如何在您的环境中启用StorageGRID

How to enable StorageGRID in your environment

NetApp
April 15, 2025

目录

如何在您的环境中启用StorageGRID

访问StorageGRID评估软件的步骤

本说明面向与NetApp合作的NetApp销售人员、合作伙伴和潜在客户。

注册帐户

1. 使用您的业务电子邮件在上注册帐户 "NetApp 支持站点" 。
   a. 确保您未使用新创建的帐户登录。
   b. 如果您已有帐户、请确保您未登录、然后继续下一步。
2. 创建非技术支持案例、将访问级别提升到"潜在客户"。要执行此操作、请单击 ""报告问题"网站页脚中的""链接。
3. 选择"注册问题"作为反馈类别。
4. 在"注释"部分中、写下："我的帐户电子邮件地址是_您的电子邮件地址_。我希望获得潜在客户访问权限、以下载StorageGRID评估软件。"
   a. 提及建议潜在客户访问请求的NetApp内部人员的姓名。

下载StorageGRID

1. 在您的支持案例经过审核和批准后、NetApp支持部门将通过电子邮件通知您、您的帐户已获得潜在客户访问权限。
2. 下载 "StorageGRID评估软件"。

此Eval许可证文件位于此zip文件中。解压缩后、文件名称为StorageGRID-WebScale <version>\vSphere NLF000000.txt。

下载软件是一个涉及贸易合规措施以遵守法律要求的过程。为了确保合规性、用户必须先创建帐户并创建支持案例、然后才能获得访问权限。此流程有助于我们保持适当的控制和文档记录、同时为潜在客户提供他们所需的生产就绪软件。

我们提供StorageGRID的"生产就绪"版本、它不是开源版本或替代版本。需要注意的是，除非潜在客户升级到生产许可证，否则不提供*支持*。

如在上述步骤中遇到任何问题、请联系StorageGRID.Feedback@netapp.com。

经验证的第三方解决方案

经验证的第三方解决方案：概述

NetApp与我们的合作伙伴合作、已对这些解决方案进行了验证、以供StorageGRID 使用。查看本节中的信息、了解哪些解决方案已通过验证、并在适用时获取其他说明。

与NetApp携手合作、在您创建经过测试的同类最佳NetApp解决方案时、加快产品组合创新、提高市场知名度并提高销量。 "立即成为联盟合作伙伴"。

StorageGRID 11.9经验证的第三方解决方案

以下第三方解决方案已通过验证、可用于StorageGRID 11.9.+如果未列出您要查找的解决方案 、请联系您的NetApp客户代表。

已在StorageGRID 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Alluxio
- Apache Kafka
- AWS装载点
- Bridgestor
- Cantemo
- Citrix内容协作
- 短对影(最低对影数据质量版本2024.02)
- Commvault 11
- Ctera门户6.
- 达莱特
- Datadobi
- Data Dynamics StorageX
- 默认X
- 磁盘转换数据
- Dremio
- EIASCSearch Snapshot (包括冻结层)
- 员工
- 富士尼尔姆对象归档
- GitHub企业服务器

- IBM文件集
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Microsoft SQL Server大数据集群
- 模式9
- Modzy
- Moonwalk Universal
- 很好
- Nasuni
- OpenText文档16.4
- OpenText文档21.4
- OpenText InfoArchive 16 EP7
- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura
- PixitMedia ngena
- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10内部版本220706或更高版本
- Rubrik CDM
- S3a
- Signiant
- 白雪片
- 光谱逻辑在本机Glacier
- Splunk智能存储
- 星突发
- 轻松实现存储
- Trino
- varnish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更高版本
- Vertica 10.x
- Viispine

- Virtalica StorageFabric
- Weka v3.10或更高版本

第三方解决方案已在具有对象锁定的**StorageGRID** 上进行验证

这些解决方案已与相应的合作伙伴合作进行了测试。

- Commvault 11功能版本26
- IBM文件集
- OpenText文档21.4
- Rubeck
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更高版本

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架
- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID支持密钥管理器

这些解决方案已经过测试。

- Entrust KeyControl 10.2
- Hashitorp Vault 1.15.0.
- 《Terles CipherTrust Manager 2.0》
- 《Terles CipherTrust Manager 2.1》
- 《Terles CipherTrust Manager 2.2》
- Terles CipherTrust Manager 2.3
- Terles CipherTrust Manager 2.4
- Terles CipherTrust Manager 2.8
- Terles CipherTrust Manager 2.9
- Terles CipherTrust Manager 2.10
- 《Terles CipherTrust Manager 2.11》
- Terles CipherTrust Manager 2.12
- Terles CipherTrust Manager 2.13
- Terles CipherTrust Manager 2.14

StorageGRID 11.8经验证的第三方解决方案

以下第三方解决方案已通过验证、可用于StorageGRID 11.8.+
如果您要查找的解决方案未列出、请联系您的NetApp客户代表。

已在StorageGRID 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Alluxio
- Apache Kafka
- AWS装载点
- Bridgestor
- Cantemo
- Citrix内容协作
- 短对影(最低对影数据质量版本2024.02)
- Commvault 11
- Ctera门户6.
- 达莱特
- Datadobi

- Data Dynamics StorageX
- 默认X
- 磁盘转换数据
- Dremio
- ElASCSearch Snapshot (包括冻结层)
- 员工
- 富士尼尔姆对象归档
- GitHub企业服务器
- IBM文件集
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Microsoft SQL Server大数据集群
- 模式9
- Modzy
- Moonwalk Universal
- 很好
- Nasuni
- OpenText文档16.4
- OpenText文档21.4
- OpenText InfoArchive 16 EP7
- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura
- PixitMedia ngena
- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10内部版本220706或更高版本
- Rubrik CDM
- S3a
- Signiant
- 白雪片
- 光谱逻辑在本机Glacier
- Splunk智能存储

- 星突发
- 轻松实现存储
- Trino
- varnish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更高版本
- Vertica 10.x
- Viispine
- Virtalica StorageFabric
- Weka v3.10或更高版本

第三方解决方案已在具有对象锁定的**StorageGRID** 上进行验证

这些解决方案已与相应的合作伙伴合作进行了测试。

- Commvault 11功能版本26
- IBM文件集
- OpenText文档21.4
- Rubeck
- Veeam 12.
- Veritas Enterprise Vault 15.1
- Veritas NetBackup 10.1.1及更高版本

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架
- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库
- Gitlab
- Hyland Acuo
- IBM Aspera

- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID支持密钥管理器

这些解决方案已经过测试。

- Entrust KeyControl 10.2
- Hashitorp Vault 1.15.0.
- 《Terles CipherTrust Manager 2.0》
- 《Terles CipherTrust Manager 2.1》
- 《Terles CipherTrust Manager 2.2》
- Terles CipherTrust Manager 2.3
- Terles CipherTrust Manager 2.4
- Terles CipherTrust Manager 2.8
- Terles CipherTrust Manager 2.9
- Terles CipherTrust Manager 2.10
- 《Terles CipherTrust Manager 2.11》
- Terles CipherTrust Manager 2.12
- Terles CipherTrust Manager 2.13
- Terles CipherTrust Manager 2.14

StorageGRID 11.7经验证的第三方解决方案

以下第三方解决方案已通过验证、可用于StorageGRID 11.7。+如果未列出您要查找的解决方案 、请联系您的NetApp客户代表。

已在StorageGRID 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Alluxio
- Apache Kafka
- AWS装载点

- Bridgestor
- Cantemo
- Citrix内容协作
- 短对影(最低对影数据质量版本2024.02)
- Commvault 11
- Ctera门户6.
- 达莱特
- Datadobi
- Data Dynamics StorageX
- 默认X
- 磁盘转换数据
- Dremio
- ElASCSearch Snapshot (包括冻结层)
- 员工
- 富士尼尔姆对象归档
- GitHub企业服务器
- IBM文件集
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Microsoft SQL Server大数据集群
- 模式9
- Modzy
- Moonwalk Universal
- 很好
- Nasuni
- OpenText文档16.4
- OpenText文档21.4
- OpenText InfoArchive 16 EP7
- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura
- PixitMedia ngena
- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream

- Quantum StorNext 5.4.0.1
- Reveille v10内部版本220706或更高版本
- Rubrik CDM
- S3a
- Signiant
- 白雪片
- 光谱逻辑在本机Glacier
- Splunk智能存储
- 轻松实现存储
- Trino
- varnish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 14
- Veritas NetBackup 10.1.1及更高版本
- Vertica 10.x
- Viispine
- Virtalica StorageFabric
- Weka v3.10或更高版本

第三方解决方案已在具有对象锁定的**StorageGRID** 上进行验证

这些解决方案已与相应的合作伙伴合作进行了测试。

- Commvault 11功能版本26
- IBM文件集
- OpenText文档21.4
- Rubeck
- Veeam 12.
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1及更高版本

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架

- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库
- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID支持密钥管理器

这些解决方案已经过测试。

- 《Terles CipherTrust Manager 2.0》
- 《Terles CipherTrust Manager 2.1》
- 《Terles CipherTrust Manager 2.2》
- Terles CipherTrust Manager 2.3
- Terles CipherTrust Manager 2.4
- Terles CipherTrust Manager 2.8
- Terles CipherTrust Manager 2.9

StorageGRID 11.6经验证的第三方解决方案

以下第三方解决方案已通过验证、可与StorageGRID 11.6结合使用。+如果未列出您要查找的解决方案 、请联系您的NetApp客户代表。

已在StorageGRID 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Alluxio
- Apache Kafka
- Bridgestor

- Cantemo
- Citrix内容协作
- Commvault 11
- Ctera门户6.
- 达莱特
- Datadobi
- Data Dynamics StorageX
- 默认X
- 磁盘转换数据
- Dremio
- 员工
- 富士尼尔姆对象归档
- GitHub企业服务器
- IBM文件集
- IBM Spectrum Protect Plus
- Interica
- Komprise
- Microsoft SQL Server大数据集群
- 模式9
- Modzy
- Moonwalk Universal
- 很好
- Nasuni
- OpenText文档16.4
- OpenText文档21.4
- OpenText InfoArchive 16 EP7
- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura
- PixitMedia ngena
- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Reveille v10内部版本220706或更高版本
- Rubrik CDM
- S3a

- Signiant
- 白雪片
- 光谱逻辑在本机Glacier
- Splunk智能存储
- 轻松实现存储
- Trino
- varnish Enterprise 6.0.4
- Veeam 12.
- Veritas Enterprise Vault 14
- Veritas NetBackup 8.0
- Vertica 10.x
- Viispine
- Virtalica StorageFabric
- Weka v3.10或更高版本

第三方解决方案已在具有对象锁定的**StorageGRID** 上进行验证

这些解决方案已与相应的合作伙伴合作进行了测试。

- Commvault 11功能版本26
- IBM文件集
- OpenText文档21.4
- Veeam 12.
- Veritas Enterprise Vault 14.2.2
- Veritas NetBackup 10.1.1及更高版本

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架
- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库
- Gitlab

- Hyland Acuo
- IBM Aspera
- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 11.5经验证的第三方解决方案

以下第三方解决方案已通过验证、可与StorageGRID 11.5结合使用。+如果未列出您要查找的解决方案 、请联系您的NetApp客户代表。

已在**StorageGRID** 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Alluxio
- Bridgestor
- Cantemo
- Citrix内容协作
- Commvault 11
- Ctera门户6.
- 达莱特
- Datadobi
- Data Dynamics StorageX
- 默认X
- Interica
- Komprise
- Moonwalk Universal
- 很好
- Nasuni
- OpenText文档16.4
- OpenText文档21.4
- OpenText InfoArchive 16 EP7

- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura
- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM
- S3a
- Signiant
- Splunk智能存储
- Trino
- varnish Enterprise 6.0.4
- Veeam 11.
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- Viispine
- Virtalica StorageFabric

第三方解决方案已在具有对象锁定的**StorageGRID** 上进行验证

这些解决方案已与相应的合作伙伴合作进行了测试。

- OpenText文档21.4
- Veeam 11.

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架
- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库

- Gitlab
- Hyland Acuo
- IBM Aspera
- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 11.4经验证的第三方解决方案

以下第三方解决方案已通过验证、可与StorageGRID 11.4结合使用。+如果未列出您要查找的解决方案 、请联系您的NetApp客户代表。

已在StorageGRID 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Bridgestor
- Cantemo
- Citrix内容协作
- Commvault 11
- Ctera门户6.
- 达莱特
- Datadobi
- Data Dynamics StorageX
- 默认X
- Interica
- Komprise
- 很好
- Nasuni
- OpenText文档16.4
- OpenText InfoArchive 16 EP7
- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura

- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM
- Signiant
- Splunk智能存储
- varnish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Vertica 10.x
- Viispine

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架
- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库
- Hyland Acuo
- IBM Aspera
- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 11.3经验证的第三方解决方案

以下第三方解决方案已通过验证、可与StorageGRID 11.3结合使用。+如果未列出您要查找的解决方案 、请联系您的NetApp客户代表。

已在**StorageGRID** 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Bridgestor
- Cantemo
- Citrix内容协作
- Commvault 11
- Ctera门户6.
- 达莱特
- Datadobi
- Data Dynamics StorageX
- 默认X
- Interica
- Komprise
- 很好
- Nasuni
- OpenText文档16.4
- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura
- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 P1-1342
- Signiant
- Splunk智能存储
- varnish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0

- Viispine

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架
- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库
- Hyland Acuo
- IBM Aspera
- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

StorageGRID 11.2验证了第三方解决方案

以下第三方解决方案已通过验证、可与StorageGRID 11.2结合使用。+如果未列出您要查找的解决方案 、请联系您的NetApp客户代表。

已在StorageGRID 上验证的第三方解决方案

这些解决方案已与相应的合作伙伴合作进行了测试。

- Activio
- Bridgestor
- Cantemo
- Citrix内容协作
- Commvault 11
- Ctera门户6.
- 达莱特

- Datadobi
- Data Dynamics StorageX
- 默认X
- Interica
- Komprise
- 很好
- Nasuni
- OpenText文档16.4
- 采用CyanGate Cloud的OpenText Media Management 16.5
- Panzura
- 点归档网关2.0
- 指向Storage Manager 6.4
- Primestream
- Quantum StorNext 5.4.0.1
- Rubrik CDM 5.0.1 P1-1342
- Signiant
- Splunk智能存储
- varnish Enterprise 6.0.4
- Veeam 9.5.4
- Veritas Enterprise Vault 11
- Veritas Enterprise Vault 12
- Veritas NetBackup 8.0
- Viispine

StorageGRID支持的第三方解决方案

这些解决方案已经过测试。

- 存档软件
- 轴通讯
- Congruity360
- 数据框架
- EcoDigital DIIVA平台
- Encoding.com
- 富士尼尔姆对象归档
- GE Centricity企业档案库
- Hyland Acuo
- IBM Aspera

- 里程碑系统
- OnSSI
- 前移发动机
- SilverTrak
- SoftNAS
- QStar
- Velasea

产品功能指南

借助StorageGRID实现零RPO—多站点复制综合指南

本技术报告为实施StorageGRID复制策略以在站点发生故障时实现零恢复点目标(RPO)提供了全面的指南。本文档详细介绍了StorageGRID的各种部署选项、包括多站点同步复制和多网格异步复制。其中介绍了如何配置StorageGRID的信息生命周期管理(ILM)策略、以确保数据在多个位置之间的持久性和可用性。此外、本报告还介绍了保持客户端操作不中断所需的性能注意事项、故障情形和恢复过程。本文档的目标是、通过利用同步和异步复制技术、提供相关信息以确保数据始终可访问且一致、即使在站点完全瘫痪的情况下也是如此。

StorageGRID概述

NetApp StorageGRID是一个基于对象的存储系统、支持行业标准Amazon Simple Storage Service (Amazon S3) API。

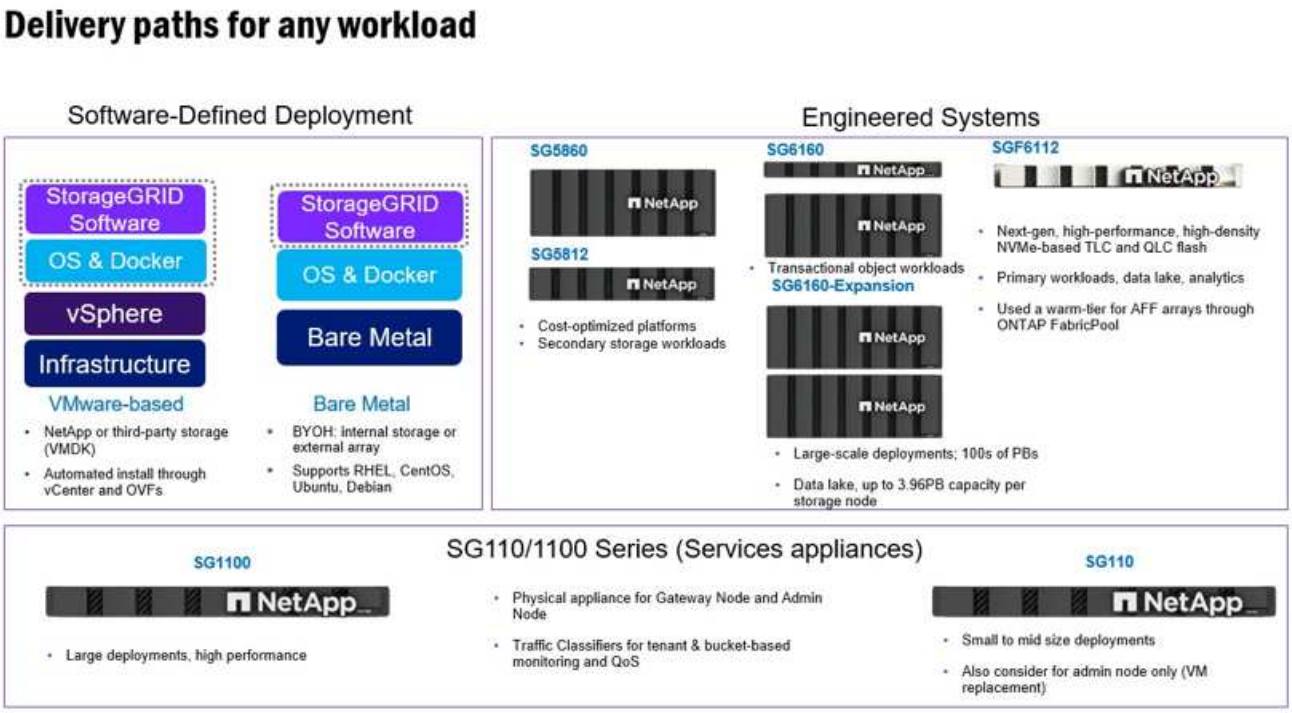
StorageGRID可跨多个位置提供一个命名空间、并根据信息生命周期管理策略(ILM)提供各种服务级别。借助这些生命周期策略、您可以优化数据在整个生命周期中的位置。

借助StorageGRID、您可以在本地和地区分布的解决方案中配置数据的持久性和可用性。无论您的数据位于内部环境还是公有云中、集成混合云工作流都可以让您的企业利用Amazon Simple Notification Service (Amazon SNS)、Google Cloud、Microsoft Azure Blb、Amazon S3 Glacier"、EliSearch等云服务。

StorageGRID规模

StorageGRID最多可部署3个存储节点、一个网格最多可扩展到200个节点。一个网格可以部署为一个站点、也可以扩展到16个站点。最小网格由一个站点中的一个管理节点和3个存储节点组成。管理节点包含管理界面、这是衡量指标和日志记录的中心点、并负责维护StorageGRID组件的配置。管理节点还包含一个用于S3 API访问的集成负载平衡器。StorageGRID可以部署为纯软件、VMware虚拟机设备或专用设备。

StorageGRID节点可以部署为仅元数据节点、最大程度地增加对象数量、仅对象存储节点、最大程度地增加对象空间、或者同时添加对象数量和对象空间的元数据和对象存储节点。每个存储节点都可以扩展到数PB的对象存储容量、从而支持数百PB的单个命名空间。StorageGRID还为S3 API操作提供了一个称为网关节点的集成负载平衡器。



StorageGRID由放置在站点拓扑中的一组节点组成。作为一种逻辑结构、StorageGRID中的站点可以是唯一的物理位置、也可以与网格中的其他站点一样驻留在共享物理位置。一个StorageGRID站点不应跨越多个物理位置。站点表示共享局域网(LAN)基础架构。

StorageGRID和故障域

StorageGRID包含多个故障域层、在决定如何构建解决方案、如何存储数据以及应将数据存储在何处以降低故障风险时、需要考虑这些故障域。

- 网格级别-由多个站点组成的网格可能会发生站点故障或隔离、可访问站点可以继续作为网格运行。
- 站点级别-站点内的故障可能会影响该站点的运行、但不会影响网格的其余部分。
- 节点级别—节点故障不会影响站点的运行。
- 磁盘级别—磁盘故障不会影响节点的运行。

对象数据和元数据

对于对象存储，存储单元是对象，而不是文件或块。与文件系统或块存储的树状层次结构不同，对象存储以非结构化的平面布局对数据进行组织。对象存储可将数据的物理位置与用于存储和检索数据的方法分离。

基于对象的存储系统中的每个对象都有两部分：对象数据和对象元数据。

- 对象数据表示实际的基础数据、例如照片、电影或病历。
- 对象元数据是指描述对象的任何信息。

StorageGRID 使用对象元数据跟踪网格中所有对象的位置，并管理每个对象的生命周期。

对象元数据包括以下信息：

- 系统元数据、包括每个对象的唯一ID (UUID)、对象名称、S3存储分段的名称、租户帐户名称或ID、对象的逻辑大小、首次创建对象的日期和时间以及上次修改对象的日期和时间。
- 每个对象副本或经过清理编码的片段的当前存储位置。
- 与对象关联的任何自定义用户元数据键值对。
- 对于S3对象、是指与该对象关联的任何对象标记键值对
- 对于分段对象和多部分对象，分段标识符和数据大小。

对象元数据可自定义并可扩展，因此应用程序可以灵活地使用。有关StorageGRID存储对象元数据的方式和位置的详细信息，请访问 "管理对象元数据存储"。

StorageGRID的信息生命周期管理(ILM)系统用于编排StorageGRID系统中所有对象数据的放置、持续时间和加载行为。ILM规则可确定StorageGRID如何使用对象副本或跨节点和站点对对象进行纠删编码来存储对象。此ILM系统负责确保网格内的对象数据一致性。

纠删编码

StorageGRID提供了在多个级别上对代码数据进行erasure的功能。借助StorageGRID设备、我们使用RAID对存储在所有驱动器上的每个节点上的数据进行了编码、从而防止因多个磁盘故障而导致数据丢失或中断。此外、StorageGRID还可以使用纠删编码方案、通过StorageGRID的ILM规则在站点内的节点之间存储对象数据、或者在StorageGRID系统中的3个或更多站点之间存储对象数据。

纠删编码提供了一种存储布局、该布局能够以较低的开销对节点故障进行恢复、而复制也可以以较高的开销完成同样的任务。只要满足存储数据块所需的最少节点数、所有StorageGRID纠删编码方案均可部署在一个站点中。这意味着、对于4+2 EC方案、至少需要6个节点可用于接收数据。

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%

元数据一致性

在StorageGRID中、元数据通常在每个站点上存储三个副本、以确保一致性和可用性。这种冗余有助于保持数据完整性和可访问性、即使在发生故障时也是如此。

默认一致性是在网格范围级别定义的。用户可以随时更改存储分段级别的一致性。

StorageGRID中提供的存储分段一致性选项包括：

- 全部：提供最高级别的一致性。网格中的所有节点都会立即接收数据、否则请求将失败。
- 强-全局：保证所有站点中所有客户端请求的写入后读一致性。
- **STRONG-GLOBAL V2**：保证所有站点上所有客户端请求的写入后读取一致性。如果可以实现元数据副本仲裁、则可以为多个节点甚至站点故障提供一致性。例如、必须从一个3站点网格创建至少5个副本、一个站点中最多3个副本。
- 强站点：保证站点内所有客户端请求的写入后读一致性。
- **read-after-new-write**(默认)：为新对象提供写入后读取一致性、并为对象更新提供最终一致性。提供高可用性和数据保护保证。建议用于大多数情况。
- 可用：为新对象和对象更新提供最终一致性。对于S3存储分段、请仅在需要时使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行HEAD或GET操作)。S3 FabricPool 存储分段不支持。

对象数据一致性

虽然元数据会在站点内和站点间自动复制、但对象数据存储放置决策由您自行决定。对象数据可以存储在站点内和站点间的副本中、也可以在站点内或站点间进行编码、或者可以组合使用副本和经过编码的存储方案。ILM规则可以应用于所有对象、也可以通过筛选仅应用于特定对象、分段或租户。ILM规则定义了对象的存储方式、副本和/或纠删编码方式、对象在这些位置的存储时间长度、副本数量或纠删编码方案是否应更改、或者位置是否应随时间而更改。

每个ILM规则都将配置以下三种用于保护对象的加注行为之一：双重提交、平衡或严格。

双提交选项将立即在网格中的任意两个不同存储节点上创建两个副本、并将请求成功返回给客户端。节点选择将在请求的站点内尝试、但在某些情况下可能会使用其他站点的节点。对象将添加到ILM队列中、以便根据ILM规则进行评估和放置。

Balanced选项会立即根据ILM策略评估对象、并在成功向客户端返回请求之前同步放置对象。如果由于中断或存储不足而无法满足放置要求、从而无法立即满足ILM规则、则会改用双提交。问题解决后、ILM将根据定义的规则自动放置对象。

"strict"选项会立即根据ILM策略评估对象、并同步放置对象、然后将请求成功返回给客户端。如果由于发生中断或存储不足以满足放置要求而无法立即满足ILM规则、则此请求将失败、客户端需要重试。

负载平衡

可以通过集成网关节点、外部第三方负载平衡器、DNS轮叫或直接部署StorageGRID来访问客户端。可以在一个站点中部署多个网关节点、并在高可用性组中配置这些节点、以便在发生网关节点中断时自动进行故障转移和故障恢复。您可以在一个解决方案中结合使用负载平衡方法、为一个解决方案中的所有站点提供单一访问点。

默认情况下、网关节点将平衡网关节点所在站点中存储节点之间的负载。可以对StorageGRID进行配置、使网关节点能够使用多个站点的节点平衡负载。此配置会将这些站点之间的延迟与客户端请求的响应延迟增加。只有在客户端可以接受总延迟时、才应配置此选项。

如何利用StorageGRID实现零RPO

要在对象存储系统中实现零恢复点目标(RPO)、在发生故障时务必：

- 元数据和对象内容是同步的、并被视为一致的
- 即使出现故障、对象内容仍可访问。

对于多站点部署、Strong Global V2是首选的一致性模型、可确保所有站点之间的元数据同步、这对于满足零RPO要求至关重要。

存储系统中的对象根据信息生命周期管理(ILM)规则进行存储、这些规则决定了数据在整个生命周期中的存储方式和位置。对于同步复制、可以考虑在严格执行或平衡执行之间进行复制。

- 为了实现零RPO、必须严格执行这些ILM规则、因为它可以确保将对象放置在定义的位置、而不会出现任何延迟或回退、从而保持数据可用性和一致性。
- StorageGRID的ILM平衡加载行为在高可用性和故障恢复能力之间实现了平衡、即使在站点发生故障时、用户也可以继续加载数据。

(可选)通过结合使用本地和全局负载平衡、确保RTO为零。要确保客户端访问不中断、需要对客户端请求进行负载平衡。一个StorageGRID解决方案可以在每个站点中包含多个网关节点和高可用性组。要使任何站点中的客户端即使在站点发生故障时也能无中断访问、您应将外部负载平衡解决方案与StorageGRID网关节点结合使用。配置网关节点高可用性组以管理每个站点中的负载、并使用外部负载平衡器在高可用性组之间平衡负载。必须将外部负载平衡器配置为执行运行状况检查、以确保仅将请求发送到正常运行的站点。有关使用StorageGRID进行负载平衡的详细信息，请参见 "StorageGRID负载平衡器技术报告"。

跨多个站点同步部署

多站点解决方案： StorageGRID允许您在网格内的多个站点之间同步复制对象。通过设置具有平衡或严格行为的信息生命周期管理(ILM)规则、对象会立即放置在指定位置。将存储分段一致性级别配置为强全局v2也可确保同步元数据复制。StorageGRID使用一个全局命名空间、将对象放置位置存储为元数据、因此每个节点都知道所有副本或经过删除的编码部分的位置。如果无法从发出请求的站点检索对象、则会自动从远程站点检索对象、而无需执行故障转移过程。

解决故障后、无需手动进行故障恢复。复制性能取决于网络吞吐量最低、延迟最高和性能最低的站点。站点的性能取决于节点数、CPU内核数和速度、内存、驱动器数量和驱动器类型。

多网格解决方案： StorageGRID可以使用跨网格复制(CGR)在多个StorageGRID系统之间复制租户、用户和分段。CGR可以将选定数据扩展到16个以上的站点、增加对象存储的可用容量并提供灾难恢复。使用CGR复制分段包括对象、对象版本和元数据、可以是双向复制、也可以是单向复制。恢复点目标(RPO)取决于每个StorageGRID系统的性能及其之间的网络连接。

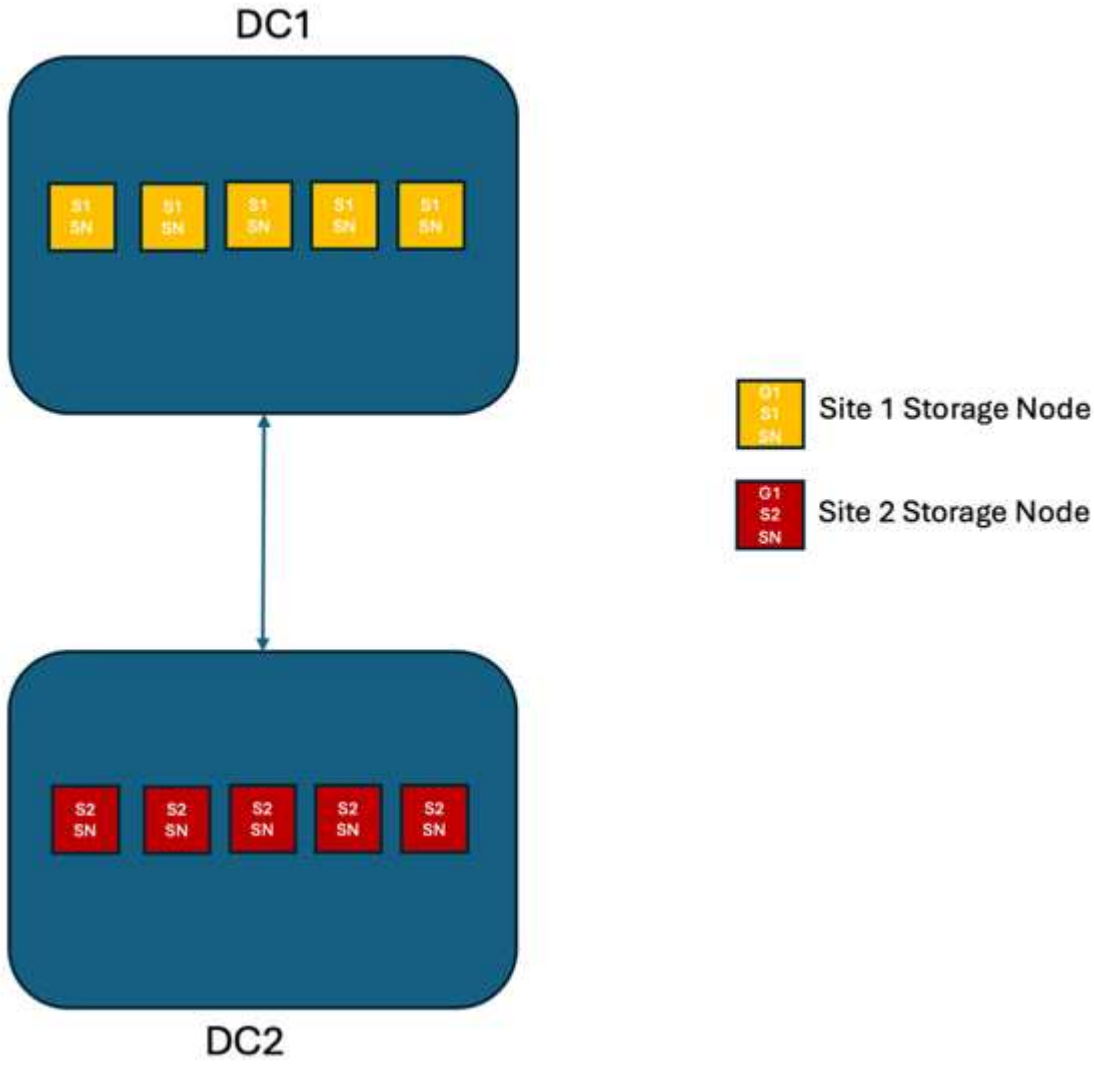
摘要:

- 网格内复制包括同步和异步复制、可使用ILM加载行为和元数据一致性控制进行配置。
- 网格间复制仅为异步复制。

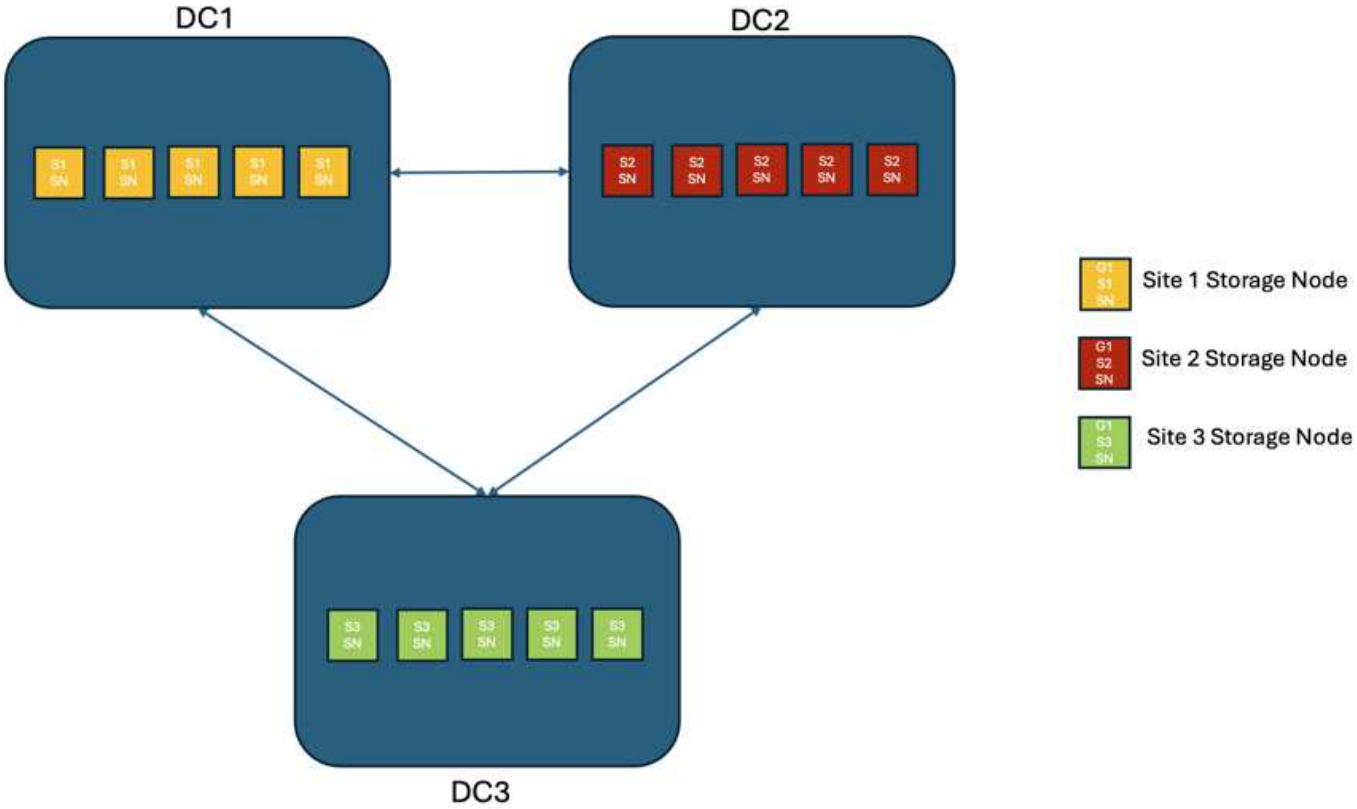
单网格多站点部署

在以下情形中、StorageGRID解决方案配置了一个可选的外部负载平衡器、用于管理对集成负载平衡器高可用性组的请求。这样、除了RPO为零之外、RTO也将为零。ILM为同步放置配置了平衡的加注保护。每个存储分段都配置了适用于3个或更多站点的网格的强全局v2一致性模型、以及适用于少于3个站点的强全局一致性。

在双站点StorageGRID解决方案中、每个对象至少有两个副本或3个EC区块、所有元数据至少有6个副本。故障恢复后、中断后的更新将自动同步到已恢复的站点/节点。如果只有2个站点、则在故障情形下、除了整个站点丢失之外、不可能实现零RPO。



在包含三个或更多站点的StorageGRID解决方案中、每个对象至少有3个副本或3个EC区块、所有元数据至少有9个副本。故障恢复后、中断后的更新将自动同步到已恢复的站点/节点。如果有三个或更多站点、则可以实现零RPO。



多站点故障情形

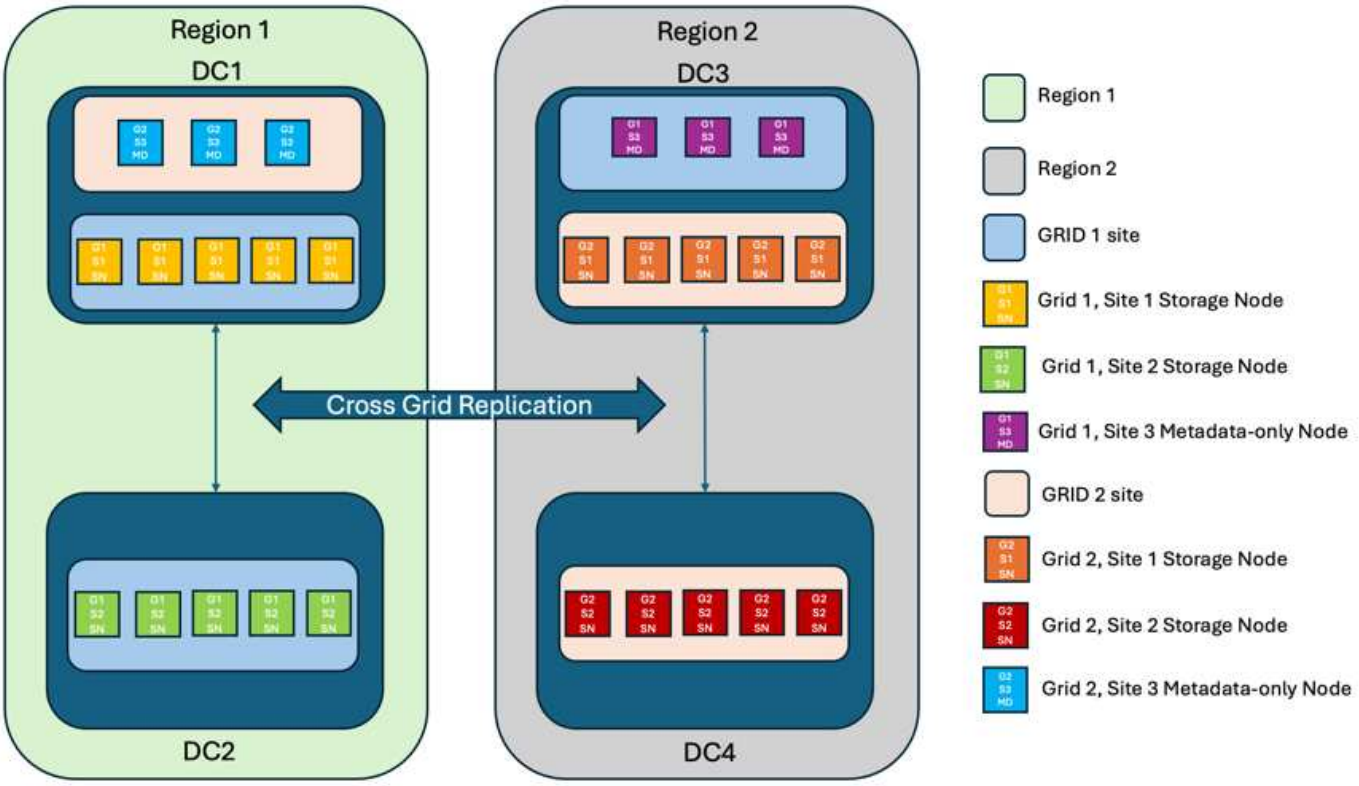
失败	双站点结果	3个或更多站点的结果
单节点驱动器故障	每个设备使用多个磁盘组、并且每个组至少可以承受1个驱动器发生故障、而不会造成中断或数据丢失。	每个设备使用多个磁盘组、并且每个组至少可以承受1个驱动器发生故障、而不会造成中断或数据丢失。
一个站点出现单节点故障	不会中断操作或丢失数据。	不会中断操作或丢失数据。
一个站点出现多节点故障	指向此站点的客户端操作中断、但不会丢失数据。 指向另一站点的操作将保持无中断、并且不会丢失任何数据。	操作将定向到所有其他站点、并且不会中断、也不会丢失任何数据。
多个站点出现单节点故障	在以下情况下、不会造成中断或数据丢失： • 网格中至少存在一个副本 • 网格中存在足够的EC数据块 在以下情况下、操作中断并存在数据丢失的风险： • 不存在副本 • EC盘头不足	在以下情况下、不会造成中断或数据丢失： • 网格中至少存在一个副本 • 网格中存在足够的EC数据块 在以下情况下、操作中断并存在数据丢失的风险： • 不存在副本 • EC读取器不足以检索对象

失败	双站点结果	**3**个或更多站点的结果
单站点故障	客户端操作将中断、直到故障得到解决、或者存储分段一致性降至强站点或强站点或低站点、以便操作成功、但不会丢失数据。	不会中断操作或丢失数据。
单站点加单节点故障	客户端操作将中断、直到故障得到解决、或者存储分段一致性降低到新写后读取或更低、以便操作成功并可能丢失数据。	不会中断操作或丢失数据。
单个站点加上其余每个站点的一个节点	客户端操作将中断、直到故障得到解决、或者存储分段一致性降低到新写后读取或更低、以便操作成功并可能丢失数据。	如果无法满足元数据副本仲裁并可能丢失数据、则操作将中断。
多站点故障	如果至少有一个站点无法完整恢复、则不会丢失任何操作站点的数据。	如果无法满足元数据副本仲裁、操作将中断。只要至少保留1个站点、就不会丢失数据。
站点的网络隔离	客户端操作将中断、直到故障得到解决、或者存储分段一致性降至强站点或强站点或低站点、以便操作成功、但不会丢失数据	隔离站点的操作将中断、但不会丢失任何数据 不会中断其余站点的运行、也不会丢失数据

