Tr-4907 : configurer StorageGRID avec veritas Enterprise Vault

How to enable StorageGRID in your environment

NetApp
October 09, 2024

Sommaire

Tr-4907 : configurer StorageGRID avec veritas Enterprise Vault

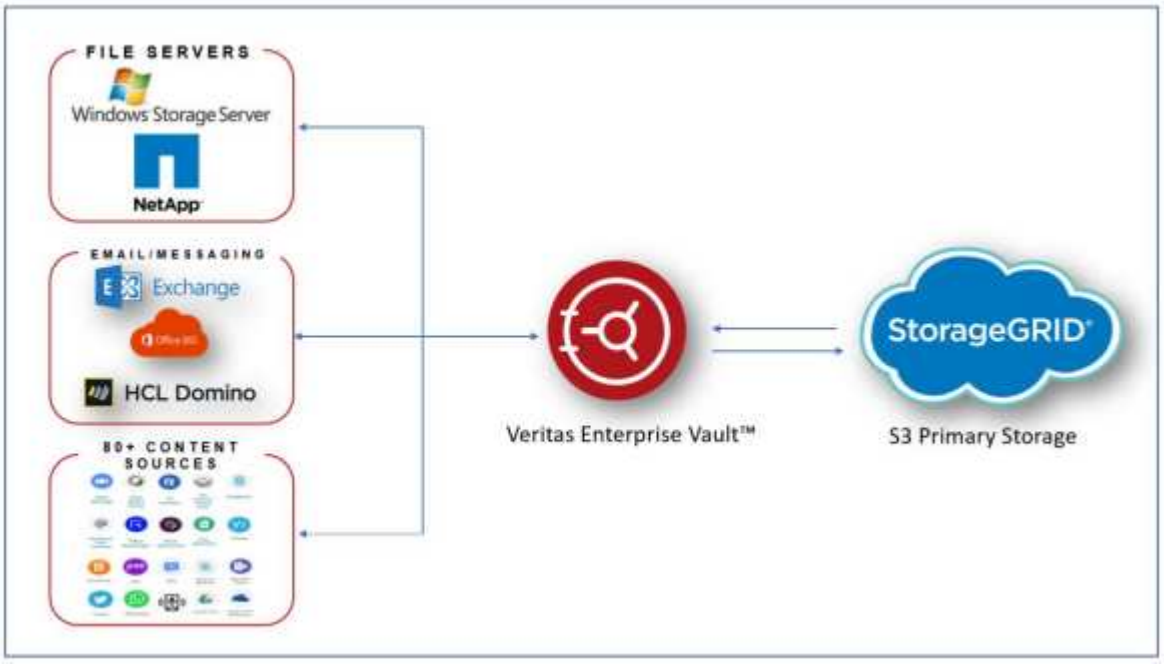
Introduction à la configuration de StorageGRID pour le basculement de site

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/
- Ressources de documentation StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/
- 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.

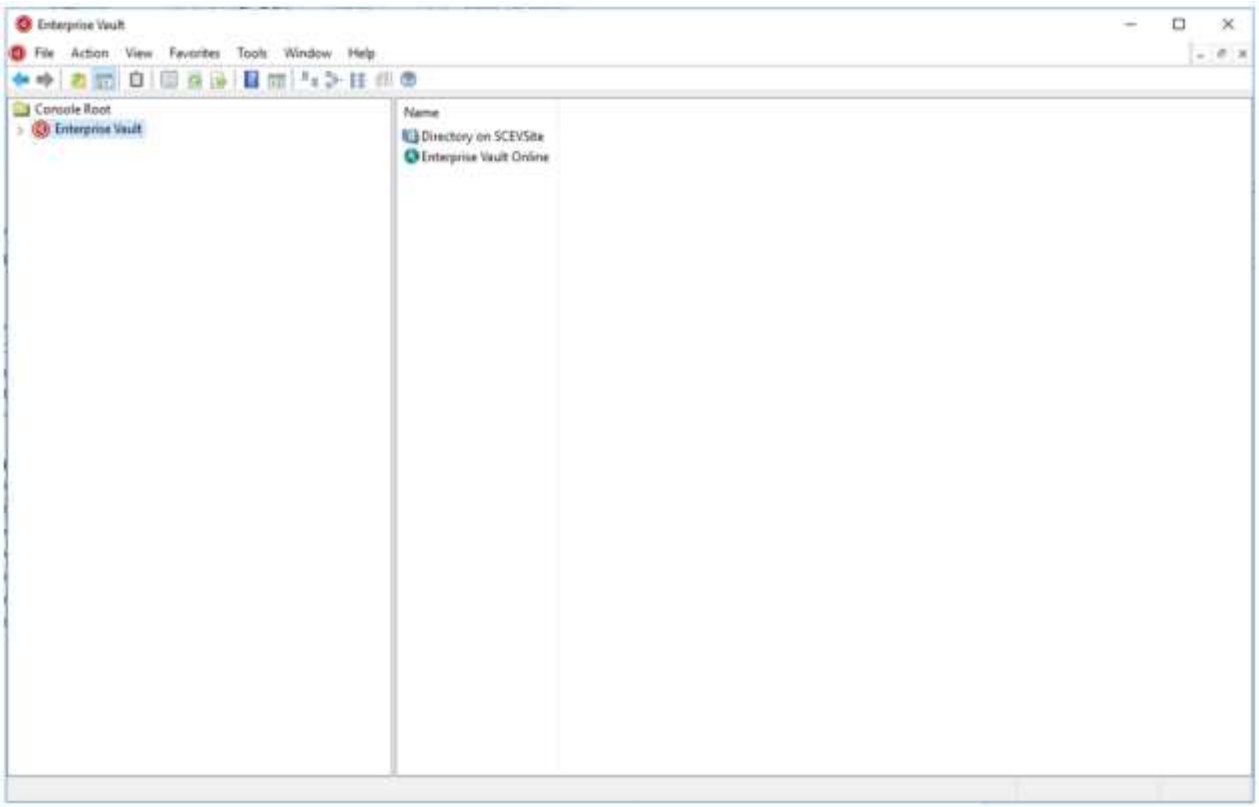
- Des groupes de magasins de coffre-fort et un magasin de coffre-fort ont été créés. Pour plus d'informations, reportez-vous au Guide d'administration de veritas Enterprise Vault.
- Un locataire StorageGRID, une clé d'accès, une clé secrète et un compartiment ont été créés.
- Un noeud final de l'équilibreur 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

