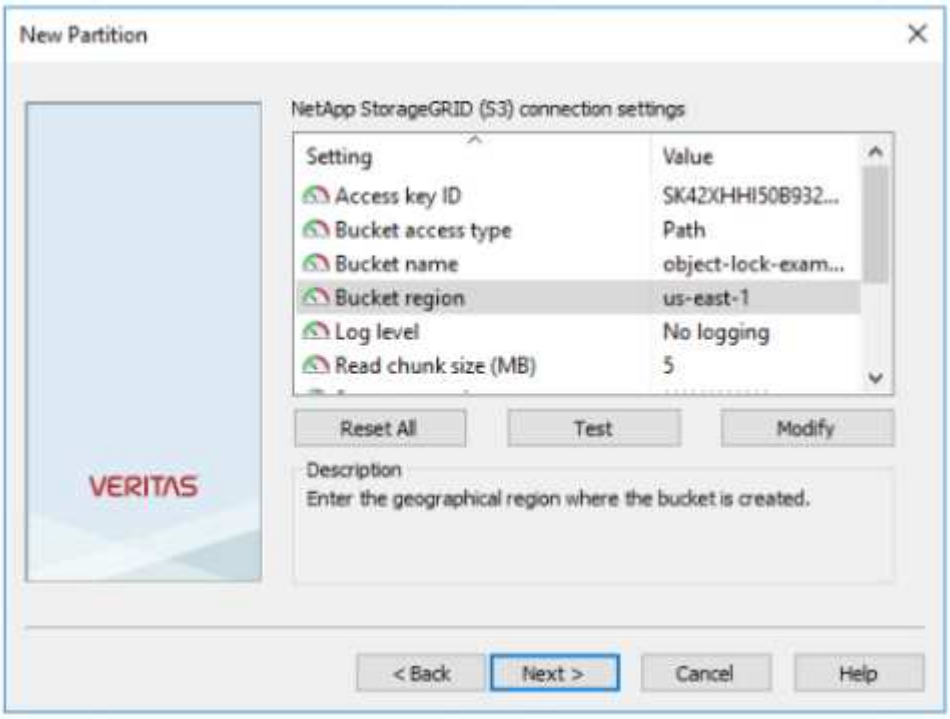


4. Ne cochez pas l'option stocker les données en mode WORM à l'aide du verrouillage d'objet S3. Cliquez sur Suivant.

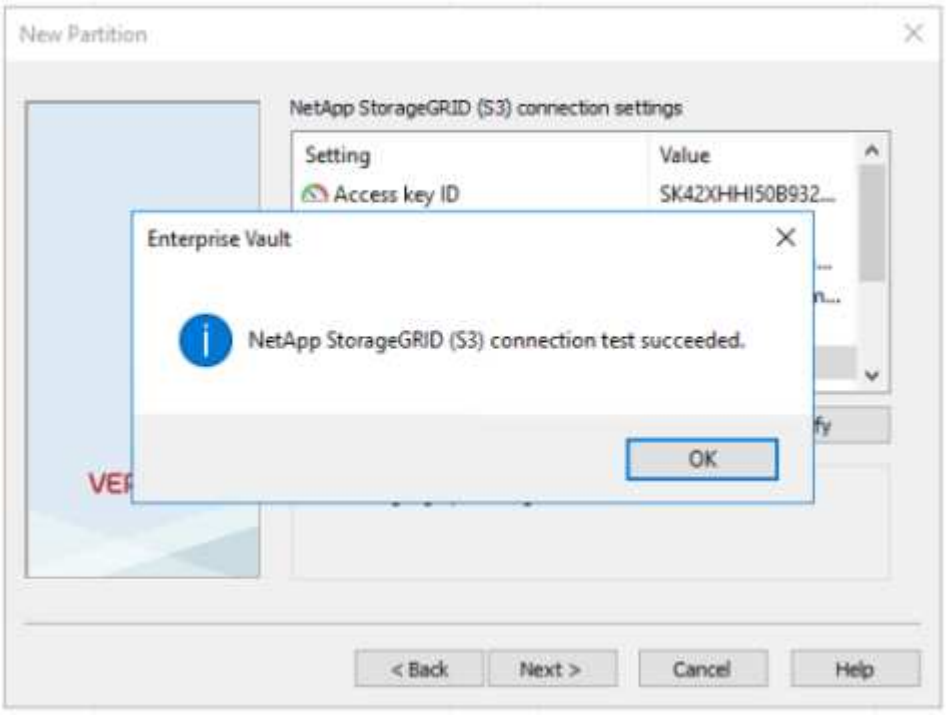


5. Sur la page des paramètres de connexion, fournissez les informations suivantes :
   - ID de clé d'accès
   - Clé d'accès secrète
   - Nom d'hôte du service : assurez-vous d'inclure le port LBE (load balancer Endpoint) configuré dans StorageGRID (tel que https://<hostname>:<LBE_port>)

- Nom du compartiment : nom du compartiment cible précréé. veritas Enterprise Vault ne crée pas le compartiment.
- Région du compartiment : `us-east-1` est la valeur par défaut.