多站点多网格部署

要添加额外的冗余层、此方案将使用两个StorageGRID集群并使用跨网格复制使其保持同步。对于此解决方案、每个StorageGRID集群将有三个站点。两个站点将用于对象存储和元数据、而第三个站点将仅用于元数据。这两个系统都将配置一个平衡ILM规则、以便在两个数据站点中的每个站点上使用纠删编码同步存储对象。分段将使用强大的全局v2一致性模型进行配置。每个网格都会在每个存储分段上配置双向跨网格复制。这样可以在区域之间进行异步复制。此外、还可以实施全局负载平衡器来管理对两个StorageGRID系统的集成负载平衡器高可用性组的请求、以实现零RPO。

该解决方案将使用四个位置、这些位置平均分为两个区域。区域1将包含网格1的2个存储站点作为区域的主网格、并包含网格2的元数据站点。区域2将包含网格2的2个存储站点作为区域的主网格、并包含网格1的元数据站点。在每个区域中、同一位置可以容纳该区域主网格的存储站点以及其他区域网格的纯元数据站点。仅使用元数据节点作为第三个站点将提供元数据所需的一致性、而不会复制该位置中的对象存储。



该解决方案具有四个独立的位置、可为两个单独的StorageGRID系统提供完全冗余、并将RPO保持为0、同时利用多站点同步复制和多网格异步复制。任何单个站点都可能发生故障、同时在两个StorageGRID系统上保持客户端操作不中断。

在该解决方案中、每个对象有四个经过删除的编码副本、所有元数据有18个副本。这样可以在不影响客户端操作的情况下实现多种故障情形。在发生故障恢复时、从中断中进行的更新将自动同步到发生故障的站点/节点。

多站点、多网格故障情形

失败	结果
单节点驱动器故障	每个设备使用多个磁盘组、并且每个组至少可以承受1个驱动器发生故障、而不会造成中断或数据丢失。
网格中一个站点出现单节点故障	不会中断操作或丢失数据。
每个网格中的一个站点发生单节点故障	不会中断操作或丢失数据。
网格中一个站点发生多节点故障	不会中断操作或丢失数据。
每个网格中一个站点发生多个节点故障	不会中断操作或丢失数据。
一个网格中的多个站点出现单节点故障	不会中断操作或丢失数据。
每个网格中的多个站点出现单节点故障	不会中断操作或丢失数据。
网格中的单站点故障	不会中断操作或丢失数据。
每个网格中的单站点故障	不会中断操作或丢失数据。
网格中的单站点和单节点故障	不会中断操作或丢失数据。
单个站点加上一个网格中其余每个站点的一个节点	不会中断操作或丢失数据。

失败	结果
单个位置故障	不会中断操作或丢失数据。
每个网格DC1和DC3中的单位置故障	操作将中断、直到故障得到解决或存储分段一致性降低；每个网格丢失2个站点 所有数据仍位于2个位置
每个网格DC1和DC4或DC2和DC3中的单位置故障	不会中断操作或丢失数据。
每个网格DC2和DC4中的单位置故障	不会中断操作或丢失数据。
站点的网络隔离	隔离站点的操作将中断、但不会丢失任何数据 不会中断其余站点的运行、也不会丢失数据。

结论

利用StorageGRID实现零恢复点目标(RPO)是在发生站点故障时确保数据持久性和可用性的关键目标。通过利用StorageGRID强大的复制策略(包括多站点同步复制和多网格异步复制)、企业可以保持客户端无中断运行、并确保多个位置之间的数据一致性。信息生命周期管理(ILM)策略的实施以及纯元数据节点的使用进一步增强了系统的弹性和性能。借助StorageGRID、企业可以信心十足地管理数据、因为企业知道、即使在复杂的故障情形下、数据仍可访问且保持一致。这种全面的数据管理和复制方法强调了细致规划和执行对实现零RPO和保护有价值信息的重要性。

为AWS或Google Cloud创建云存储池

如果要将StorageGRID 对象移动到外部S3存储分段、则可以使用云存储池。外部存储分段可以属于Amazon S3 (AWS)或Google Cloud。

您需要的内容

- 已配置StorageGRID 11.6。
- 您已在AWS或Google Cloud上设置外部S3存储分段。

步骤

1. 在网格管理器中、导航到* ILM >*存储池。
2. 在页面的 Cloud Storage Pools 部分中，选择 * 创建 * 。

   此时将显示创建云存储池弹出窗口。
3. 输入显示名称。
4. 从提供程序类型下拉列表中选择* Amazon S3*。

   此提供程序类型适用于AWS S3或Google Cloud。
5. 输入要用于云存储池的S3存储分段的URI。

允许使用两种格式：

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

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

6. 输入S3存储分段名称。

   您指定的名称必须与S3存储分段的名称完全匹配；否则、创建云存储池将失败。保存云存储池后，您无法更改此值。

7. 或者、输入访问密钥ID和机密访问密钥。
8. 从下拉列表中选择*不验证证书*。
9. 单击 * 保存 * 。

预期结果

确认已为Amazon S3或Google Cloud创建云存储池。

作者：Jonathan Wong

为Azure Blob Storage创建云存储池

如果要将StorageGRID 对象移动到外部Azure容器、则可以使用云存储池。

您需要的内容

- 已配置StorageGRID 11.6。
- 您已设置外部Azure容器。

步骤

1. 在网格管理器中、导航到* ILM >*存储池。
2. 在页面的 Cloud Storage Pools 部分中，选择 * 创建 * 。

   此时将显示创建云存储池弹出窗口。

3. 输入显示名称。
4. 从提供程序类型下拉列表中选择* Azure Blob Storage*。
5. 输入要用于云存储池的S3存储分段的URI。

   允许使用两种格式：

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

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

6. 输入Azure容器名称。

   您指定的名称必须与Azure容器名称完全匹配；否则、创建云存储池将失败。保存云存储池后，您无法更改此值。

7. 或者、输入Azure容器的关联帐户名称和帐户密钥进行身份验证。
8. 从下拉列表中选择*不验证证书*。
9. 单击 * 保存 * 。

预期结果

确认已为Azure Blob Storage创建云存储池。

作者：Jonathan Wong

使用云存储池进行备份

您可以创建ILM规则、将对象移动到云存储池进行备份。

您需要的内容

- 已配置StorageGRID 11.6。
- 您已设置外部Azure容器。

步骤

1. 在网格管理器中、导航到* ILM **>***规则>*创建*。
2. 输入问题描述。
3. 输入触发规则的条件。
4. 单击 * 下一步 * 。
5. 将对象复制到存储节点。
6. 添加布局规则。
7. 将对象复制到云存储池
8. 单击 * 下一步 * 。
9. 单击 * 保存 * 。

预期结果

确认保留示意图显示了存储在StorageGRID 本地和云存储池中用于备份的对象。

确认在触发ILM规则后、云存储池中存在副本、您可以在本地检索对象而无需执行对象还原。

作者：Jonathan Wong

配置**StorageGRID** 搜索集成服务

本指南详细说明了如何为NetApp StorageGRID搜索集成服务配置Amazon OpenSearch服务或内部EI在任 一EI在任 一情况下进行搜索。

简介

StorageGRID 支持三种类型的平台服务。

- * StorageGRID CloudMirror复制*。将特定对象从StorageGRID 存储分段镜像到指定的外部目标。
- 通知。按存储分段发送事件通知、以便向指定的外部Amazon Simple Notification Service (Amazon SNS)发送有关对对象执行的特定操作的通知。
- 搜索集成服务。将简单存储服务(S3)对象元数据发送到指定的Elasticsearch索引、您可以在该索引中使用外部服务搜索或分析元数据。

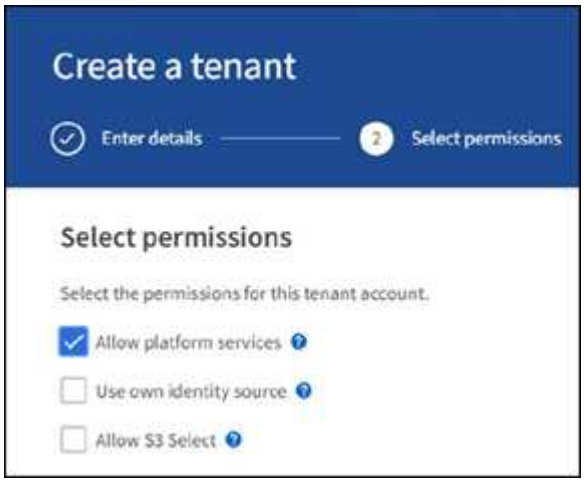
S3租户可通过租户管理器UI配置平台服务。有关详细信息，请参见 "使用平台服务的注意事项"。

本文档是对的补充 "《StorageGRID 11.6租户指南》" 和为搜索集成服务的端点和存储分段配置提供了分步说明和示例。此处提供的Amazon Web Services (AWS)或内部Elasticsearch设置说明仅用于基本测试或演示。

受众应熟悉网格管理器和租户管理器、并可访问S3浏览器、以便为StorageGRID 搜索集成测试执行基本的上传(PUT)和下载(GET)操作。

创建租户并启用平台服务

1. 使用Grid Manager创建S3租户、输入显示名称并选择S3协议。
2. 在权限页面上、选择允许平台服务选项。如果需要、也可以选择其他权限。



3. 设置租户root用户初始密码、或者如果在网格上启用了标识联合、则选择具有root访问权限的联合组来配置租户帐户。
4. 单击以root用户身份登录、然后选择分段：创建和管理分段。

   此时将转到租户管理器页面。

5. 在租户管理器中、选择我的访问密钥以创建并下载S3访问密钥、以供日后测试。

使用**Amazon OpenSearch**搜索集成服务

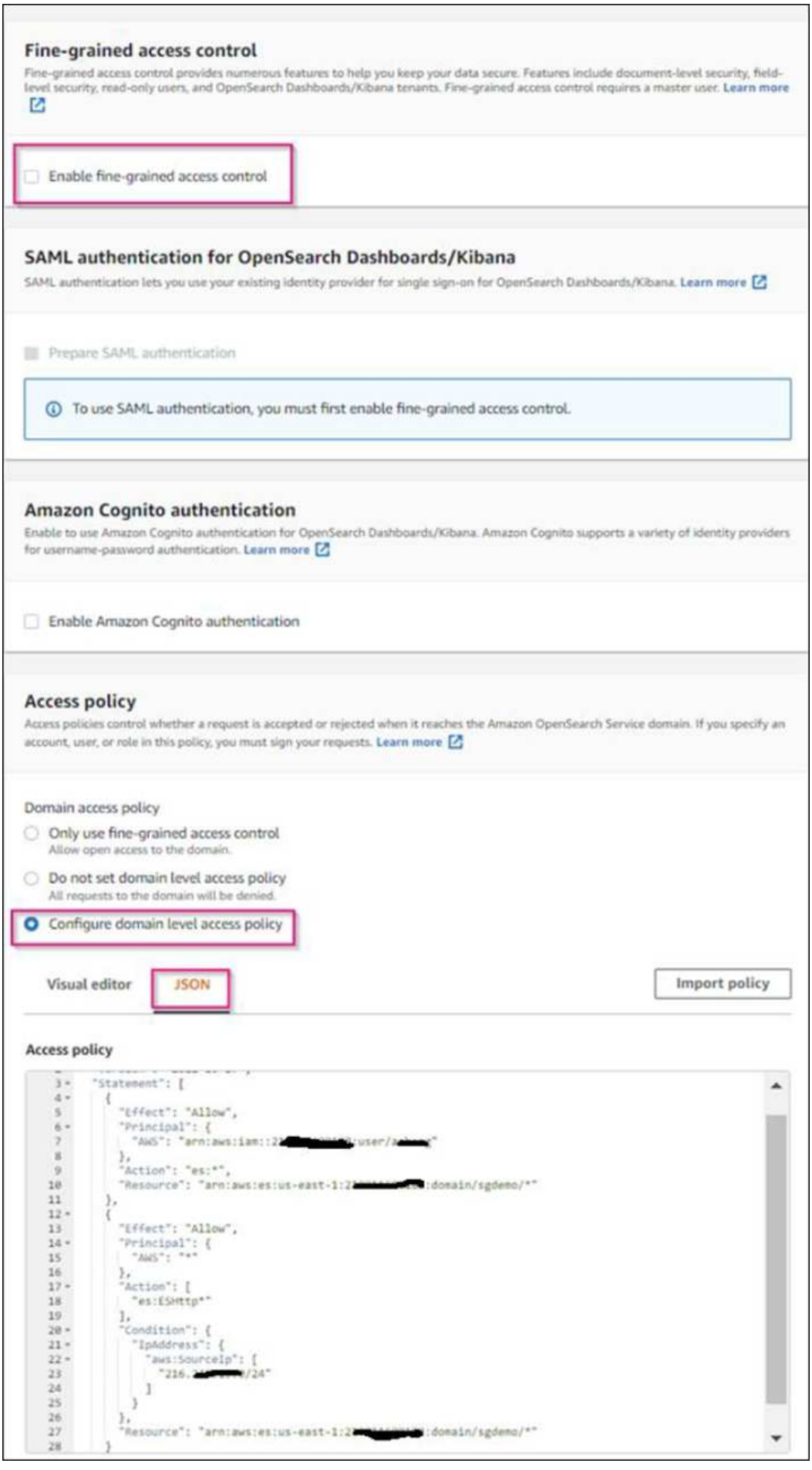
Amazon OpenSearch (以前称为Elasticsearch)服务设置

使用此操作步骤 可以快速简单地设置OpenSearch服务、但仅用于测试/演示。如果您使用内部Elasticsearch搜索集成服务、请参见一节 使用内部Elasticsearch搜索集成服务。

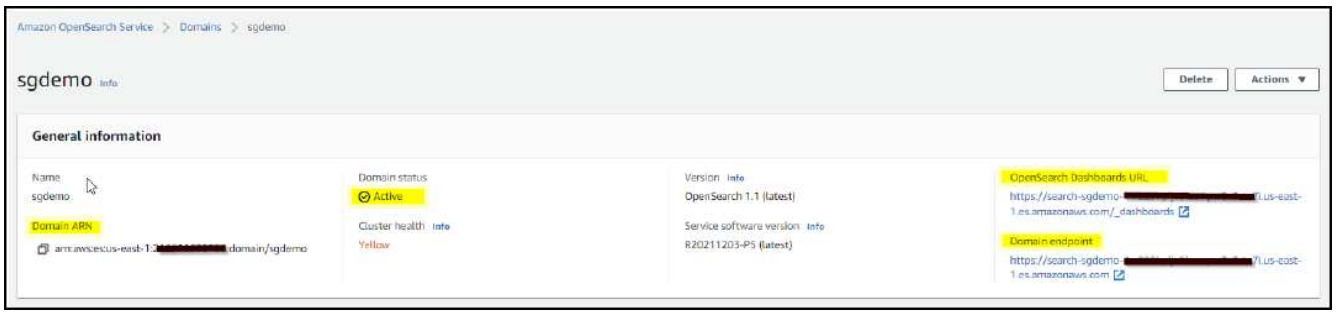
要订阅OpenSearch服务、您必须拥有有效的AWS控制台登录名、访问密钥、机密访问密钥和权限。

1. 按照中的说明创建新域 "AWS OpenSearch服务入门"、但以下情况除外：
   - 第 4 步域名：sgdemo
   - 第10步：细化访问控制：取消选择启用细化访问控制选项。
   - 第12步：访问策略：选择配置级别访问策略、然后选择JSON选项卡以使用以下示例修改访问策略：
     - 将突出显示的文本替换为您自己的AWS身份和访问管理(IAM) ID和用户名。
     - 将突出显示的文本(IP地址)替换为用于访问AWS控制台的本地计算机的公有 IP地址。
     - 打开浏览器选项卡以 "https://checkip.amazonaws.com" 以查找公有 IP。

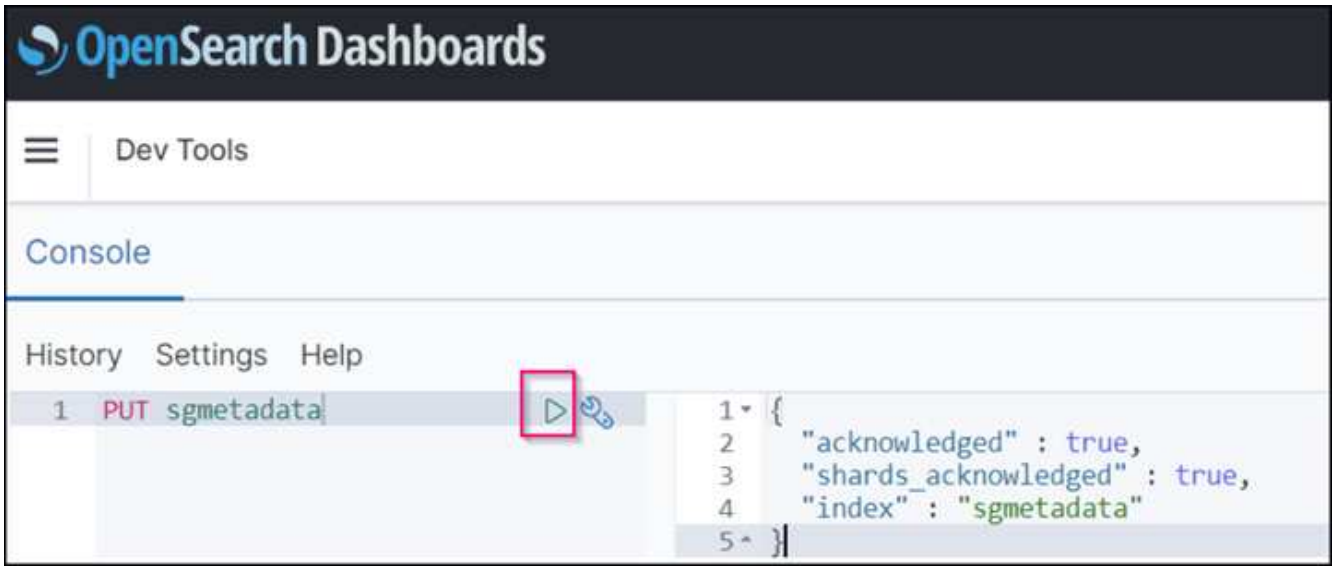
```
{

    "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/*"
}

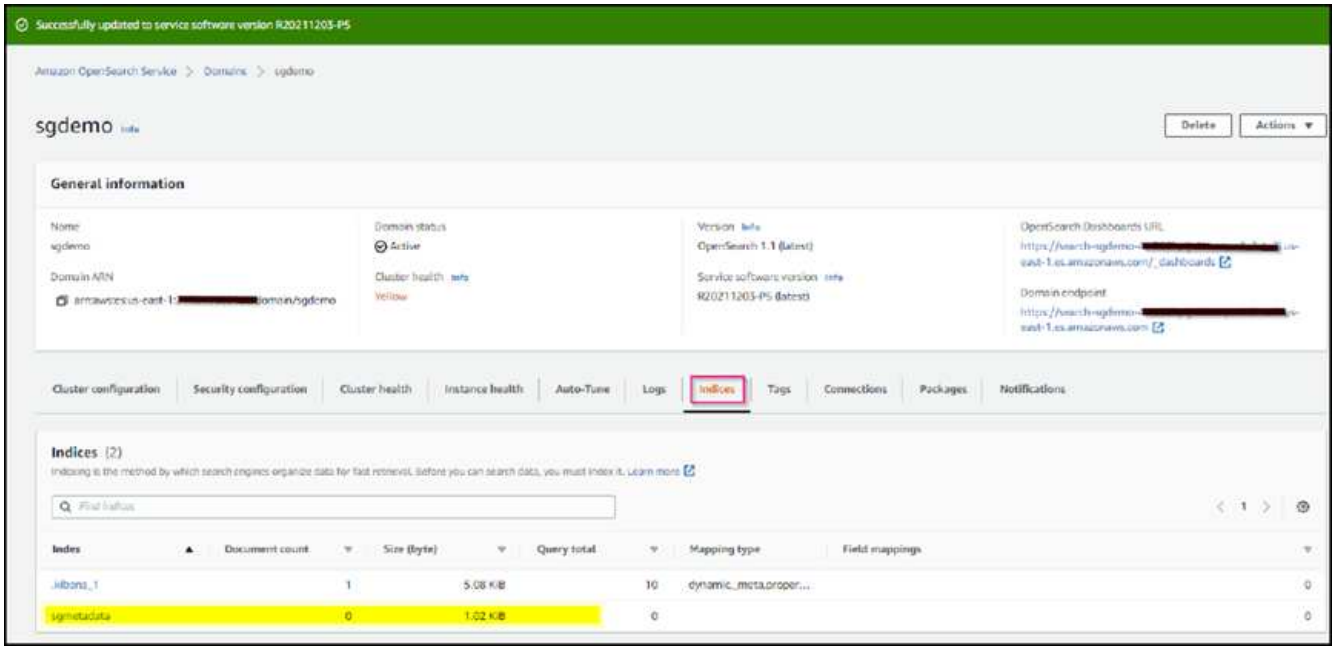
2. 等待15到20分钟、使此域变为活动状态。



3. 单击OpenSearch Dashboards URL以在新选项卡中打开域以访问此信息板。如果出现访问被拒绝错误、请验证访问策略源IP地址是否已正确设置为您的计算机公有 IP、以允许访问域信息板。
4. 在信息板欢迎页面上、选择"Explore on your own"。从菜单中、转到"Management"→"Dev Tools"
5. 在Dev Tools → Console下、输入`PUT <index>`、在此可以使用索引存储StorageGRID 对象元数据。我们在以下示例中使用索引名称"gmetadata"。单击小三角形符号以执行PUT命令。预期结果显示在右侧面板上、如以下示例屏幕截图所示。



6. 验证索引是否可从Amazon OpenSearch UI的sgdomain >索引下查看。

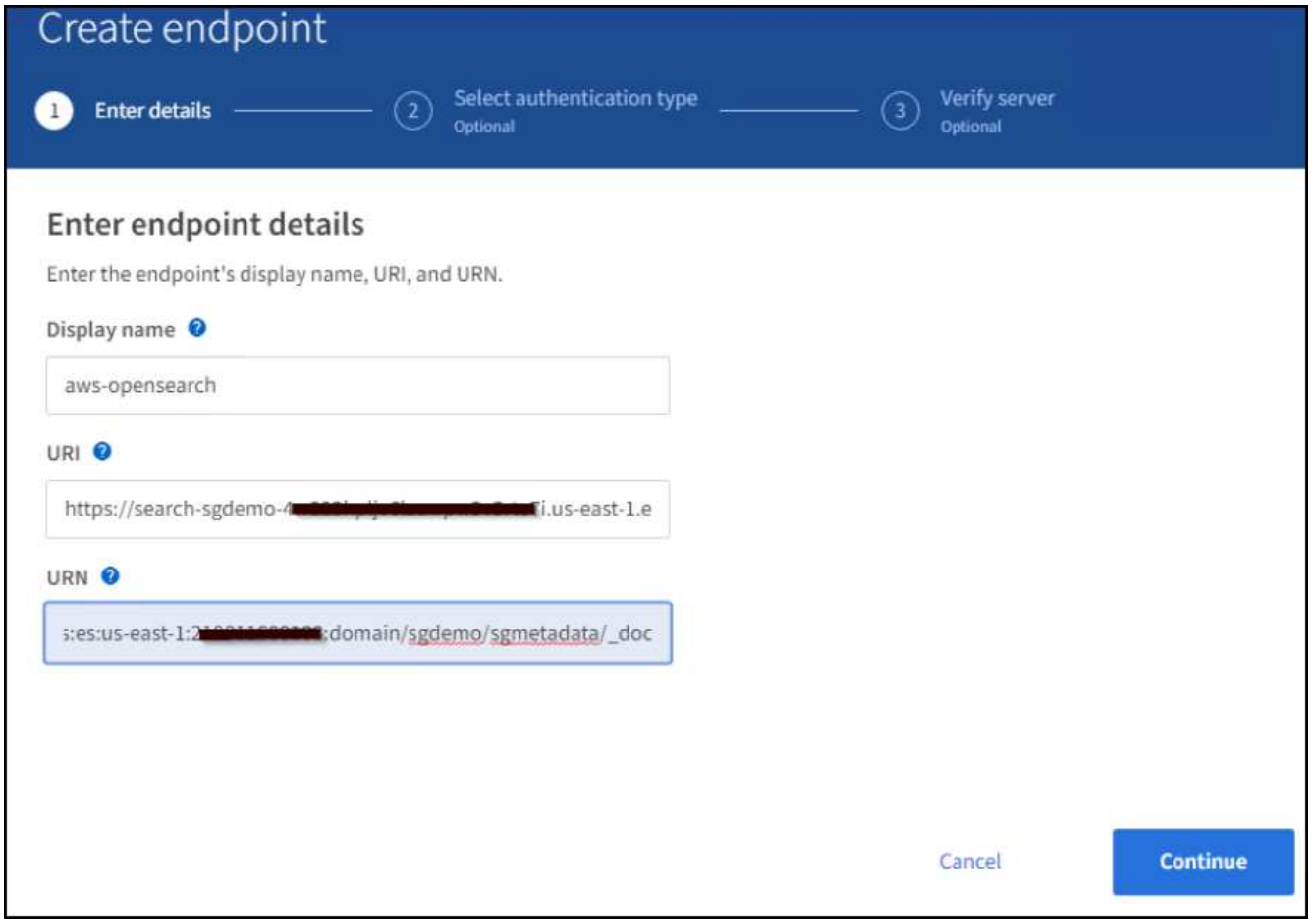


平台服务端点配置

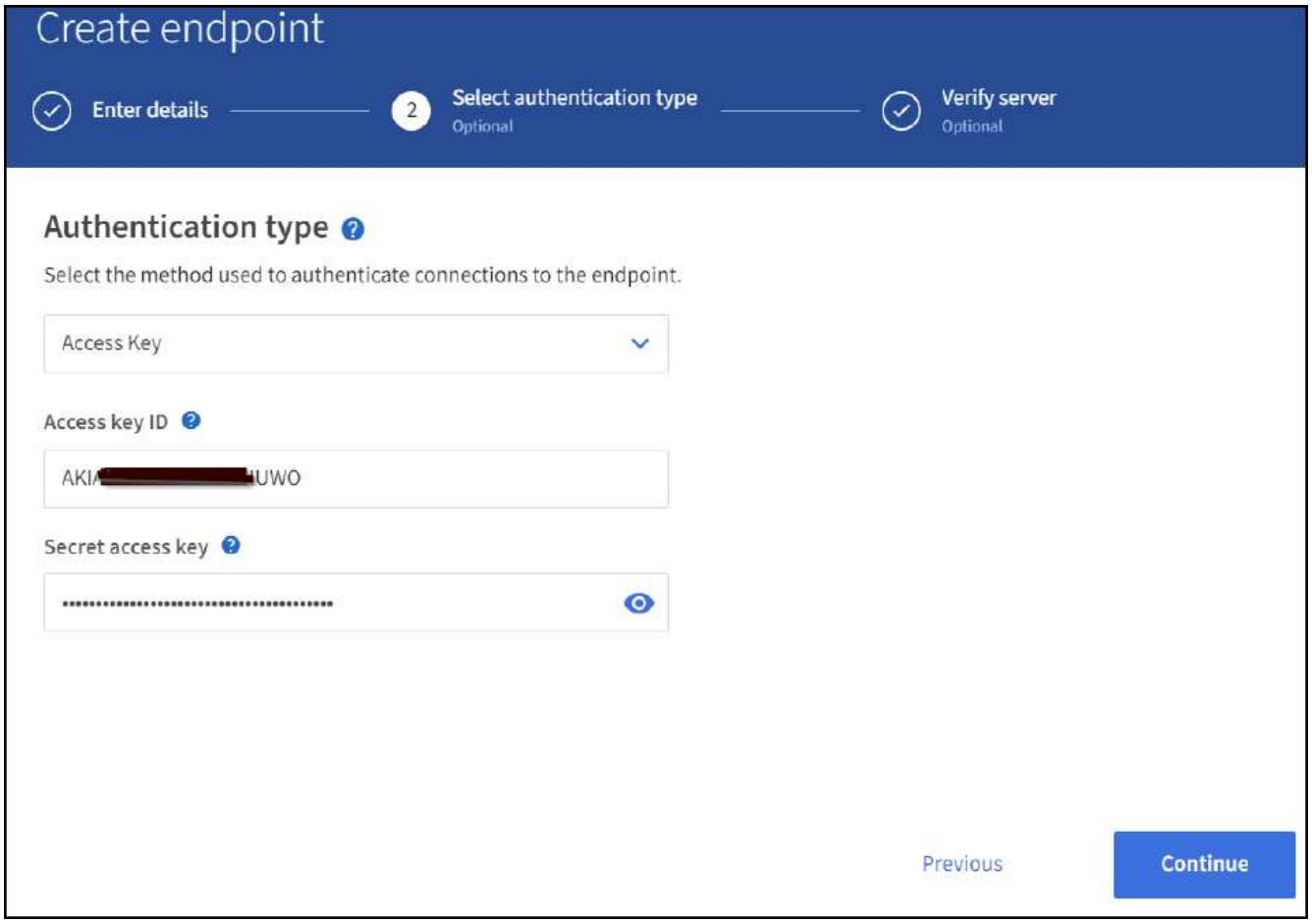
要配置平台服务端点、请执行以下步骤：

1. 在租户管理器中、转至存储(S3)>平台服务端点。
2. 单击创建端点、输入以下内容、然后单击继续：
   - 显示名称示例`AWS-OpenSearch`
   - 示例中的域端点会在URI字段中的上述操作步骤 的步骤2下显示屏幕截图。
   - 在URN字段中、上述操作步骤 的步骤2中使用的域ARN、并将`/<index>/_doc`添加到ARN末尾。

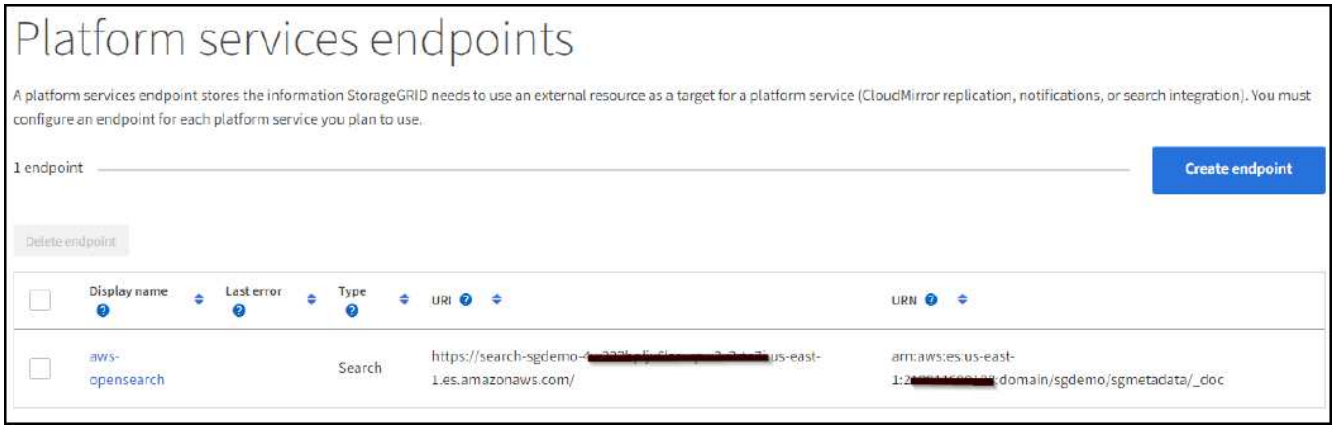
     在此示例中、URN变为`arn：AWS：es：us-east-1：211234567890：domain/sgdemo /sgmedata/_doc`。



3. 要访问Amazon OpenSearch sgdomain、请选择访问密钥作为身份验证类型、然后输入Amazon S3访问密钥和机密密钥。要转到下一页、请单击继续。



4. 要验证端点、请选择使用操作系统CA证书和测试并创建端点。如果验证成功、则会显示一个类似于下图的端点屏幕。如果验证失败、请确认URN在路径末尾包含`/<index>/_doc`、并且AWS访问密钥和机密密钥正确无误。



使用内部**Elasticsearch**搜索集成服务

内部**Elasticsearch**设置

此操作步骤 仅用于使用Docker快速设置内部Elasticsearch和Kibana、以便用于测试目的。如果Elasticsearch和Kibana服务器已存在、请转至步骤5。

1. 请遵循此操作 "Docker安装操作步骤" 安装Docker。我们使用 "CentOS Docker安装操作步骤" 在此设置中。

```
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
```

- 要在重新启动后启动Docker、请输入以下内容：

```
sudo systemctl enable docker
```

- 将`vm.max_map_count`值设置为262144：

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

- 要在重新启动后保留此设置、请输入以下内容：

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

2. 按照 "Elasticsearch快速入门指南" 自管理部分、用于安装和运行Elasticsearch和Kibana Docker。在此示例中、我们安装了8.1版。

记下由Elasticsearch创建的用户名/密码和令牌、您需要使用它们来启动Kibana UI和StorageGRID 平台端点身份验证。

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.

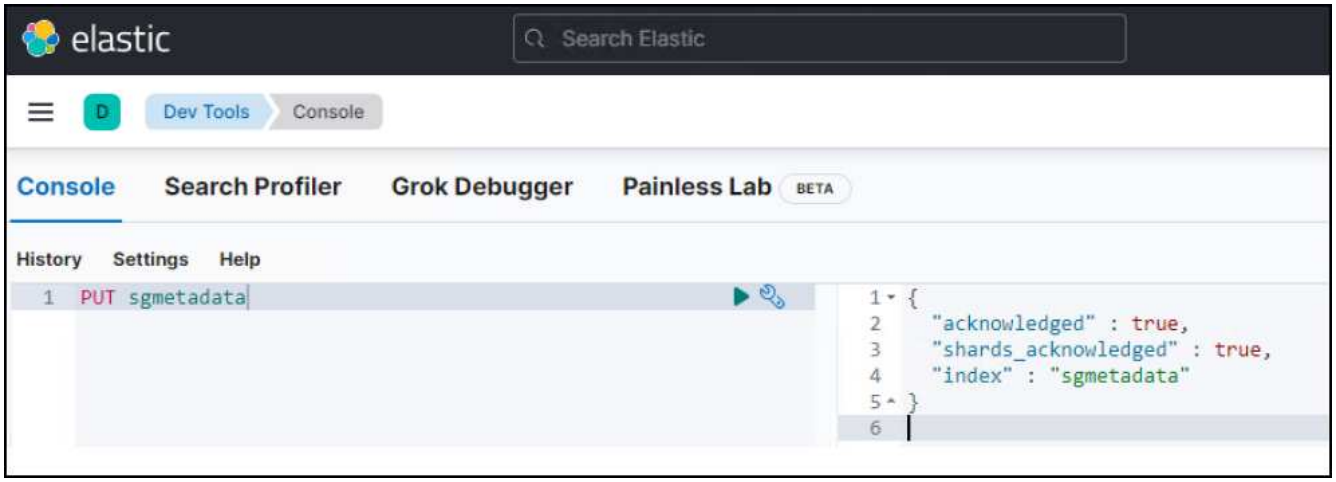
1. In a new terminal session, run:

```
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.

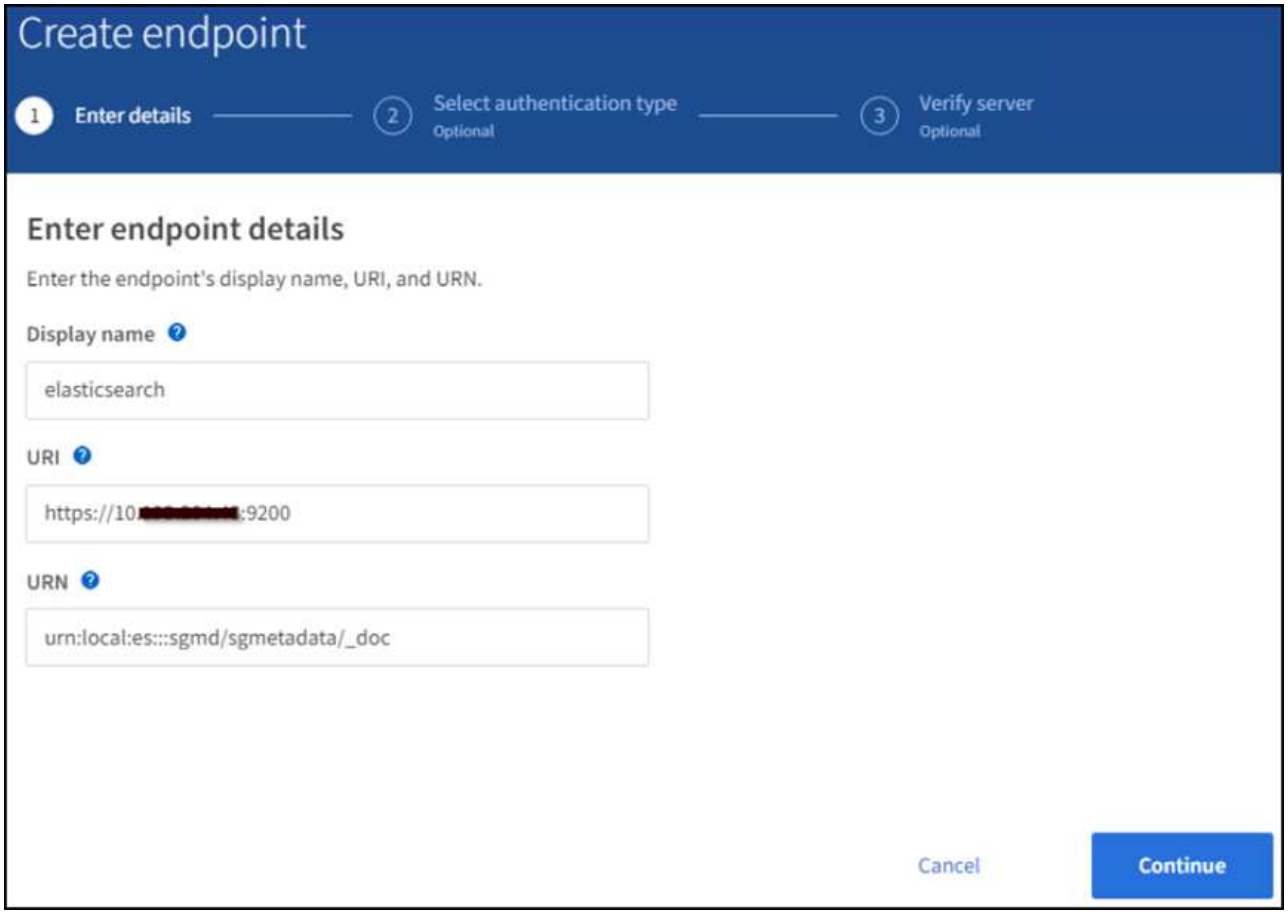
3. 启动Kibana Docker容器后、控制台中将显示URL链接`\https://0.0.0.0:5601`。将0.0.0.0替换为URL中的服务器IP地址。
4. 使用用户名`弹性`和Elastic在上一步中生成的密码登录到Kibana UI。
5. 首次登录时、请在信息板欢迎页面上选择"Explore on your own"。从菜单中、选择"Management">"Dev Tools"。
6. 在开发工具控制台屏幕上、输入`PUT <index>`、在此可以使用此索引存储StorageGRID 对象元数据。我们在此示例中使用索引名称`sgmetadata`。单击小三角形符号以执行PUT命令。预期结果显示在右侧面板上、如以下示例屏幕截图所示。



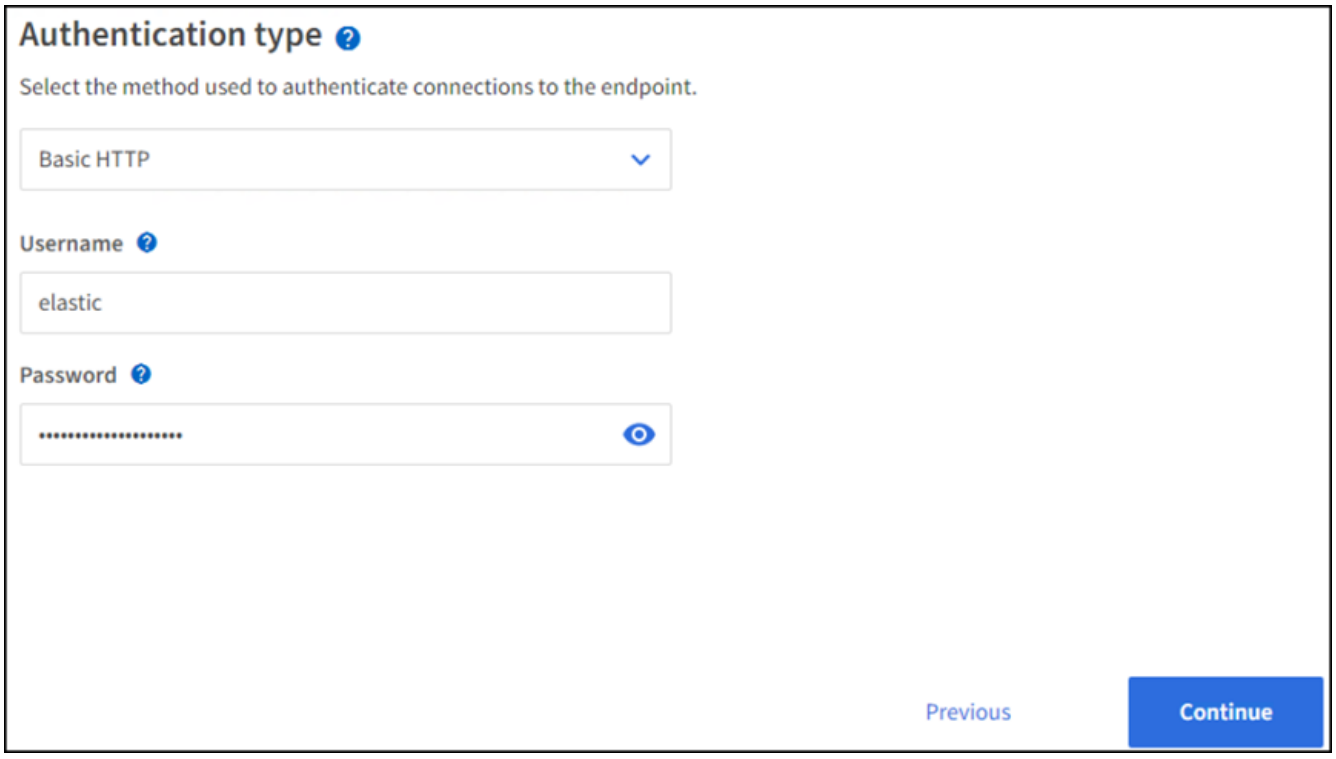
平台服务端点配置

要为平台服务配置端点、请执行以下步骤：

1. 在租户管理器上、转至存储(S3)>平台服务端点
2. 单击创建端点、输入以下内容、然后单击继续：
   - 显示名称示例：**弹性搜索**
   - URI：`https://<elasticsearch-server-ip或hostname>：9200`
   - urn：`urn：<something>：es：：：<部分唯一文本>/<索引名称>/_doc`、其中索引名称是您在Kibana控制台上使用的名称。示例：`urn：local：es：：：sgmd/sgmetadata/_doc`