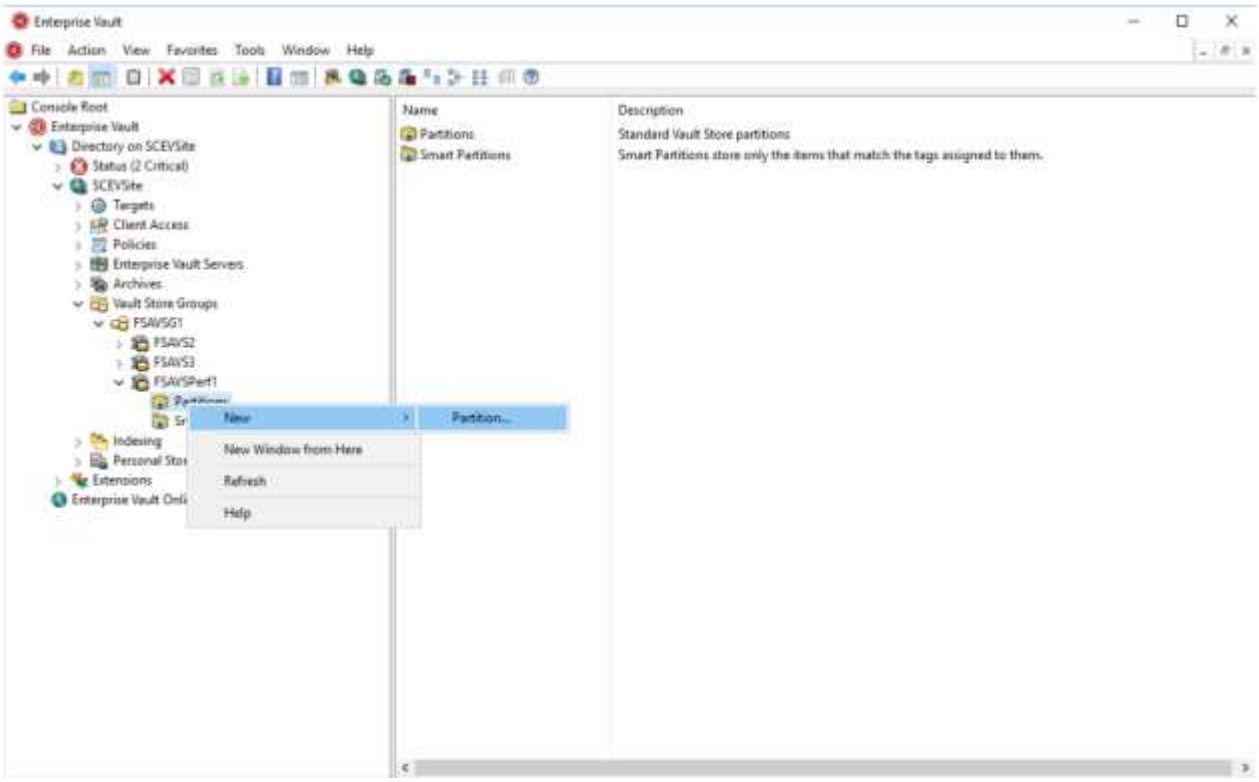
Pour configurer StorageGRID avec veritas Enterprise Vault, procédez comme suit :

Étapes

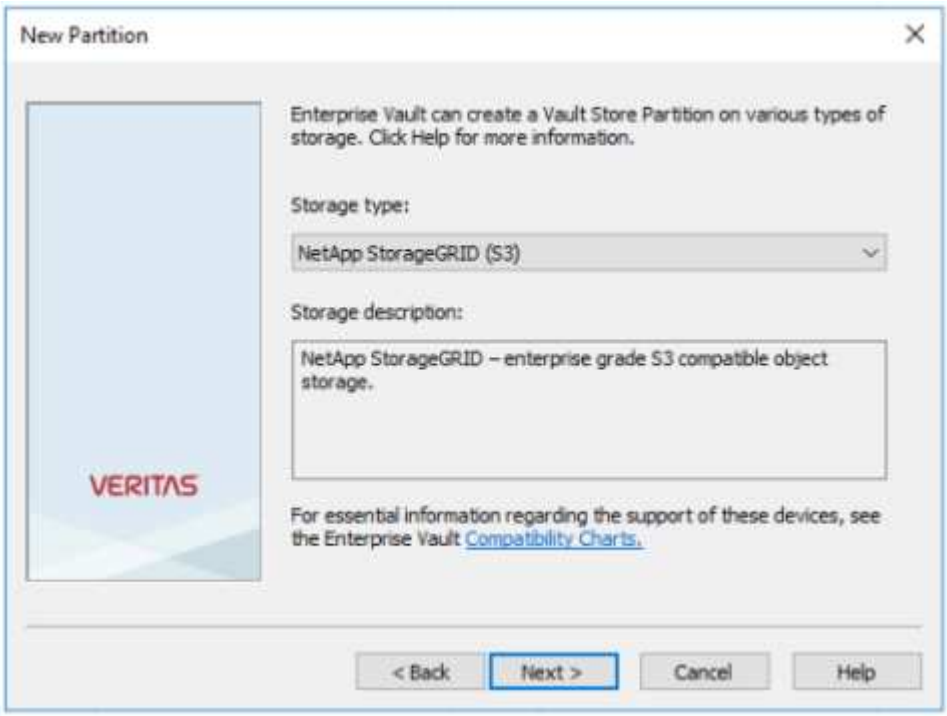
1. Lancez la console Enterprise Vault Administration.