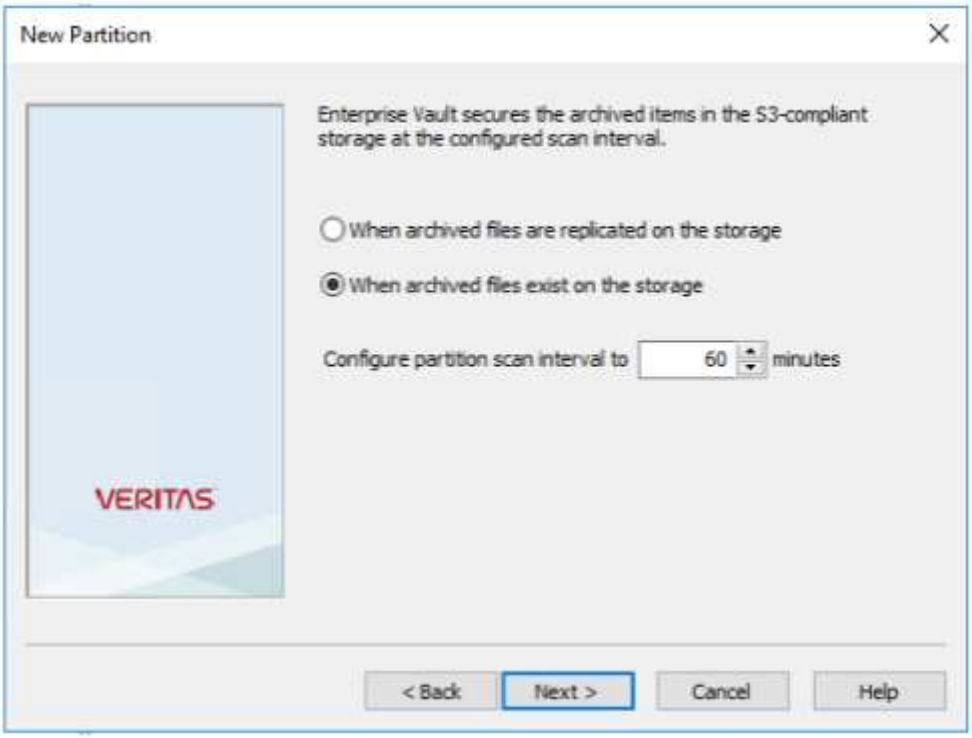


6. Pour vérifier la connexion au compartiment StorageGRID, cliquez sur Test. Vérifiez que le test de connexion a réussi. Cliquez sur OK, puis sur Suivant.

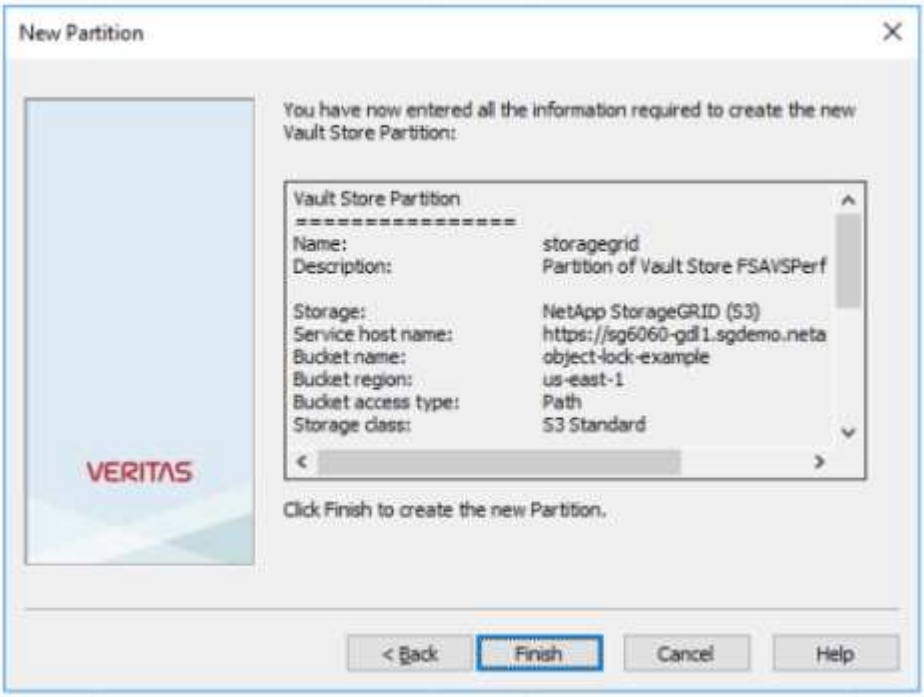


7. StorageGRID ne prend pas en charge le paramètre de réplication S3. Pour protéger vos objets, StorageGRID utilise des règles de gestion du cycle de vie des informations (ILM) afin de spécifier des schémas de protection des données : copies multiples ou code d'effacement. Sélectionnez l'option lorsque

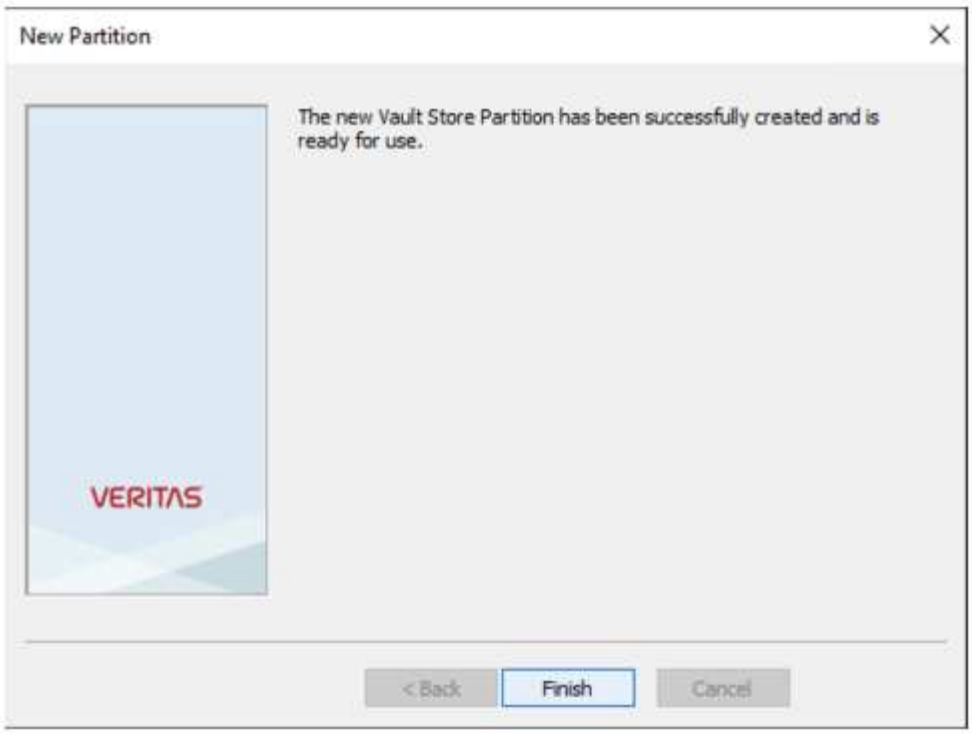
des fichiers archivés existent dans le stockage et cliquez sur Suivant.