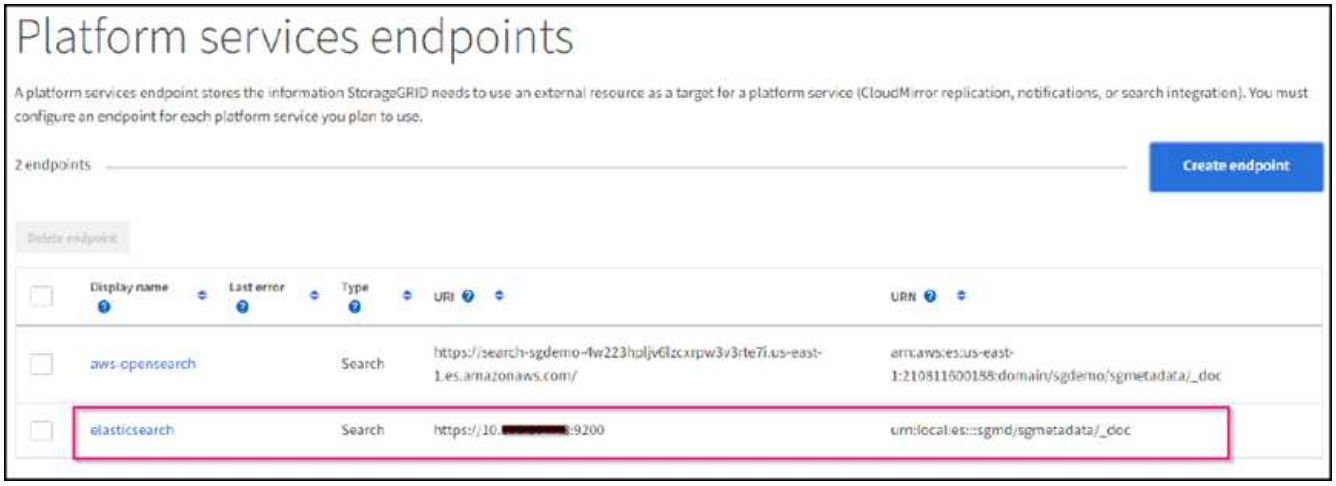


3. 选择基本HTTP作为身份验证类型、输入用户名`弹性`以及Elasticsearch安装过程生成的密码。要转到下一页、请单击继续。



4. 选择不验证证书和测试并创建端点以验证端点。如果验证成功、则会显示类似于以下屏幕截图的端点屏幕。

如果验证失败、请验证URN、URI和用户名/密码条目是否正确。



存储分段搜索集成服务配置

创建平台服务端点后、下一步是在存储分段级别配置此服务、以便在创建、删除对象或更新其元数据或标记时将对象元数据发送到定义的端点。

您可以使用租户管理器配置搜索集成、以便将自定义StorageGRID 配置XML应用于存储分段、如下所示：

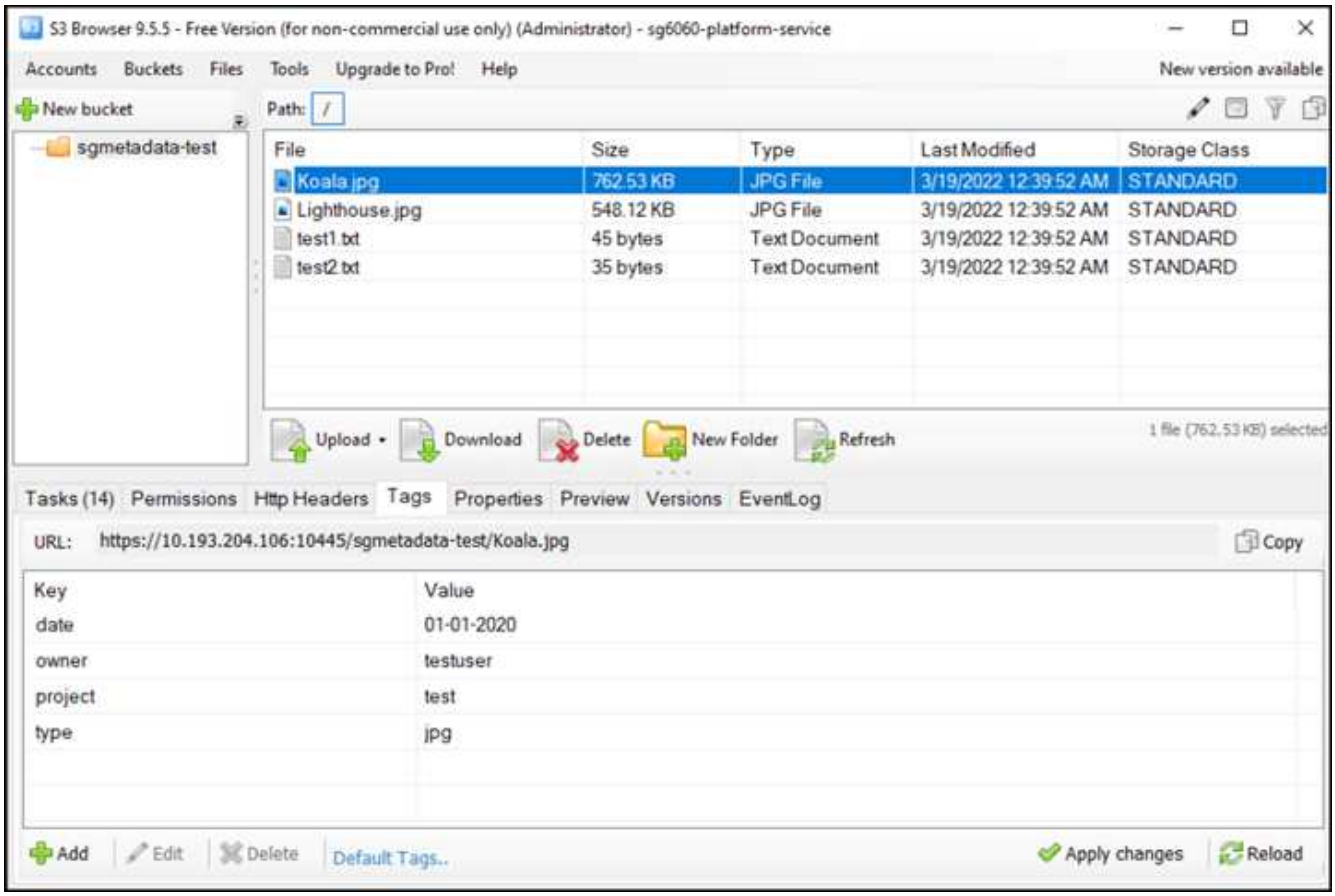
1. 在租户管理器中、转至存储(S3)>分段
2. 单击Create Bucket、输入存储分段名称(例如、`sgmetada-test`)并接受默认值`us-east-1` Region。
3. 单击"继续">"创建存储分段"。
4. 要打开存储分段概述页面、请单击存储分段名称、然后选择平台服务。
5. 选择启用搜索集成对话框。在提供的XML框中、使用以下语法输入配置XML。

   突出显示的URN必须与您定义的平台服务端点匹配。您可以打开另一个浏览器选项卡以访问租户管理器、并从定义的平台服务端点复制URN。

   在此示例中、我们不使用前缀、这意味着此分段中每个对象的元数据将发送到先前定义的Elasticsearch端点。

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

6. 使用S3浏览器使用租户访问/密钥连接到StorageGRID 、将测试对象上传到`sgmetada-test`存储分段、并向对象添加标记或自定义元数据。



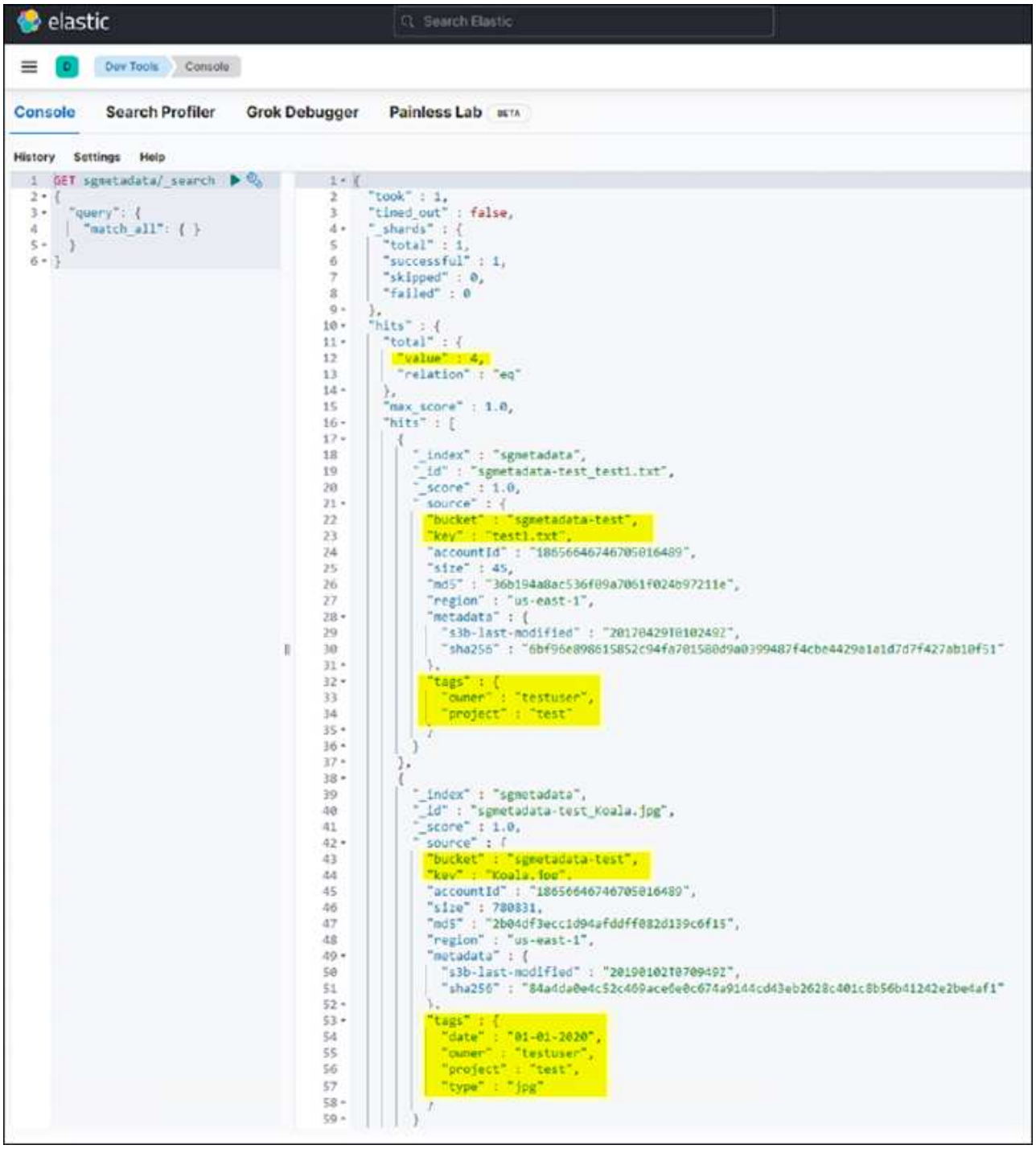
7. 使用Kibana UI验证对象元数据是否已加载到sgmetadata的索引中。

   a. 从菜单中、选择"Management">"Dev Tools"。

   b. 将示例查询粘贴到左侧的控制台面板中、然后单击三角形符号以执行该查询。

      以下示例屏幕截图中的查询1示例结果显示了四条记录。这与存储分段中的对象数匹配。

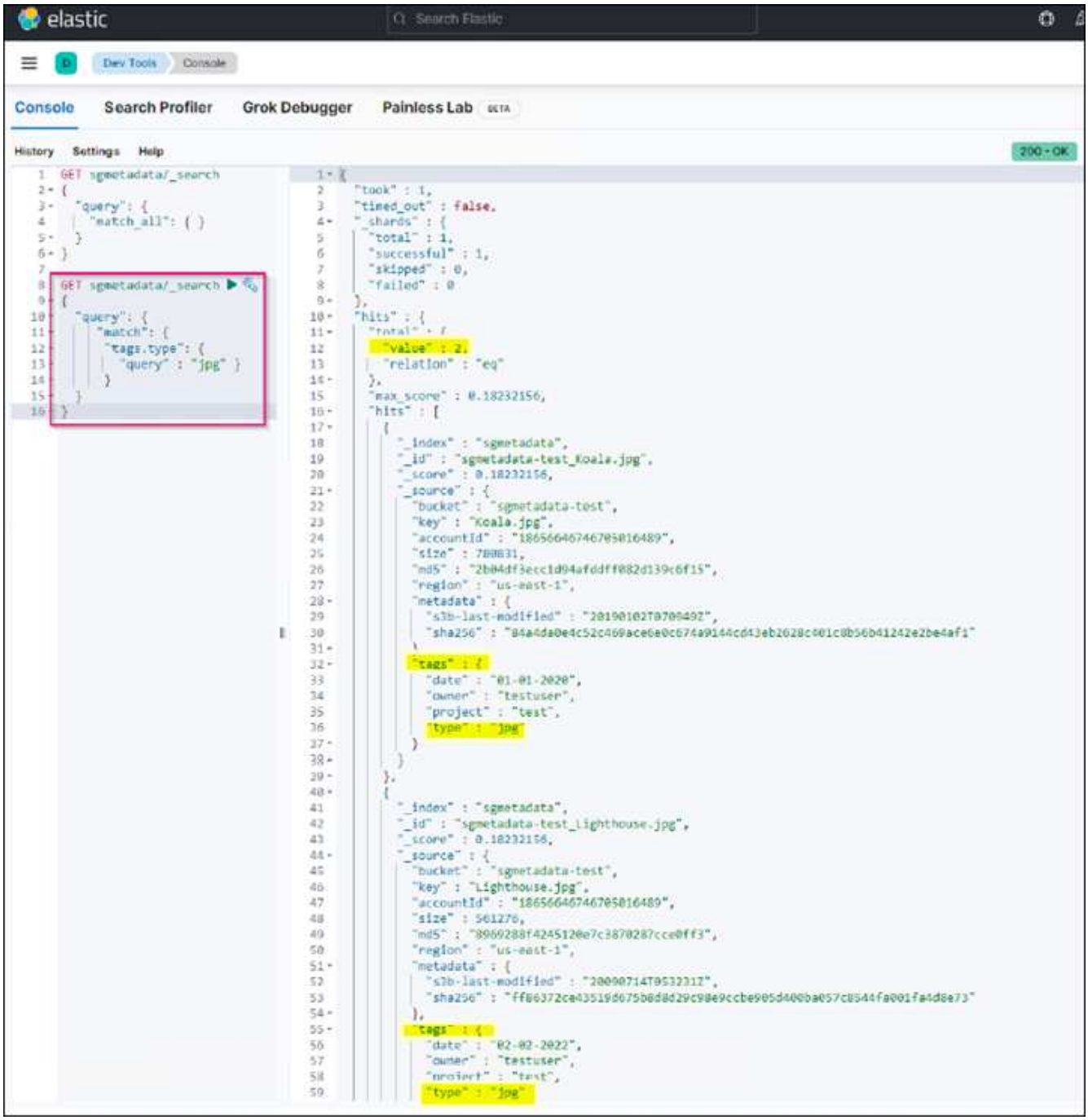
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



以下屏幕截图中的查询2示例结果显示了标记类型为jpg的两条记录。

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

+



从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- "什么是平台服务"
- "StorageGRID 11.6 文档"

作者：郑安杰

节点克隆

节点克隆注意事项和性能。

节点克隆注意事项

节点克隆可以更快地替换现有设备节点、以便进行技术更新、增加容量或提高StorageGRID 系统的性能。节点克隆对于使用KMS转换为节点加密或将存储节点从DDP8更改为DDP16也很有用。

- 源节点的已用容量与完成克隆过程所需的时间无关。节点克隆是节点的完整副本、包括节点中的可用空间。
- 源设备和目标设备必须处于同一PGE版本
- 目标节点的容量必须始终大于源节点的容量
  - 确保新目标设备的驱动器大小大于源设备
  - 如果目标设备具有相同大小的驱动器、并且已为DDP8配置驱动器、则可以为DDP16配置目标。如果已为源配置了DDP16、则无法执行节点克隆。
  - 从SG5660或SG5760设备迁移到SG6060设备时、请注意SG5x60具有60个容量驱动器、而SG6060只有58个容量驱动器。
- 节点克隆过程要求源节点在克隆过程中与网格脱机。如果在此期间另一个节点脱机、则客户端服务可能会受到影响。
- 11.8和以下内容：存储节点只能脱机15天。如果克隆过程估计接近15天或将超过15天、请使用扩展和停用过程。
  - 11．9：15天的限制已取消。
- 对于带有扩展架的SG6060或SG6160、您需要将正确磁盘架驱动器大小所需的时间与基本设备时间相加、以获取完整克隆持续时间。
- 目标存储设备中的卷数必须大于或等于源节点中的卷数。即使目标设备的容量大于源节点、您也无法将包含16个对象存储卷(rangedb)的源节点克隆到包含12个对象存储卷的目标存储设备。大多数存储设备都有16个对象存储卷、但只有12个对象存储卷的SGF6112存储设备除外。例如、不能将SG5760克隆到SGF6112。

估计节点克隆性能

下表包含节点克隆持续时间的计算估计值。条件会有所不同、因此、如果节点关闭、*粗体*中的条目可能会超过15天的限制。

DDP8.

SG5612/SG5712/SG5812 →任意

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	1 天	2天	2.5天	3天	4天	4.5天	5.5天
25 GB	1 天	2天	2.5天	3天	4天	4.5天	5.5天

SG5660 → SG5760/SG5860

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	3.5天	7 天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*
25 GB	3.5天	7 天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*

SG5660 → SG6060/SG6160

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	2.5天	4.5天	5.5天	6.5天	9天	10天	• 12天*
25 GB	2天	4天	5天	6天	8天	9天	10天

SG5760/SG5860 → SG5760/SG5860

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	3.5天	7 天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*
25 GB	3.5天	7 天	8.5天	10.5天	• 13.5天*	• 15.5天*	• 18.5天*

SG5760/SG5860 → SG6060/SG6160

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	2.5天	4.5天	5.5天	6.5天	9天	10天	• 12天*
25 GB	2天	3.5天	4.5天	5.5天	7 天	8天	9.5天

SG6060/SG6160 → SG6060/SG6160

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	2.5天	4.5天	5.5天	6.5天	8.5天	9.5天	11.5天
25 GB	2天	3天	4天	4.5天	6天	7 天	8.5天

DDP16

SG5760/SG5860 → SG5760/SG5860

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	3.5天	6.5天	8天	9.5天	• 12.5天*	• 14天*	• 17天*
25 GB	3.5天	6.5天	8天	9.5天	• 12.5天*	• 14天*	• 17天*

SG5760/SG5860 → SG6060/SG6160

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	2.5天	5天	6天	7.5天	10天	11天	• 13天*
25 GB	2天	3.5天	4天	5天	6.5天	7 天	8.5天

SG6060/SG6160 → SG6060/SG6160

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	3天	5天	6天	7 天	9.5天	10.5天	• 13天*

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
25 GB	2天	3.5天	4.5天	5天	7 天	7.5天	9天

扩展架(为源设备上的每个磁盘架添加**SG6060/SG6160**以上的磁盘架)

网络接口速度	**4 TB**驱动器大小	**8 TB**驱动器大小	**10 TB**驱动器大小	**12 TB**驱动器大小	**16 TB**驱动器大小	**18 TB**驱动器大小	**22 TB**驱动器大小
10 Gb	3.5天	5天	6天	7 天	9.5天	10.5天	• 12天*
25 GB	2天	3天	4天	4.5天	6天	7 天	8.5天

作者：*Aron Klein*

如何使用端口重新映射

由于多种原因、您可能需要重新映射传入或出站端口。您可以从原有的CLB负载平衡器服务迁移到当前的nginx服务负载平衡器端点、并保持相同的端口以减少对客户端的影响、或者希望在管理节点客户端网络上为客户端S3使用端口443、或者设置防火墙限制。

通过端口重新映射将**S3**客户端从**CLB**迁移到**NGINX**

在StorageGRID 11.3之前的版本中、网关节点上包含的负载平衡器服务是连接负载平衡器(CLB)。在StorageGRID 11.3中、NetApp引入了NGINX服务、作为功能丰富的集成解决方案 、用于平衡HTTP流量的负载。由于CLB服务在当前版本的StorageGRID 中仍然可用、因此您不能在新的负载平衡器端点配置中重复使用端口8082。要解决此问题、8082入站端口将重新映射到10443。这样、传入网关端口8082的所有HTTPS请求都会重定向到端口10443、从而绕过CLB服务、而是连接到NGINX服务。尽管以下说明适用于VMware、但所有安装方法都具有port_remap功能、您可以对裸机部署和设备使用类似的过程。

VMware虚拟机网关节点部署

以下步骤适用于使用StorageGRID 开放式虚拟化格式(OVF)在VMware vSphere 7中将网关节点部署为VM的StorageGRID 部署。此过程需要删除虚拟机并使用相同名称和配置重新部署虚拟机。在启动VM之前、请更改vApp属性以重新映射端口、然后启动VM并按照节点恢复过程进行操作。

前提条件

- 您正在运行StorageGRID 11.3或更高版本
- 您已下载并有权访问已安装的StorageGRID 版本VMware安装文件。
- 您拥有一个vCenter帐户、该帐户有权打开/关闭VM、更改VM和vApp的设置、从vCenter中删除VM以及通过OVF部署VM。
- 您已创建负载平衡器端点
  - 此端口已配置为所需的重定向端口

- 端点SSL证书与在配置/服务器证书/对象存储API服务端点服务器证书中为CLB服务安装的证书相同、或者客户端可以接受证书更改。

> If your existing certificate is self-signed, you cannot reuse it in the new endpoint. You must generate a new self-signed certificate when creating the endpoint and configure the clients to accept the new certificate.

销毁第一个网关节点

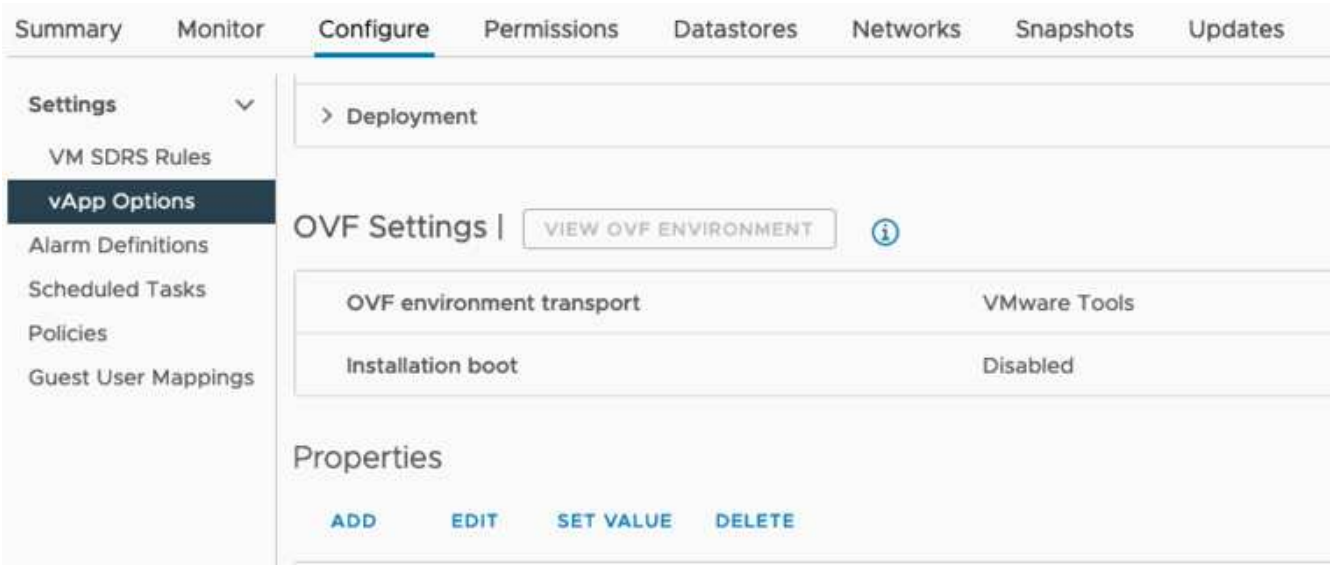
要销毁第一个网关节点、请执行以下步骤：

1. 如果网格包含多个、请选择要从其开始的网关节点。
2. 如果适用、从所有DNS轮循实体或负载平衡器池中删除节点IP。
3. 等待生存时间(TTL)并打开会话过期。
4. 关闭VM节点。
5. 从磁盘中删除VM节点。

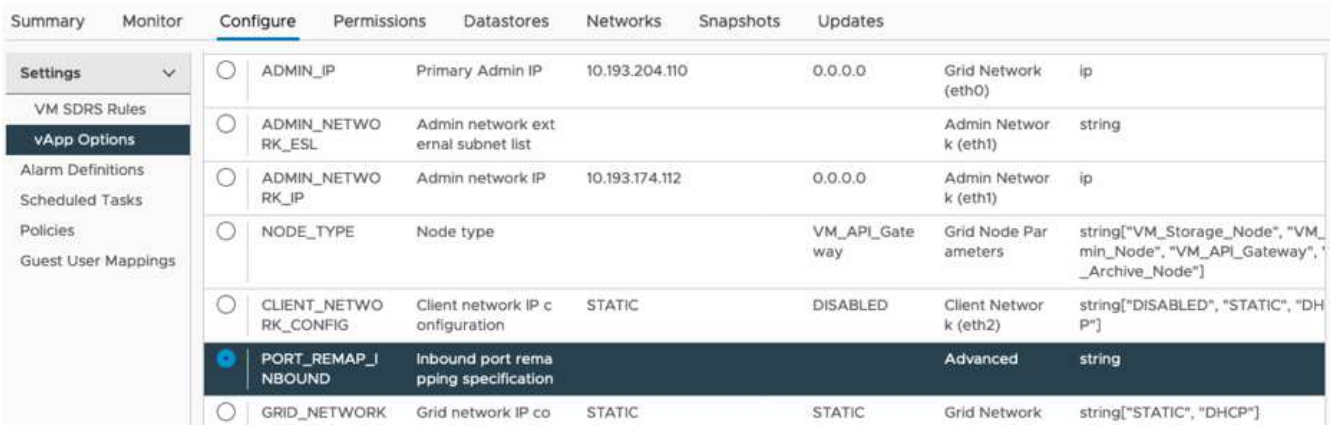
部署替代网关节点

要部署替代网关节点、请执行以下步骤：

1. 从OVF部署新虚拟机、从从从支持站点下载的安装包中选择.OVF、.MF和.vmdk文件：
   - vsphere-gateway.mf
   - vsphere-gateway.OVF
   - netapp-sg-11.4.0-20200721.1338.d3969b3.vmdk
2. 部署虚拟机后、从虚拟机列表中选择该虚拟机、然后选择配置选项卡vApp选项。



3. 向下滚动到属性部分、然后选择port_remap_inbound属性

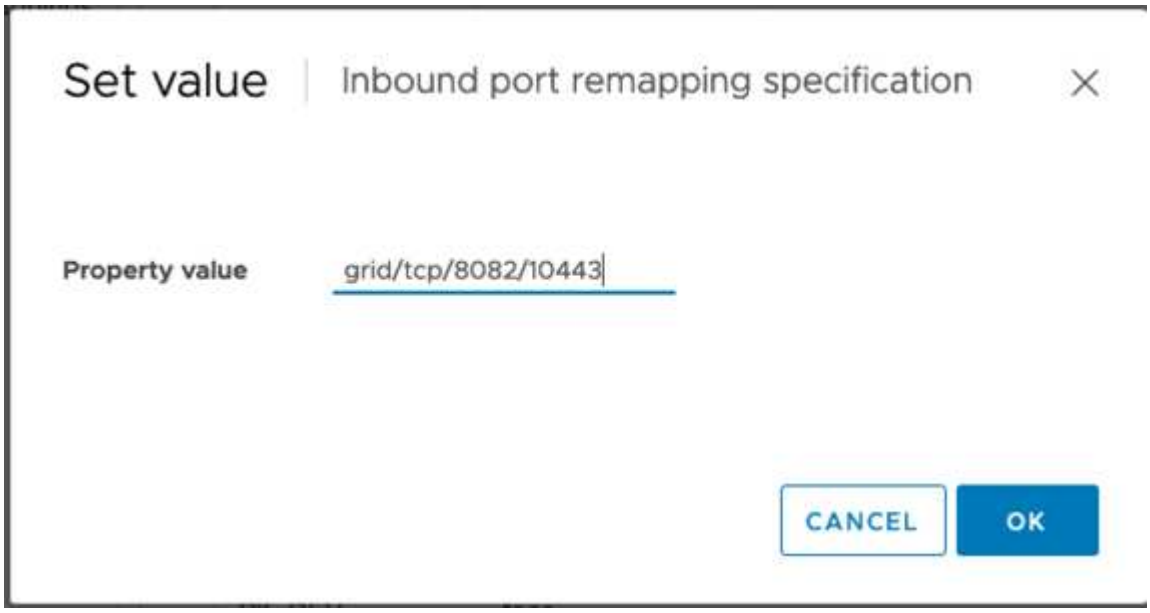


4. 滚动到属性列表顶部、然后单击编辑

5. 选择类型选项卡、确认已选中用户可配置复选框、然后单击保存。

6. 在"Properties"列表顶部、仍选择了"port_remap_inbound"属性、然后单击"Set value"。

7. 在属性值字段中、输入网络(网格、管理员或客户端)、TCP、原始端口(8082)和新端口(10443)、每个值之间均包含"/"、如下所示。

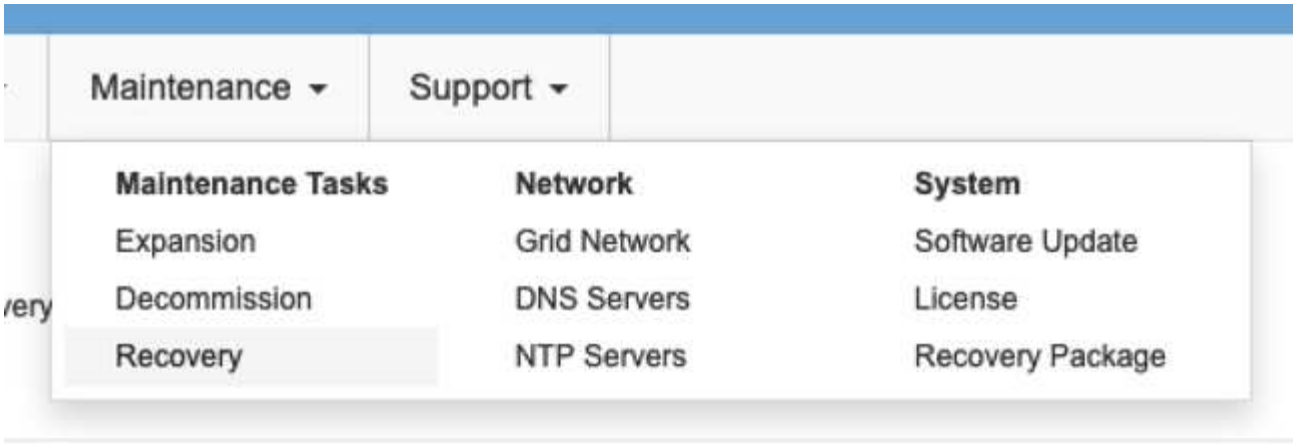


8. 如果使用多个网络、请使用逗号(、)分隔网络字符串、例如GRIDE/TCP/8082/10443、admin/TCP/8082/10443、client/TCP/8082/10443

恢复网关节点

要恢复网关节点、请执行以下步骤：

1. 导航到网格管理UI的维护/恢复部分。



2. 打开VM节点的电源、并等待此节点显示在网格管理UI的维护/恢复待定节点部分中。

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

3. 恢复节点后、如果适用、可以将此IP包括在所有DNS轮循实体或负载平衡器池中。

   现在、端口8082上的任何HTTPS会话都会转到端口10443

重新映射端口443、以便在管理节点上进行客户端S3访问

StorageGRID 系统中管理节点或包含管理节点的HA组的默认配置是、为管理和租户管理器UI保留端口443和80、并且不能用于负载平衡器端点。要执行此操作、解决方案 将使用端口重新映射功能并将入站端口443重定向到将配置为负载平衡器端点的新端口。完成后的客户端S3流量将能够使用端口443后、网格管理UI将只能通过端口8443访问、租户管理UI将只能通过端口9443访问。重新映射端口功能只能在节点安装时进行配置。要对网格中的活动节点实施端口重新映射、必须将其重置为预安装状态。这是一个具有破坏性的操作步骤 、在进行配置更改后会进行节点恢复。

备份日志和数据库

管理节点包含审核日志、Prometheus指标以及有关属性、警报和警报的历史信息。拥有多个管理节点意味着您拥有此数据的多个副本。如果您的网格中没有多个管理节点、则应确保保留此数据、以便在此过程结束时恢复此

节点后进行还原。如果网格中还有其他管理节点、则可以在恢复过程中从该节点复制数据。如果网格中没有其他管理节点、则可以按照以下说明复制数据、然后再销毁此节点。

复制审核日志

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件
   e. 将 SSH 专用密钥添加到 SSH 代理。输入 … `ssh-add`
   f. 输入中列出的SSH访问密码 `Passwords.txt` 文件

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

2. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置。使用_storage_node_01_：
   a. `ssh admin@storage_node_01_IP`
   b. `mkdir -p /var/local/tmp/saved-audit-logs`
3. 返回管理节点、停止AMS服务以防止其创建新的日志文件： `service ams stop`
4. 重命名 audit.log 文件，使其在复制到已恢复的管理节点时不会覆盖现有文件。
   a. 将 audit.log 重命名为唯一编号的文件名，例如 yyyy-mm-dd.txt.1 。例如、您可以将审核日志文件重命名为2015-10-25.txt

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

5. 重新启动AMS服务： `service ams start`
6. 复制所有审核日志文件： `scp * admin@storage_node_01_IP:/var/local/tmp/saved-audit-logs`

复制**Prometheus**数据

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在管理节点上停止服务时、某些Grid Manager功能将不可用。

1. 创建目录以将Prometheus数据复制到单独网格节点上的临时位置、我们将再次使用_storage_node_01_：
   a. 登录到存储节点：
      i. 输入以下命令： `ssh admin@storage_node_01_IP`
      ii. 输入中列出的密码 `Passwords.txt` 文件

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

2. 登录到管理节点：
   a. 输入以下命令： `ssh admin@admin_node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件
   e. 将 SSH 专用密钥添加到 SSH 代理。输入 ... `ssh-add`
   f. 输入中列出的SSH访问密码 `Passwords.txt` 文件

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

3. 从管理节点中、停止Prometheus服务： `service prometheus stop`
   a. 将Prometheus数据库从源管理节点复制到存储节点备份位置节点： `/rsync -azh --stats "/var/local/mysql_ibdata/prometheus/data" " storage_node_01_IP:/var/local/tmp/prometheus/"`
4. 在源管理节点上重新启动Prometheus服务.`service prometheus start`

备份历史信息

历史信息存储在mysql数据库中。要转储数据库的副本、您需要NetApp提供的用户和密码。如果网格中有另一个管理节点、则无需执行此步骤、在恢复过程中、可以从其余管理节点克隆数据库。

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@admin_node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件
   e. 将 SSH 专用密钥添加到 SSH 代理。输入 ... `ssh-add`
   f. 输入中列出的SSH访问密码 `Passwords.txt` 文件

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

2. 停止管理节点上的StorageGRID 服务并启动NTP和mysql
   a. 停止所有服务： `service servermanager stop`
   b. 重新启动NTP服务： `service ntp start`..restart mysql服务： `service mysql start`
3. 将mi数据库转储到/var/local/tmp
   a. 输入以下命令： `mysqldump -u username -p password mi > /var/local/tmp/mysql-mi.sql`

4. 将mysql转储文件复制到备用节点、我们将使用_storage_node_01：
   `scp /var/local/tmp/mysql-mi.sql storage_node_01_IP:/var/local/tmp/mysql-mi.sql`
   a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入 … `ssh-add -D`

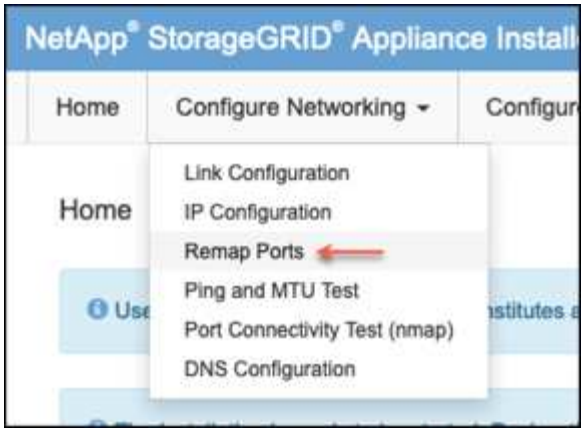
重建管理节点

现在、您已获得所有所需数据的备份副本、并将日志记录在网格中的另一个管理节点上或存储在临时位置、现在是时候重置设备了、以便可以配置端口重新映射了。

1. 重置设备会使其恢复到预安装状态、在此状态下、它仅保留主机名、IP和网络配置。所有数据都将丢失、因此我们确保备份任何重要信息。
   a. 输入以下命令： `sgareinstall`

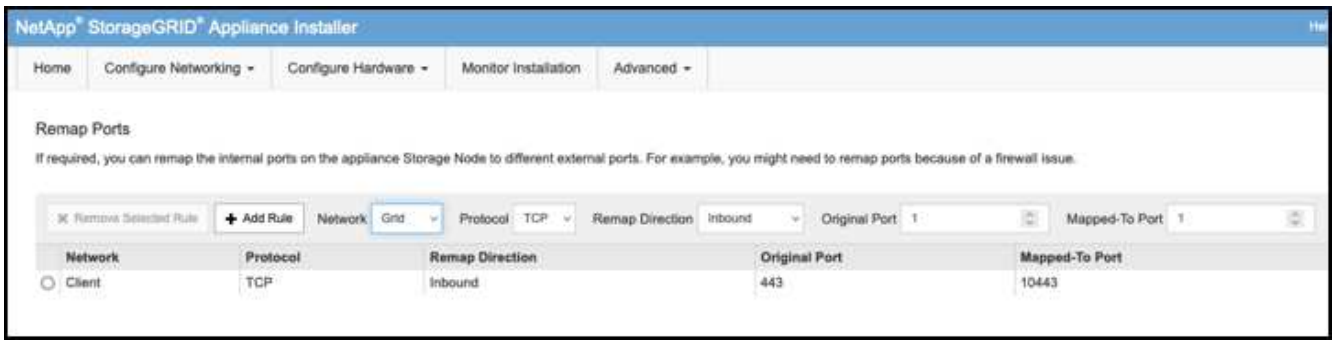
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

After running this command and waiting a few minutes for the node to
reboot,
browse to one of the following URLs to reinstall StorageGRID Webscale
on
this node:

    https://10.193.174.192:8443
    https://10.193.204.192:8443
    https://169.254.0.1:8443