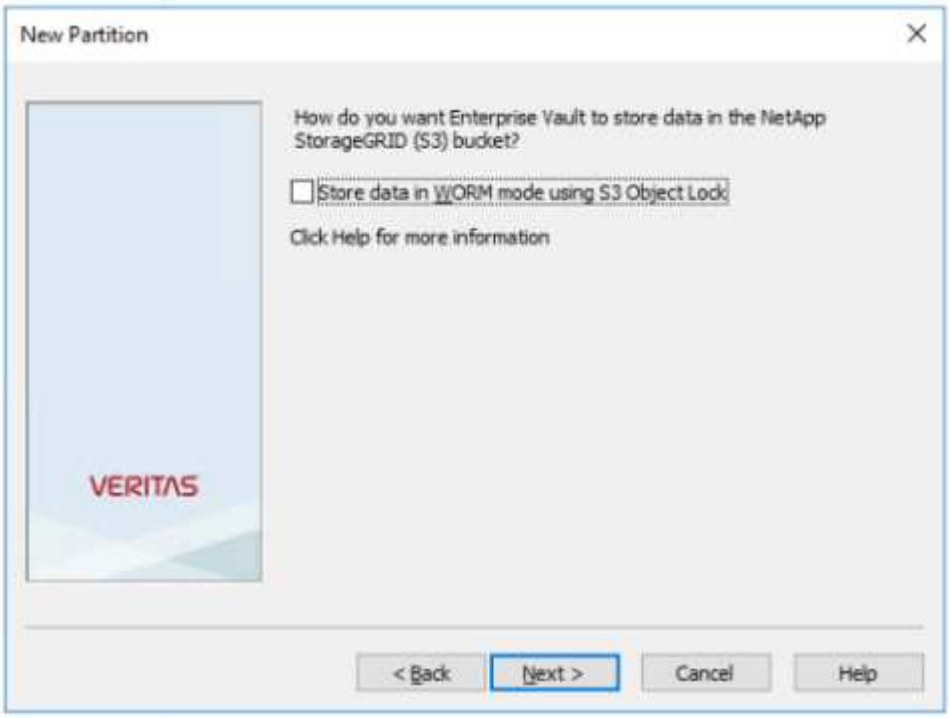
2. Créez une nouvelle partition de magasin de coffre-fort dans le magasin de coffre-fort approprié. Développez le dossier groupes du magasin Vault, puis le magasin de coffre-fort approprié. Cliquez avec le bouton droit de la souris sur partition et sélectionnez **New › partition**.



3. Suivez l’assistant de création de nouvelle partition. Dans le menu déroulant Type de stockage, sélectionnez NetApp StorageGRID (S3). Cliquez sur Suivant.

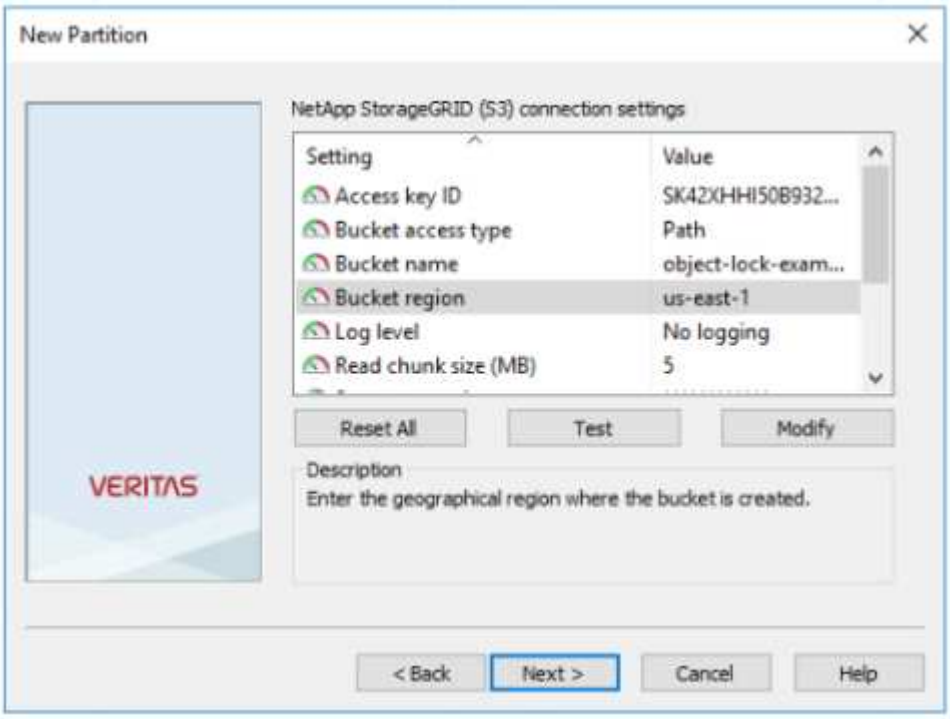


4. Ne cochez pas l'option stocker les données en mode WORM à l'aide du verrouillage d'objet S3. Cliquez sur Suivant.

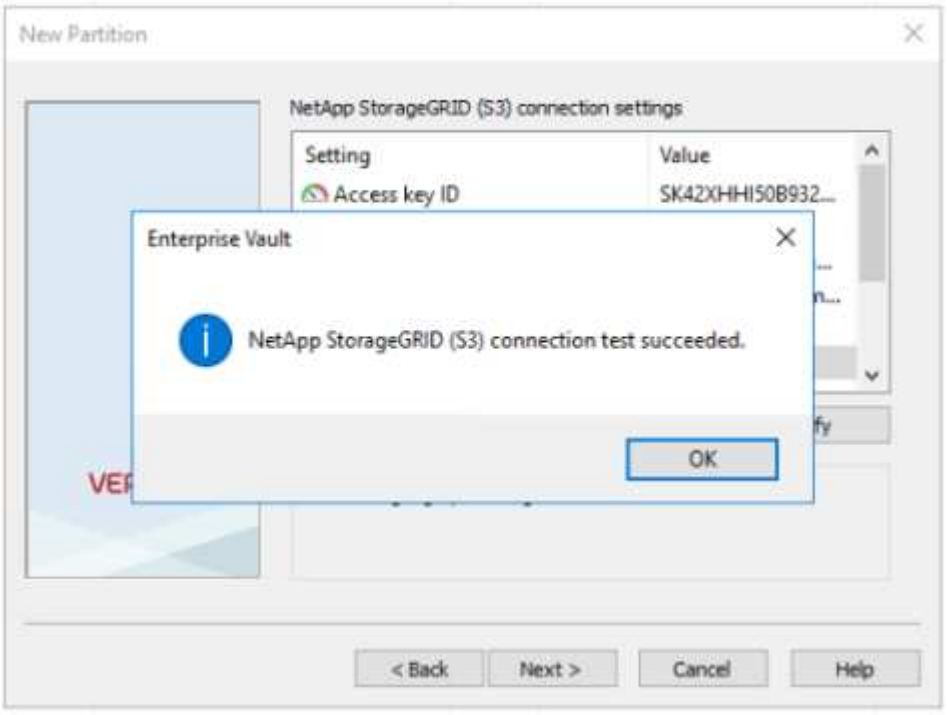


5. Sur la page des paramètres de connexion, fournissez les informations suivantes :
   - ID de clé d'accès
   - Clé d'accès secrète
   - Nom d'hôte du service : assurez-vous d'inclure le port LBE (load balancer Endpoint) configuré dans StorageGRID (tel que https://<hostname>:<LBE_port>)

- 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.