8. Vérifiez les informations sur la page de résumé et cliquez sur Terminer.



9. Une fois la nouvelle partition de magasin de coffre-fort créée, vous pouvez archiver, restaurer et rechercher des données dans le coffre-fort d'entreprise avec StorageGRID comme stockage principal.



Configuration du verrouillage objet StorageGRID S3 pour le stockage WORM

Découvrez comment configurer StorageGRID pour le stockage WORM à l'aide du verrouillage objet S3.

Conditions préalables à la configuration de StorageGRID pour le stockage WORM

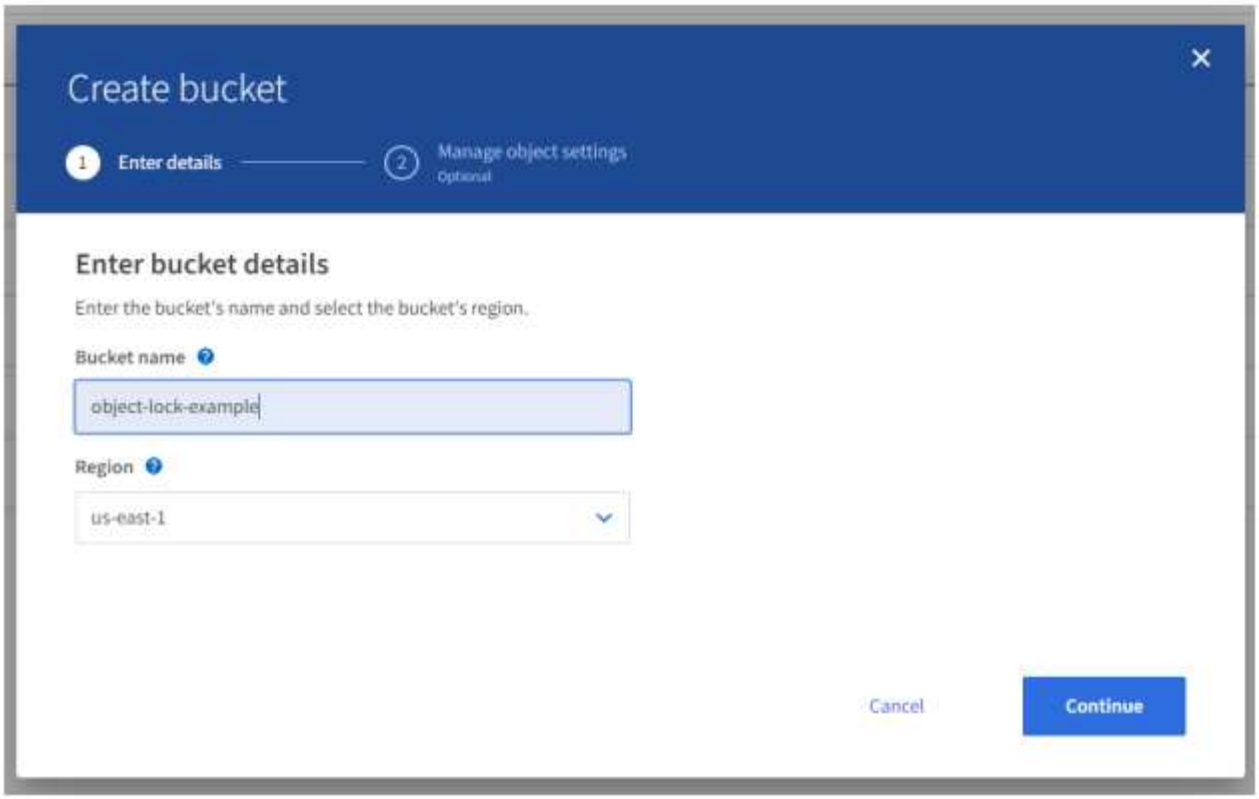
Pour le stockage WORM, StorageGRID utilise le verrouillage objet S3 pour conserver les objets à des fins de conformité. Ceci requiert StorageGRID 11.6 ou version supérieure, où une fonctionnalité de conservation par défaut des compartiments du verrouillage objet S3 a été ajoutée. Enterprise Vault requiert également la version 14.2.2 ou supérieure.

Configuration de la rétention des compartiments par défaut du verrouillage objet StorageGRID S3