Are you sure you want to continue (y/n)? y
Renaming SG installation flag file.
Initiating a reboot to trigger the StorageGRID Webscale appliance
installation wizard.
```

2. 经过一段时间后、设备将重新启动、您将能够访问节点PGE UI。
3. 浏览到Configure Networking



4. 选择所需的网络、协议、方向和端口、然后单击添加规则按钮。

   重新映射网格网络上的入站端口443将中断安装和扩展过程。建议不要重新映射网格网络上的端口443。



5. 添加了所需的端口重新映射之一、您可以返回到主页选项卡并单击开始安装按钮。

现在、您可以按照中的管理节点恢复过程进行操作 "产品文档"

还原数据库和日志

现在、管理节点已恢复、您可以还原指标、日志和历史信息。如果网格中还有其他管理节点、请按照执行操作 "产品文档" 使用_Prometheus-clone-db.sh_和_mi-clone-db.sh_脚本。如果这是您的唯一管理节点、而您选择备份此数据、则可以按照以下步骤还原此信息。

将审核日志复制回

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件
   e. 将 SSH 专用密钥添加到 SSH 代理。输入 ... `ssh-add`
   f. 输入中列出的SSH访问密码 `Passwords.txt` 文件

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

2. 将保留的审核日志文件复制到已恢复的管理节点： `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`
3. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
4. 更新已恢复管理节点上审核日志文件的用户和组设置： `chown ams-user:bycast *`

您还必须还原对审核共享的任何已有客户端访问。有关详细信息，请参见有关管理 StorageGRID 的说明。

还原**Prometheus**指标

复制 Prometheus 数据库可能需要一个小时或更长时间。在管理节点上停止服务时、某些Grid Manager功能将不可用。

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件
   e. 将 SSH 专用密钥添加到 SSH 代理。输入 ... `ssh-add`
   f. 输入中列出的SSH访问密码 `Passwords.txt` 文件

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

2. 从管理节点中、停止Prometheus服务： `service prometheus stop`
   a. 将Prometheus数据库从临时备份位置复制到管理节点： `/rsync -azh --stats "backup_node:/var/local/tmp/prometheus/" "/var/local/mysql_ibdata/prometheus/"`
   b. 验证数据是否位于正确路径中且完整 `ls /var/local/mysql_ibdata/prometheus/data/`
3. 在源管理节点上重新启动Prometheus服务.`service prometheus start`

还原历史信息

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

e. 将 SSH 专用密钥添加到 SSH 代理。输入 … `ssh-add`

f. 输入中列出的SSH访问密码 `Passwords.txt` 文件

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

2. 从备用节点复制mysql转储文件： `scp grid_node_IP_:/var/local/tmp/mysql-mi.sql /var/local/tmp/mysql-mi.sql`
3. 停止管理节点上的StorageGRID 服务并启动NTP和mysql
   a. 停止所有服务： `service servermanager stop`
   b. 重新启动NTP服务： `service ntp start`..restart mysql服务： `service mysql start`
4. 丢弃mi数据库并创建新的空数据库： `mysql -u username -p password -A mi -e "drop database mi; create database mi;"`
5. 从数据库转储还原mysql数据库： `mysql -u username -p password -A mi < /var/local/tmp/mysql-mi.sql`
6. 重新启动所有其他服务 `service servermanager start`

作者：*Aron Klein*

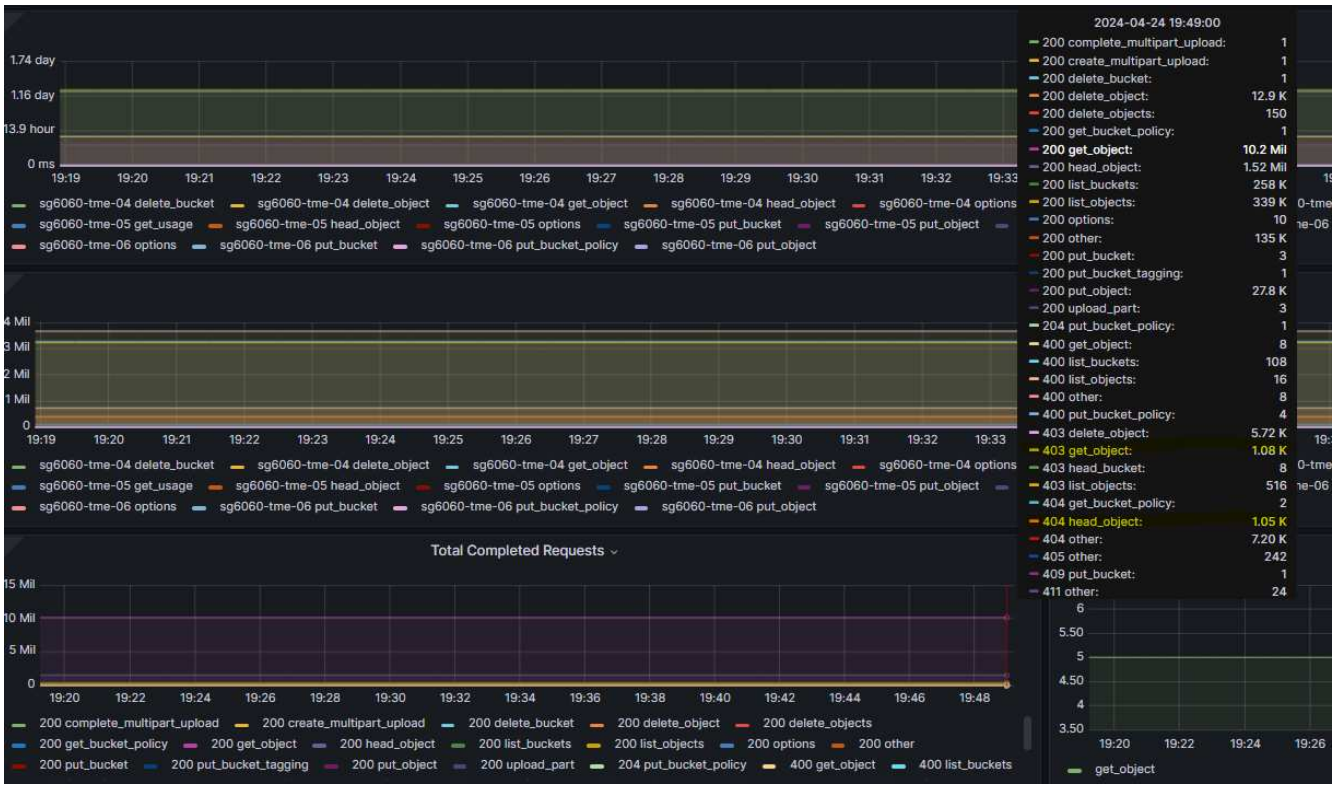
网格站点重新定位和站点范围网络更改操作步骤

本指南介绍了在多站点网格中进行StorageGRID站点重新定位的准备和操作步骤。您应全面了解此操作步骤、并提前做好规划、以确保流程顺畅、最大限度地减少对客户的中断。

如果需要更改整个网格的网格网络、请参见
"更改网格中所有节点的 IP 地址"。

站点重新定位前的注意事项

- 应在15天内完成站点移动并使所有节点联机、以避免重建cassandrebuild数据库。
  "将存储节点恢复到关闭状态超过 15 天"
- 如果活动策略中的任何ILM规则使用严格的写入行为、如果客户希望在站点重新定位期间继续将对象放入网格、请考虑将其更改为平衡或双重提交。
- 对于包含60个或更多驱动器的存储设备、切勿移动安装了磁盘驱动器的磁盘架。 在打包/移动之前、为每个磁盘驱动器贴上标签并将其从存储机箱中取出。
- 更改StorageGRID设备网格网络VLAN可以通过管理网络或客户端网络远程执行。 或者计划在重新定位之前或之后到现场执行更改。
- 检查客户应用程序是否正在使用HEAD或在放置前获取不存在的对象。如果是、请将存储分段一致性更改为强站点、以避免出现HTTP 500错误。 如果不确定，请查看S3概述Grafana图表*网格管理器>支持>指标*，将鼠标悬停在"已完成请求总数"图表上。 如果404 GET对象或404 HEAD对象的计数非常高、则一个或多个应用程序可能正在使用HEAD或GET不存在对象。计数会累计、将鼠标悬停在不同的时间线上可查看差异。



操作步骤以在站点重新定位之前更改网格**IP**地址

步骤

1. 如果新位置要使用新的网格网络子网、
   "将子网添加到网格网络子网列表"
2. 登录到主管理节点、使用change-ip进行网格IP更改、必须*暂存*更改、然后才能关闭节点进行重新定位。
   a. 选择2、然后选择1以更改网格IP

```
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. 选择5以显示更改

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

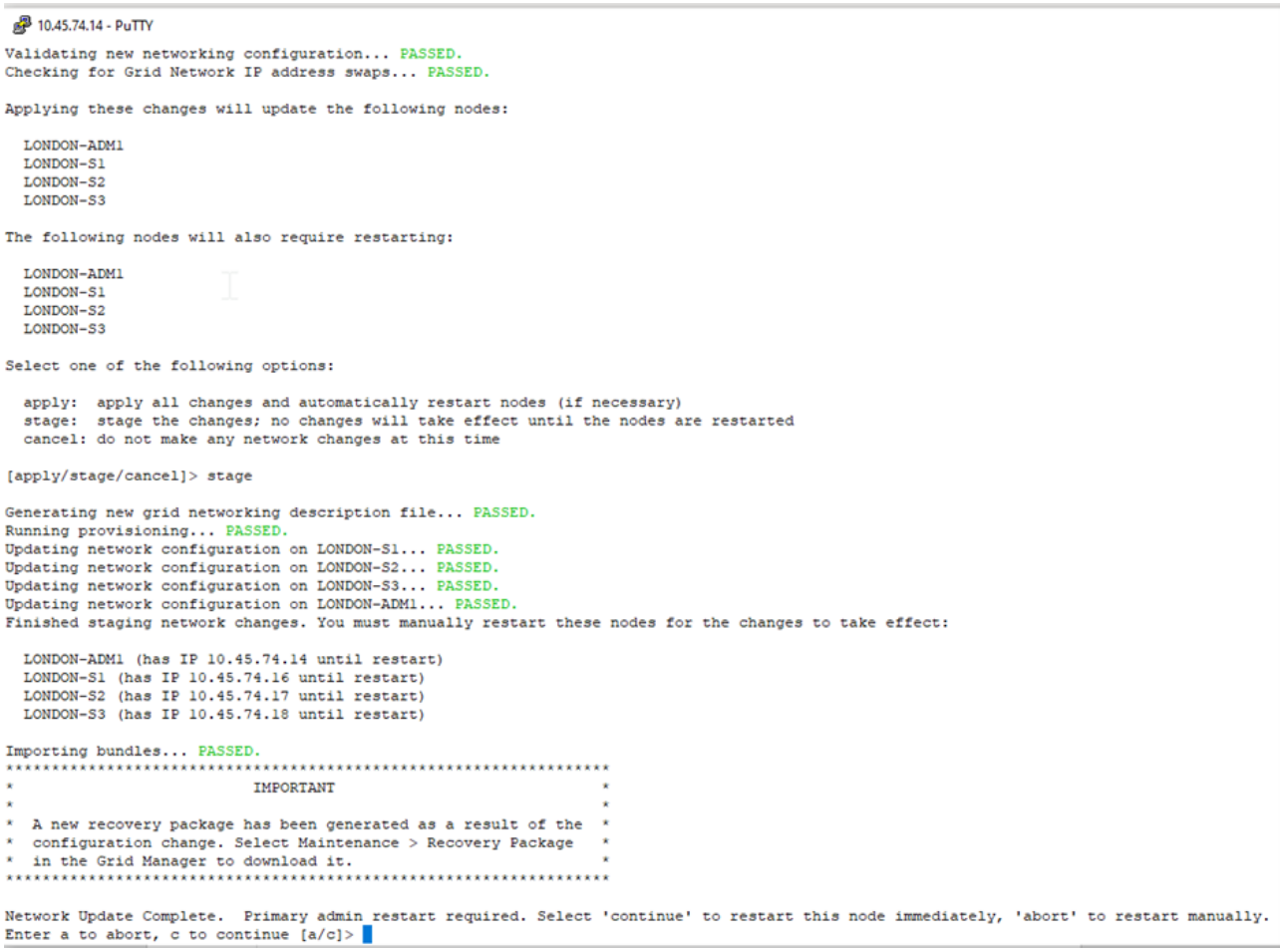
c. 选择10以验证并应用更改。

```
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
```