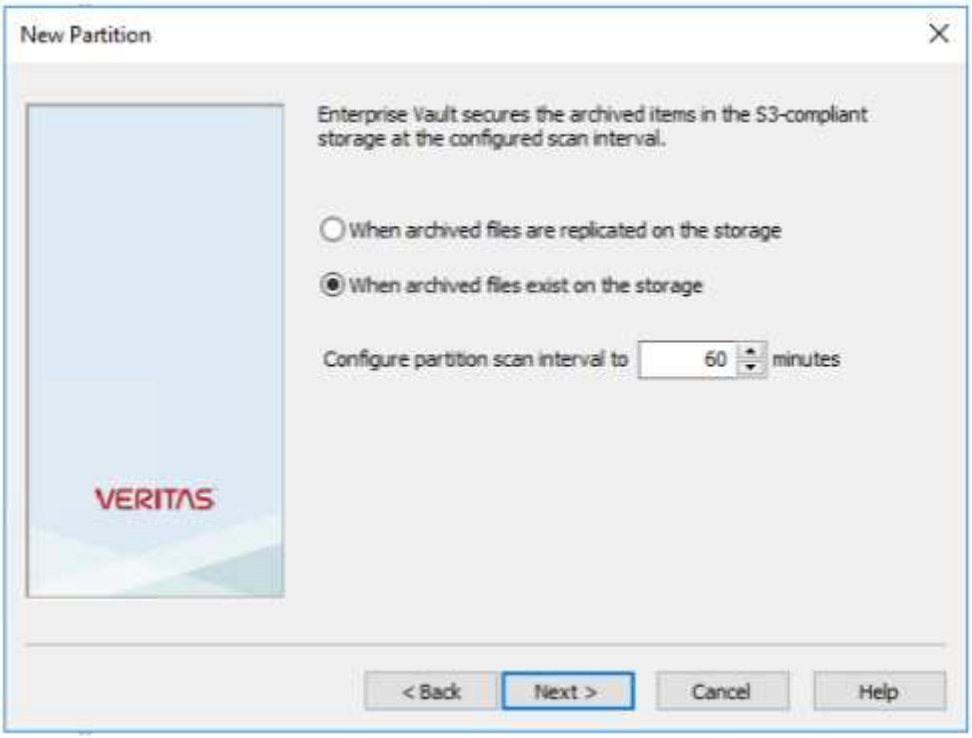


6. Pour vérifier la connexion au compartiment StorageGRID, cliquez sur Test. Vérifiez que le test de connexion a réussi. Cliquez sur OK, puis sur Suivant.

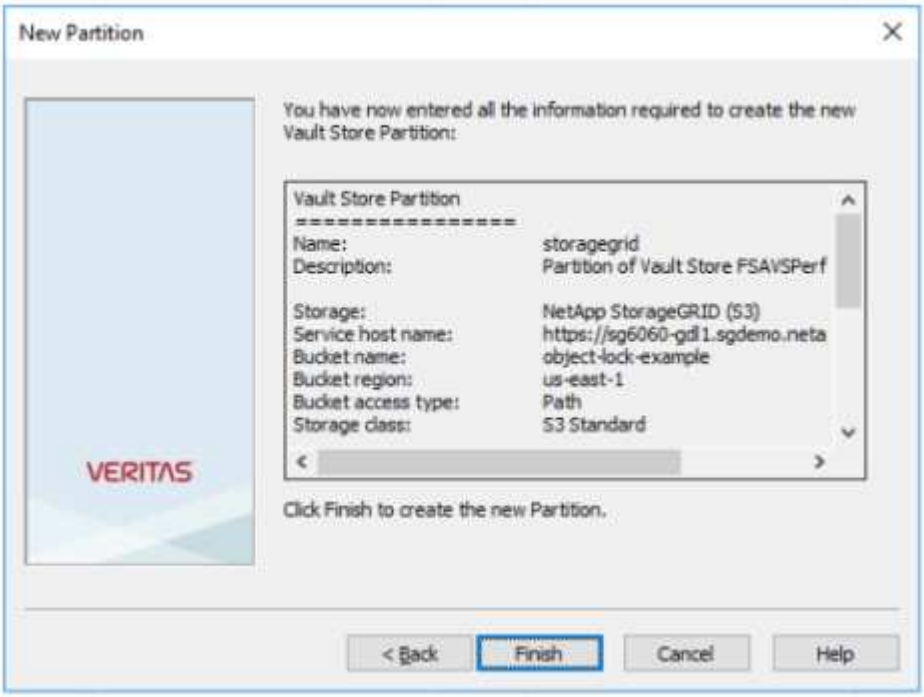


7. StorageGRID ne prend pas en charge le paramètre de réplication S3. Pour protéger vos objets, StorageGRID utilise des règles de gestion du cycle de vie des informations (ILM) afin de spécifier des schémas de protection des données : copies multiples ou code d'effacement. Sélectionnez l'option lorsque