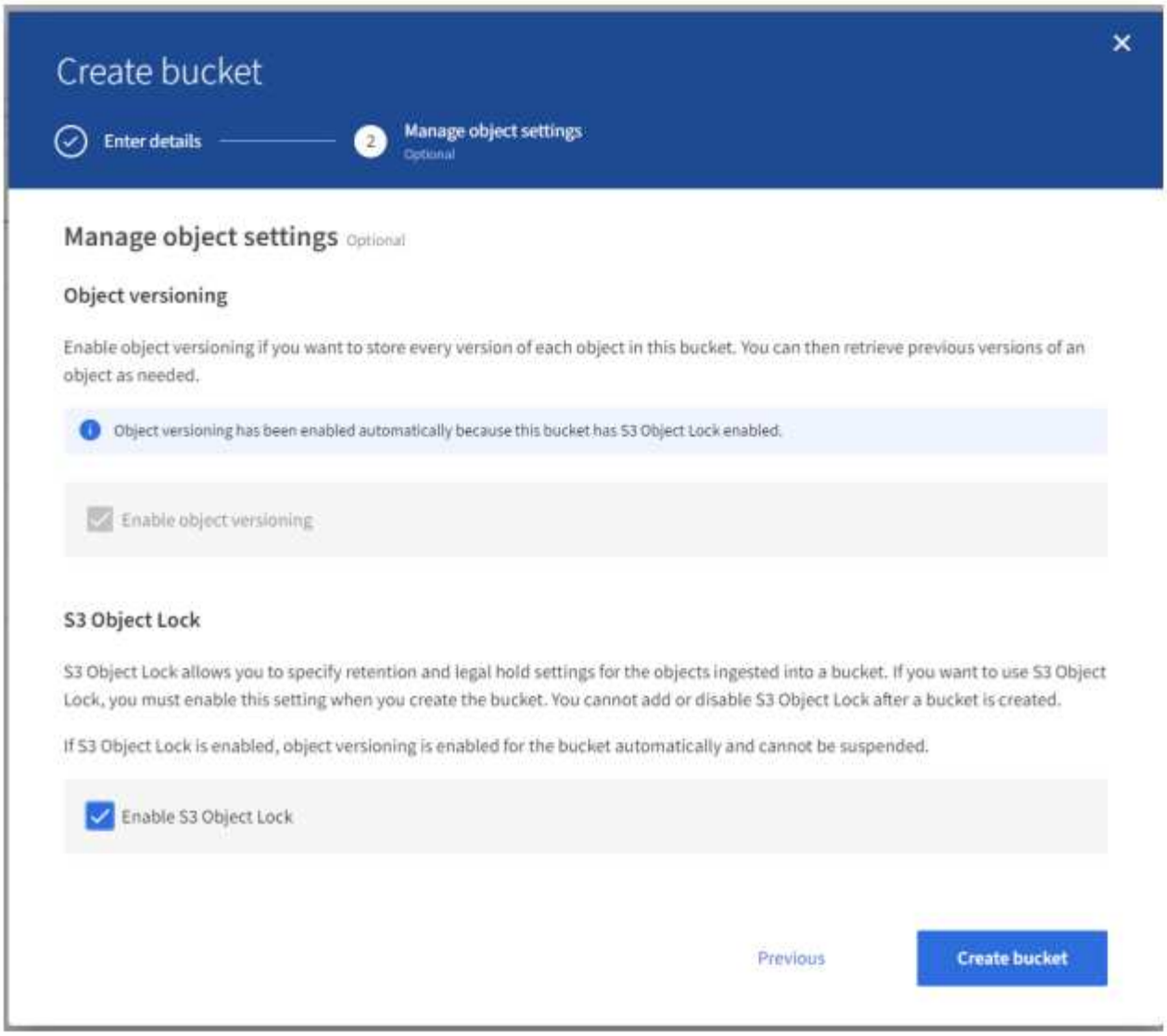
Pour configurer la rétention des compartiments par défaut du verrouillage objet StorageGRID S3, effectuez les opérations suivantes :

Étapes

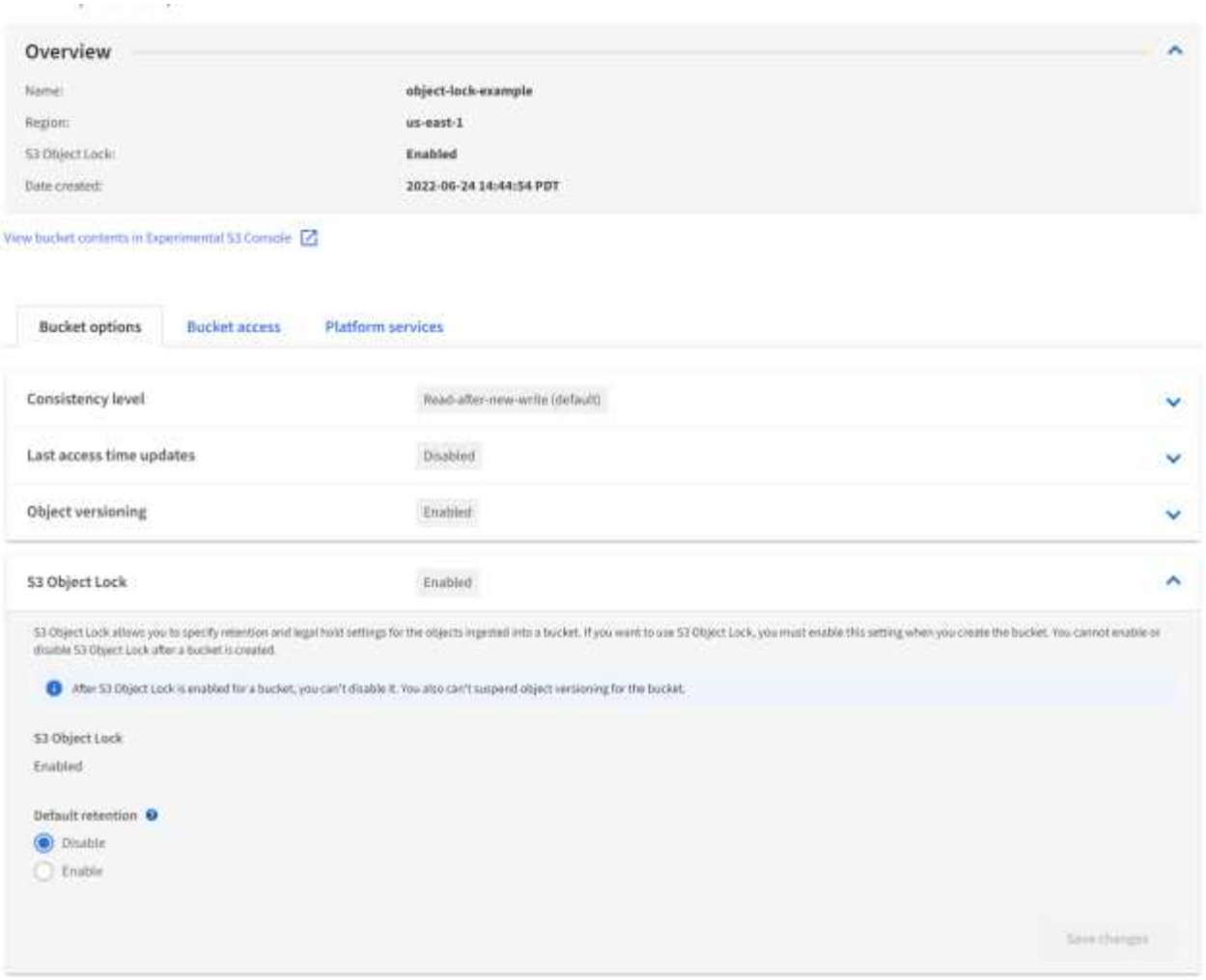
1. Dans le gestionnaire de locataires StorageGRID, créez un compartiment et cliquez sur Continuer