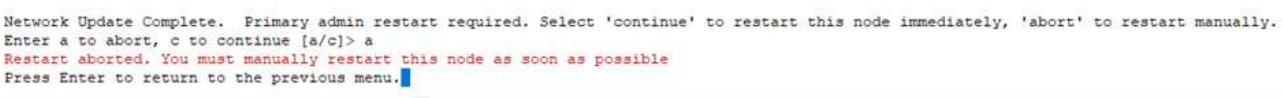
d. 必须在此步骤中选择*阶段*。

```
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. 如果上述更改中包括主管理节点，请输入*'A'手动重新启动主管理节点*



f. 按ENTER键返回上一菜单并退出change-ip界面。



3. 从Grid Manager中下载新的恢复软件包。网格管理器>*维护*>*恢复包*
4. 如果StorageGRID设备需要更改VLAN、请参见一节 设备VLAN更改。
5. 关闭站点上的所有节点和/或设备、根据需要标记/移除磁盘驱动器、然后卸载、打包和移动。
6. 如果您计划更改管理网络IP和/或客户端VLAN和IP地址、则可以在重新定位后执行更改。

设备**VLAN**更改

以下操作步骤假定您可以远程访问StorageGRID设备的管理或客户端网络以远程执行更改。

步骤

1. 在关闭设备之前，
"将设备置于维护模式"。
2. 使用浏览器访问StorageGRID设备安装程序图形用户界面 https://<admin-or-client-network-ip>:8443。 设备启动至维护模式后、无法使用Grid IP作为新的Grid IP。
3. 更改网格网络的VLAN。 如果您正在通过客户端网络访问设备、则此时无法更改客户端VLAN、可以在移动后进行更改。

4. 通过SSH连接到设备并使用"shutdoown -h now "关闭节点
5. 在新站点上准备好设备后、使用访问StorageGRID设备安装程序图形用户界面 https://<grid-network-ip>:8443。 在GUI中使用Ping/nmap工具确认存储处于最佳状态、并确认与其他网格节点的网络连接。
6. 如果计划更改客户端网络IP、则可以在此阶段更改客户端VLAN。 在稍后使用change-ip工具更新客户端网络IP之前、客户端网络尚未准备就绪。
7. 退出维护模式：在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。
8. 在所有节点均已启动且网格未显示任何连接问题描述后、根据需要使用change-ip更新设备管理网络和客户端网络。

将基于对象的存储从**ONTAP S3**迁移到**StorageGRID**

通过将基于对象的存储从**ONTAP S3**无缝迁移到**StorageGRID**来实现企业级**S3**

通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

迁移演示

本演示将用户和分段从ONTAP S3迁移到StorageGRID。

通过将基于对象的存储从**ONTAP S3**无缝迁移到**StorageGRID**来实现企业级**S3**

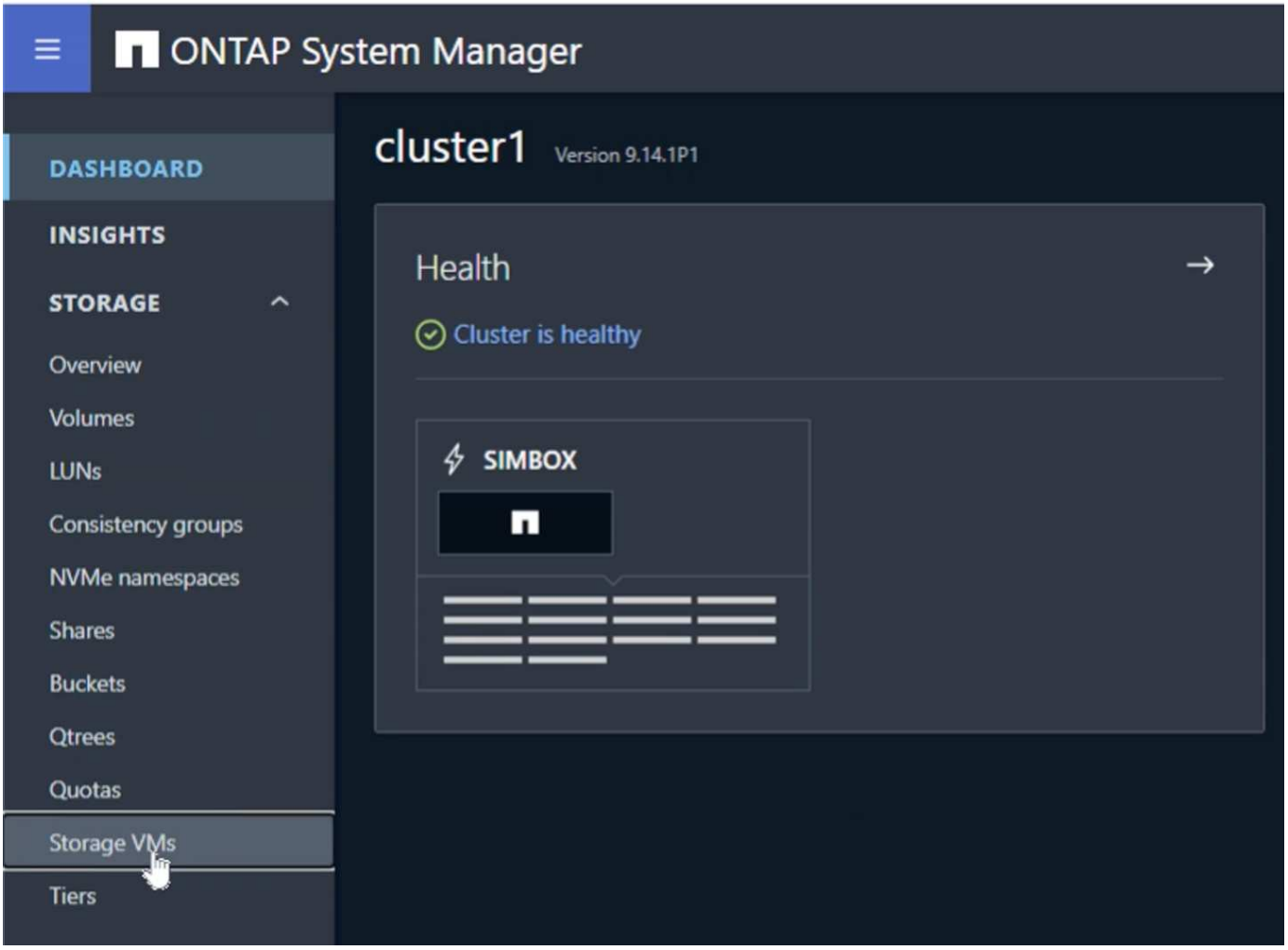
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

正在准备**ONTAP**

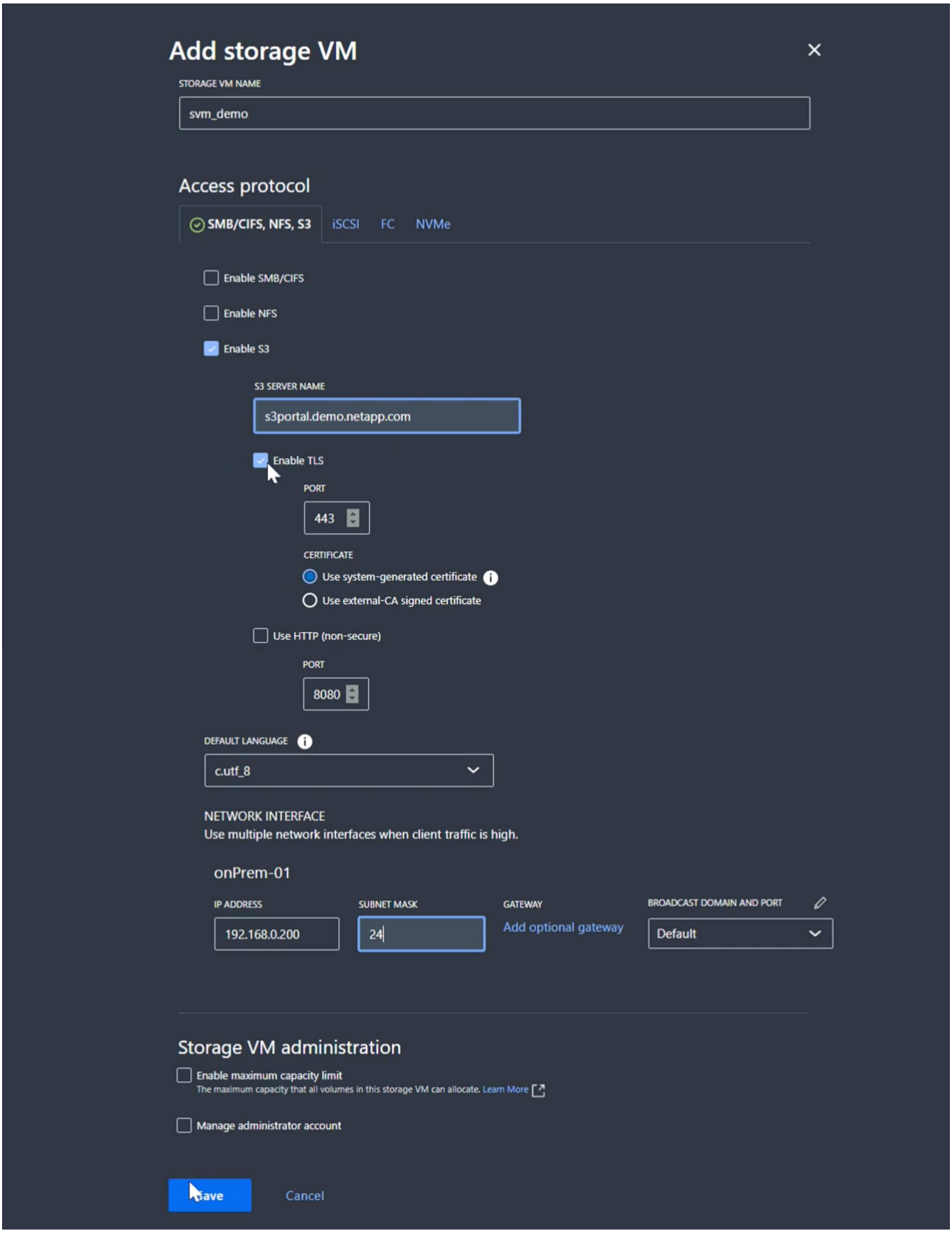
为了便于演示、我们将创建SVM对象存储服务器、用户、组、组策略和分段。

创建**Storage Virtual Machine**

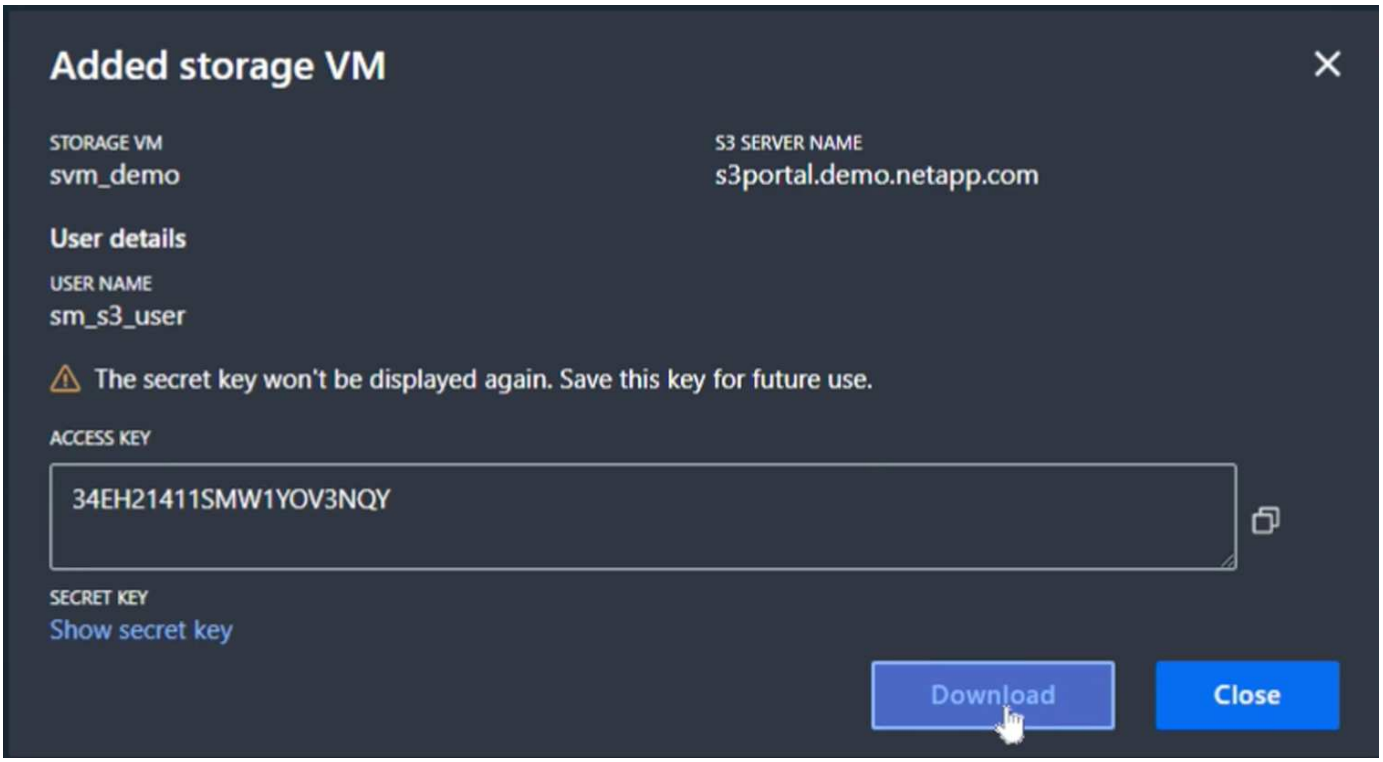
在ONTAP系统管理器中、导航到Storage VM并添加新的Storage VM。



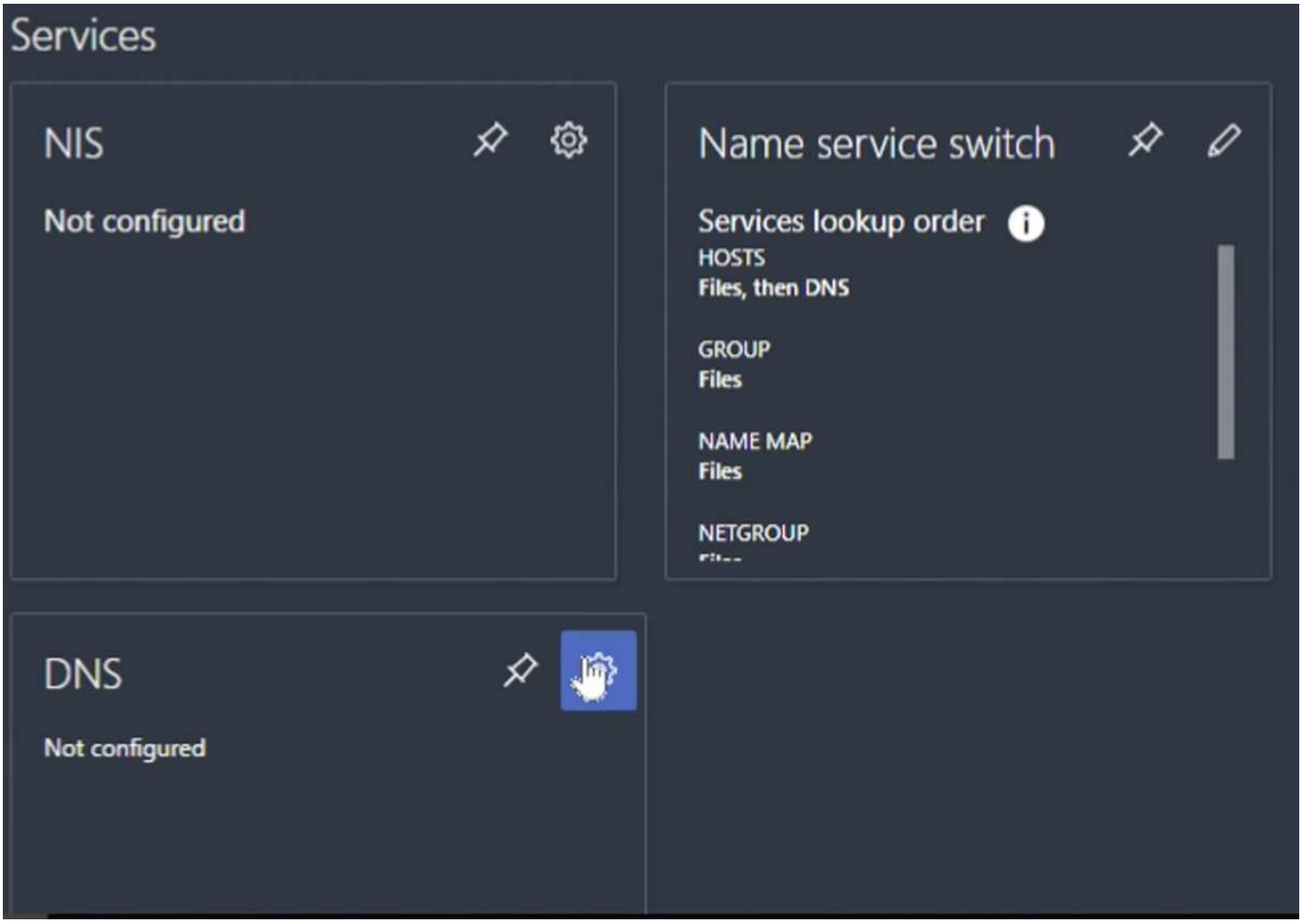
选中"启用S3"和"启用TLS"复选框并配置HTTP (S)端口。如果您的环境未使用默认值或不需要、请定义IP、子网掩码并定义网关和广播域。



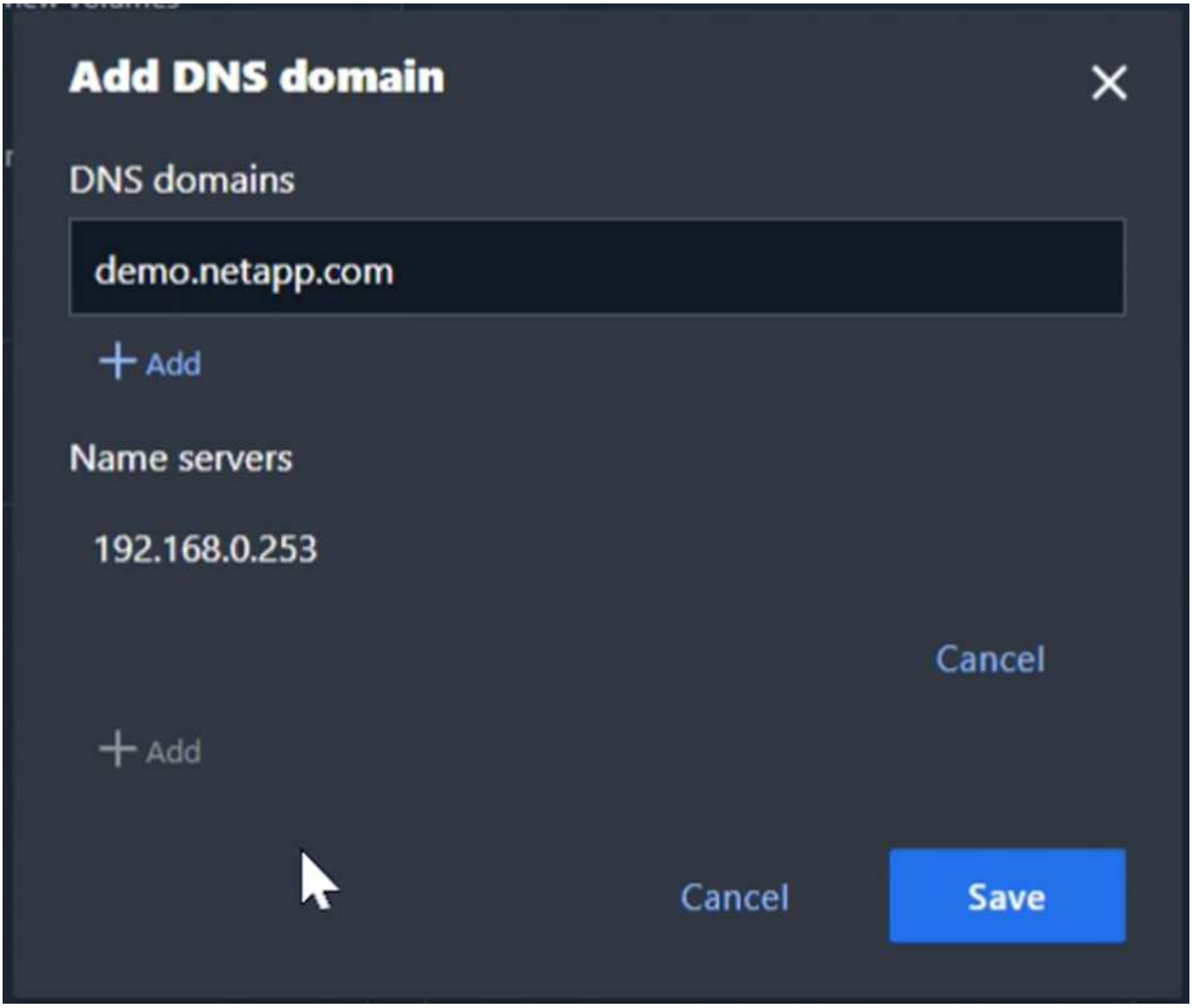
在创建SVM过程中、将创建用户。下载此用户的S3密钥并关闭窗口。



创建SVM后、编辑SVM并添加DNS设置。

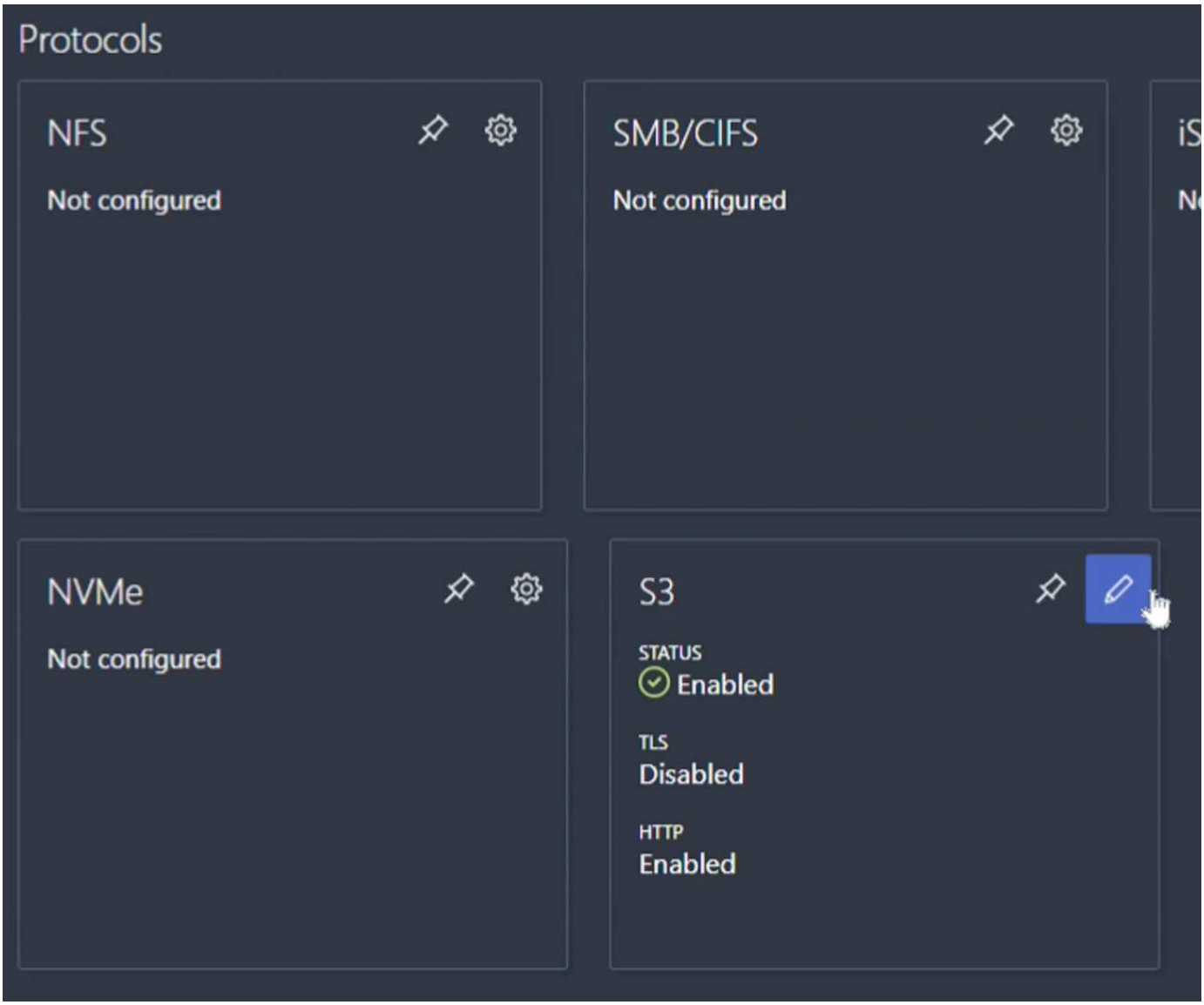


定义DNS名称和IP。

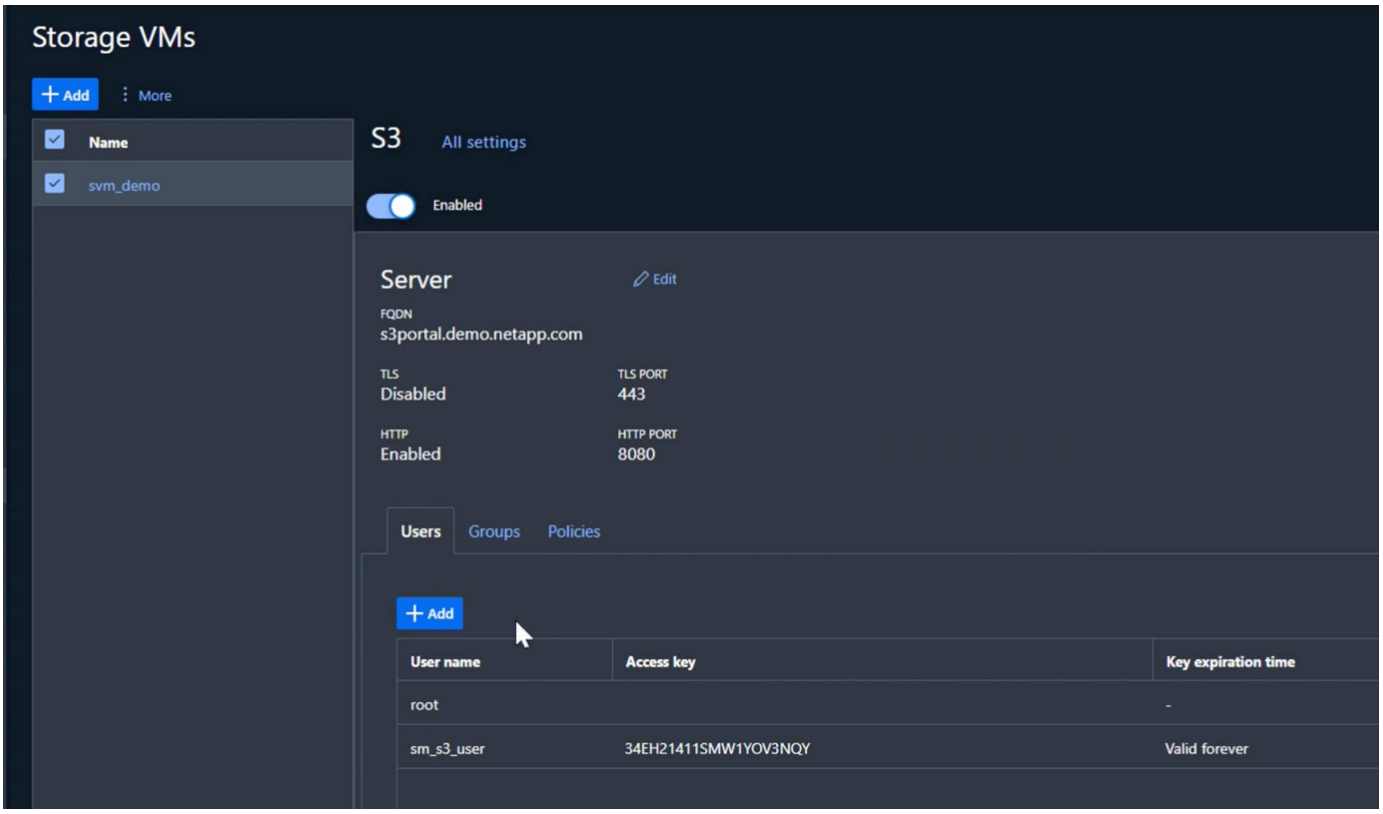


创建**SVM S3**用户

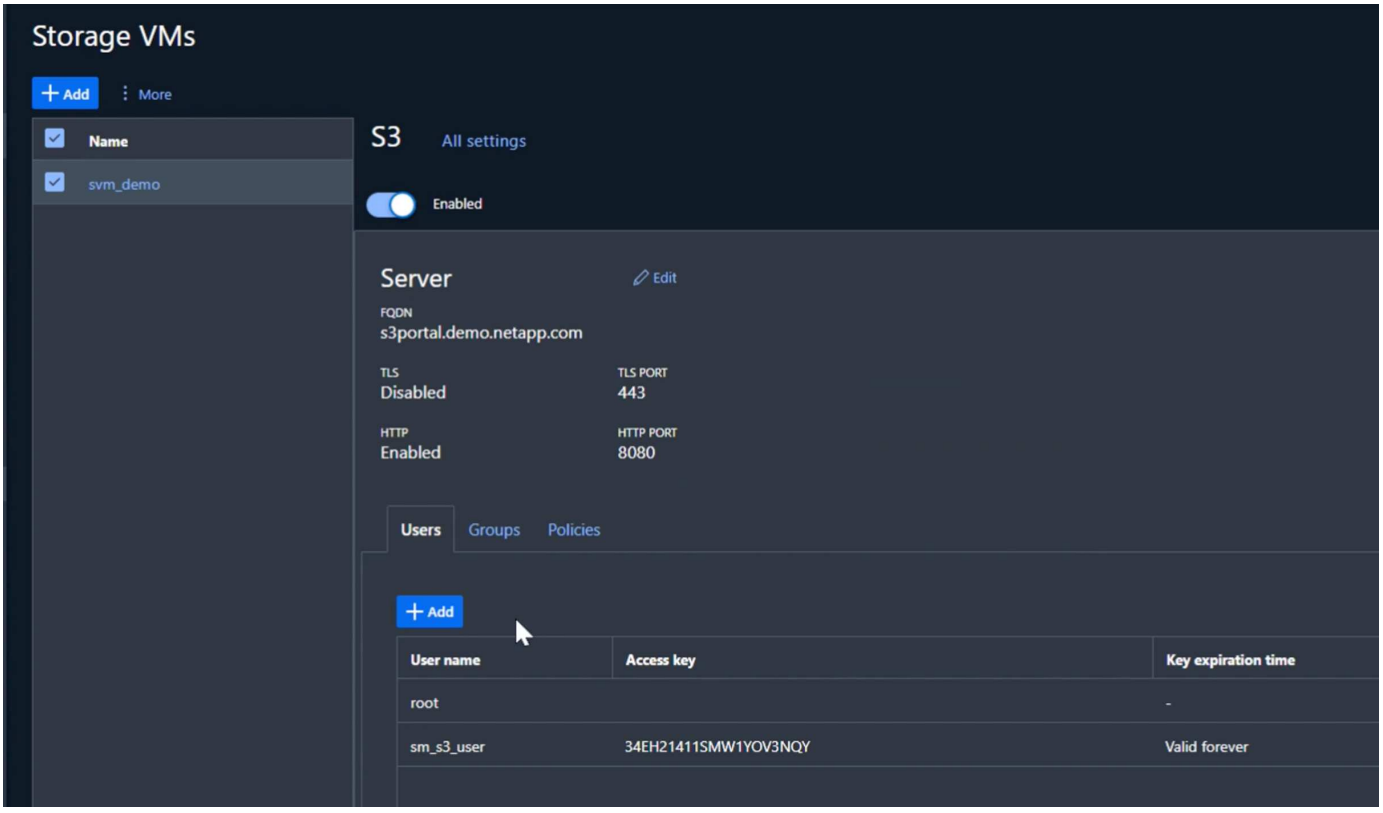
现在、我们可以配置S3用户和组。编辑S3设置。


Protocols
NFS
Not configured
SMB/CIFS
Not configured
NVMe
Not configured
S3
STATUS
Enabled
TLS
Disabled
HTTP
Enabled

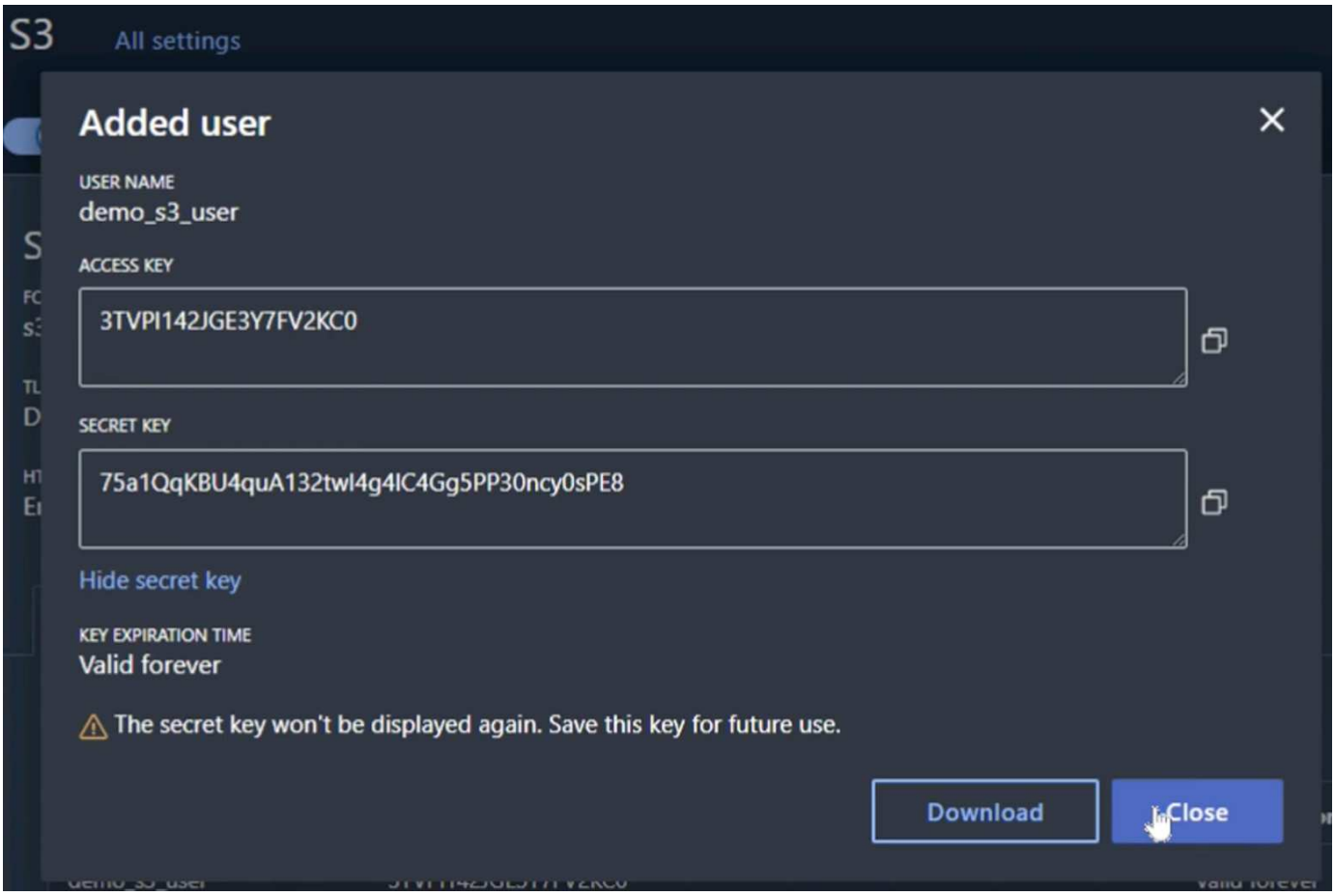
添加新用户。



输入用户名和密钥到期日期。

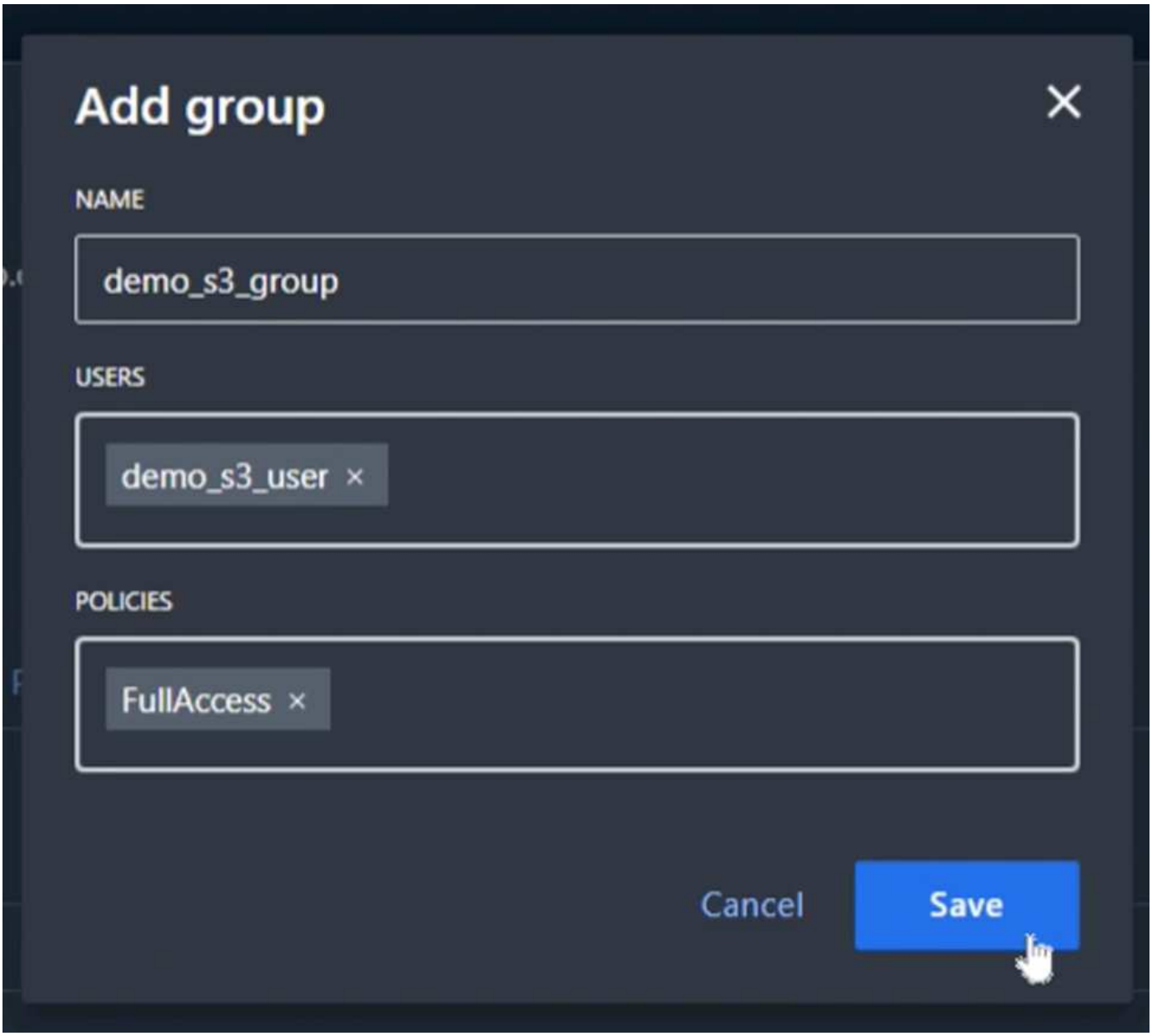


为新用户下载S3密钥。



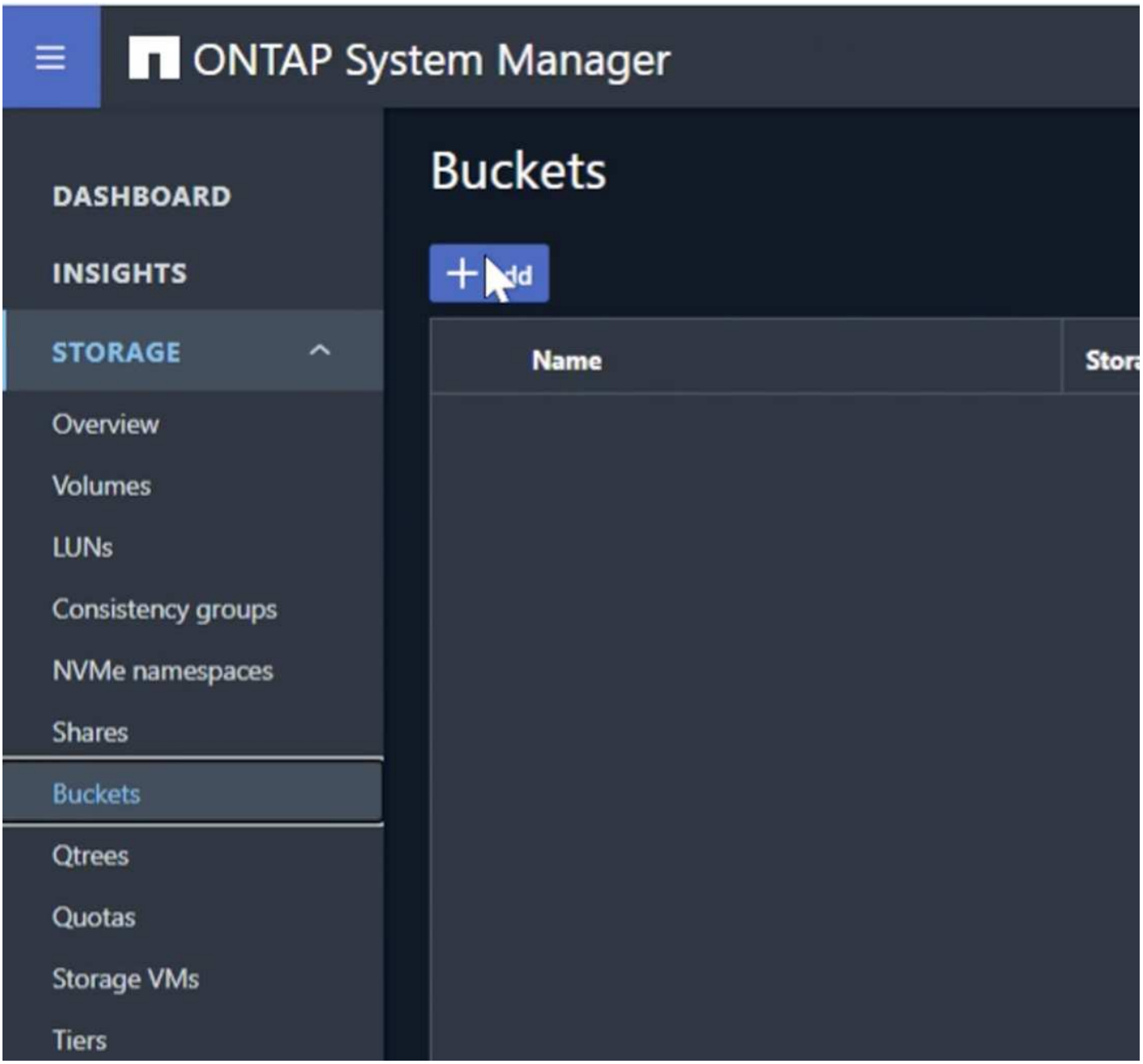
创建**SVM S3**组

在SVM S3设置的组选项卡上、添加一个具有上述创建用户和FullAccess权限的新组。

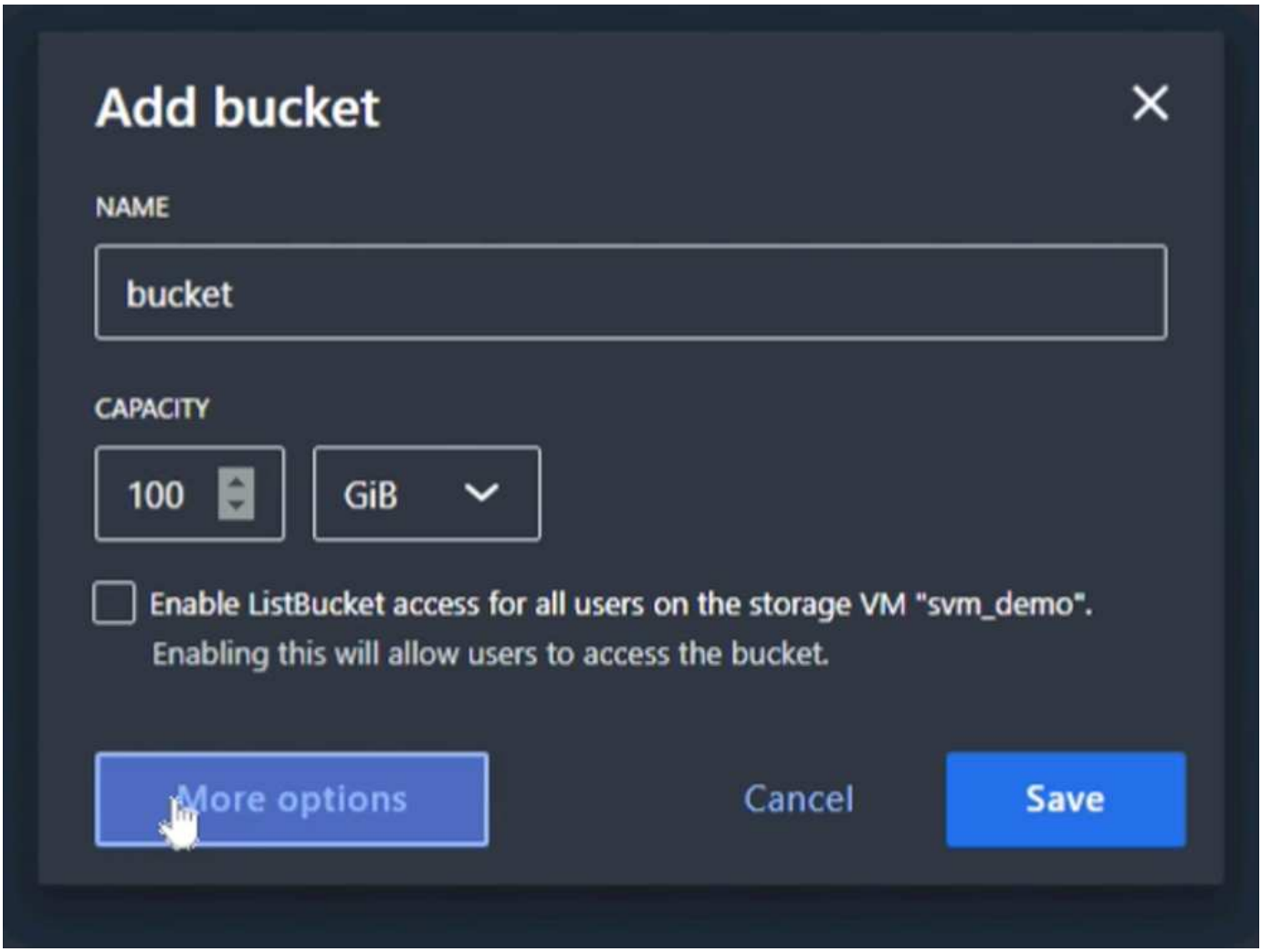


创建**SVM S3**存储分段

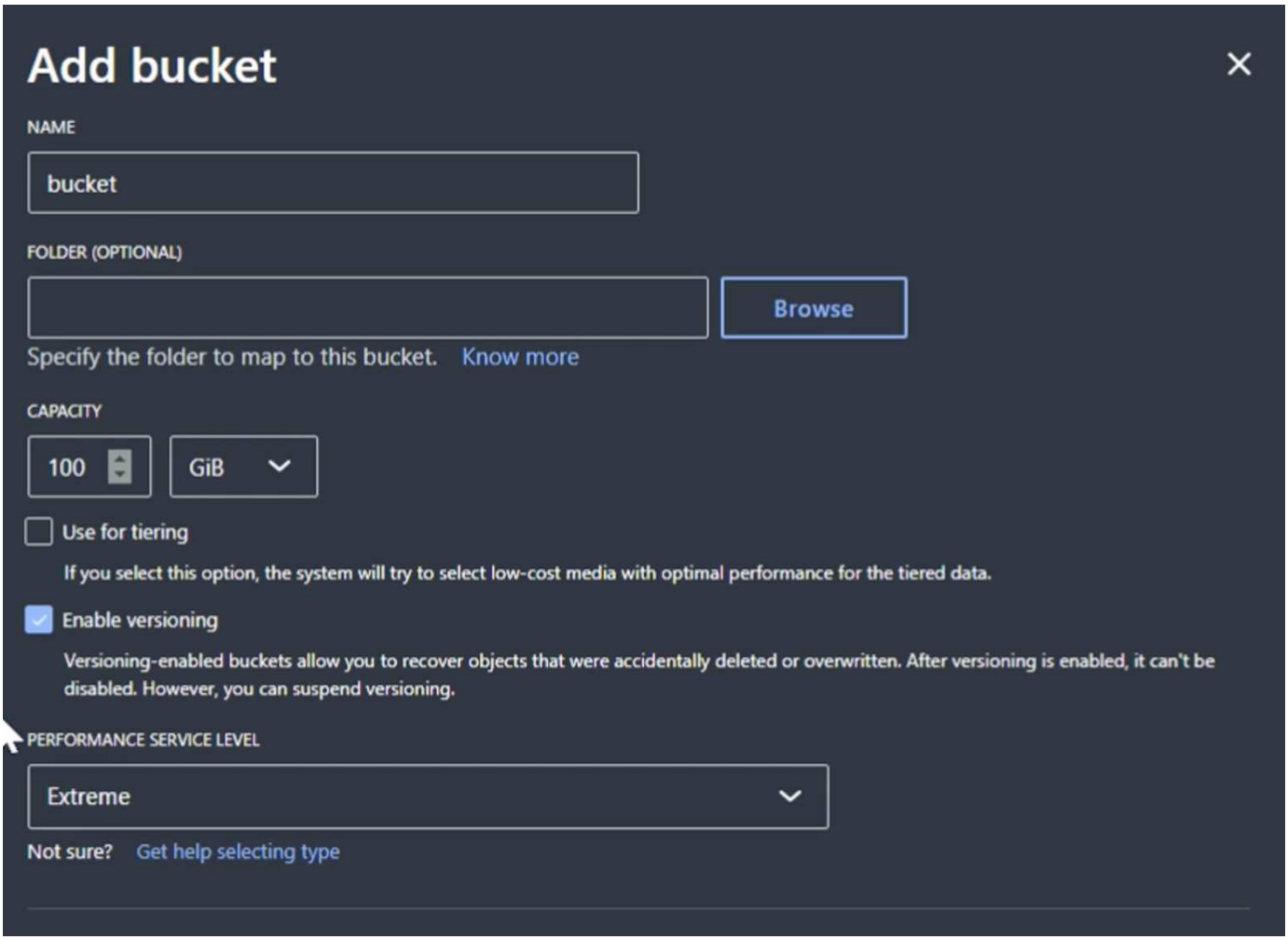
导航到"存储分段"部分、然后单击"+Add"按钮。



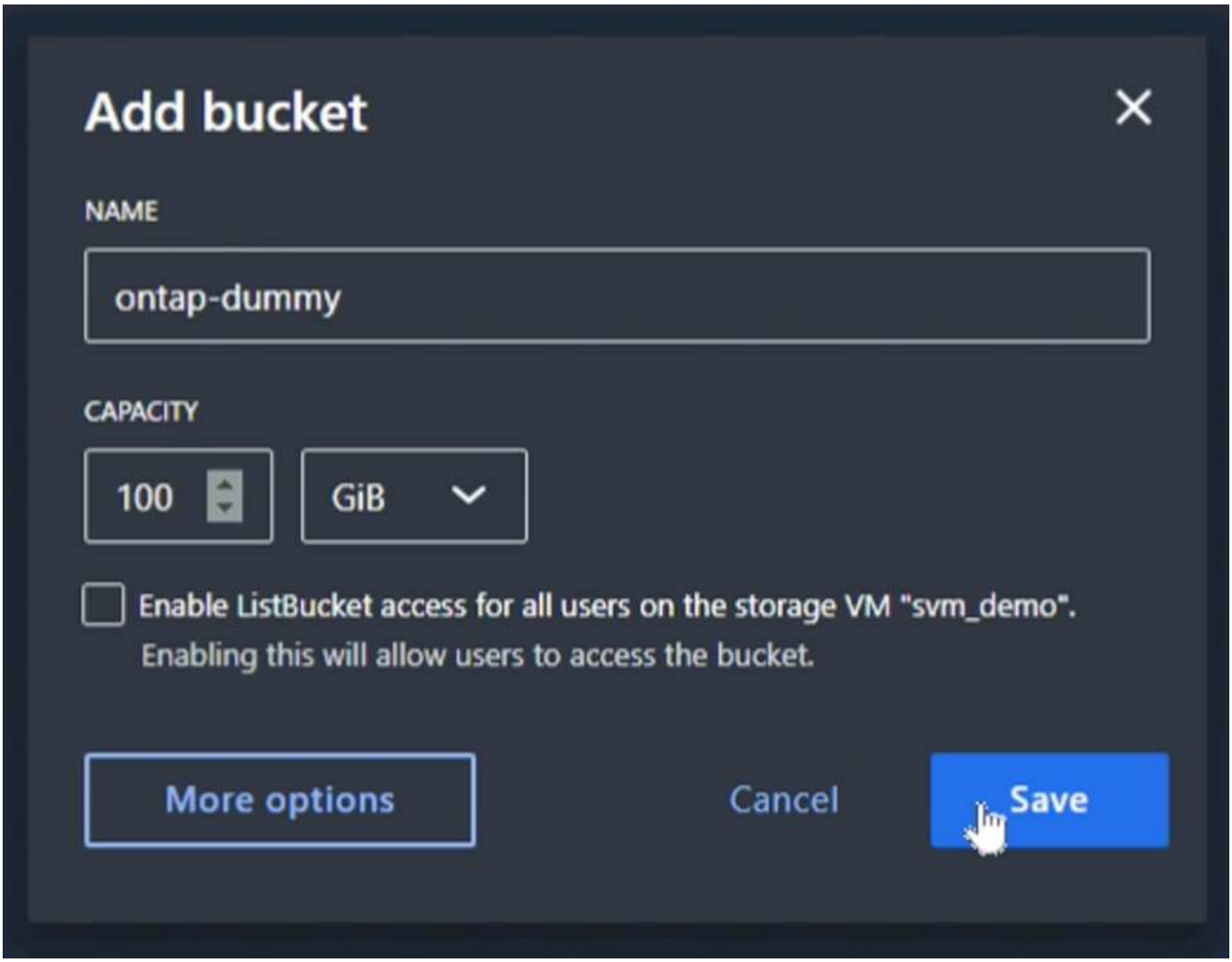
输入名称、容量并取消选中"Enable ListBucket"复选框、然后单击"更多选项"按钮。



在"更多选项"部分中、选中"启用版本控制"复选框、然后单击"保存"按钮。



重复此过程、并在未启用版本控制的情况下创建第二个存储分段。输入一个名称、与存储分段1的容量相同、并取消选中"Enable ListBucket"复选框、然后单击"Save (保存)"按钮。



作者：拉斐尔·吉德斯和阿伦·克莱因

通过将基于对象的存储从**ONTAP S3**无缝迁移到**StorageGRID**来实现企业级**S3**

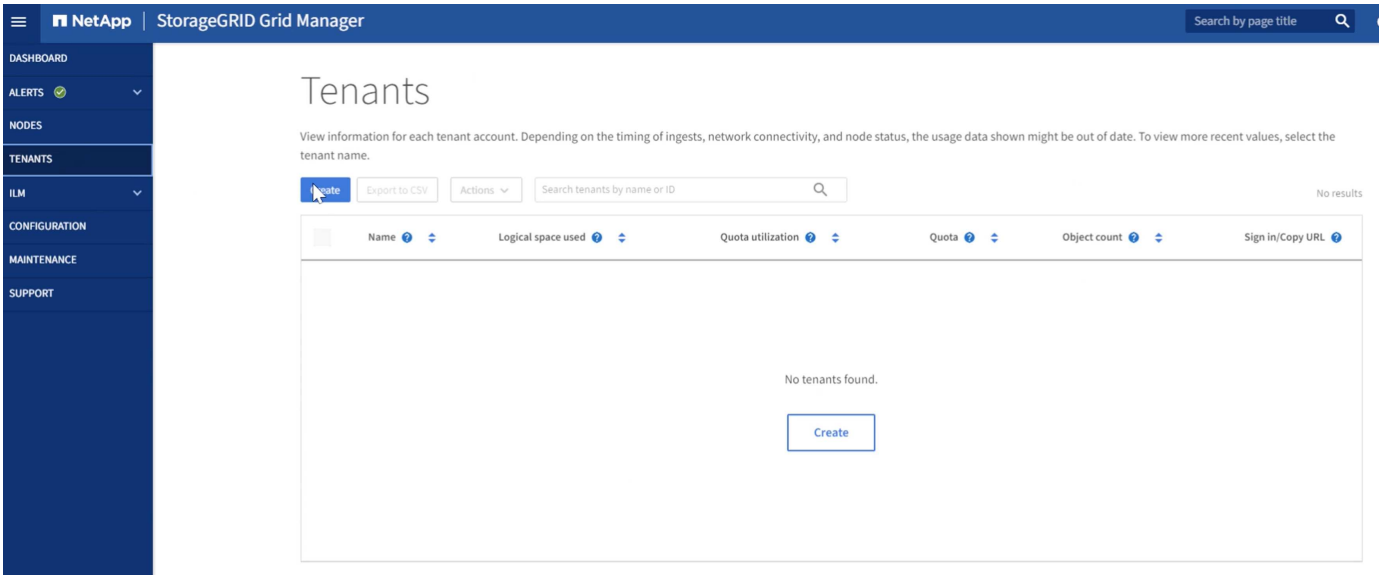
通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

正在准备 **StorageGRID**