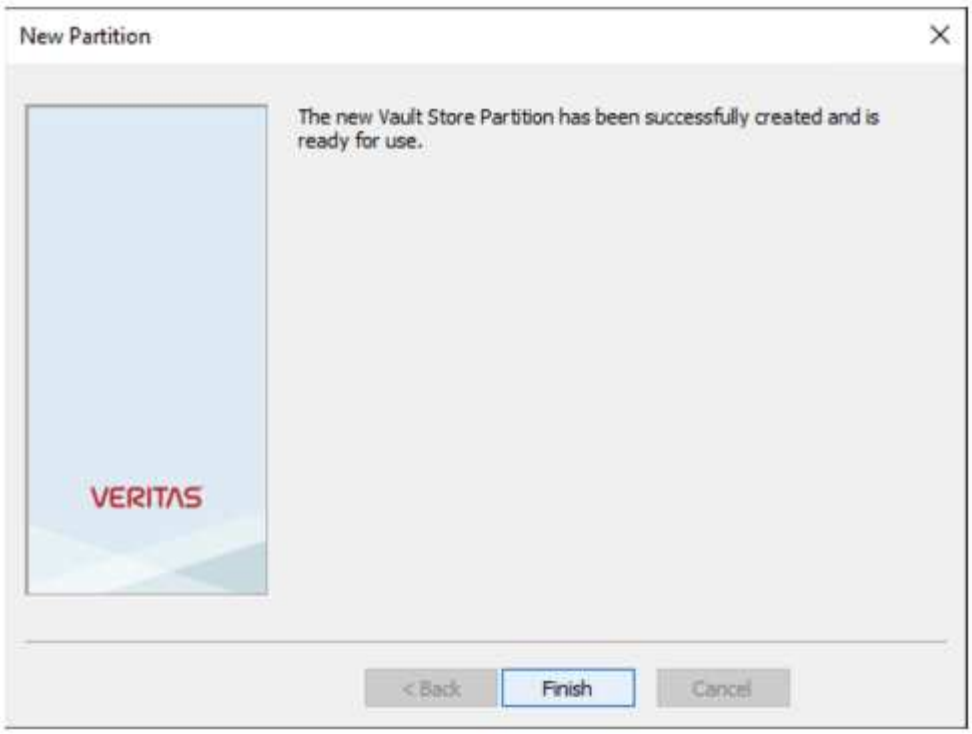
des fichiers archivés existent dans le stockage et cliquez sur Suivant.



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

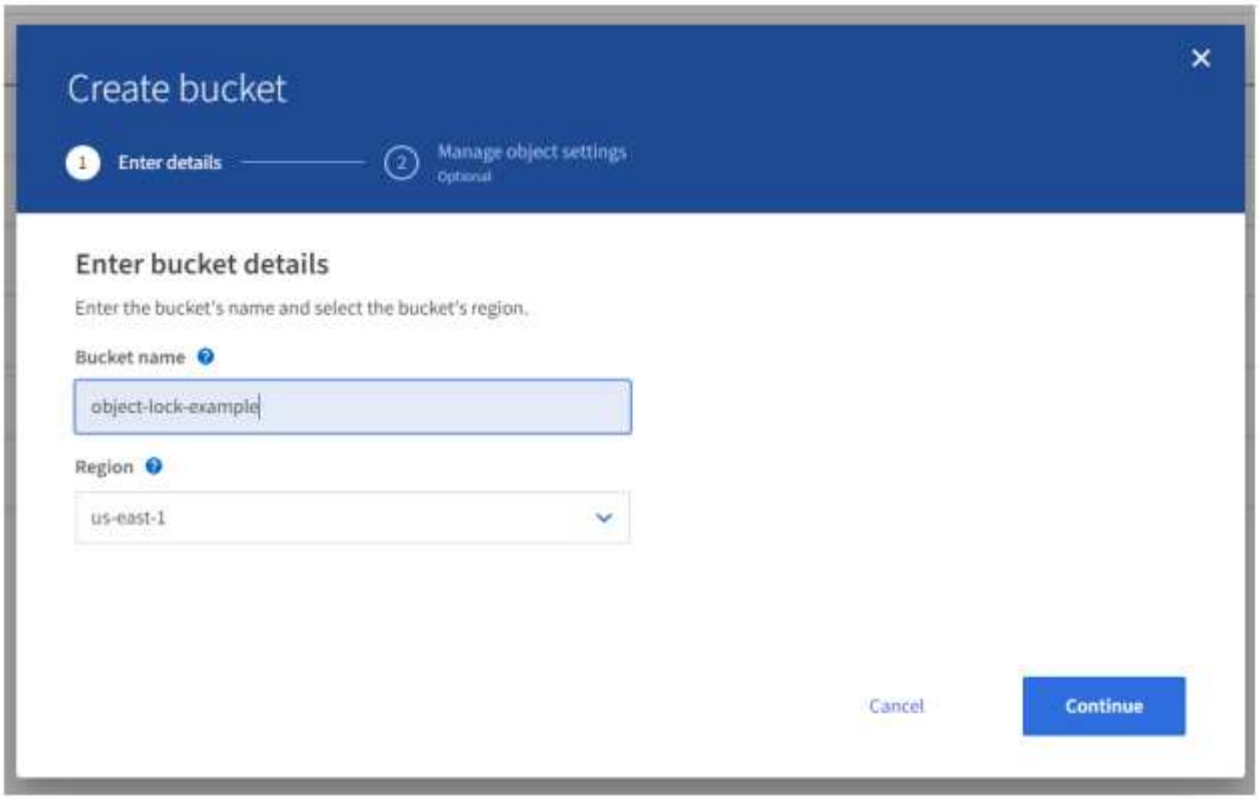
Pour le stockage WORM, StorageGRID utilise le verrouillage objet S3 pour conserver les objets à des fins de conformité. Ceci requiert StorageGRID 11.6 ou version supérieure, où une fonctionnalité de conservation par défaut des compartiments du verrouillage objet S3 a été ajoutée. Enterprise Vault requiert également la version 14.2.2 ou supérieure.