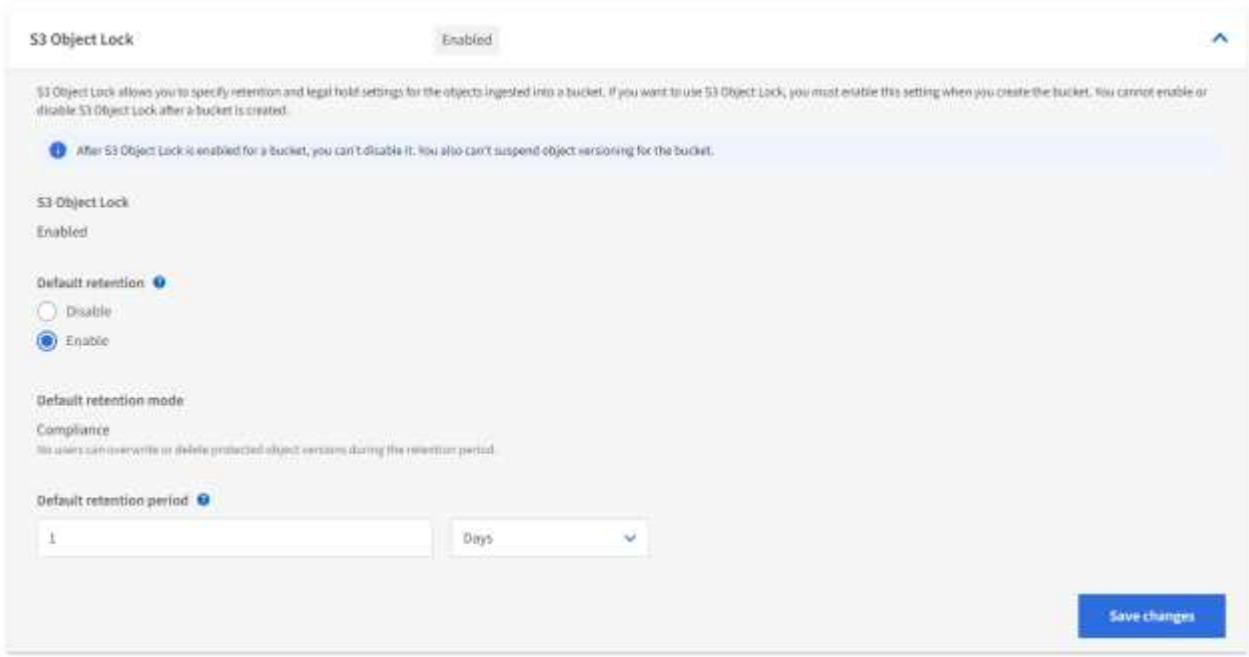
2. Sélectionnez l’option Activer le verrouillage d’objet S3 et cliquez sur Créer un compartiment.



3. Une fois le godet créé, sélectionner le godet pour afficher les options de compartiment. Développez l'option de liste déroulante verrouillage objet S3.



4. Sous conservation par défaut, sélectionnez Activer et définissez une période de conservation par défaut de 1 jour. Cliquez sur Save Changes.



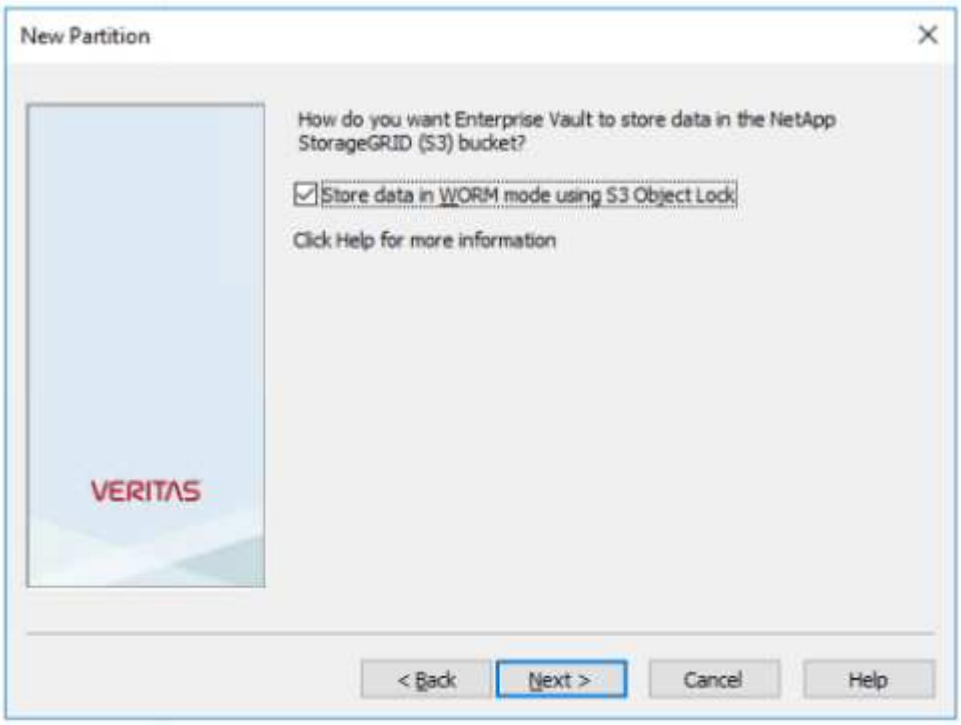
Le compartiment est désormais prêt à être utilisé par Enterprise Vault pour stocker les données WORM.