继续配置此演示、我们将创建租户、用户、安全组、组策略和存储分段。

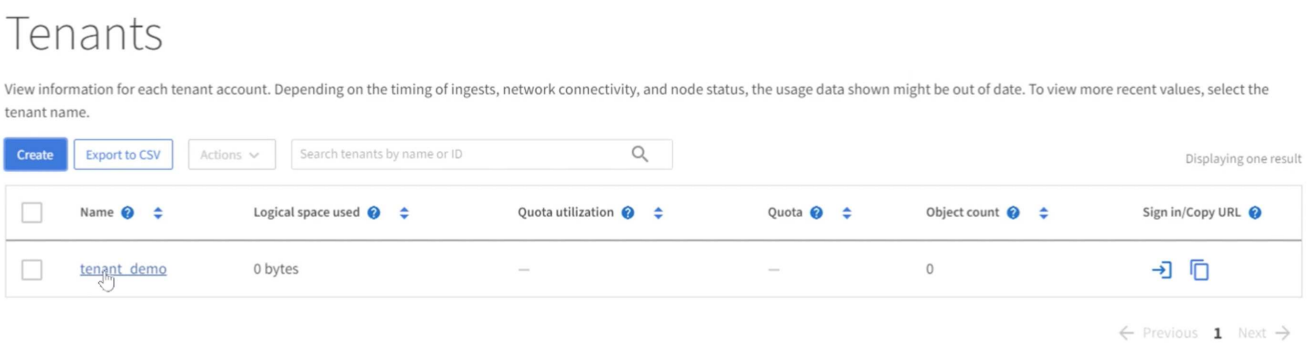
创建租户

导航到"租 户"选项卡、然后单击"创建"按钮

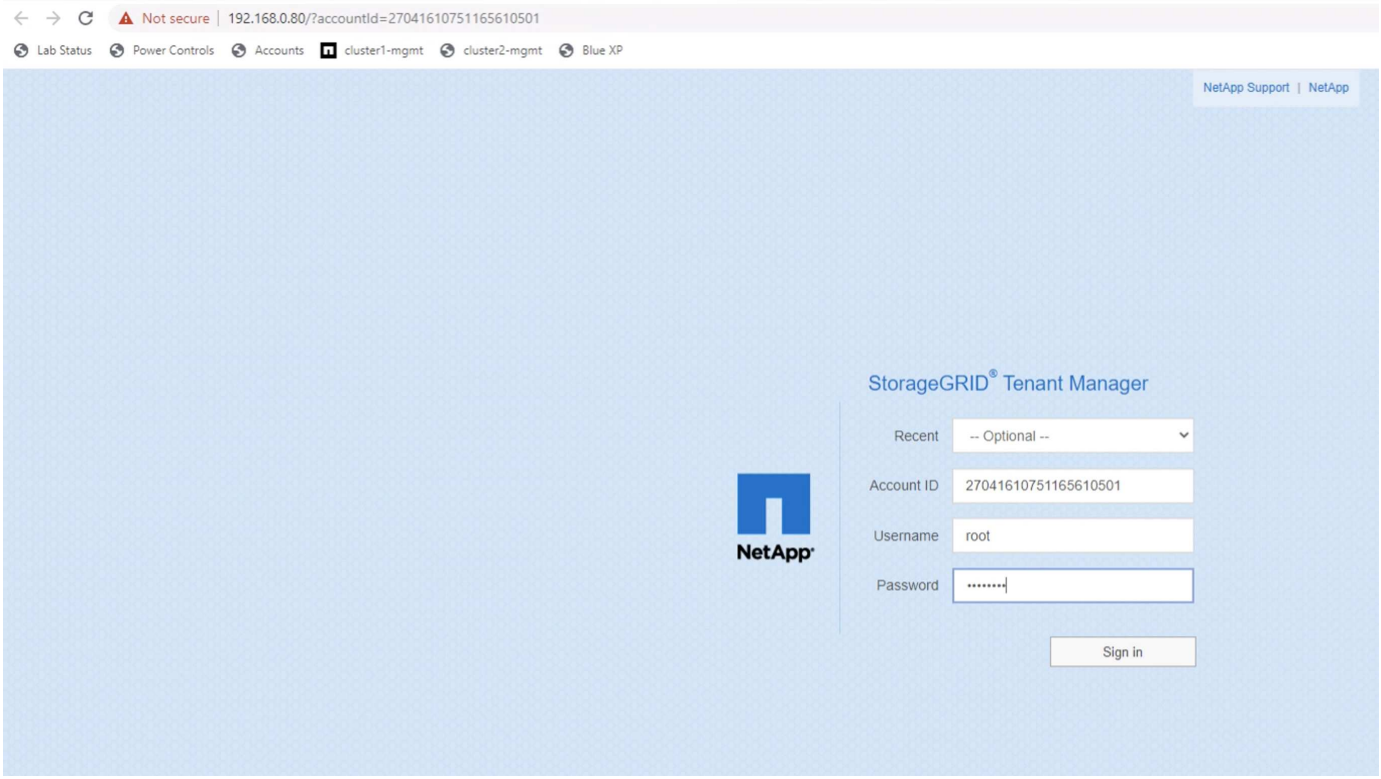


填写提供租户名称的租户的详细信息、选择S3作为客户端类型、不需要配额。无需选择平台服务或允许S3选择。如果选择、您可以选择使用自己的身份源。设置root密码、然后单击完成按钮。

单击租户名称可查看租户详细信息。稍后您将需要租户**ID**、因此请将其复制。单击登录按钮。此操作将转到租户门户登录页面。保存此URL以供将来使用。

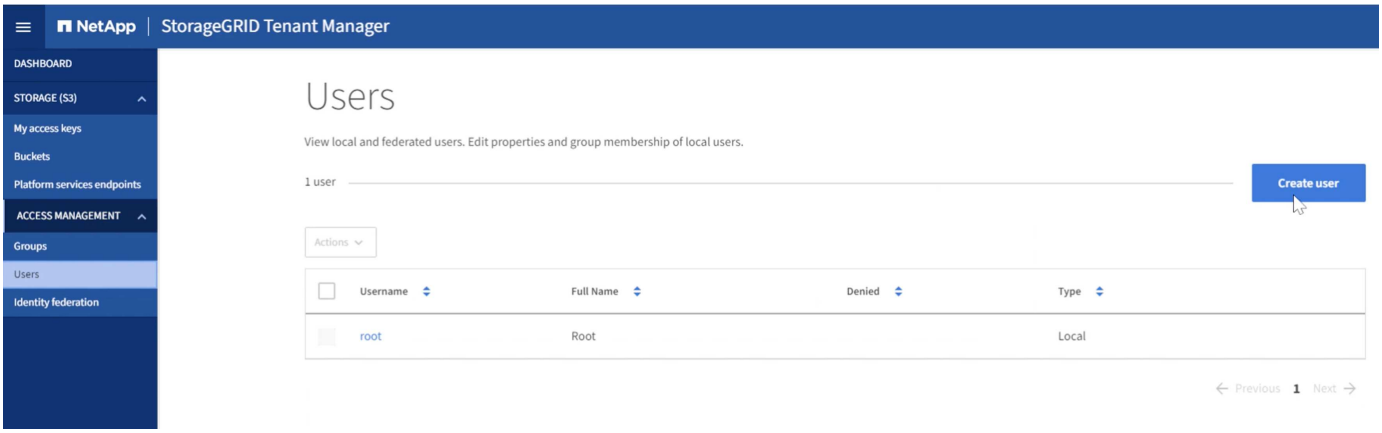


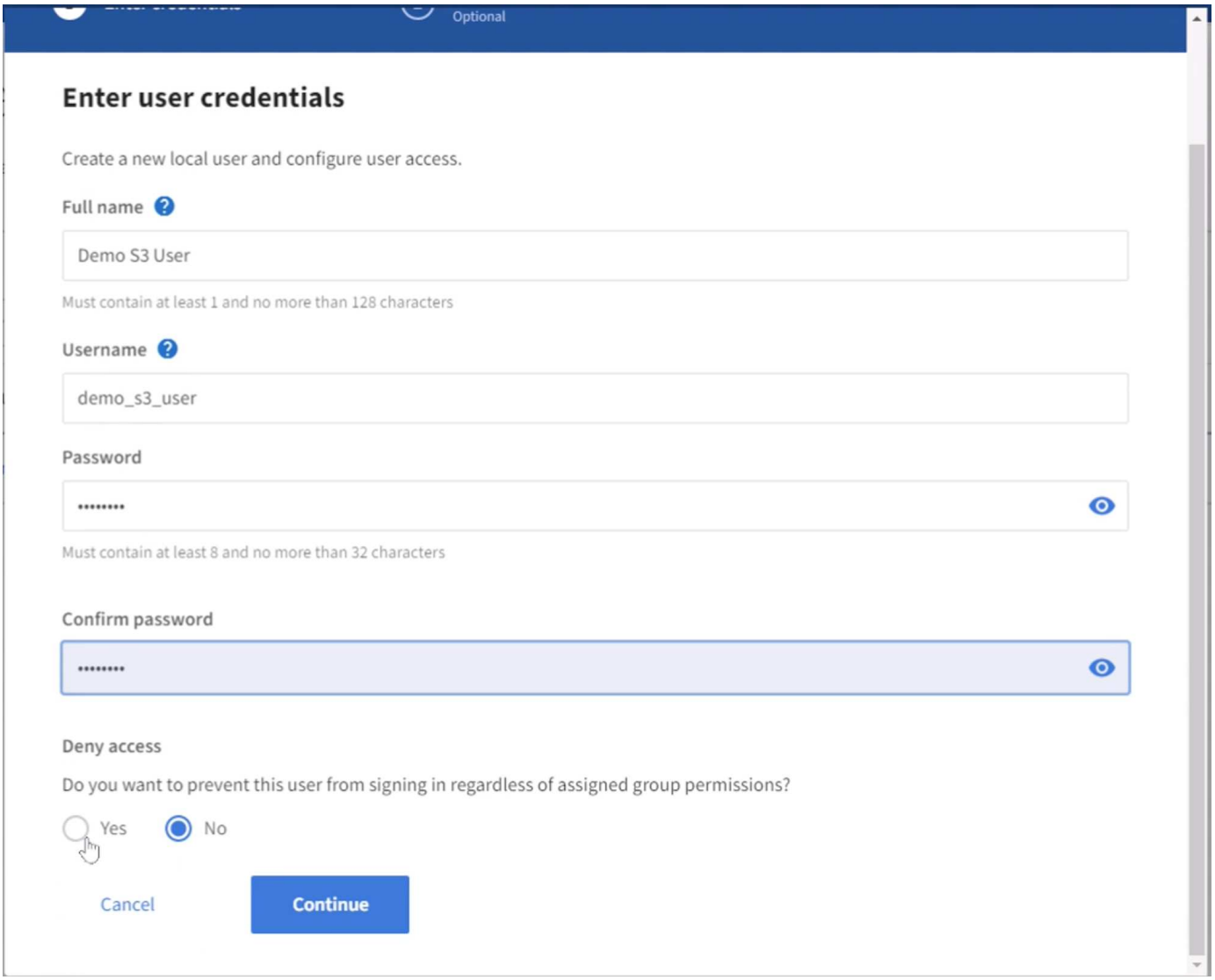
此操作将转到租户门户登录页面。保存此URL以供将来使用、然后输入root用户凭据。



创建用户

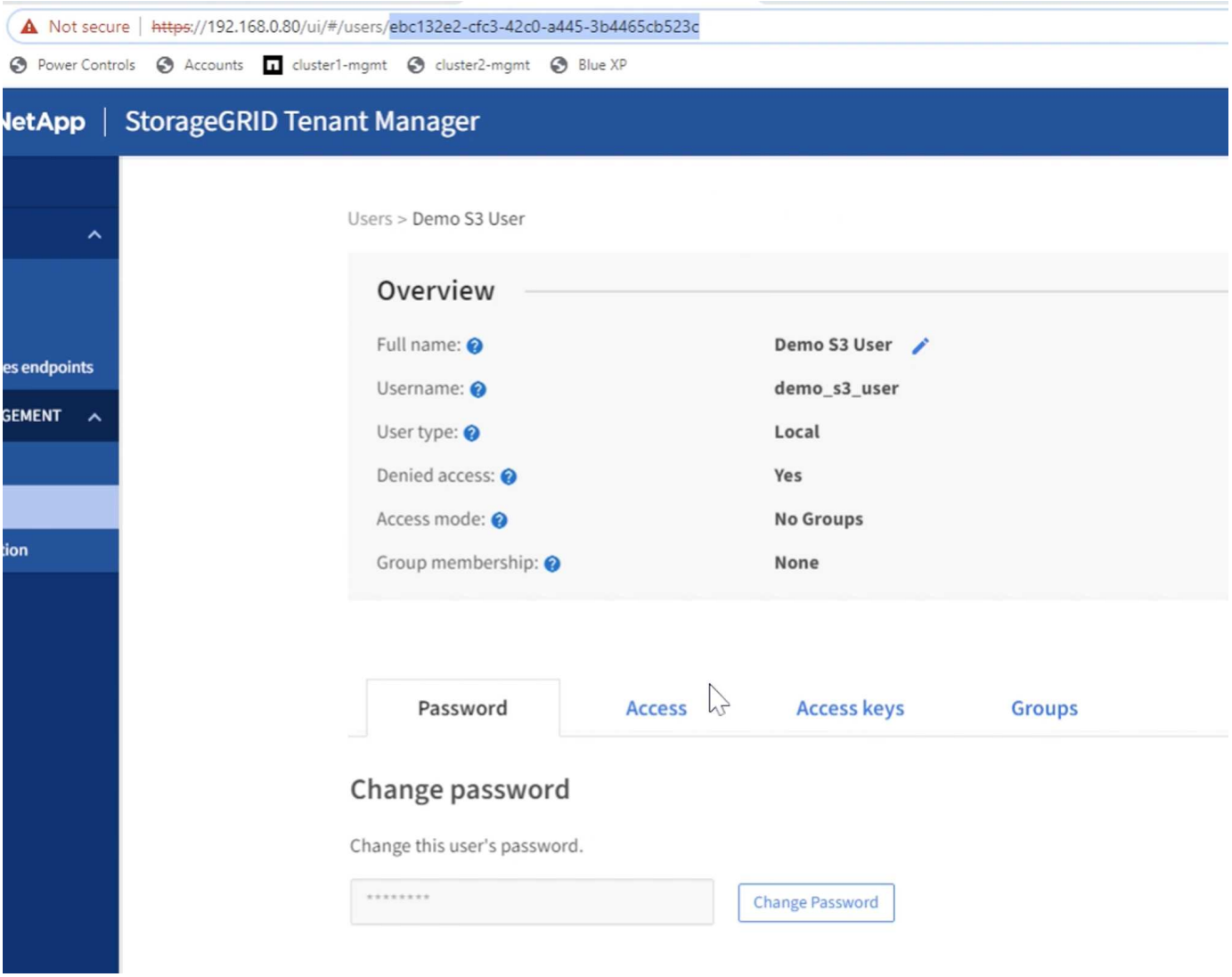
导航到用户选项卡并创建新用户。



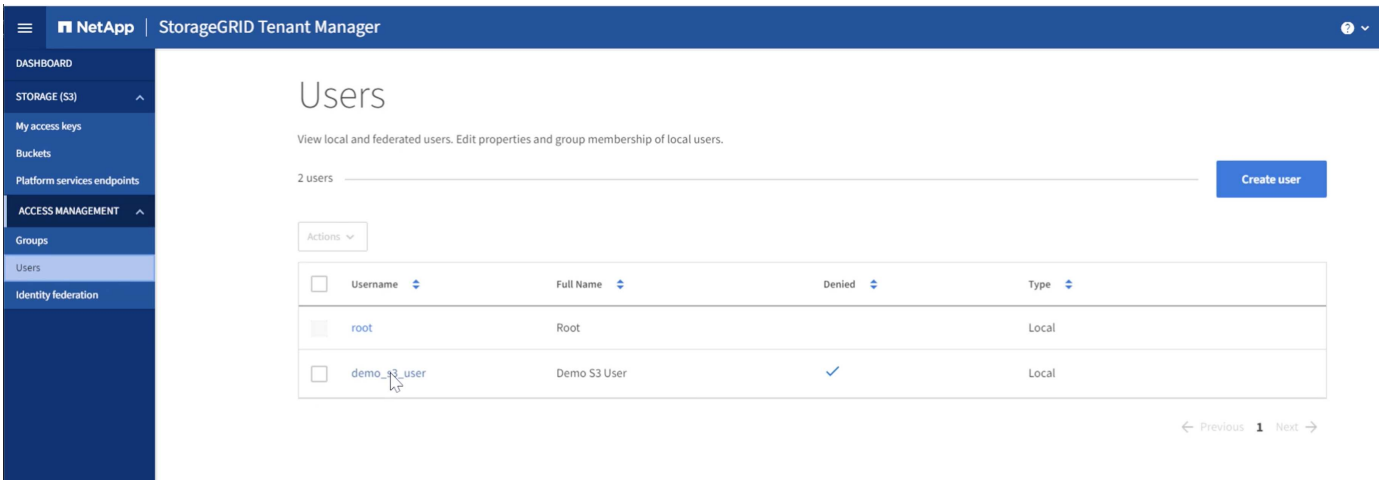


创建新用户后、单击用户名以打开该用户的详细信息。

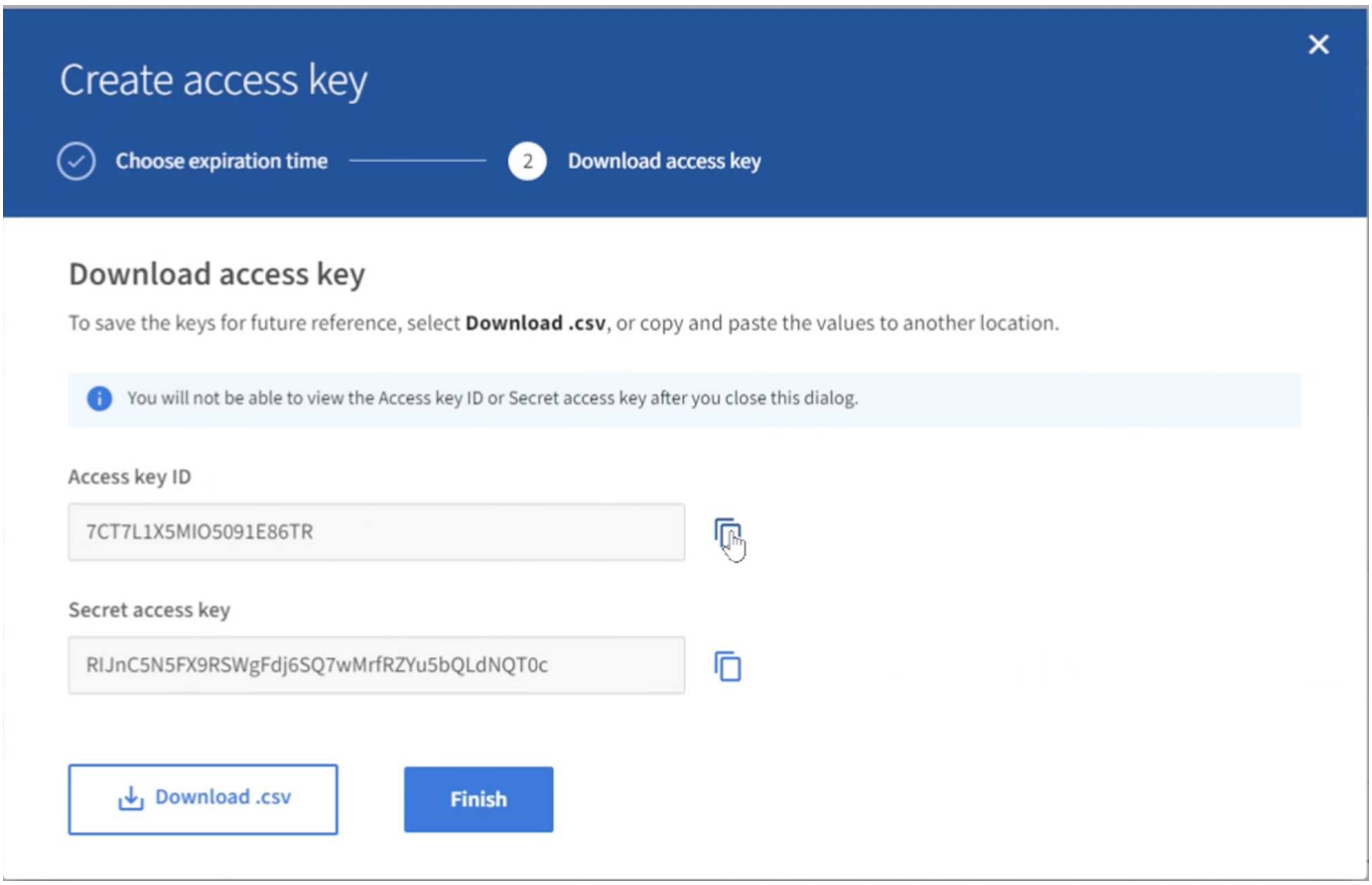
复制URL中的用户ID、以供日后使用。



要创建S3密钥、请单击用户名。

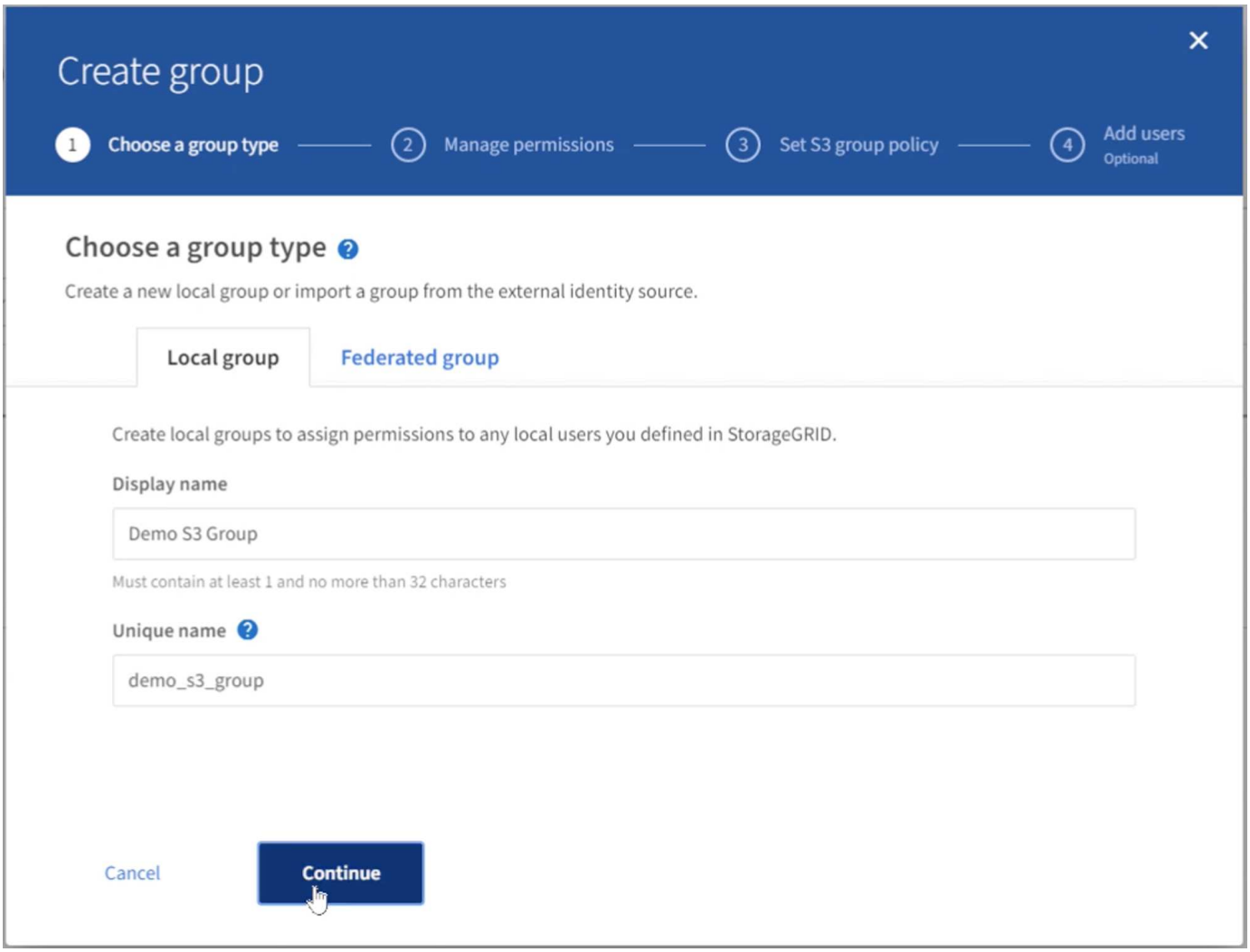


选择"Access keys"(访问密钥)选项卡、然后单击"Create Key"(创建密钥)按钮。无需设置到期时间。下载S3密钥、因为关闭窗口后将无法再次检索这些密钥。

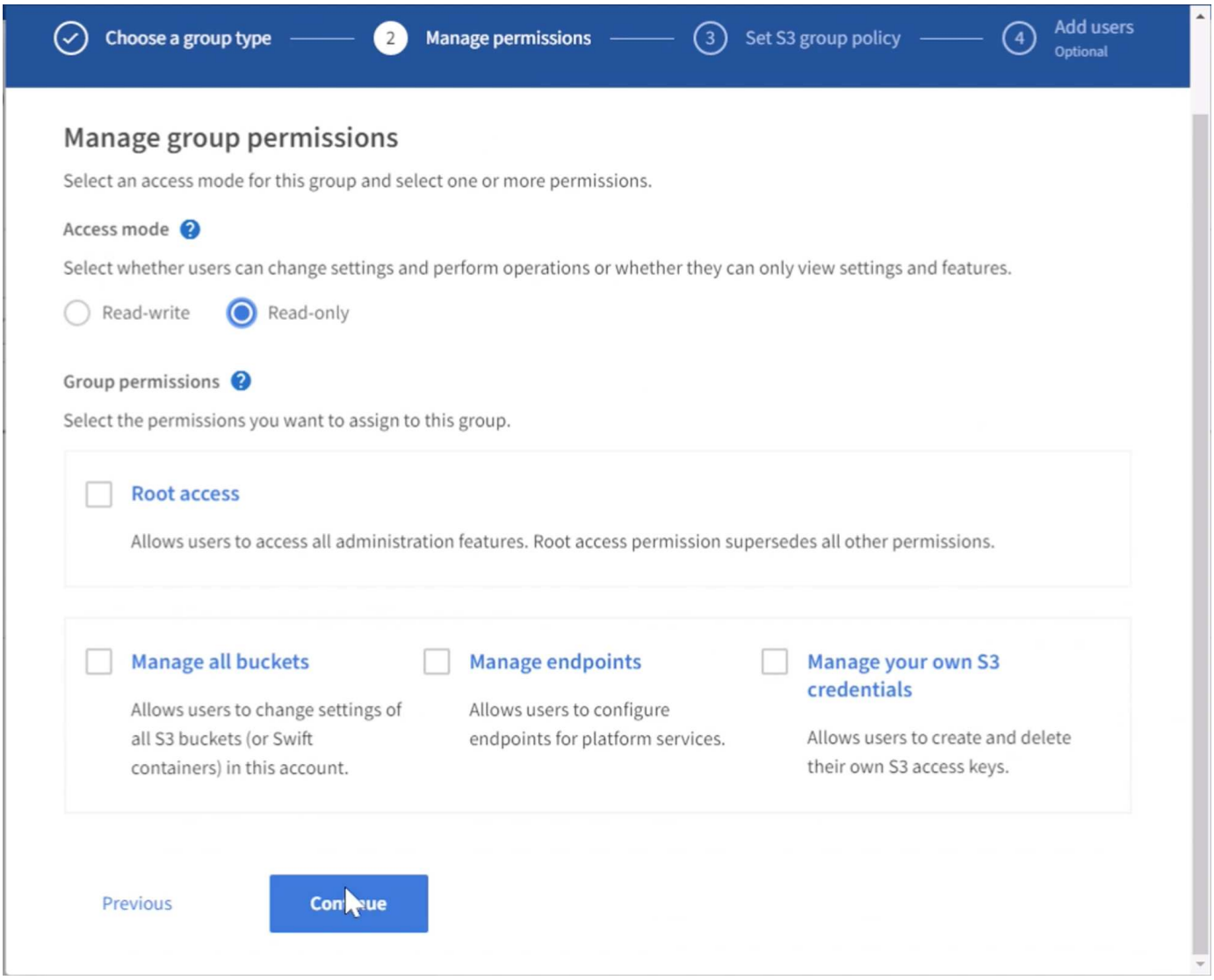


创建安全组

现在转到组页面并创建新组。

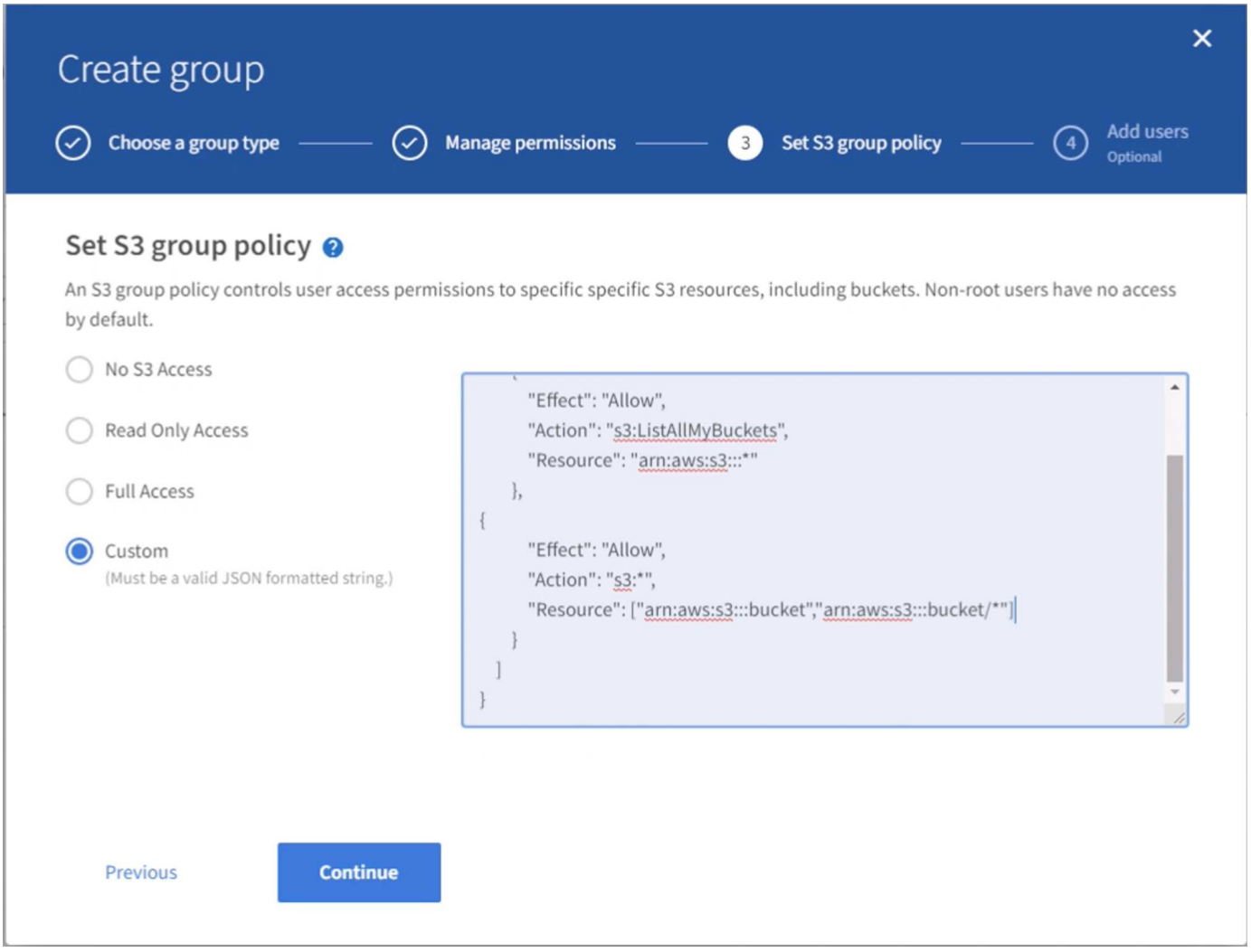


将组权限设置为只读。这是租户UI权限、而不是S3权限。

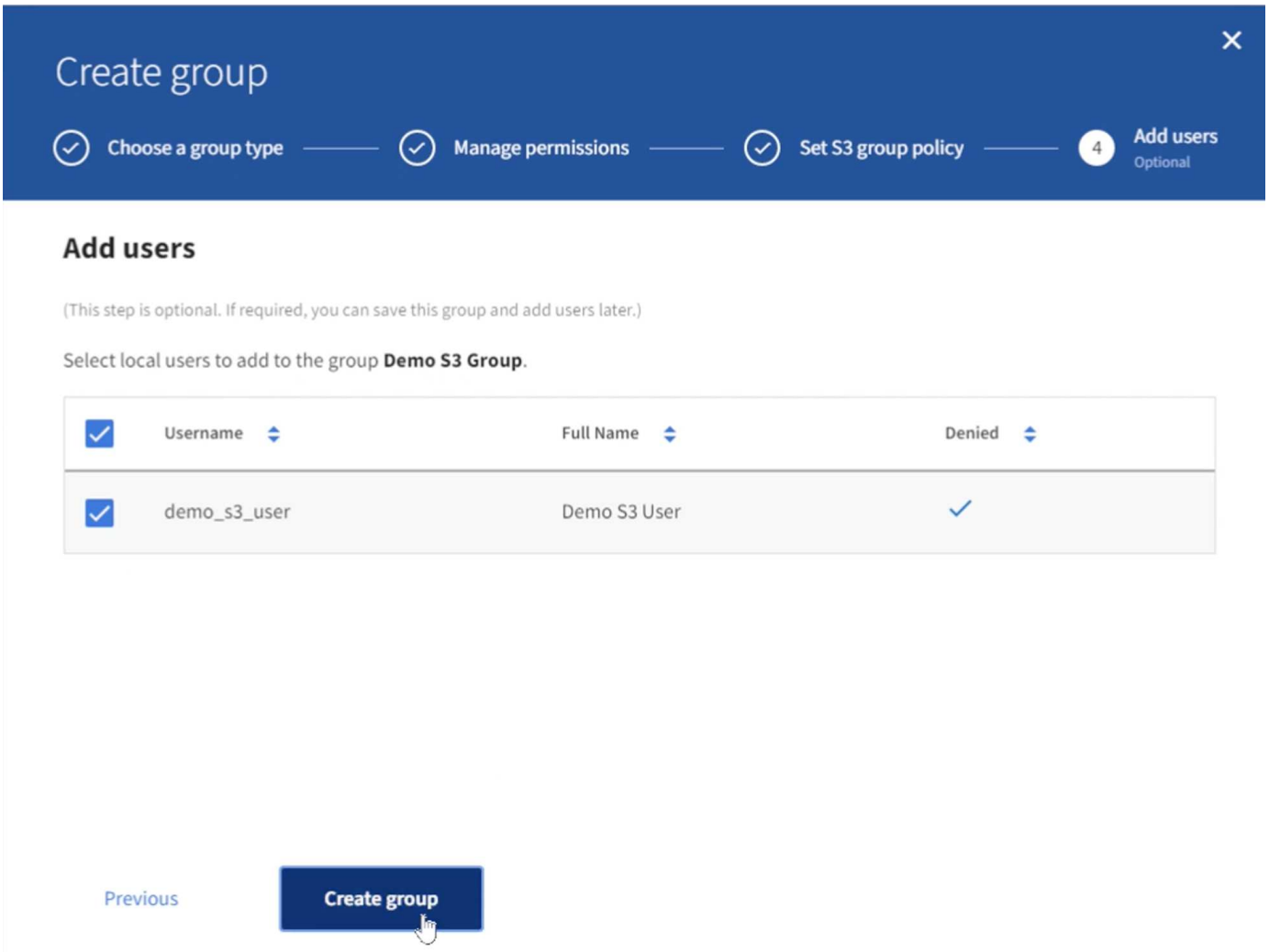


S3权限通过组策略(IAM策略)进行控制。将组策略设置为自定义、然后将json策略粘贴到框中。此策略将允许此组的用户列出租户的分段、并在名为"分段"的分段中执行任何S3操作、或者在名为"分段"的分段中执行子文件夹。

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

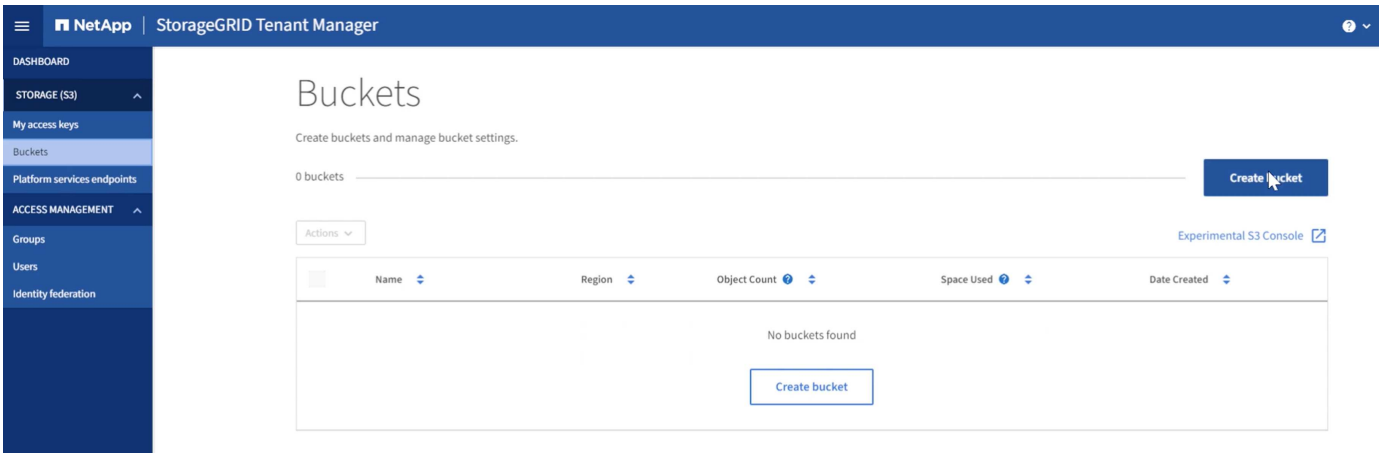


最后、将用户添加到组中并完成操作。

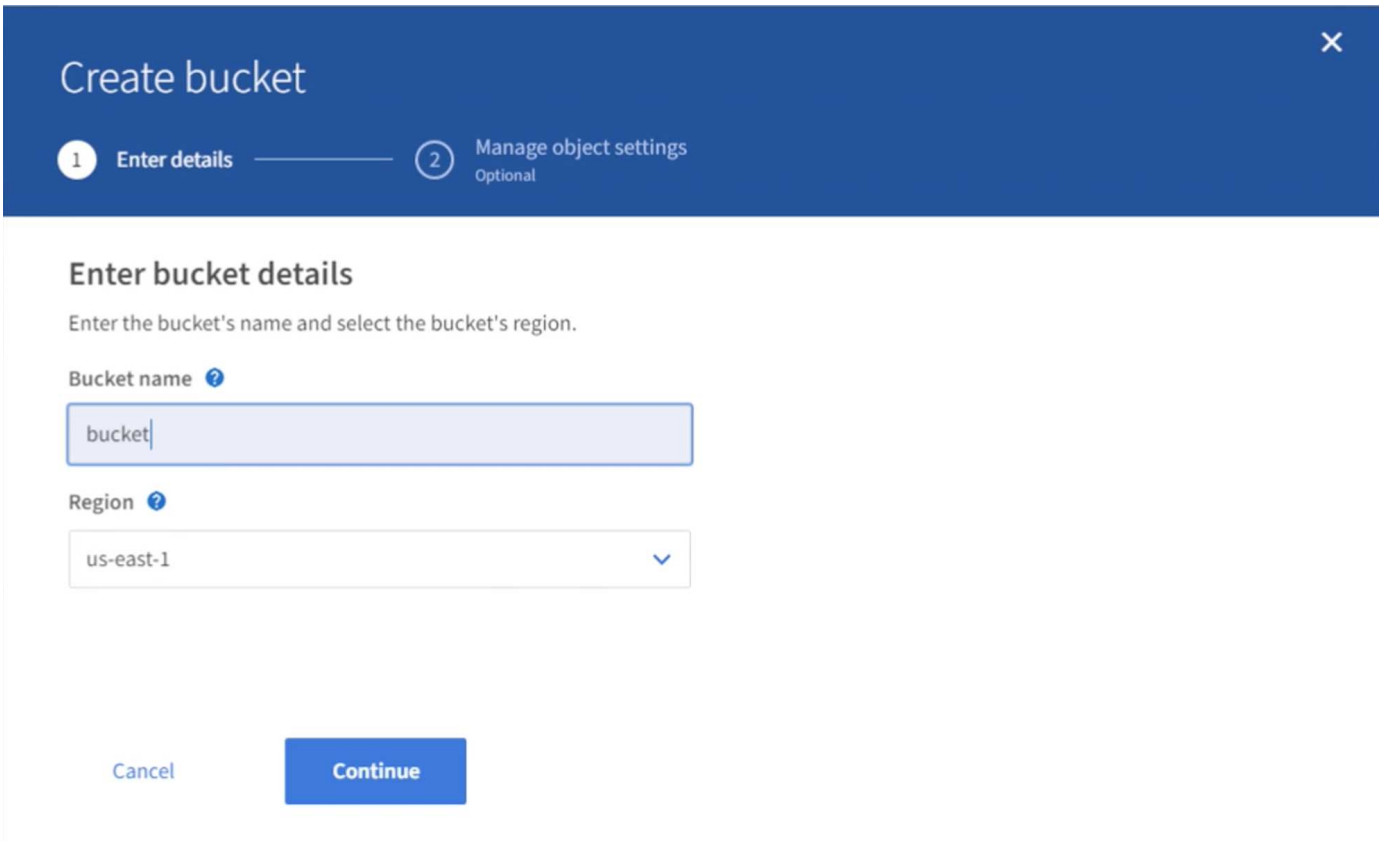


创建两个存储分段

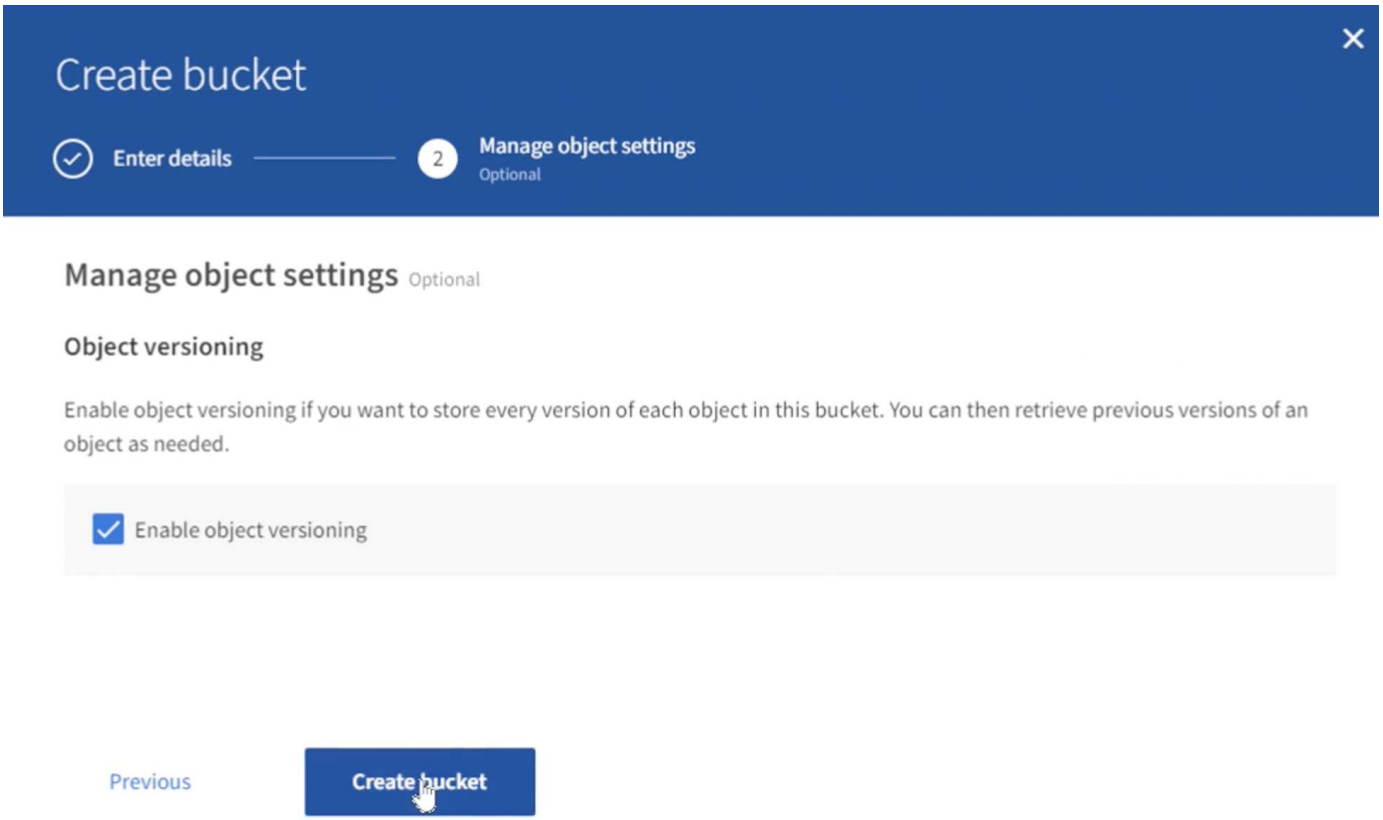
导航到存储分段选项卡、然后单击创建存储分段按钮。



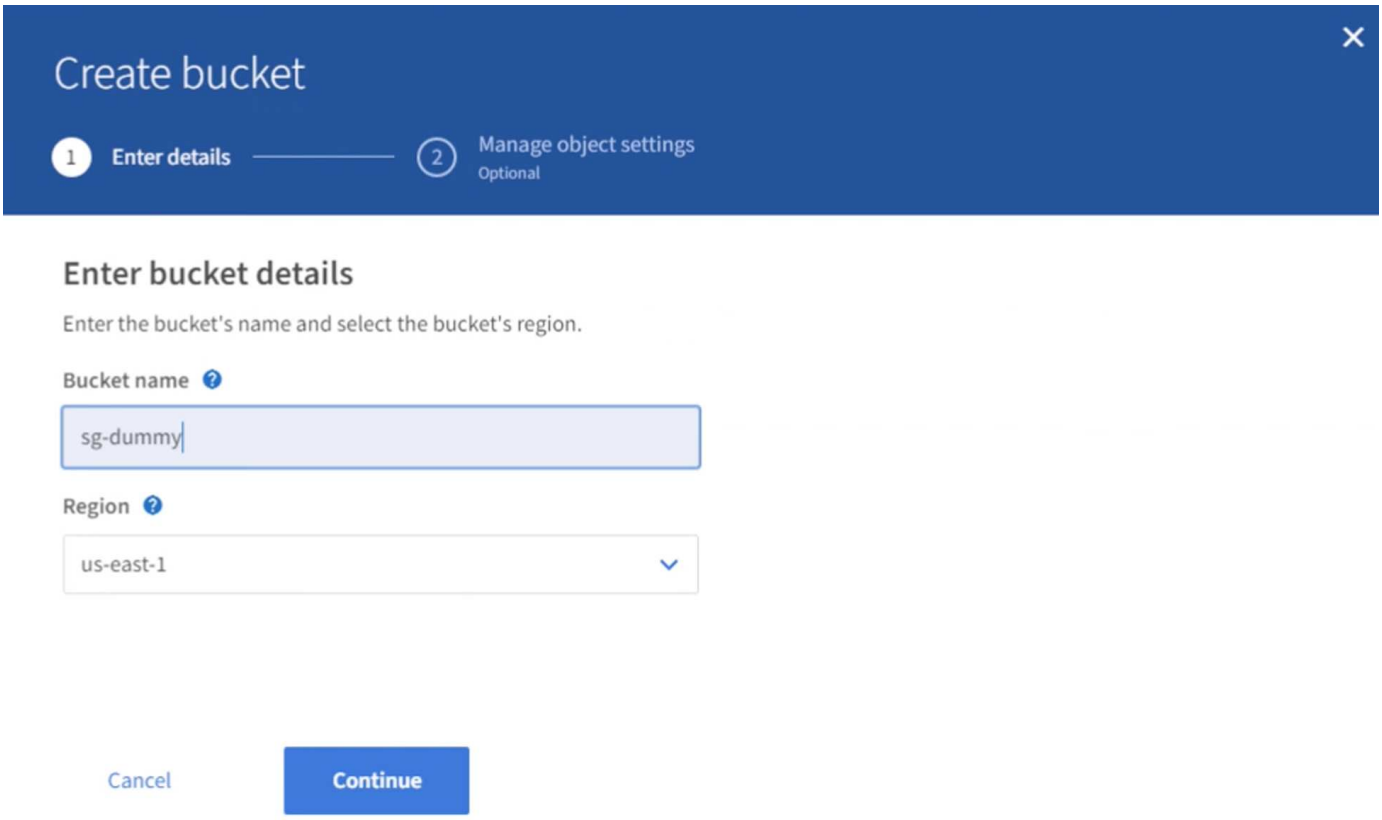
定义分段名称和区域。



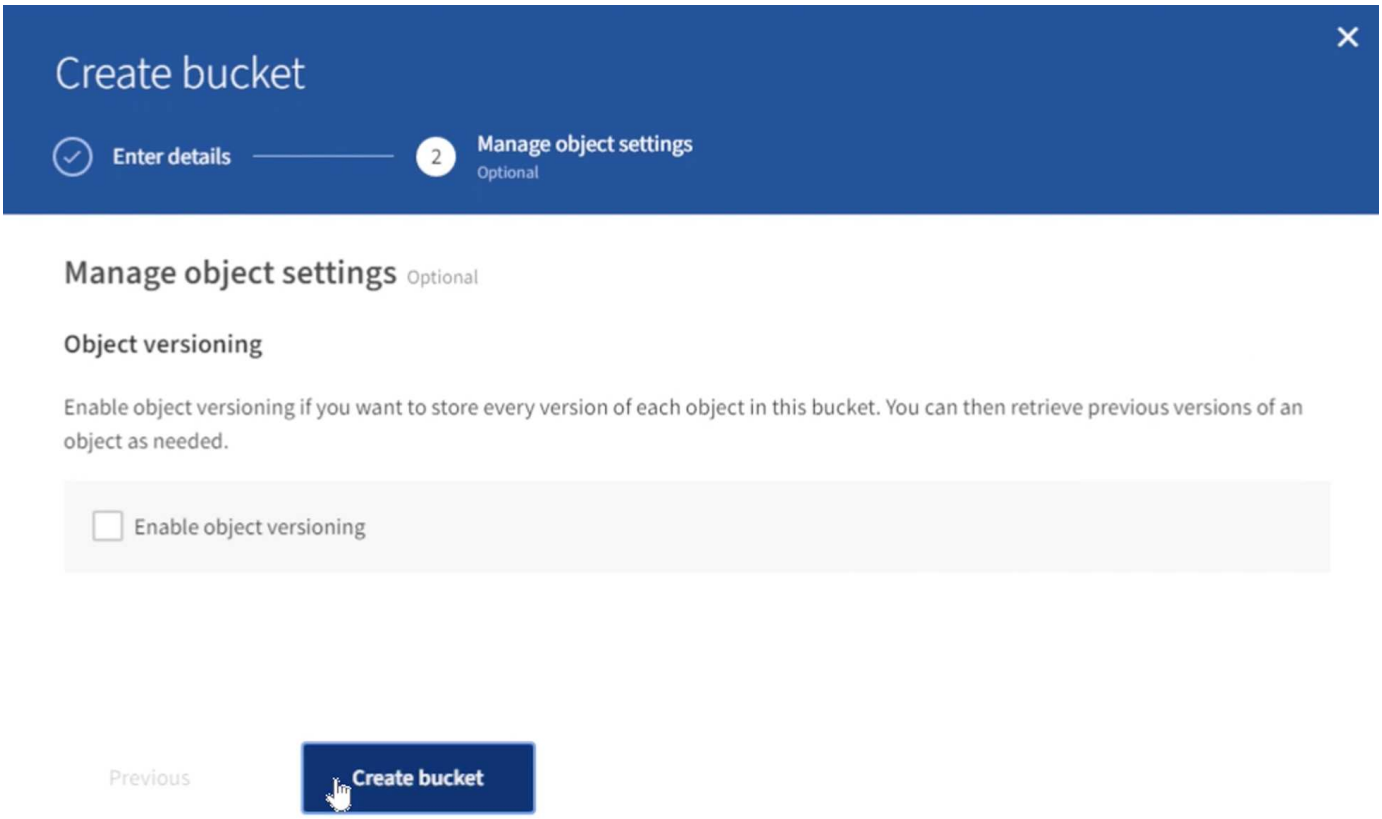
在第一个存储分段上启用版本控制。



现在、在未启用版本控制的情况下创建第二个存储分段。



请勿在此第二个存储分段上启用版本控制。



作者：拉斐尔·吉德斯和阿伦·克莱因

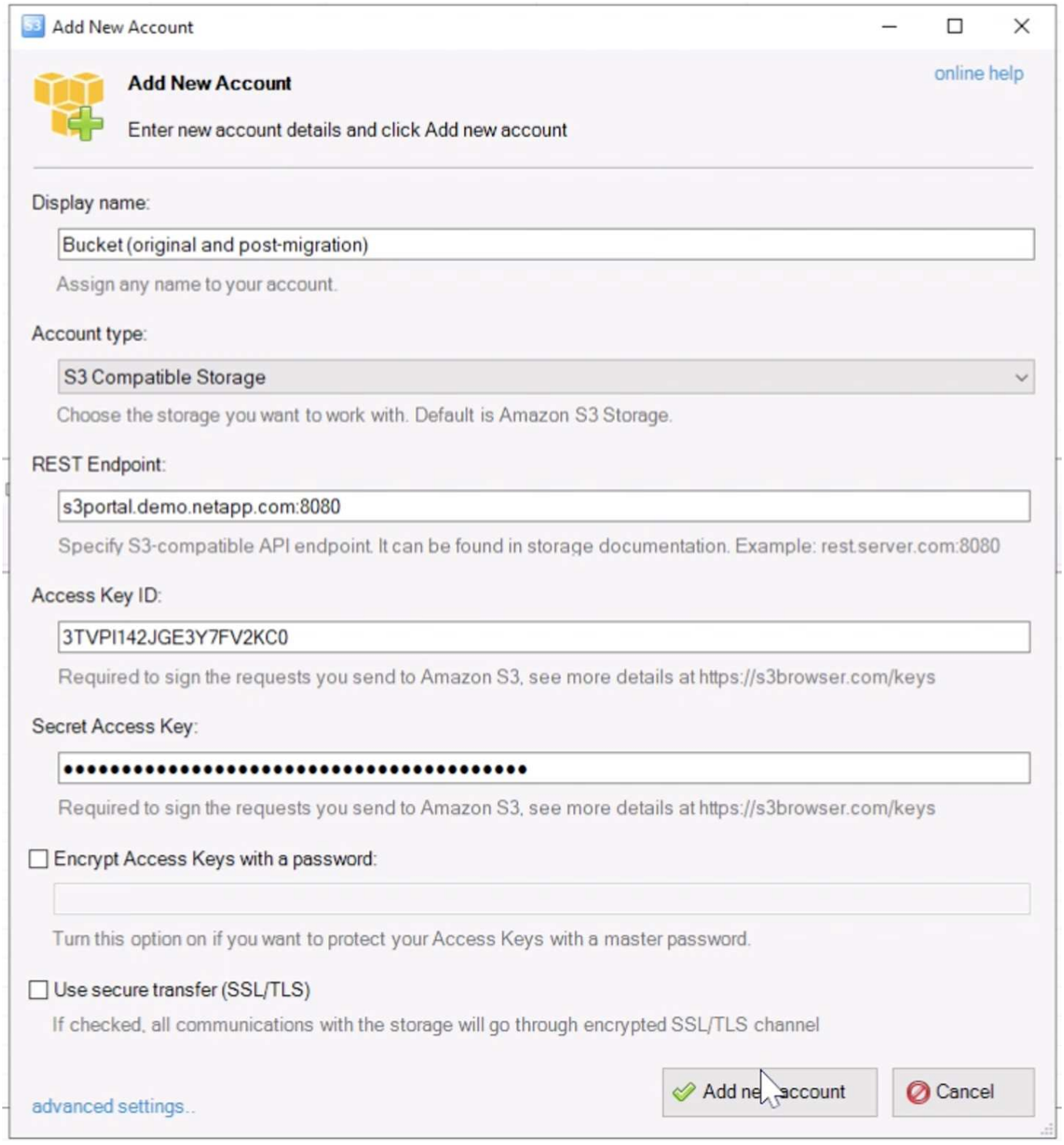
通过将基于对象的存储从**ONTAP S3**无缝迁移到**StorageGRID**来实现企业级**S3**

通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

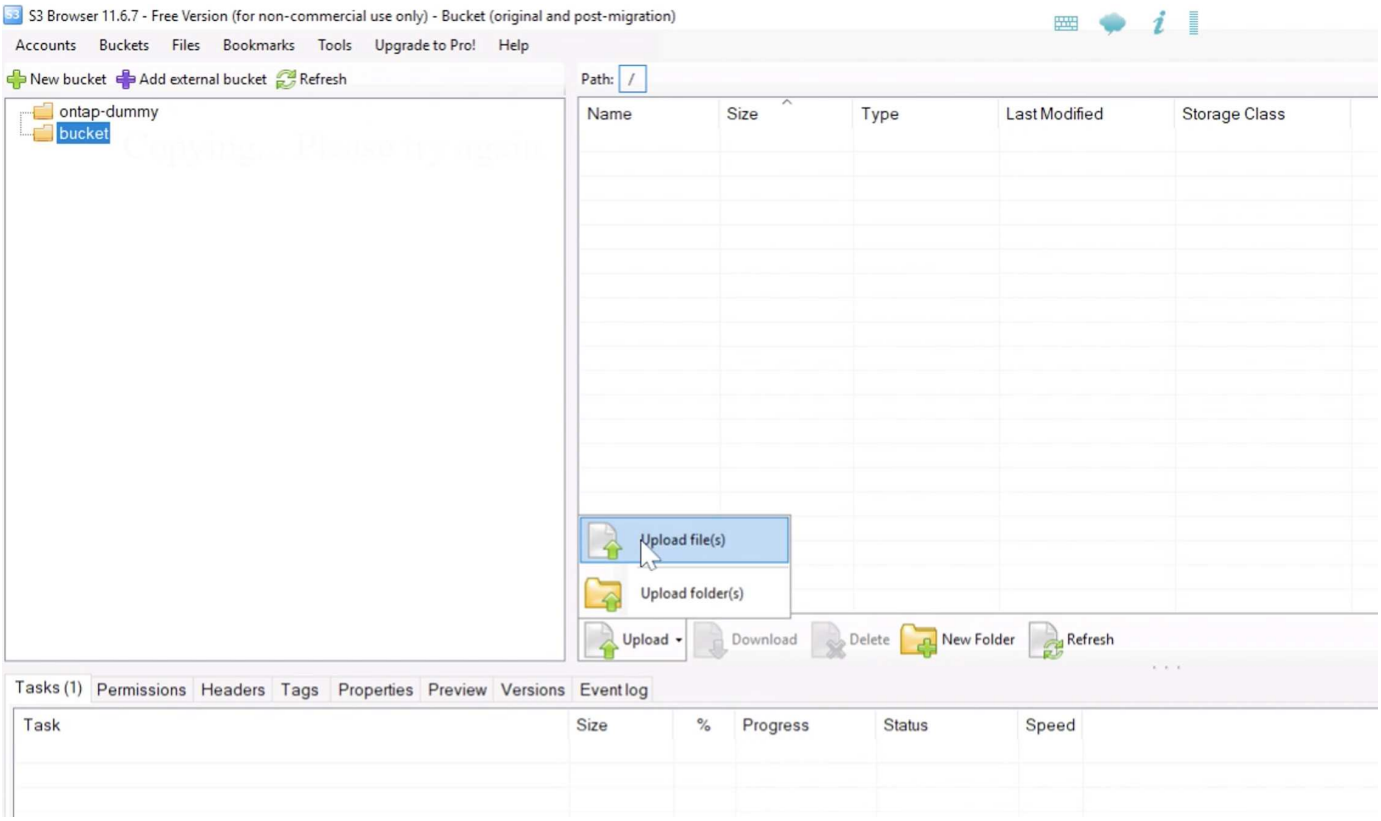
填充源存储分段

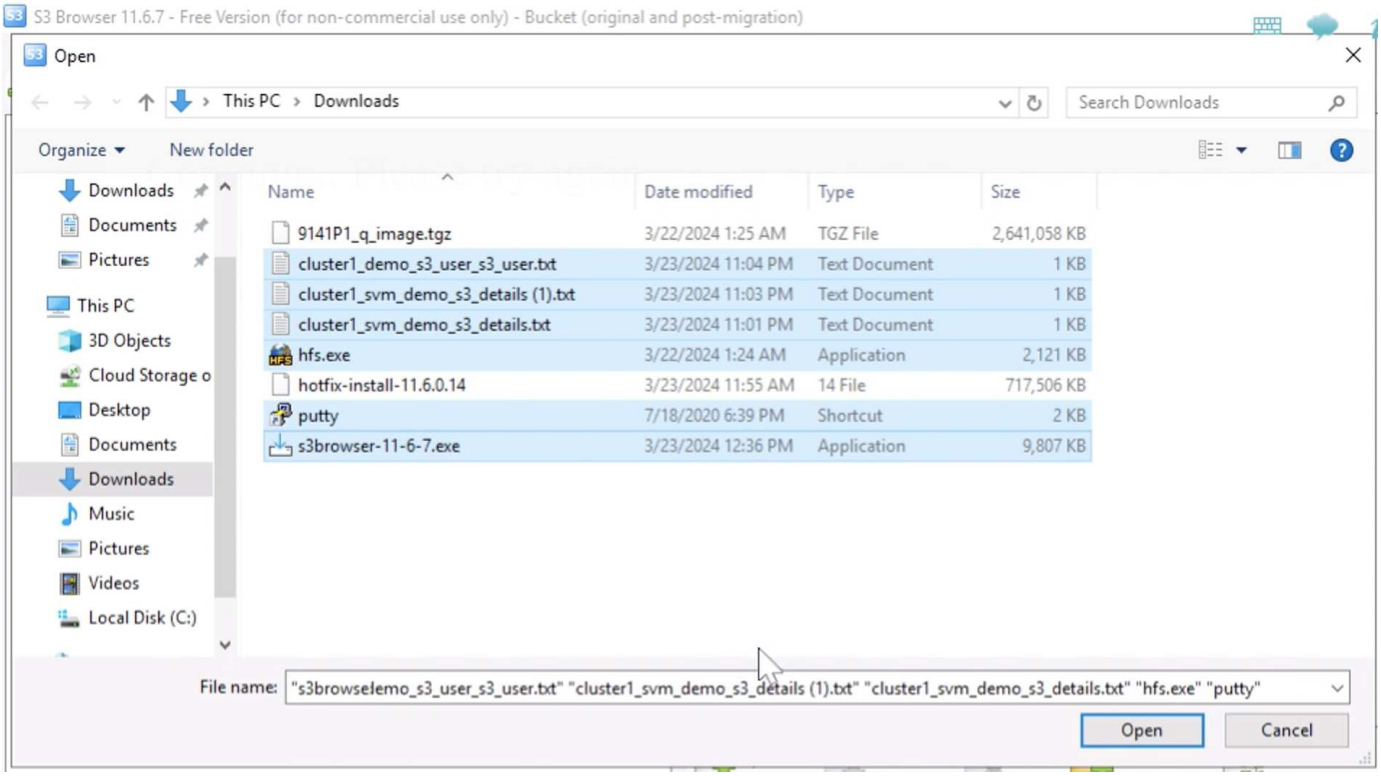
让我们将一些对象放在源ONTAP分段中。我们将使用S3Browser进行此演示、但您可以使用您熟悉的任何工具。

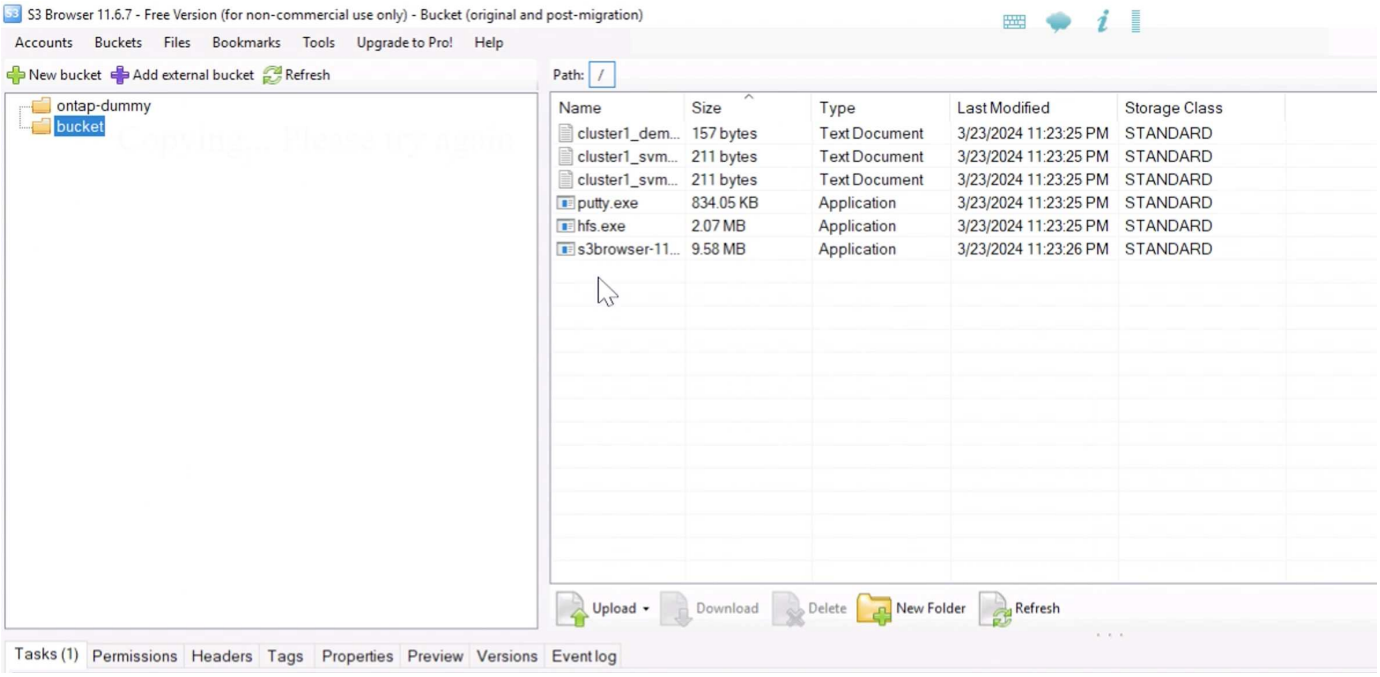
使用上面创建的ONTAP用户S3密钥、将S3Browser配置为连接到ONTAP系统。



现在、我们将一些文件上传到启用了版本控制的存储分段。

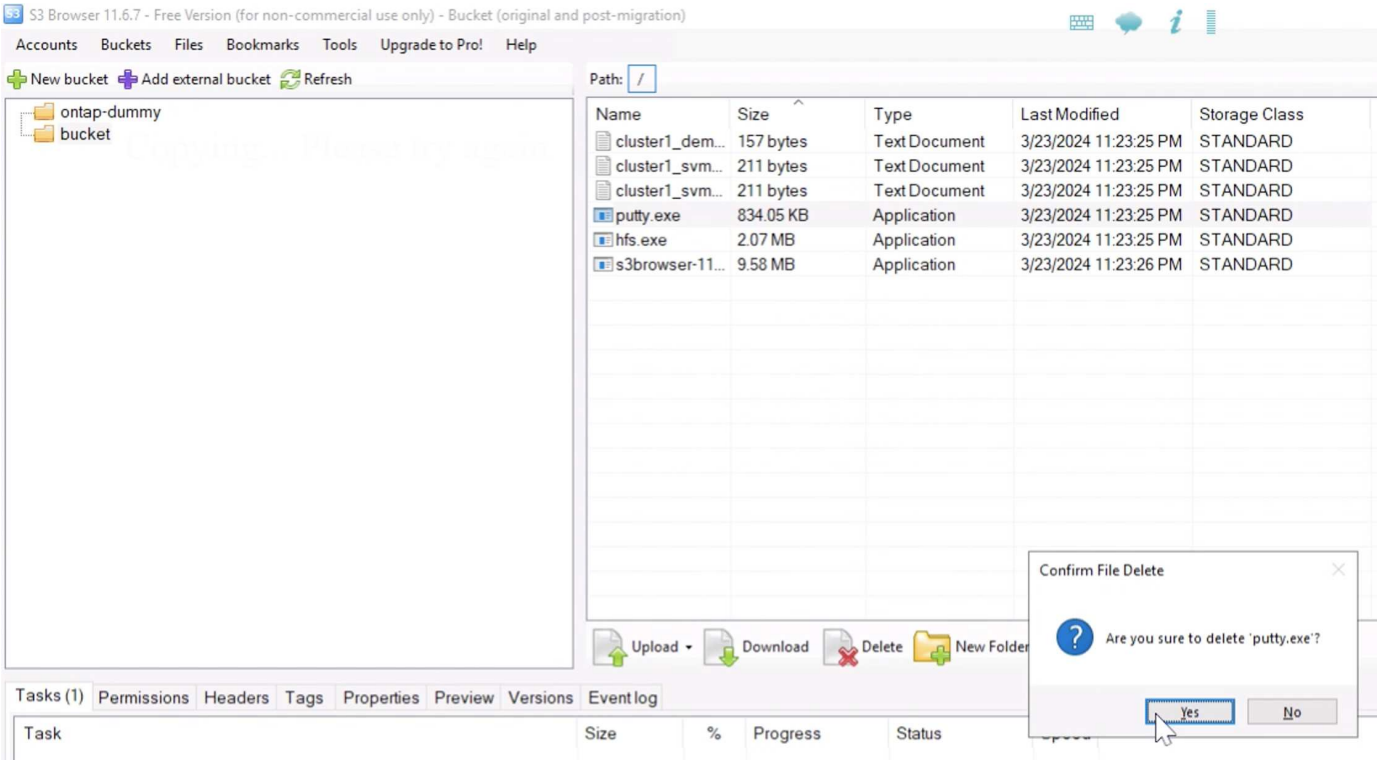




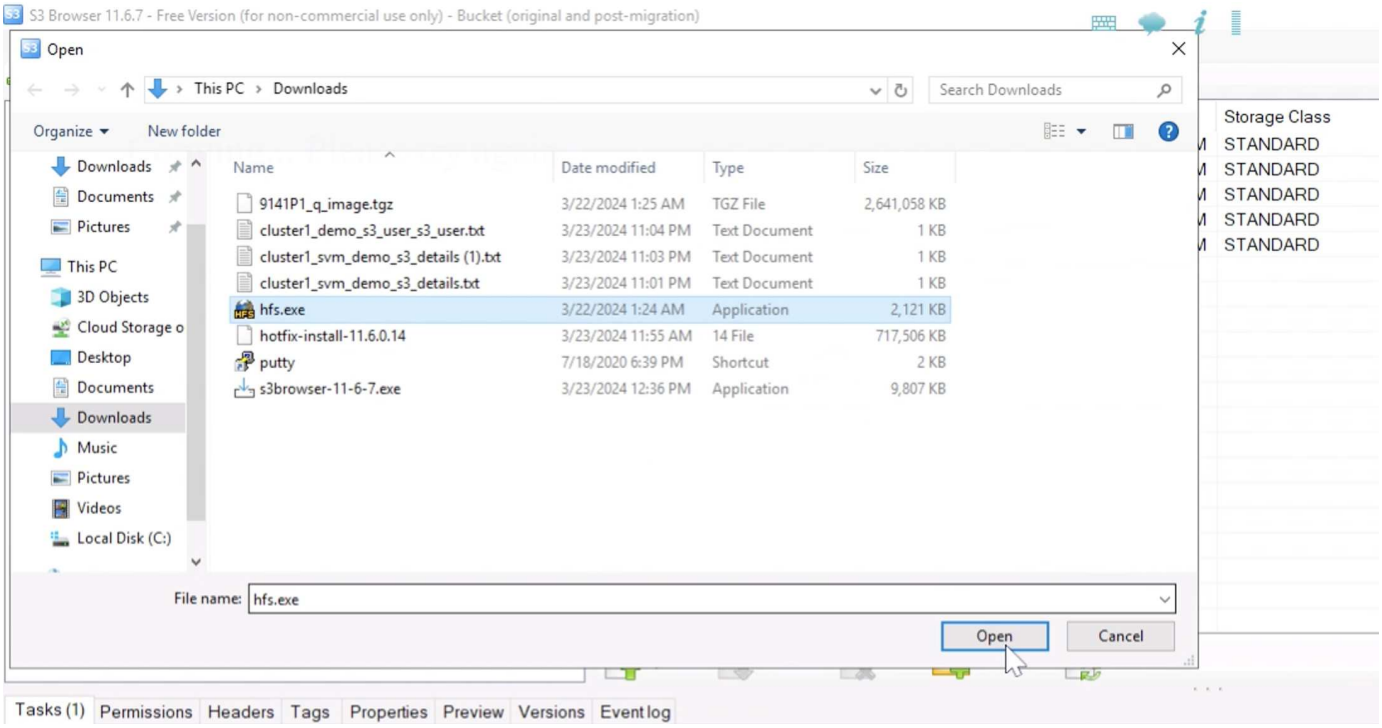


现在、让我们在分段中创建一些对象版本。

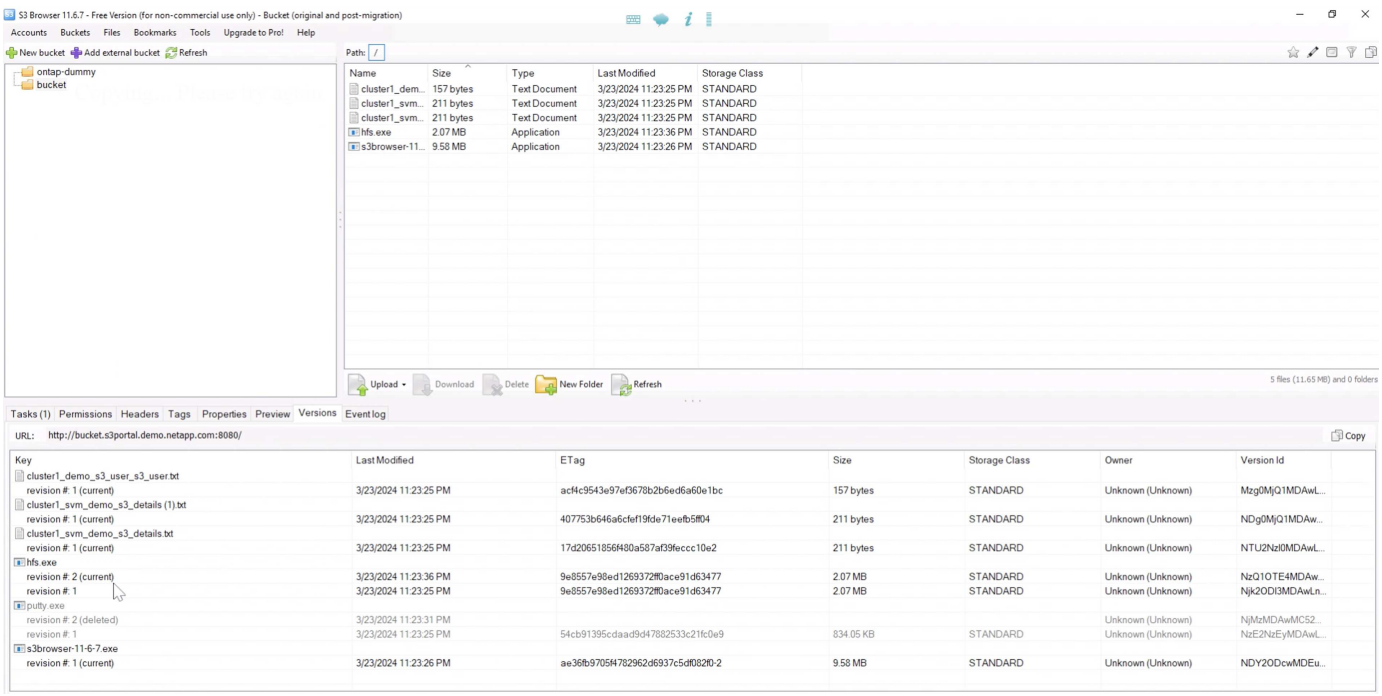
删除文件。



上传存储分段中已存在的文件以复制该文件并创建其新版本。



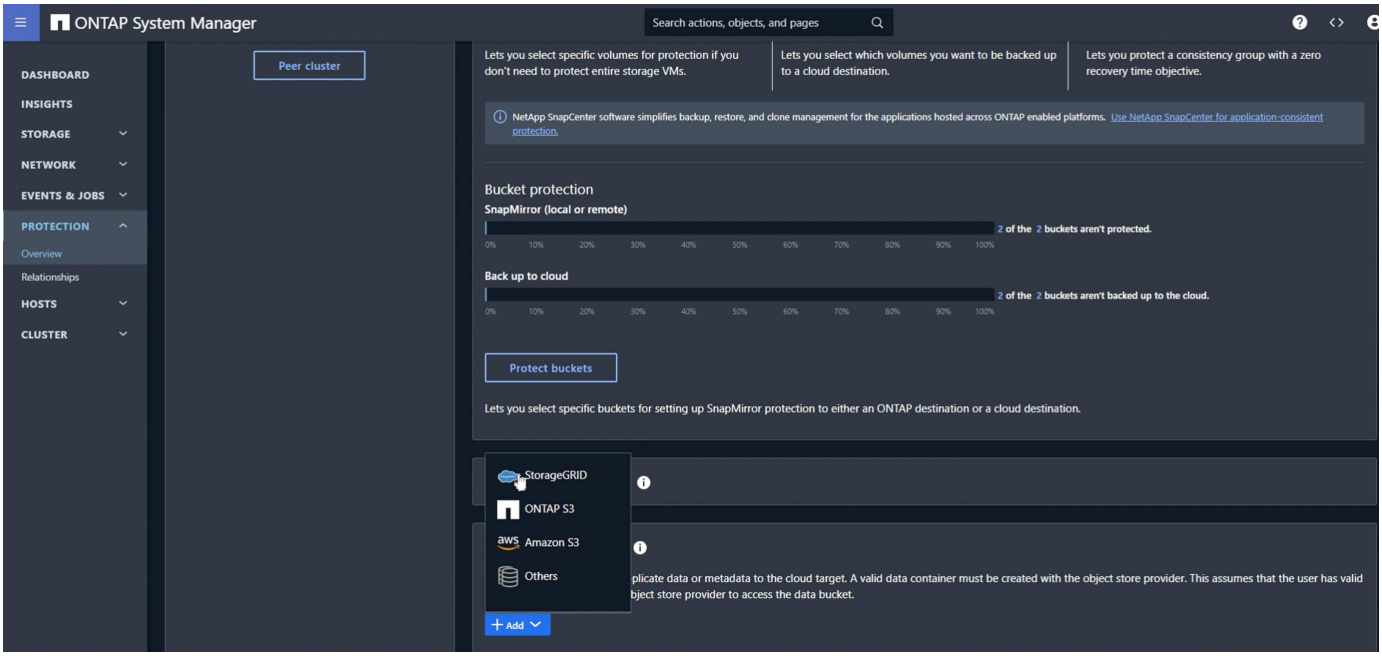
在S3Browser中、我们可以查看刚刚创建的对象的版本。



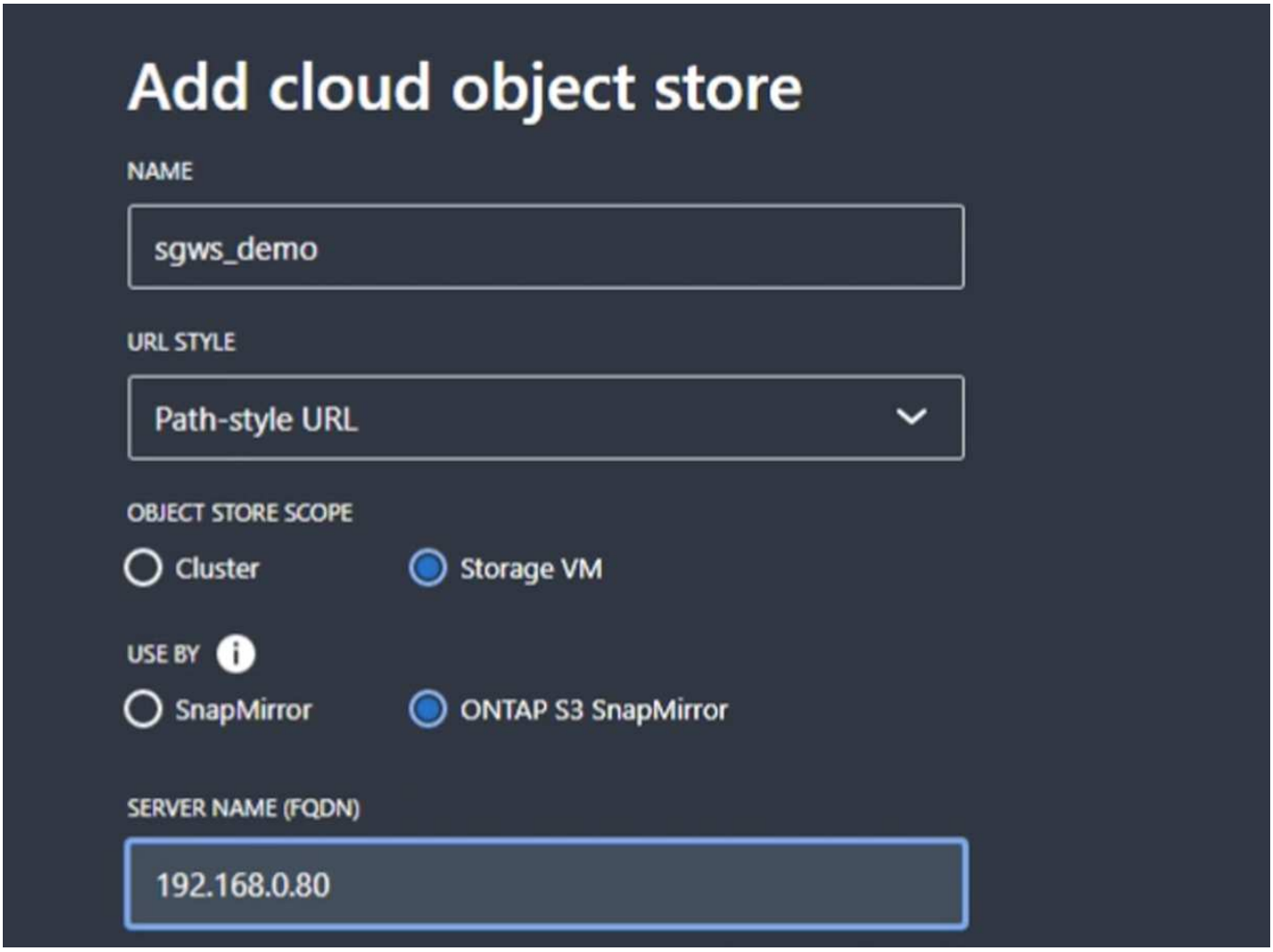
建立复制关系

让我们开始将数据从ONTAP发送到StorageGRID。

在ONTAP系统管理器中、导航到"保护/概述"。向下滚动到"Cloud object stores"(云对象存储)、然后单击"Add"(添加)按钮并选择StorageGRID (添加)。



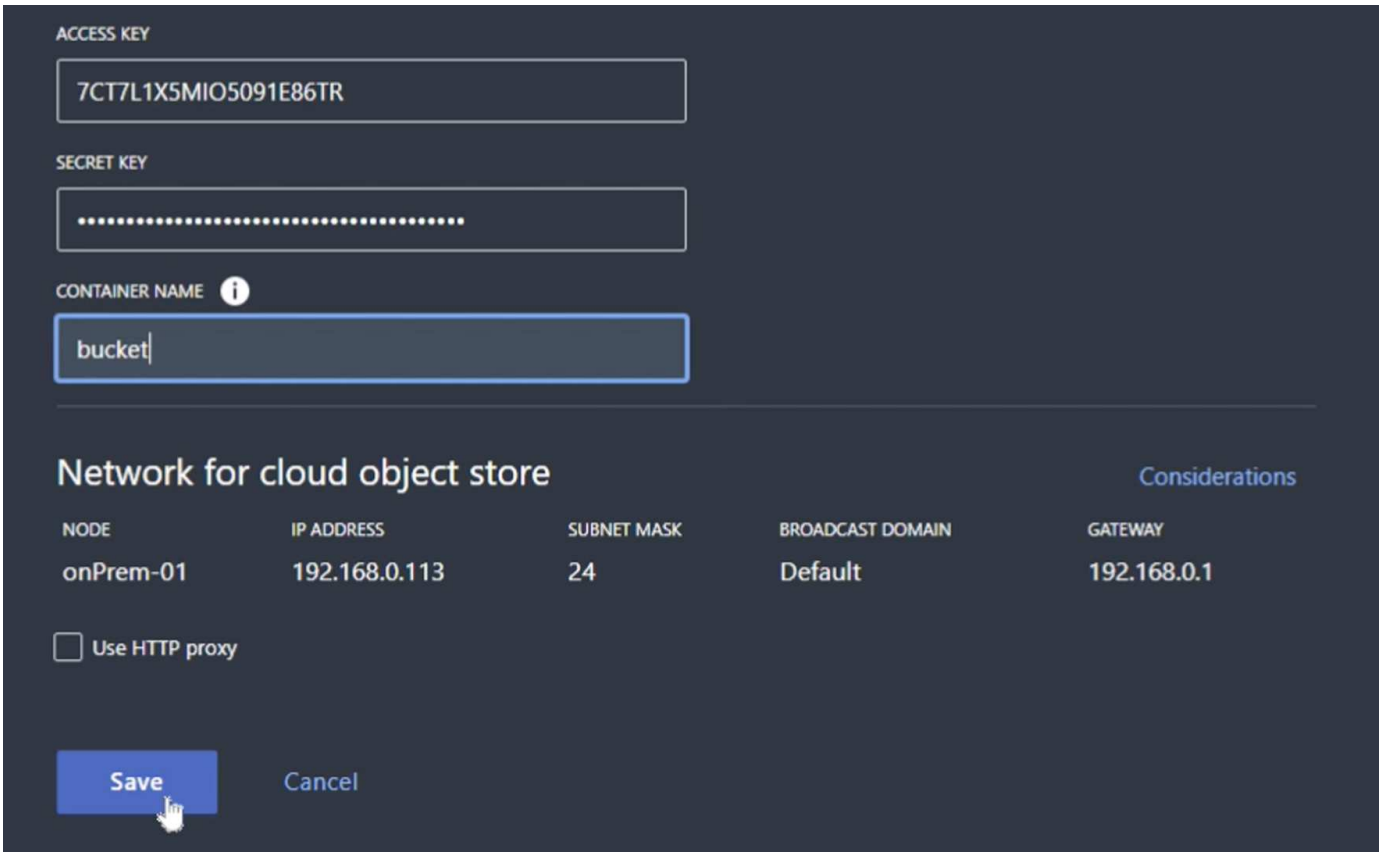
通过提供名称和URL样式来输入StorageGRID信息(在此演示中、我们将使用Path-styleURL)。将对象存储范围设置为"Storage VM"。



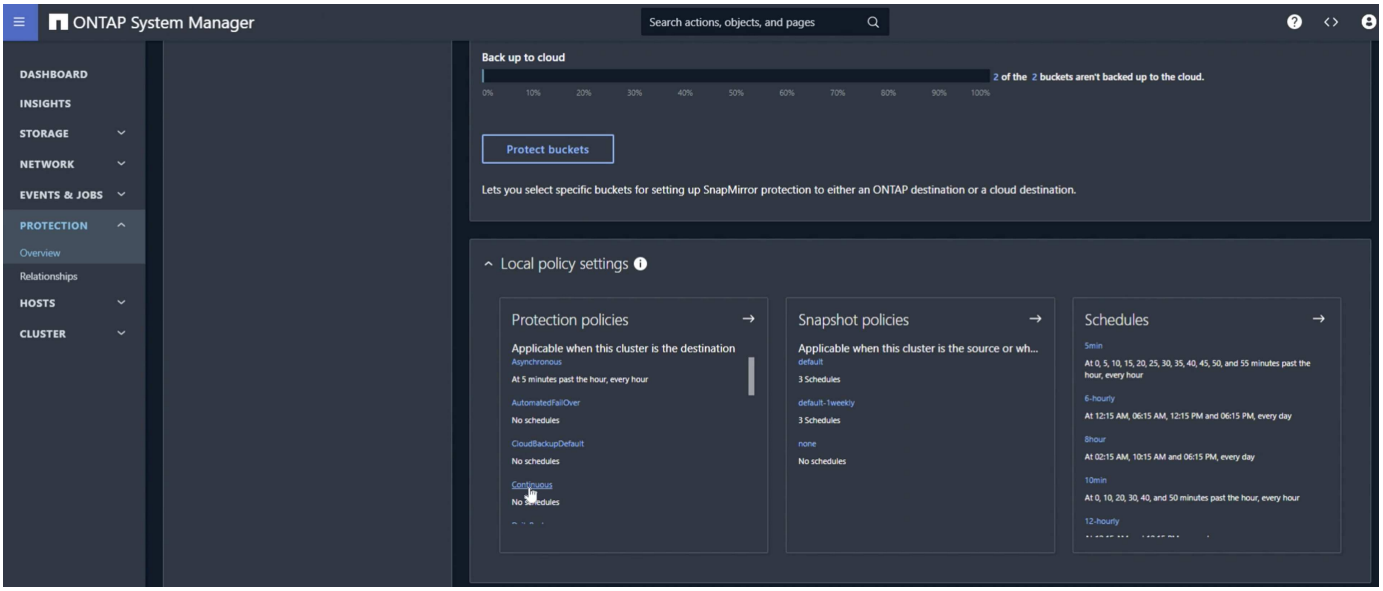
如果您使用的是SSL、请设置负载平衡器端点端口并在此处复制StorageGRID端点证书。否则、请取消选

中"SSP"框并在此处输入HTTP端点端口。

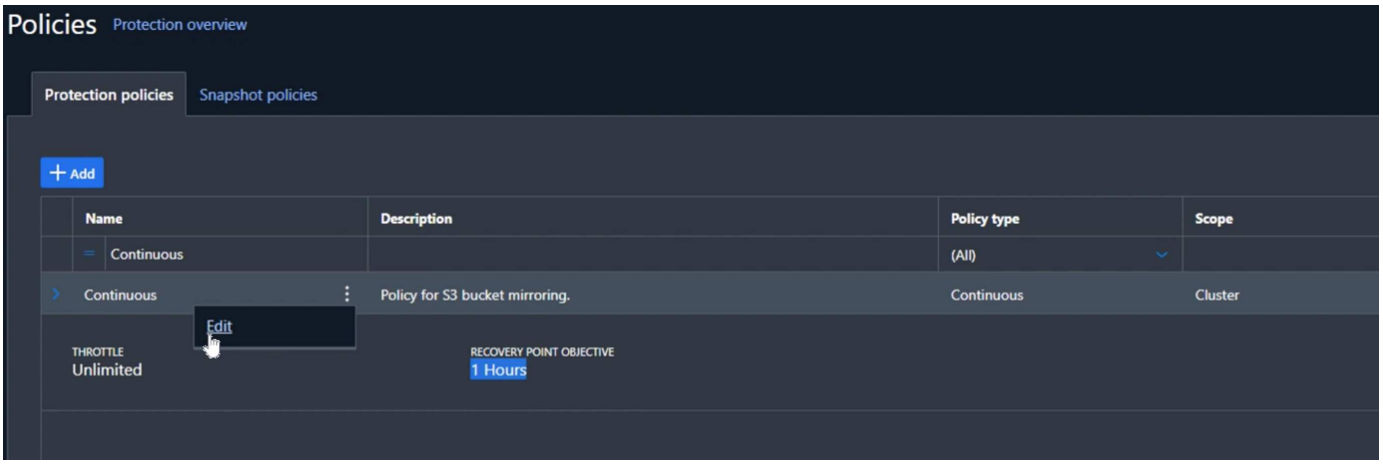
为目标输入上述StorageGRID配置中的StorageGRID用户S3密钥和存储分段名称。



现在、我们已配置目标、可以为此目标配置策略设置。展开"本地策略设置"、然后选择"持续"。



编辑持续策略并将"恢复点目标"从"1小时"更改为"3秒"。

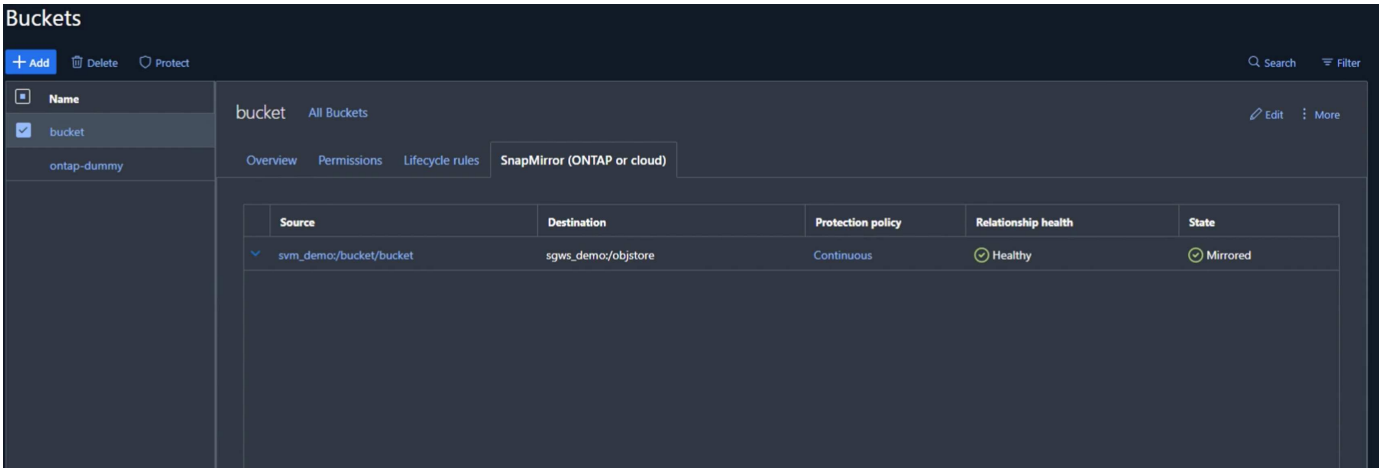


现在、我们可以将SnapMirror配置为复制存储分段。