Configuration de la rétention des compartiments par défaut du verrouillage objet StorageGRID S3

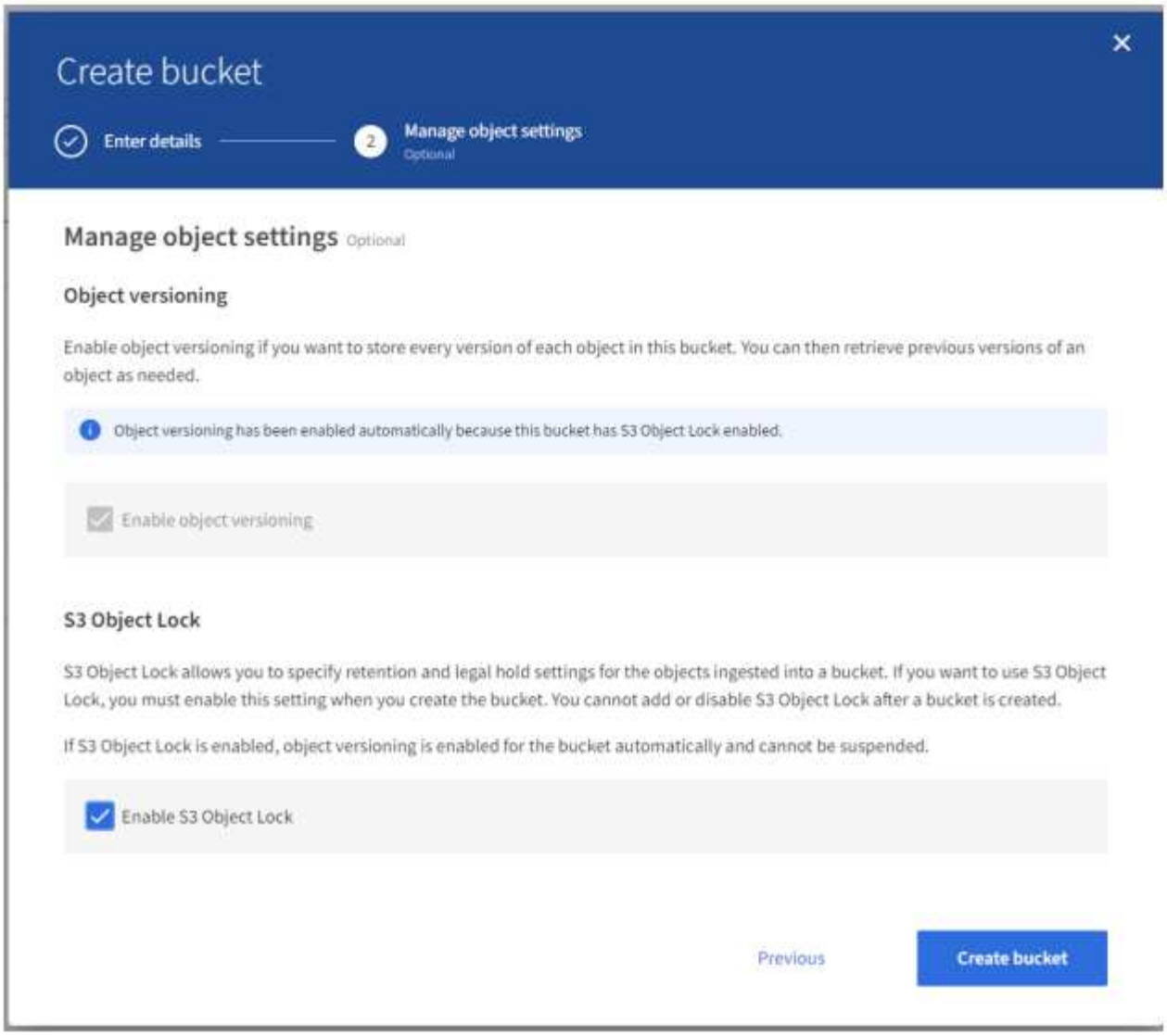
Pour configurer la rétention des compartiments par défaut du verrouillage objet StorageGRID S3, effectuez les opérations suivantes :

Étapes

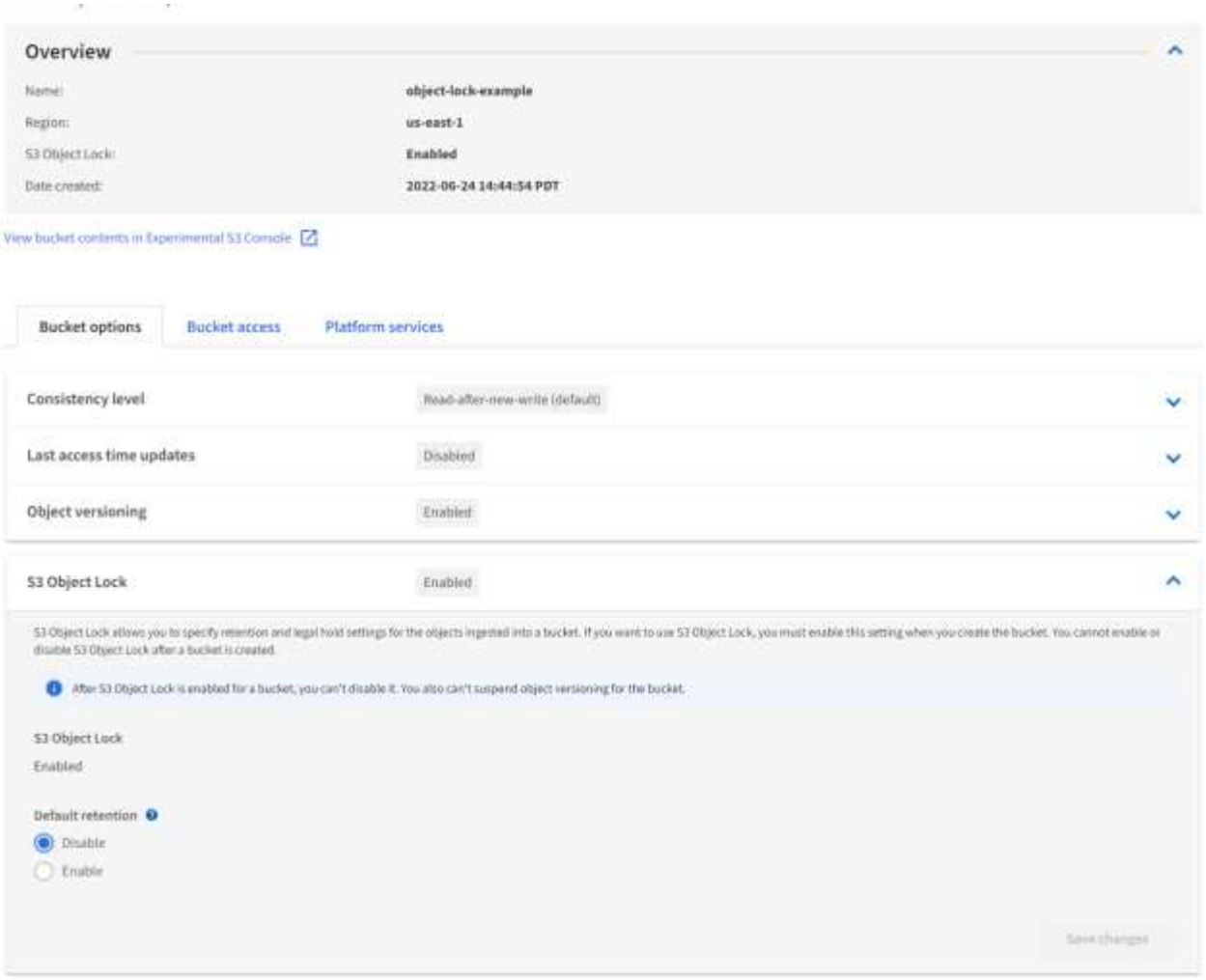
1. Dans le gestionnaire de locataires StorageGRID, créez un compartiment et cliquez sur Continuer