Configurer Enterprise Vault

Pour configurer Enterprise Vault, procédez comme suit :

Étapes

1. Répétez les étapes 1 à 1-3 de la "Configuration de base" section, mais cette fois, sélectionnez l'option stocker les données en mode WORM à l'aide du verrouillage objet S3. Cliquez sur Suivant.



2. Lorsque vous entrez vos paramètres de connexion du compartiment S3, assurez-vous d'entrer le nom d'un compartiment S3 pour lequel la conservation par défaut du verrouillage objet S3 est activée.
3. Testez la connexion pour vérifier les paramètres.

Configurez le basculement de site StorageGRID pour la reprise après incident

Découvrez comment configurer le basculement de site StorageGRID dans un scénario de reprise d'activité.

Il est courant que le déploiement d'une architecture StorageGRID soit multisite. Les sites peuvent être de type actif-actif ou actif-passif pour la reprise après incident. En cas de reprise après incident, assurez-vous que veritas Enterprise Vault peut maintenir la connexion à son stockage primaire (StorageGRID) et continuer à ingérer et à récupérer les données en cas de panne sur un site. Cette section fournit des conseils de configuration de haut niveau pour un déploiement actif-passif sur deux sites. Pour plus d'informations sur ces instructions, rendez-vous "Documentation StorageGRID" sur la page ou contactez un expert StorageGRID.

Conditions préalables à la configuration de StorageGRID avec veritas Enterprise Vault

Avant de configurer le basculement de site StorageGRID, vérifiez les conditions préalables suivantes :

- Il existe un déploiement StorageGRID sur deux sites, par exemple, le SITE 1 et le SITE 2.
- Un nœud d'administration exécutant le service d'équilibrage de la charge ou un nœud de passerelle sur chaque site pour l'équilibrage de la charge a été créé.
- Un terminal de l'équilibreur de charge StorageGRID a été créé.

Configurer le basculement de site StorageGRID

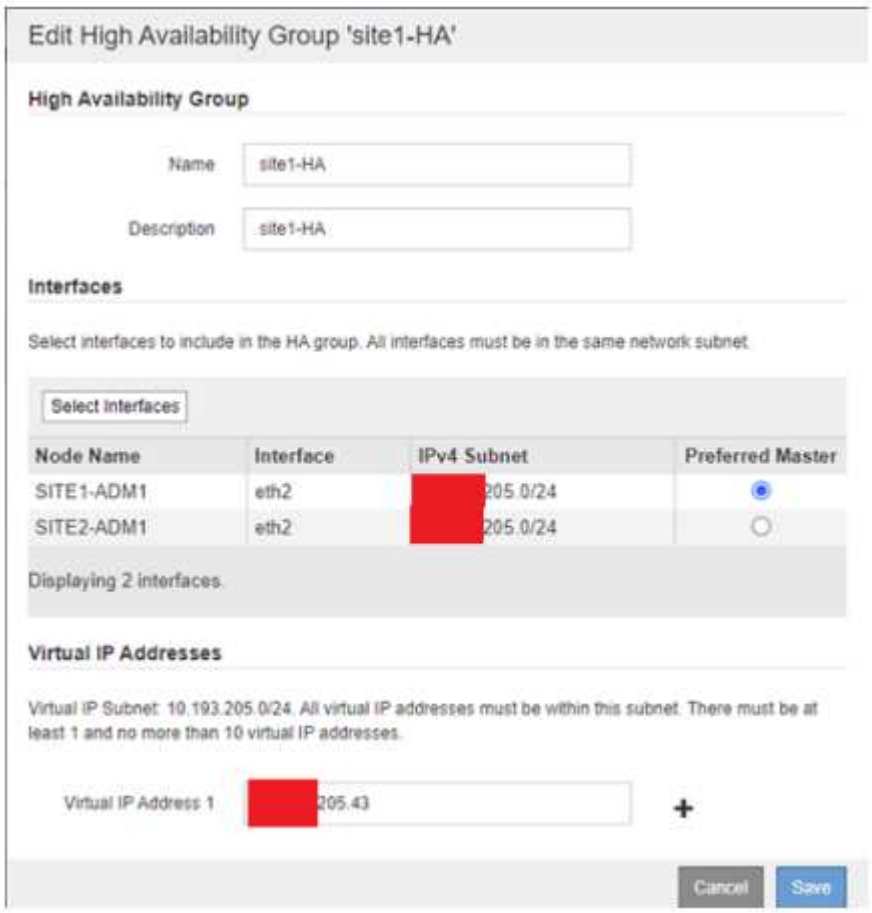
Pour configurer le basculement de site StorageGRID, procédez comme suit :

Étapes

1. Pour assurer la connectivité à StorageGRID en cas de défaillance d'un site, configurez un groupe haute disponibilité (HA). Dans l'interface GMI (StorageGRID Grid Manager interface), cliquez sur Configuration, groupes haute disponibilité, puis sur + Créer.