```
SnapMirror create -ssource-path sv_demo：/bket/bket-target-path sgws_demo：/objstore -policy continuous
```

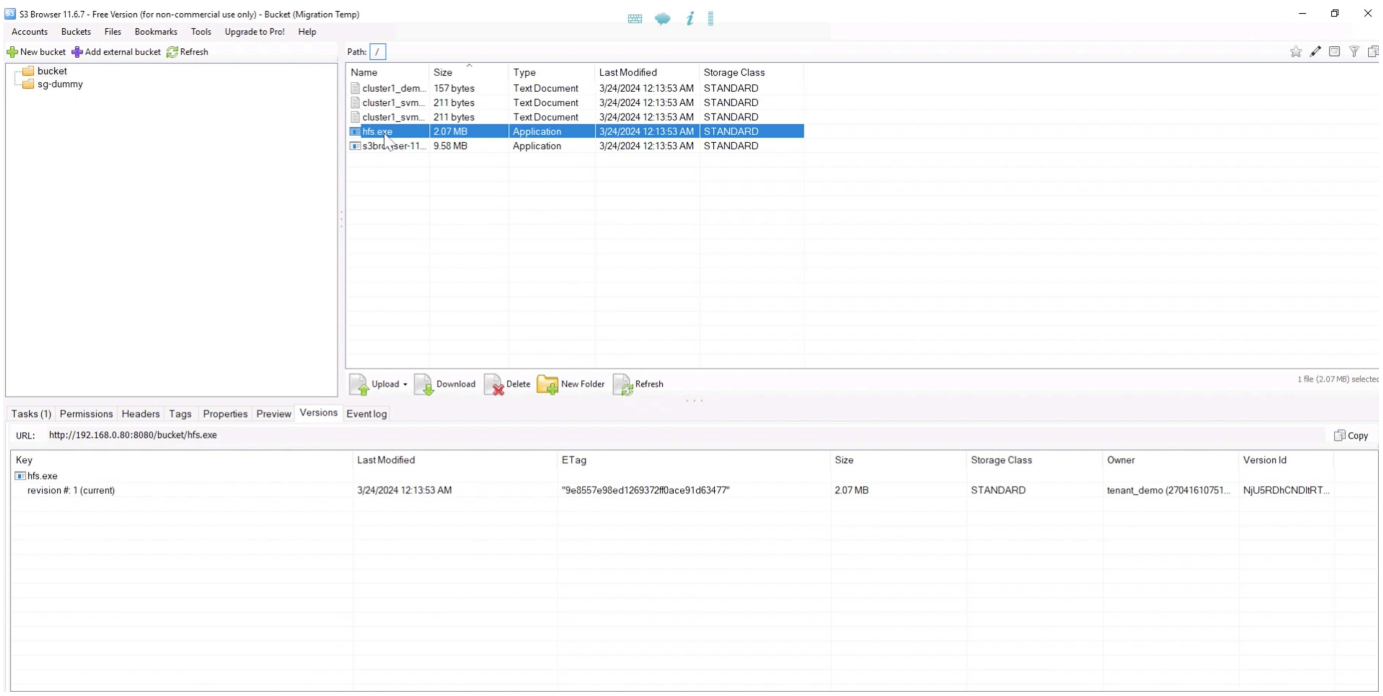
此时、存储分段将在受保护的存储分段列表中显示一个云符号。

如果我们选择存储分段并转到SnapMirror (ONTAP或云)选项卡、我们将看到SnapMirror repationship状态。

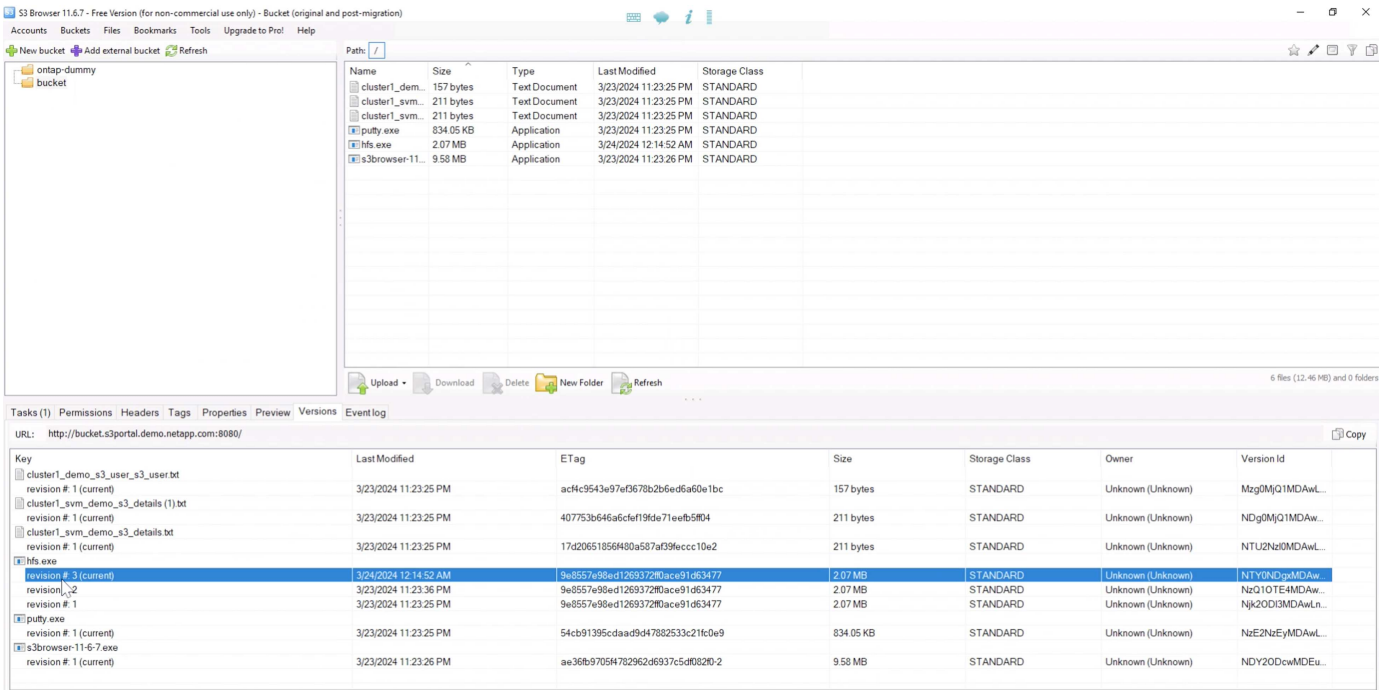


复制详细信息

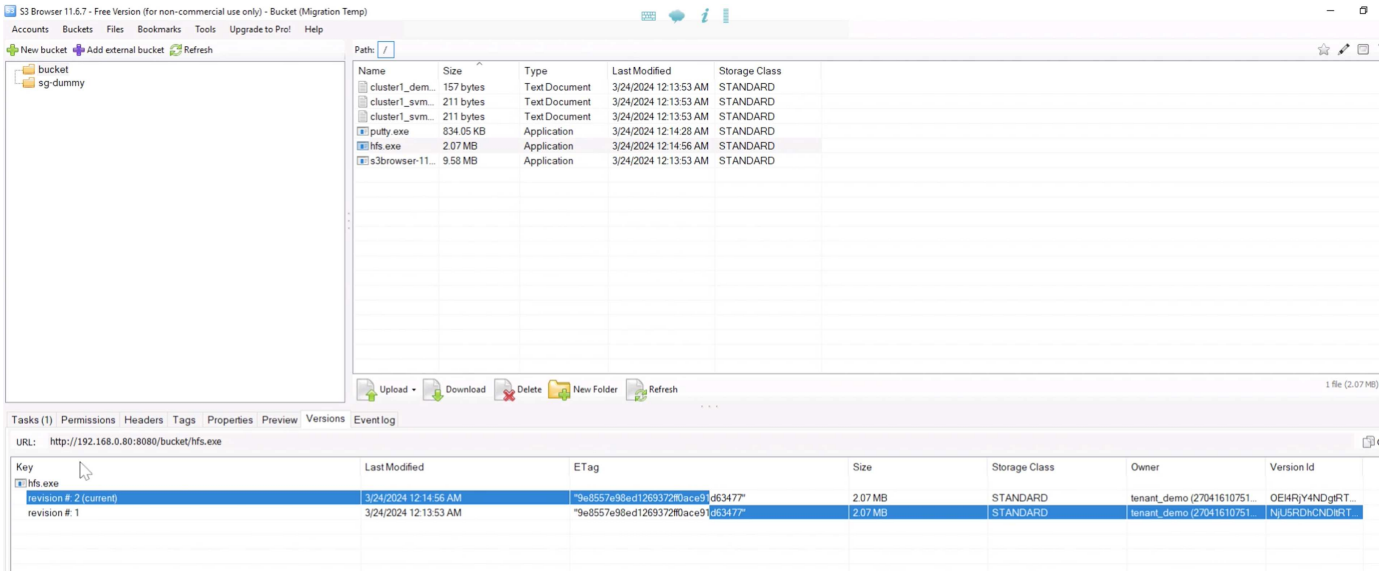
现在、我们已成功将存储分段从ONTAP复制到StorageGRID。但实际上复制的是什么？我们的源和目标都是分版本分段。先前版本是否也会复制到目标？如果我们使用S3Browser查看StorageGRID存储分段、我们会发现现有版本未复制、删除的对象不存在、该对象的删除标记也不存在。我们的复制对象在StorageGRID存储分段中只有1个版本。



在ONTAP分段中、让我们向先前使用的同一对象添加一个新版本、并了解其复制方式。



从StorageGRID的角度来看、我们会发现此存储分段中也创建了一个新版本、但缺少SnapMirror关系之前的初始版本。



这是因为ONTAP SnapMirror S3进程仅复制对象的当前版本。这就是我们在StorageGRID端创建分版本存储分段作为目标的原因。这样、StorageGRID就可以维护对象的版本历史记录。

作者：拉斐尔·吉德斯和阿伦·克莱因

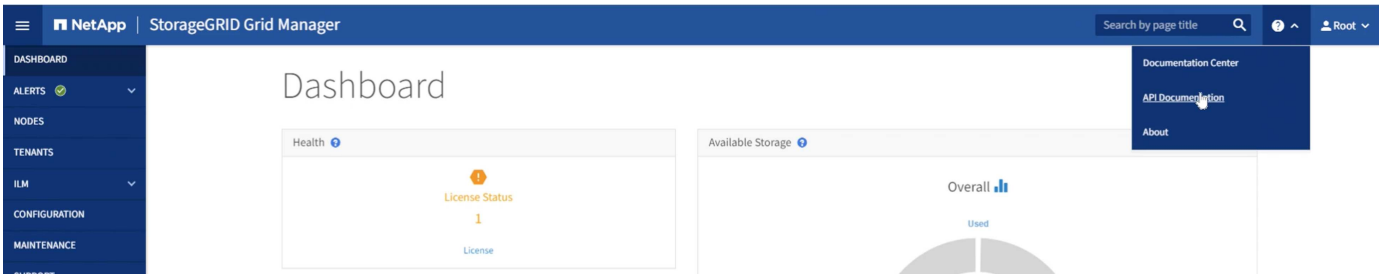
通过将基于对象的存储从**ONTAP S3**无缝迁移到**StorageGRID**来实现企业级**S3**

通过将基于对象的存储从ONTAP S3无缝迁移到StorageGRID来实现企业级S3

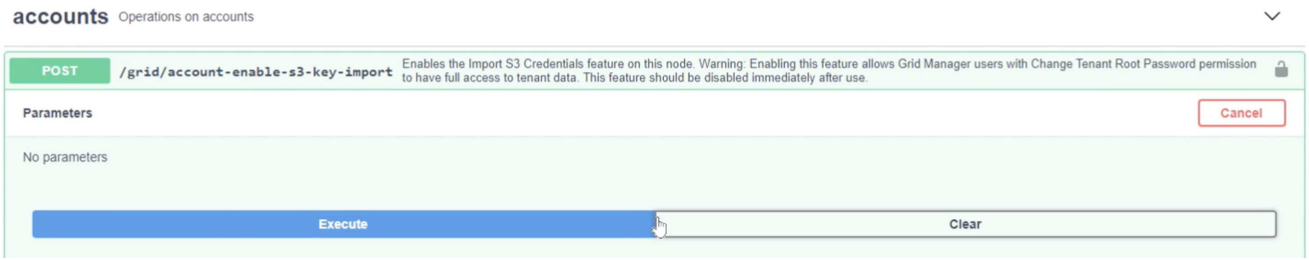
迁移**S3**密钥

对于迁移、大多数情况下您都需要迁移用户的凭据、而不是在目标端生成新的凭据。StorageGRID提供API以允许将S3密钥导入到用户。

登录到StorageGRID管理UI (而不是租户管理器UI)、打开API文档Swagger页面。

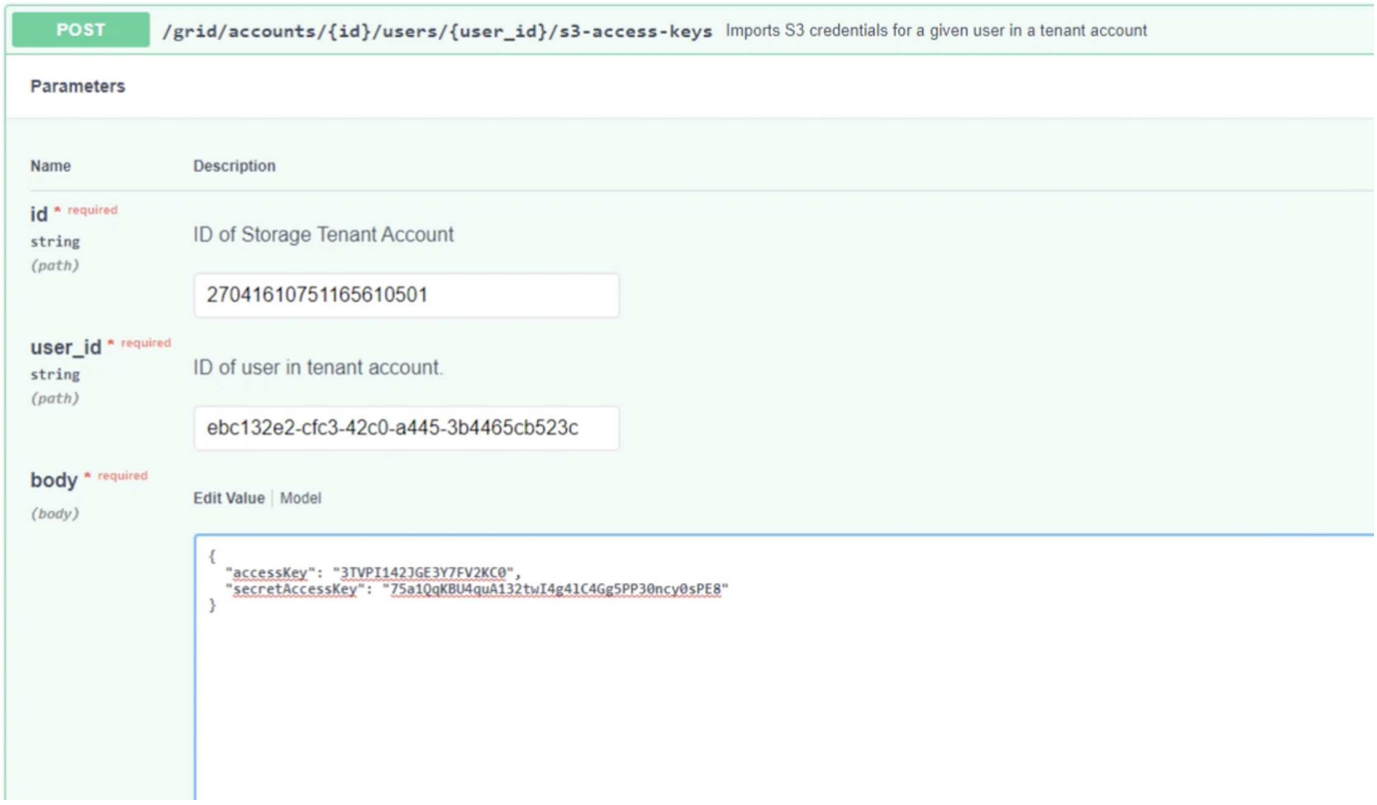


展开"accounts"(帐户)部分、选择"POST /grid /account-enable－s3-key-import "、单击"试用"按钮、然后单击"execute"(执行)按钮。

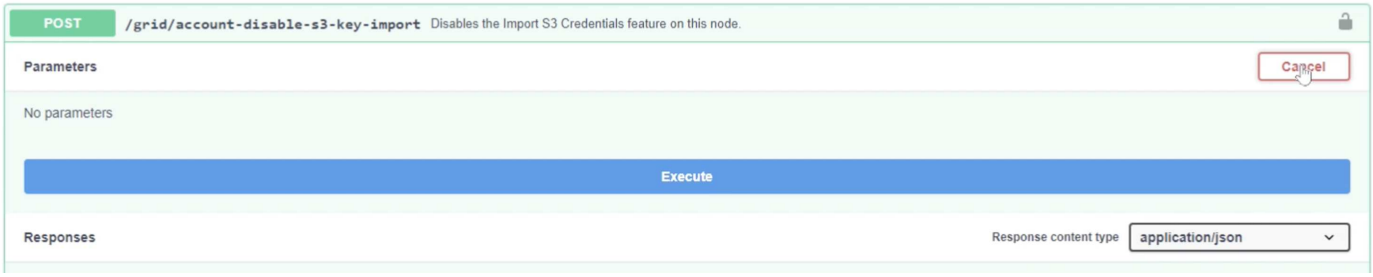


现在仍在"accounts"下向下滚动到"POST /grid /accounts/ {id} /user/ {user_id} /s3-access-keys"

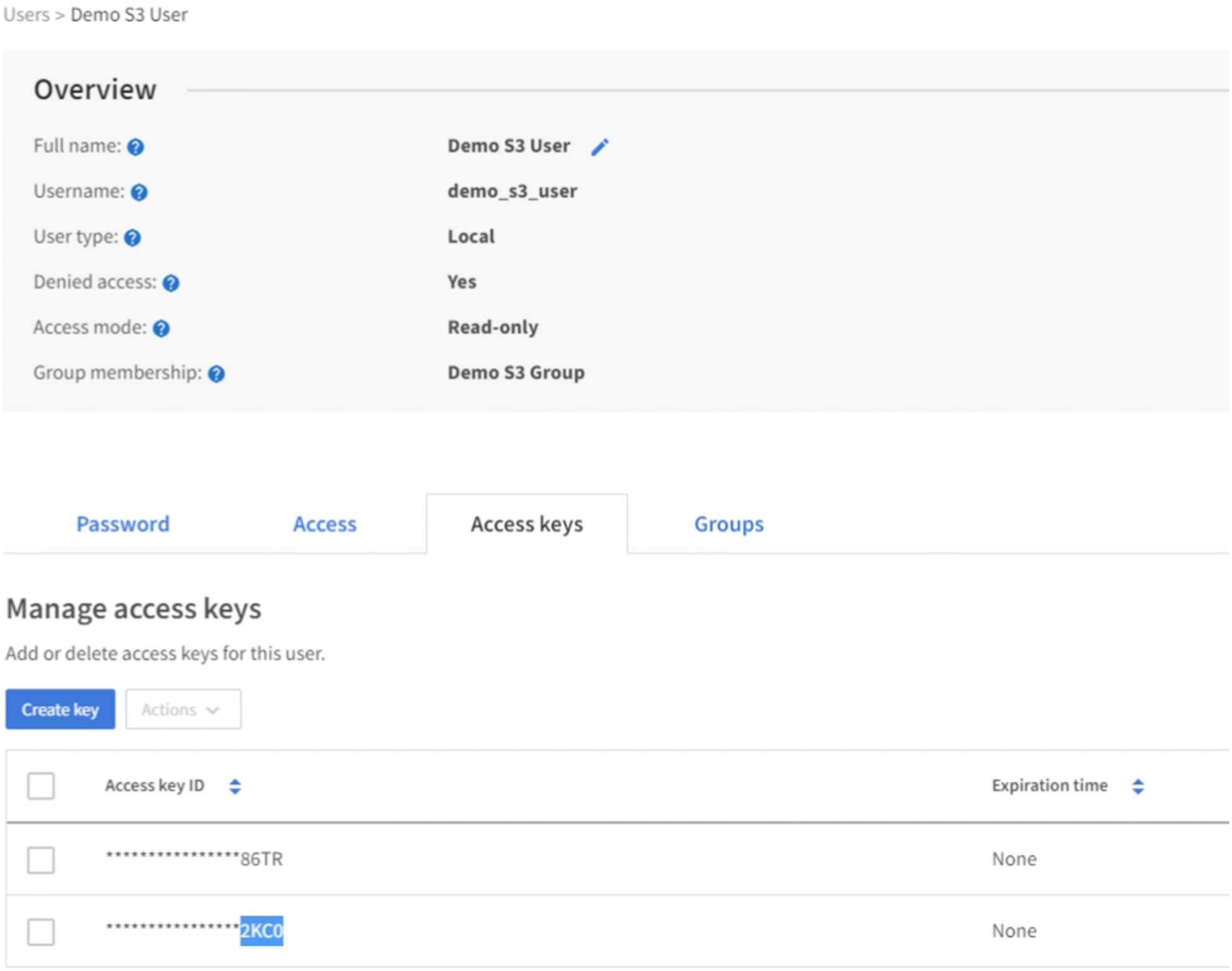
下面是我们要输入先前收集的租户ID和用户帐户ID的位置。在json框中填写来自我们的ONTAP用户的字段和密钥。您可以设置密钥的到期时间、也可以删除"、"Expires"：3456789 "、然后单击"执行"。



完成所有用户密钥导入后、您应在"accounts""POST /grid /account-disable" s3-key-import"中禁用密钥导入功能



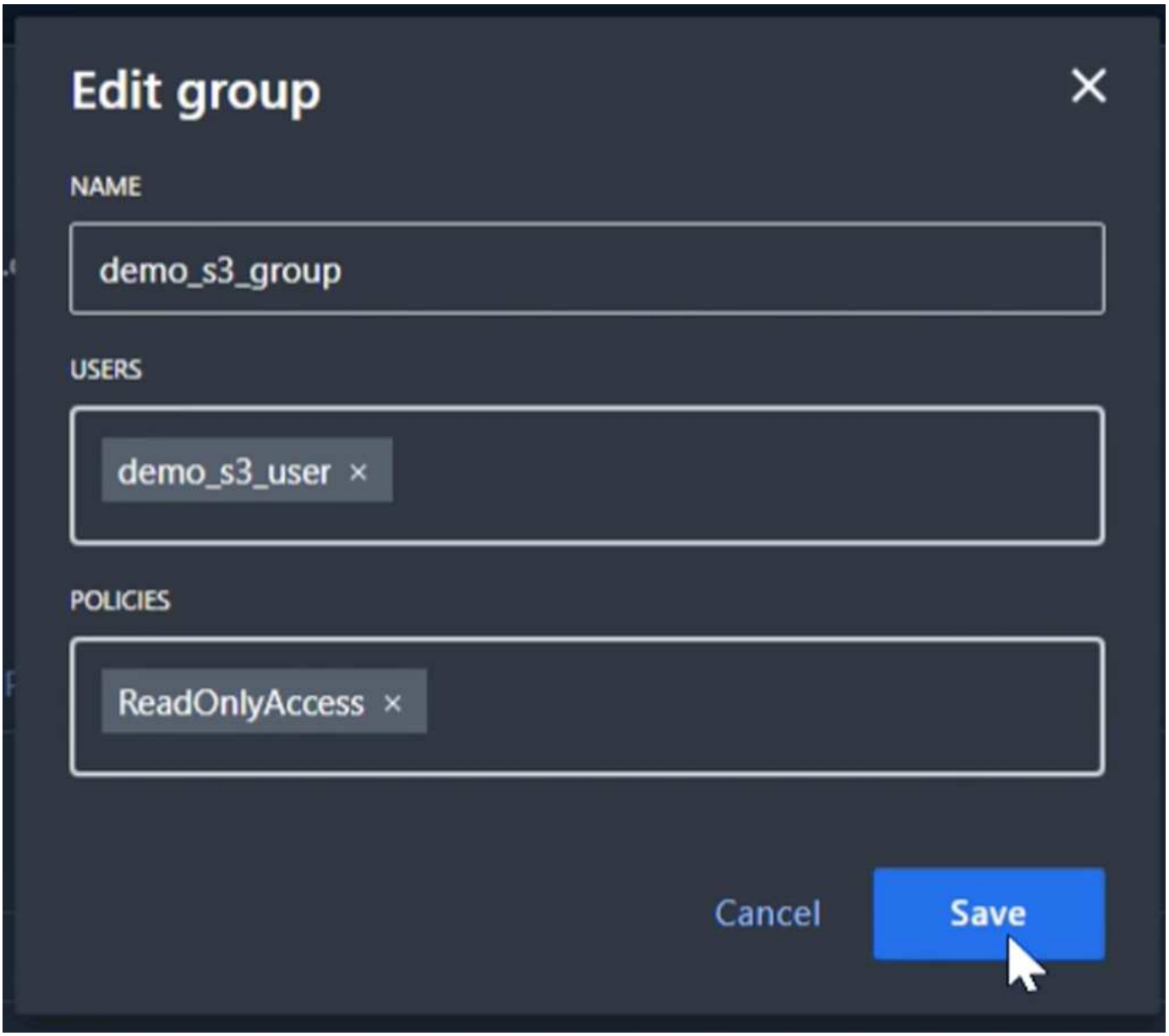
如果我们在租户管理器UI中查看用户帐户、可以看到新密钥已添加。



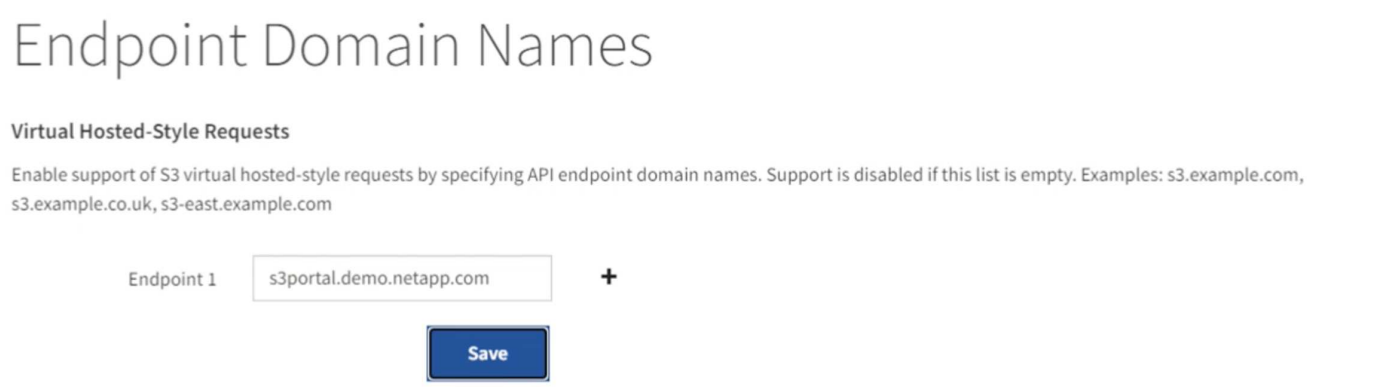
最终转换

如果打算永久将存储分段从ONTAP复制到StorageGRID、您可以到此结束。如果是从ONTAP S3迁移到StorageGRID、则需要结束迁移并进行转换。

在ONTAP系统管理器中、编辑S3组并将其设置为"ReadOnlyAccess"。这将防止用户再向ONTAP S3存储分段写入数据。



只需将DNS配置为从ONTAP集群指向StorageGRID端点即可。请确保端点证书正确无误、如果需要虚拟托管模式请求、请在StorageGRID中添加端点域名



您的客户端需要等待TTL过期、或者刷新DNS以解析到新系统、以便您可以测试一切正常。剩下的只是清理用于测试StorageGRID数据访问的初始临时S3密钥(而不是导入的密钥)、删除SnapMirror关系、然后删除ONTAP数据。

作者：拉斐尔·吉德斯和阿伦·克莱因

工具和应用程序指南

将Cloudera Hadoop S3A连接器与StorageGRID 结合使用

作者：郑安杰

一段时间以来、Hadoop一直是数据科学家的最爱。通过Hadoop、可以使用简单的编程框架在多个计算机集群之间分布式处理大型数据集。Hadoop旨在从单个服务器扩展到数千台计算机、每台计算机都拥有本地计算和存储。

为什么要使用S3A执行Hadoop工作流?

随着数据量的不断增长、使用自己的计算和存储添加新计算机的方法变得效率低下。线性扩展为高效使用资源和管理基础架构带来了挑战。

为了应对这些挑战、Hadoop S3A客户端可为S3对象存储提供高性能I/O。使用S3A实施Hadoop工作流有助于将对象存储用作数据存储库、并将计算和存储分开、进而使您能够独立扩展计算和存储。通过分离计算和存储、您还可以将适当数量的资源专用于计算作业、并根据数据集的大小提供容量。因此、您可以降低Hadoop工作流的总体TCO。

将S3A连接器配置为使用StorageGRID

前提条件

- 用于Hadoop S3A连接测试的StorageGRID S3端点URL、租户S3访问密钥和机密密钥。
- Cloudera集群以及对集群中每个主机的root或sudo权限、用于安装Java软件包。

截至2022年4月、使用Cloudera 7.1.7的Java 11.0.14已针对StorageGRID 11.5和11.5进行了测试。但是、新安装时的Java版本号可能会有所不同。

安装Java软件包

1. 检查 "Cloudera支持表" 支持的JDK版本。
2. 下载 "Java 11.x软件包" 与Cloudera集群操作系统匹配。将此软件包复制到集群中的每个主机。在此示例中、rpm软件包用于CentOS。
3. 以root身份或使用具有sudo权限的帐户登录到每个主机。在每个主机上执行以下步骤：
   a. 安装软件包：

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

   b. 检查Java的安装位置。如果安装了多个版本、请将新安装的版本设置为默认值：