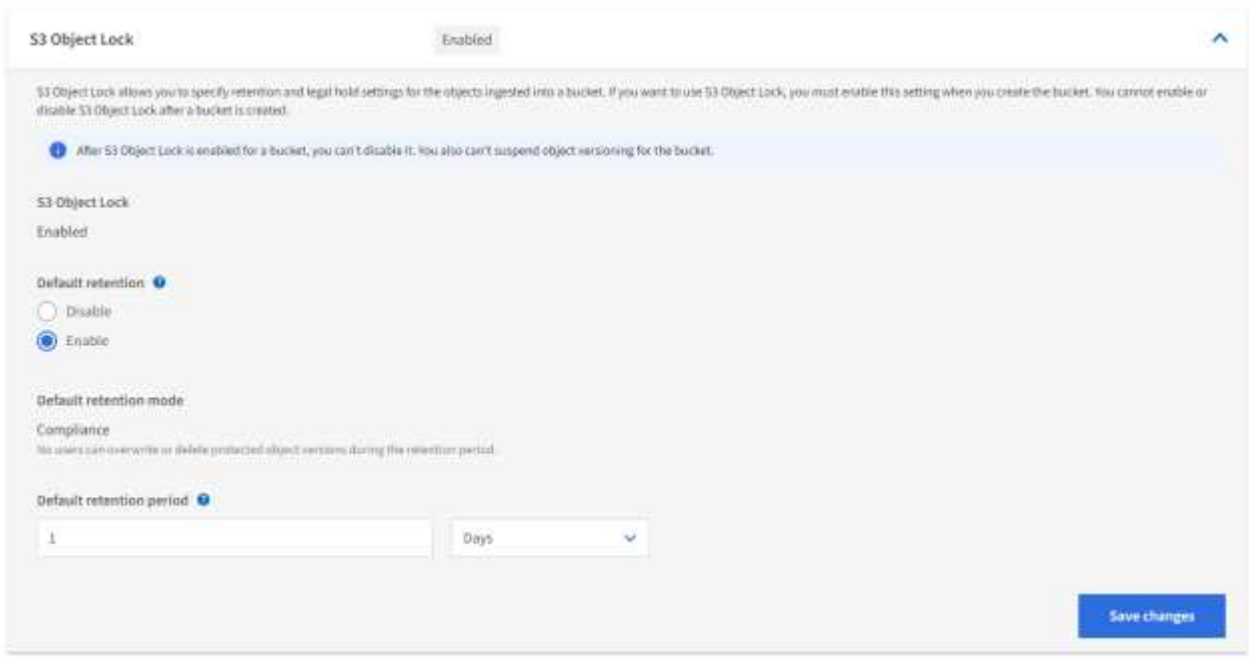
2. Sélectionnez l’option Activer le verrouillage d’objet S3 et cliquez sur Créer un compartiment.



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.



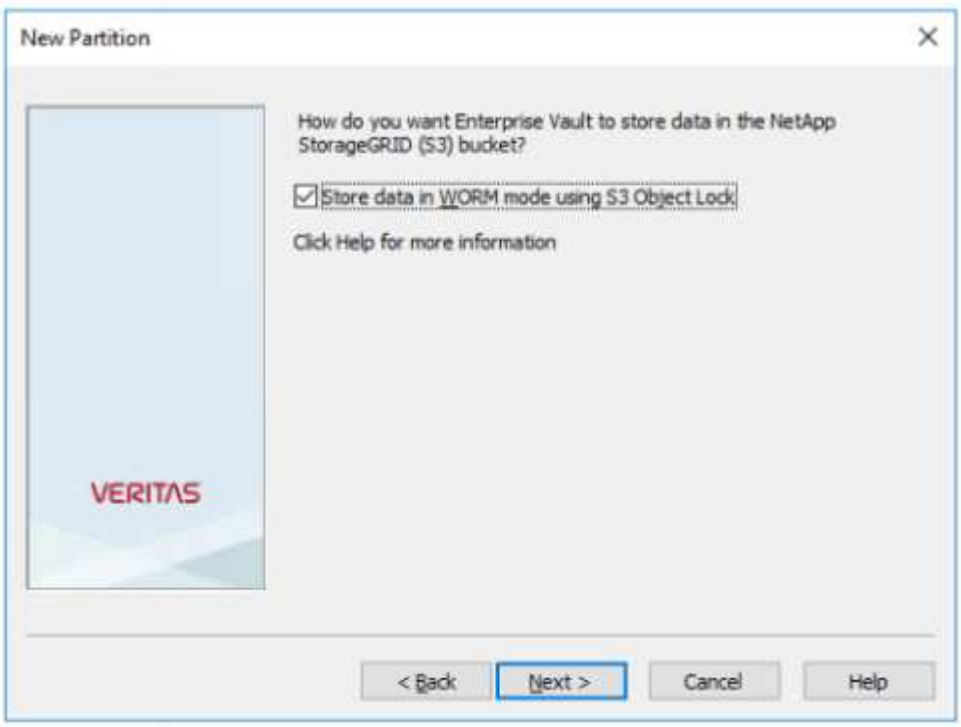
Le compartiment est désormais prêt à être utilisé par Enterprise Vault pour stocker les données WORM.