   [vertias/veritas-create-high-availability-group]

2. Entrez les informations requises. Cliquez sur Sélectionner les interfaces et incluez les interfaces réseau du SITE 1 et du SITE 2 où le site 1 (site principal) est le maître préféré. Attribuez une adresse IP virtuelle au sein du même sous-réseau. Cliquez sur Enregistrer.

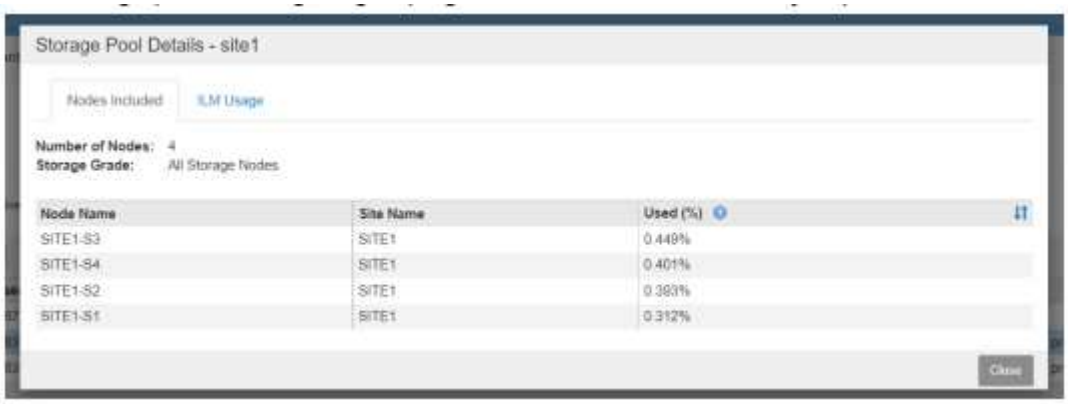


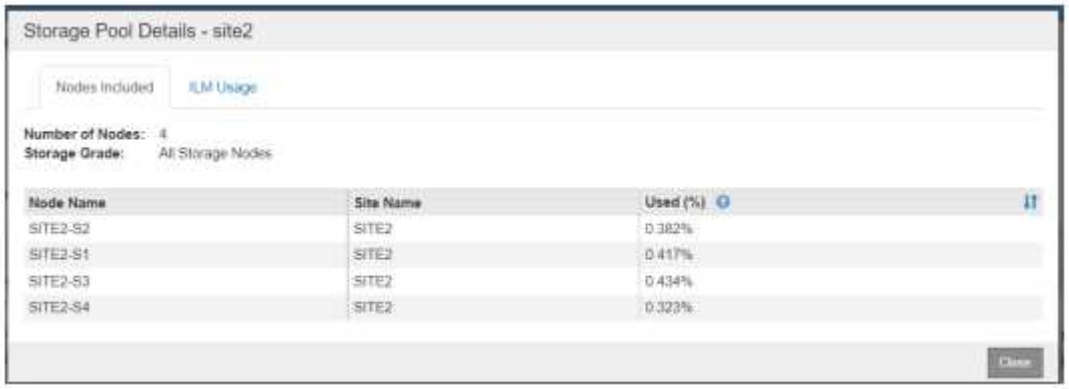
3. Cette adresse IP virtuelle (VIP) doit être associée au nom d'hôte S3 utilisé lors de la configuration de la partition de veritas Enterprise Vault. L'adresse VIP résout le trafic vers le SITE 1 et, en cas de défaillance du SITE 1, l'adresse VIP réachemine le trafic vers le SITE 2 de manière transparente.
4. Assurez-vous que les données sont répliquées sur le SITE 1 et le SITE 2. Ainsi, si SITE1 échoue, les

données de l'objet sont toujours disponibles à partir du SITE2. Pour ce faire, vous devez d'abord configurer les pools de stockage.

Dans l'interface GMI de StorageGRID, cliquez sur ILM, pools de stockage, puis sur + Create. Suivez l'assistant pour créer deux pools de stockage : un pour le SITE 1 et un autre pour le SITE 2.

Les pools de stockage sont des regroupements logiques de nœuds utilisés pour définir le placement des objets





5. Dans l'interface GMI de StorageGRID, cliquez sur ILM, Rules, puis sur + Create. Suivez les instructions de l'assistant pour créer une règle ILM spécifiant une copie à stocker par site avec un comportement d'ingestion équilibré.

6. Ajoutez la règle ILM à une règle ILM et activez cette règle.

Cette configuration entraîne les résultats suivants :

- IP de point de terminaison S3 virtuel où SITE1 est le point de terminaison principal et SITE2 le point de terminaison secondaire. Si LE SITE 1 échoue, le VIP bascule sur le SITE 2.
- Lorsque des données archivées sont envoyées depuis veritas Enterprise Vault, StorageGRID s'assure qu'une copie est stockée dans LE SITE 1 et qu'une autre copie de reprise après incident est stockée dans le SITE 2. Si SITE1 échoue, Enterprise Vault continue à ingérer et à récupérer depuis le SITE2.

Ces deux configurations sont transparentes pour veritas Enterprise Vault. Le terminal S3, le nom de compartiment, les clés d'accès, etc. Sont identiques. Il n'est pas nécessaire de reconfigurer les paramètres de connexion S3 sur la partition veritas Enterprise Vault.

Procédure d’accès au logiciel d’évaluation StorageGRID

Cette instruction s’adresse aux commerciaux, aux partenaires et aux prospects NetApp qui travaillent avec NetApp.