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

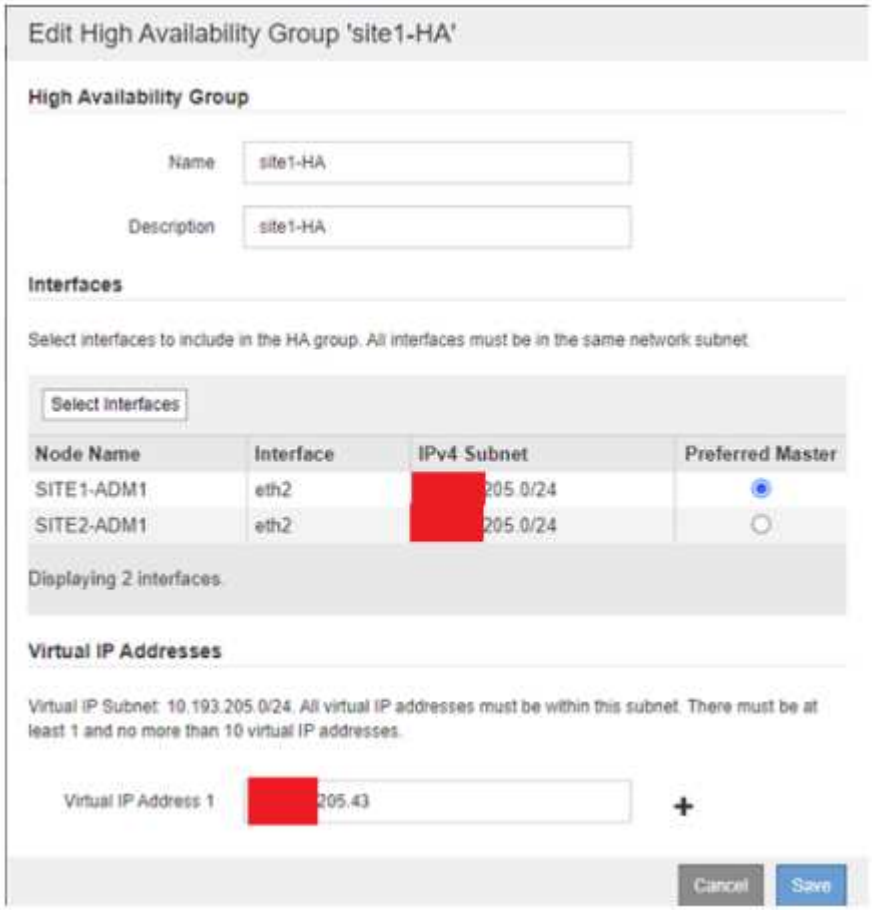
Pour configurer le basculement de site StorageGRID, procédez comme suit :

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]

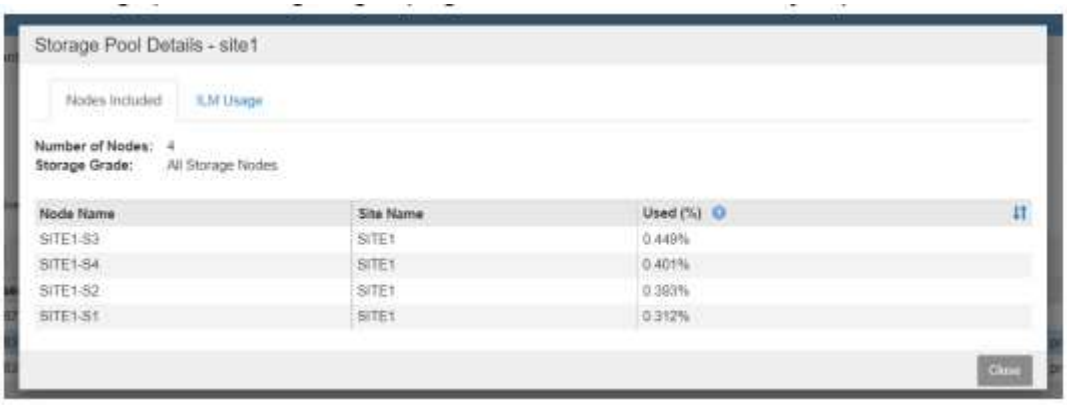
2. Entrez les informations requises. Cliquez sur Sélectionner les interfaces et incluez les interfaces réseau du SITE 1 et du SITE 2 où le site 1 (site principal) est le maître préféré. Attribuez une adresse IP virtuelle au sein du même sous-réseau. Cliquez sur Enregistrer.

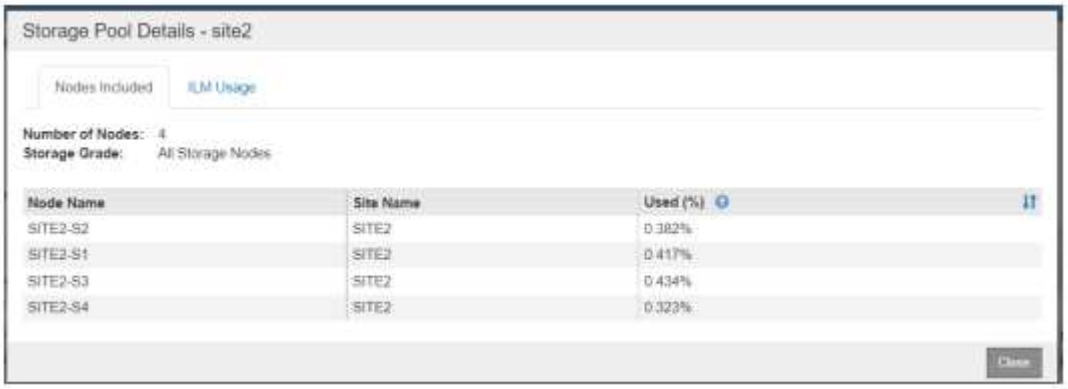


3. Cette adresse IP virtuelle (VIP) doit être associée au nom d'hôte S3 utilisé lors de la configuration de la partition de veritas Enterprise Vault. L'adresse VIP résout le trafic vers le SITE 1 et, en cas de défaillance du SITE 1, l'adresse VIP réachemine le trafic vers le SITE 2 de manière transparente.
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.