Créez un compte

1. Créez un compte sur le "Site de support NetApp" à l’aide de votre adresse e-mail professionnelle.
   a. Assurez-vous que vous n’êtes pas connecté avec le nouveau compte créé.
   b. Si vous possédez déjà un compte, assurez-vous que vous n’êtes pas connecté et passez à l’étape suivante.
2. Créez un dossier de support non technique afin d’élever les niveaux d’accès au « prospect ». Pour ce faire, cliquez sur le ""Signalez les problèmes"lien " dans le pied de page du site Web.
3. Sélectionnez « problème d’enregistrement » comme catégorie de commentaires.
4. Dans la section des commentaires, écrivez : « mon adresse e-mail de compte est *votre-adresse e-mail*. J’aimerais obtenir un accès prospect pour télécharger le logiciel d’évaluation StorageGRID. »
   a. Mentionnez le nom de la personne interne de NetApp qui a suggéré l’accès du prospect.

Télécharger StorageGRID

1. Une fois que votre dossier de demande de support a été examiné et approuvé, le support NetApp vous informe par e-mail que votre compte a été autorisé à accéder à vos prospects.
2. Téléchargez le "Logiciel d’évaluation StorageGRID".

Le fichier de licence Eval se trouve dans le fichier zip. Il s’agit de StorageGRID-Webscale-<version>\vsphere\NLF000000.txt une fois décompressé.

Le téléchargement du logiciel est un processus qui implique des mesures de conformité commerciale pour se conformer aux exigences légales. Pour garantir la conformité, les utilisateurs doivent créer un compte et ouvrir un dossier de demande de support avant d’accéder à ce service. Ce processus nous aide à maintenir un contrôle et une documentation appropriés tout en fournissant aux prospects le logiciel prêt à la production dont ils ont besoin.

Nous fournissons la version « prête pour la production » de StorageGRID, qui n’est pas une version open source ou alternative. Il est important de noter que **le support n’est pas fourni** à moins que le prospect ne passe à une licence de production.

Veuillez contacter StorageGRID.Feedback@netapp.com pour tout problème avec les étapes ci-dessus.

Blogs NetApp StorageGRID

Vous trouverez d'excellents blogs NetApp StorageGRID ici :

- 16 2024 février : "Présentation de StorageGRID 11.8 : sécurité améliorée, simplicité et expérience utilisateur"
- 16 2024 février : "Présentation de StorageGRID 11.8"
- 2 février 2024 : "Annonce de la description de la solution StorageGRID + lakeFS"
- Décembre 12 2023 : "Analytique Big Data sur StorageGRID : Dremio est 23 fois plus rapide qu'Apache Hive"
- Novembre 7 2023 : "Spectra Logic On-sur-site Glacier avec StorageGRID"
- 17 2023 octobre : "Hadoop, modernisation de l'analytique avec Dremio et StorageGRID"
- 1er septembre 2023 : "Utilisation de Cloud Insights pour surveiller et collecter les journaux à l'aide du bit Fluent"
- 30 2023 août : "Le point de montage pour Amazon S3 File System est désormais GA"
- Mai 16 2023 : "Présentation d'StorageGRID 11.7 et du nouveau système SGF6112 de stockage objet 100 % Flash"
- Mai 16 2023 : "Nouveautés de la gamme de stockage objet StorageGRID"
- 30 2023 mars : "Point de montage pour Amazon S3 version alpha avec StorageGRID"
- 30 2023 mars : "Utilisez BlueXP pour protéger les dossiers médicaux électroniques Epic avec une règle de sauvegarde conforme à 3:2:1"
- 14 2023 mars : "Comment sauvegarder des bases de données DME des systèmes Epic à l'aide d'une seule commande dans une architecture 3:2:1"
- 14 2023 février : "Qu'ont en commun le chocolat, le ski, les montres et les gros systèmes ?"
- Janvier 18 2023 : "Verrouillage objet StorageGRID S3 validé pour veritas NetBackup"
- Janvier 16 2023 : "StorageGRID renouvelle la certification de conformité NF203 et ISO/IEC 25051"
- Décembre 6 2022 : "StorageGRID obtient la certification de conformité KPMG"
- Novembre 23 2022 : "Découvrez l'IA explicable avec MLOps optimisée par NetApp et Modzy"
- Novembre 7 2022 : "Prise en charge d'StorageGRID et d'ONTAP S3 : différences, similarités et intégration"
- 5 2022 octobre : "NetApp Cloud Insights ajoute les tableaux de bord de la galerie StorageGRID"
- 5 2022 octobre : "Décongelez vos données sur StorageGRID pour Snowflake"
- 26 2022 septembre : "NetApp StorageGRID pour les fournisseurs de services"
- 19 2022 septembre : "Prise en charge de DataLock et de la protection contre les ransomware pour StorageGRID"
- 1er septembre 2022 : "Prenez ces mesures et Graph IT"
- 23 2022 août : "Bâtissez votre data Lake sur StorageGRID"
- 17 2022 août : "Tout commence par le verrouillage d'objet… Création d'un écosystème de stockage S3 pour les applications de sauvegarde stratégiques"
- 16 2022 août : "Intégration de StorageGRID à la pile ELK open source pour améliorer l'expérience client"
- 5 2022 août : "NetApp StorageGRID obtient la certification de sécurité Common Criteria"

- 26 2022 juillet : "Consultez la liste croissante des solutions partenaires validées pour StorageGRID"
- 9 2022 juin : "Utilisez le connecteur Cloudera Hadoop S3A avec StorageGRID"
- Mai 26 2022 : "StorageGRID : stockage et gestion des données de réplication et de sauvegarde sur site"
- Mai 24 2022 : "Modernisez vos workloads d'analytique avec NetApp et Alluxio"
- Mai 10 2022 : "Lab on Demand est votre meilleur outil de vente pour StorageGRID"

Documentation NetApp StorageGRID

Tous les documents relatifs à chaque version de NetApp StorageGRID sont disponibles ici :

- "Appliances StorageGRID"
- "Logiciel StorageGRID 11.5 - 12.0"

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d’auteur

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

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

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

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

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

Politique de confidentialité

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

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d’auteur et les licences de tiers utilisés dans le logiciel NetApp.

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

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