```
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. 将此行添加到`/etc/profile`的末尾。路径应与上述选择的路径匹配：

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

d. 运行以下命令以使配置文件生效：

```
source /etc/profile
```

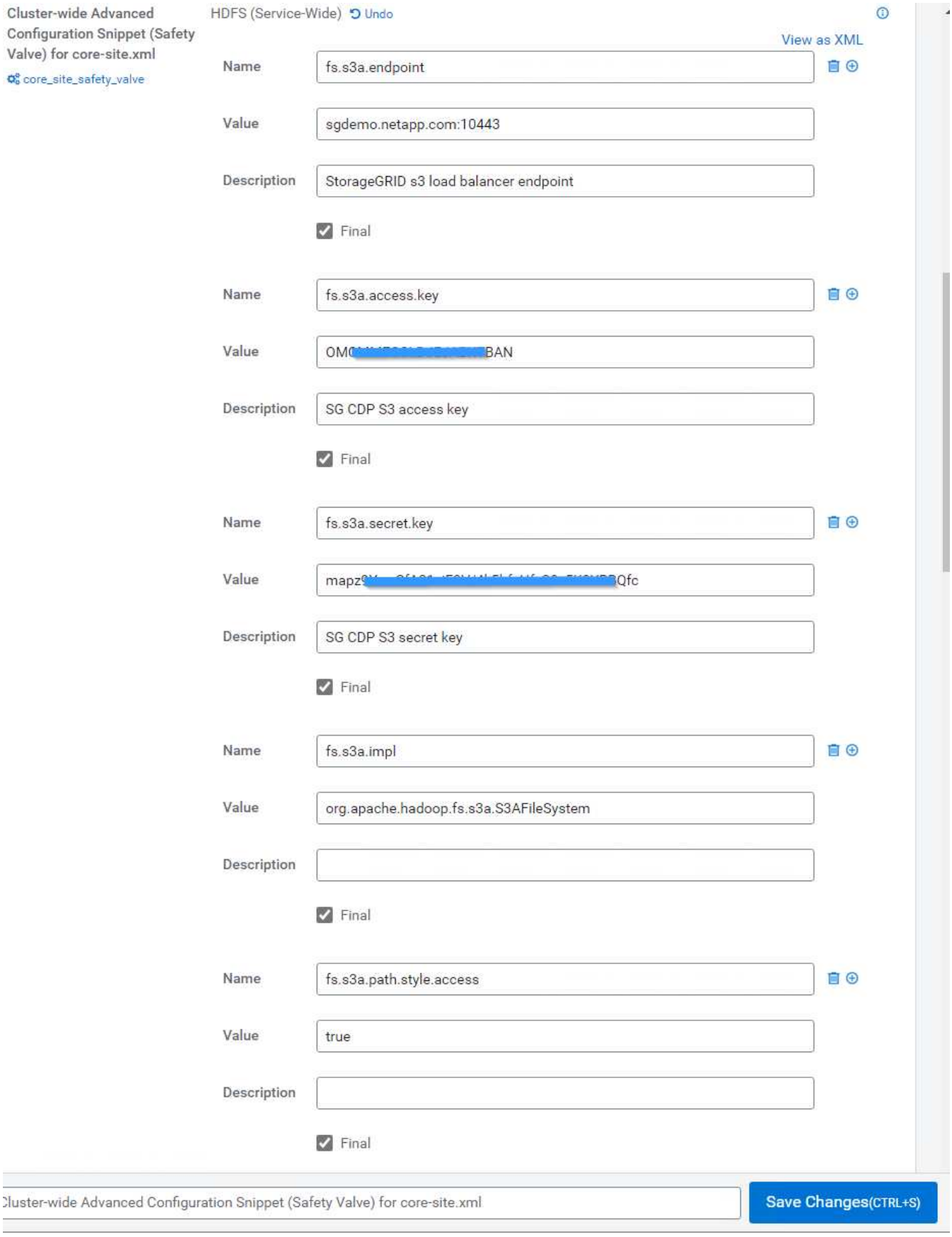
Cloudera HDFS S3A配置

- 步骤 *

1. 从Cloudera Manager GUI中、选择Clusters > HDFS、然后选择Configuration。
2. 在类别下、选择高级、然后向下滚动以找到`core-site.xml的集群范围高级配置片段(安全阀)`。
3. 单击(+)符号并添加以下值对。

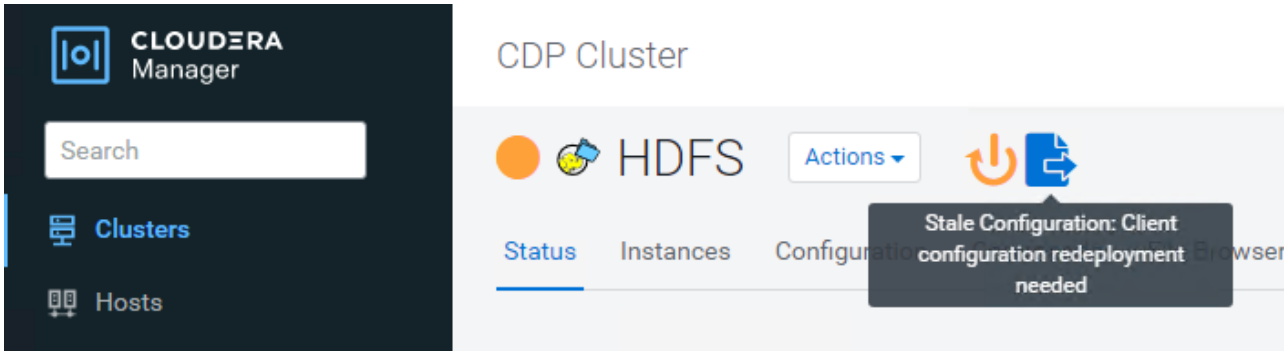
Name	价值
fs.s3a.access.key	< *StorageGRID* 中的租户*S3*访问密钥>
fs.s3a.secret.key	< *StorageGRID* 中的租户*S3*密钥>
fs.s3a.connection.ssl.enabled	true或false (如果缺少此条目、则默认为https)
fs.s3a.endpoint	StorageGRID S3端点：端口>_
fs.s3a.impl	org.apache.hadoop.fs.s3a.s3AFileSystem
fs.s3a.path.style.access	true或false (如果缺少此条目、则默认为虚拟主机模式)

屏幕截图示例



1. 单击保存更改按钮。从HDFS菜单栏中选择陈旧配置图标、在下一页上选择重新启动陈旧服务、然后选

择立即重新启动。



测试与StorageGRID 的S3A连接

执行基本连接测试

登录到Cloudera集群中的一个主机、然后输入`Hadoop FS -ls S3a：//<bucket-name>_/`。

以下示例将使用路径sysle和已有的HDFS-test分段以及一个测试对象。

```
[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.
```

故障排除

场景 **1**

使用HTTPS连接到StorageGRID 、并在15分钟超时后收到`shapore_failure`错误。

*原因：*旧版JRE/JDK使用过时或不受支持的TLS密码套件连接到StorageGRID。

错误消息示例

```
[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
```

*解析：*确保已安装JDK 11.x或更高版本并将其设置为默认Java库。请参见 安装Java软件包 部分、了解更多信息。

场景**2**:

无法连接到StorageGRID 、并显示错误消息`无法找到所请求目标的有效证书路径`。

原因： StorageGRID S3端点服务器证书不受Java程序信任。

错误消息示例：

```
[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
```

解决方法： NetApp建议使用由已知的公有 证书签名颁发机构颁发的服务器证书、以确保身份验证安全。或者、也可以向Java信任存储库添加自定义CA或服务器证书。

要将StorageGRID 自定义CA或服务器证书添加到Java信任存储、请完成以下步骤。

1. 备份现有的默认Java cacerts.

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

2. 将StorageGRID S3端点证书导入到Java信任存储。

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

1. 提高Hadoop日志级别以进行调试。

   ```
   export Hadoop_root_logger = hadoop.root.logger = debug、console
   ```

2. 执行命令、并将日志消息定向到error.log。

   ```
   Hadoop FS -ls S3a：//<bucket-name>_/&>error.log
   ```

作者：郑安杰

使用S3cmd测试和演示StorageGRID 上的S3访问

作者：*Aron Klein*

S3cmd是一个用于S3操作的免费命令行工具和客户端。您可以使用s3cmd在StorageGRID 上测试和演示S3访问。

安装和配置S3cmd

要在工作站或服务器上安装S3cmd、请从下载它 "命令行S3客户端"。s3cmd会作为一种工具预先安装在每个StorageGRID 节点上、以协助进行故障排除。

初始配置步骤

1. s3cmd -configure
2. 请仅提供access_key和secret_key、其余请保留默认值。
3. 是否使用提供的凭据测试访问？[Y/n]：n (跳过测试、因为测试将失败)
4. 是否保存设置？[Y/N] y
   a. 配置已保存到"/root/.s3cfg"
5. 在.s3cfg中、使"="符号后面的字段host_base和host_bucket为空：
   a. host_base =
   b. host_bucket =

如果在步骤4中指定host_base和host_bucket、则无需在命令行界面中使用-host指定端点。示例

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

基本命令示例

- 创建存储分段：

```
s3cmd MB S3：//s3cmdbucket -host=<endpoint>：<port>-no-check-certificate
```

- 列出所有分段：

```
s3ls命令-host=<endpoint>：<port>-no-check-certificate
```

- 列出所有分段及其内容：

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

- 列出特定分段中的对象：

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

- 删除分段：

```
s3RB cmd S3：//s3cmdbucket -host=<endpoint>：<port>-no-check-certificate
```

- 放置对象：

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

- 获取对象：

```
s3cmd get S3：//<bucket>/<object><file>-host=<endpoint>：<port>-no-check-
certificate
```

- 删除对象：

```
s3cmd del S3：//<bucket>/<object>-host=<endpoint>：<port>-no-check-certificate
```

使用NetApp StorageGRID 作为公共存储的Vertica Eon模式数据库

作者：郑安杰

本指南介绍在NetApp StorageGRID 上使用公共存储创建Vertica Eon模式数据库的操作步骤。

简介

Vertica是一款分析数据库管理软件。它是一个柱形存储平台、专为处理大量数据而设计、可在传统密集型情形下实现非常快速的查询性能。Vertica数据库以两种模式之一运行：Eon或Enterprise。您可以在内部或云中部署这两种模式。

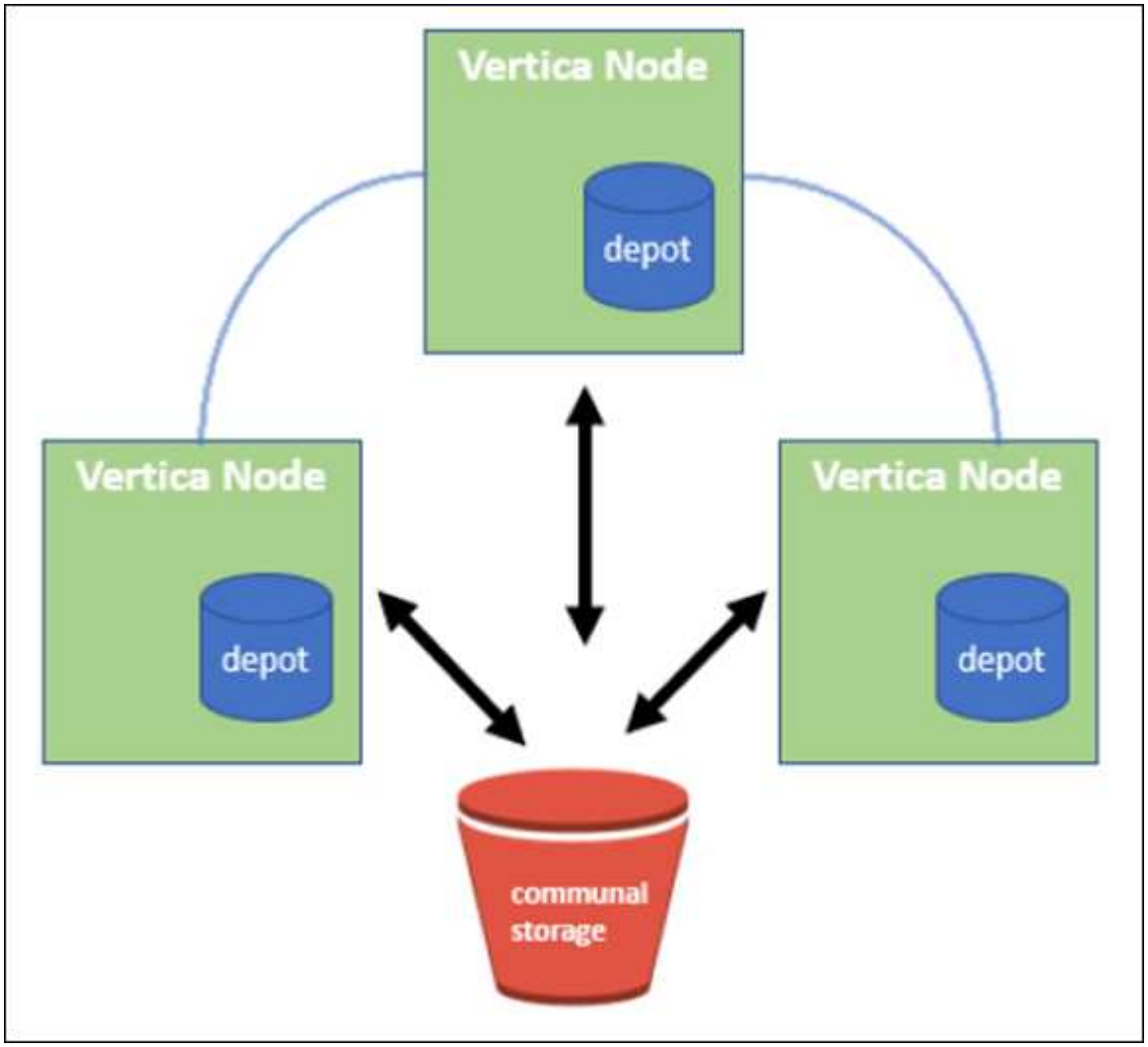
Eon和企业模式在数据存储位置方面主要不同：

- Eon模式数据库使用公共存储来存储其数据。这是Vertica的建议。
- 企业模式数据库将数据本地存储在构成数据库的节点的文件系统中。

Eon模式架构

Eon模式可将计算资源与数据库的公用存储层分离、从而使计算和存储可以单独进行扩展。Eon模式下的Vertica经过优化、可处理各种工作负载、并通过使用单独的计算和存储资源彼此隔离。

Eon模式将数据存储在名为公共存储的共享对象存储中、即S3存储分段、托管在内部或Amazon S3上。



公用存储

Eon模式不会在本地存储数据、而是对所有数据和目录(元数据)使用一个公共存储位置。公共存储是数据库的集中存储位置、在数据库节点之间共享。

公共存储具有以下属性：

- 与单个计算机上的磁盘存储相比、云或内部对象存储中的公共存储更具弹性、并且由于存储故障而不易受到数据丢失的影响。
- 任何使用相同路径的节点都可以读取任何数据。

- 容量不受节点上磁盘空间的限制。
- 由于数据是以社区方式存储的、因此您可以灵活地扩展集群以满足不断变化的需求。如果数据存储在节点本地、则添加或删除节点需要在节点之间移动大量数据、以便将其从要删除的节点或新创建的节点上移出。

仓库

公共存储的一个缺点是速度。从共享云位置访问数据比从本地磁盘读取数据要慢。此外、如果许多节点同时从公共存储读取数据、则与该存储的连接可能会成为瓶颈。为了提高数据访问速度、Eon模式数据库中的节点会维护一个名为存储库的本地数据磁盘缓存。执行查询时、节点会首先检查所需数据是否位于仓库中。如果是、则它将使用数据的本地副本完成查询。如果数据不在存储库中、则节点将从公共存储中提取数据、并在存储库中保存一份副本。

NetApp StorageGRID 建议

Vertica将数据库数据存储在对象存储中、即数千(或数百万)个压缩对象(观察到的大小为每个对象200到500 MB)。当用户运行数据库查询时、Vertica会使用byte-range get调用并行从这些压缩对象检索选定的数据范围。每个字节范围GET大约为8 KB。

在10 TB数据库仓库用户查询测试期间、每秒向网格发送4、000到10、000个GET (字节范围GET)请求。在使用SG6060设备运行此测试时、尽管每个设备节点的CPU利用率百分比较低(约为20%到30%)、但2/3的CPU时间正在等待I/O在SGF6024上观察到I/O等待的百分比非常小(0%到0.5%)。

由于对小型IOPS的需求较高且延迟要求非常低(平均值应小于0.01秒)、NetApp建议对对象存储服务使用SFG6024。如果非常大的数据库需要使用SG6060、则客户应与Vertica客户团队合作进行仓库规模估算、以支持主动查询的数据集。

对于管理节点和API网关节点、客户可以使用SG100或SG1000。选择此选项取决于并行用户查询请求的数量和数据库大小。如果客户希望使用第三方负载平衡器、NetApp建议为高性能需求工作负载配置一个专用的负载平衡器。有关StorageGRID 规模估算、请咨询NetApp客户团队。

其他StorageGRID 配置建议包括：

- 网格拓扑。请勿在同一网格站点上将SGF6024与其他存储设备型号混合使用。如果您希望使用SG6060进行长期归档保护、请在其自己的网格站点(物理或逻辑站点)中为活动数据库保留具有专用网格负载平衡器的SGF6024、以提高性能。在同一站点混用不同型号的设备会降低站点的整体性能。
- 数据保护。使用复制副本进行保护。请勿对活动数据库使用纠删编码。客户可以使用纠删编码对非活动数据库进行长期保护。
- 请勿启用网格压缩。Vertica会先压缩对象、然后再存储到对象存储。启用网格压缩不会进一步节省存储使用量、并且会显著降低字节范围GET性能。
- * HTTP与HTTPS S3端点连接*。在基准测试期间、我们观察到从Vertica集群到StorageGRID 负载平衡器端点使用HTTP S3连接时、性能提高了大约5%。此选项应根据客户的安全要求来选择。

Vertica配置的建议包括：

- 读取和写入操作已启用* Vertica数据库默认存储库设置(值= 1)*。NetApp强烈建议保持启用这些仓库设置以提高性能。
- 禁用流式传输限制。有关配置详细信息、请参见一节 禁用流限制。

在StorageGRID 上使用公用存储在内部安装Eon模式

以下各节介绍了在StorageGRID 上使用公共存储在内部安装Eon模式的顺序操作步骤。用于配置内部简单存储服务(S3)兼容对象存储的操作步骤 类似于Vertica指南中的操作步骤。 "在内部安装Eon模式数据库"。

以下设置用于功能测试：

- StorageGRID 11.4.0.4
- Vertica 10.1.0
- 使用三个虚拟机(VM)和CentOS 7.x操作系统为Vertica节点构建集群。此设置仅用于功能测试、不适用于Vertica生产数据库集群。

这三个节点都设置了安全Shell (SSH)密钥、以允许在集群中的节点之间使用SSH而不使用密码。

NetApp StorageGRID 需要提供的信息

要在StorageGRID 上使用公共存储在内部安装Eon模式、您必须具备以下前提条件信息。

- StorageGRID S3端点的IP地址或完全限定域名(FQDN)和端口号。如果您使用的是HTTPS、请使用在StorageGRID S3端点上实施的自定义证书颁发机构(CA)或自签名SSL证书。
- 存储分段名称。它必须已预先存在且为空。
- 访问密钥ID和密钥访问密钥、对存储分段具有读写访问权限。

创建授权文件以访问S3端点

在创建授权文件以访问S3端点时、需要满足以下前提条件：

- 已安装Vertica。
- 集群已设置、配置完毕、可用于创建数据库。

要创建授权文件以访问S3端点、请执行以下步骤：

1. 登录到要运行`admintools`的Vertica节点以创建Eon模式数据库。

   默认用户为`dbadmin`、在Vertica集群安装期间创建。

2. 使用文本编辑器在`/home/DBadmin`目录下创建文件。文件名可以是所需的任何内容、例如、`sg_auth.conf`。
3. 如果S3端点使用的是标准HTTP端口80或HTTPS端口443、请跳过端口号。要使用HTTPS、请设置以下值：

   - `awsenablehttps = 1`、否则将值设置为`0`。
   - `awsauth =<S3 access key ID>`：<机密访问密钥>
   - `awsendpoint =< StorageGRID S3 Endpoint>`：<端口>

     要对StorageGRID S3端点HTTPS连接使用自定义CA或自签名SSL证书、请指定证书的完整文件路径和文件名。此文件必须位于每个Vertica节点上的同一位置、并对所有用户具有读取权限。如果StorageGRID S3端点SSL证书由公共已知CA签名、请跳过此步骤。

-awscfilm =<文件路径/文件名>

例如、请参见以下示例文件：

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

+

在生产环境中、客户应在StorageGRID S3负载平衡器端点上实施一个由公共已知CA签名的服务器证书。

在所有**Vertica**节点上选择存储库路径

在每个节点上为存储库存储路径选择或创建一个目录。为depot storage path参数提供的目录必须具有以下内容：

- 集群中所有节点上的相同路径(例如、`/home/DBadmin/depot`)
- 可由DBadmin用户读取和写入
- 存储充足

  默认情况下、Vertica会将包含目录的文件系统空间的60%用于存储库存储。您可以在`create_db`命令中使用`-storage-size`参数来限制存储库的大小。请参见 "估算Eon模式数据库的Vertica集群规模" 有关Vertica规模估算一般准则的文章、或者咨询您的Vertica客户经理。

  如果不存在存储库路径、`admintools create_db`工具会尝试为您创建一个路径。

创建**Eon**内部数据库

要创建Eon内部数据库、请执行以下步骤：

1. 要创建数据库、请使用`admintools create_db`工具。

   以下列表简要说明了本示例中使用的参数。有关所有必需参数和可选参数的详细说明、请参见Vertica文档。

   - -x <在中创建的授权文件的路径/文件名 "创建授权文件以访问S3端点" >。

     成功创建后、授权详细信息将存储在数据库中。您可以删除此文件、以避免公开S3密钥。

   - -communal-storage-location <S3：//storagegrid bucketname>
   - -s <用于此数据库的Vertica节点的逗号分隔列表>
   - -d <要创建的数据库名称>
   - -p <要为此新数据库设置的密码>。例如、请参见以下命令示例：

```
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>'
```

根据数据库的节点数、创建新数据库需要几分钟的持续时间。首次创建数据库时、系统将提示您接受许可协议。

例如、请参见以下授权文件示例和`create db`命令：

```
[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.
```

对象大小(字节)	存储分段/对象密钥完整路径
61	s 3 : //Vertica/051/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a07/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a07_0_0_0.dfs
145	s 3 : //Vertica/2c4/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a3d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a3d_0dfdfd0.dfdf
146	s 3 : //Vertica/33c/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a1d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a1d_0_dfdfd.df
40	s 3 : //Vertica/382/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a31/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a31_0_0.dfs
145	s 3 : //Vertica/42f/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a21/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a21a21a21_0_0.dfs
34	s 3 : //Vertica/472/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a25/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a25_0_0.dfs
41	s 3 : //Vertica/476/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a2d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a2d_0_0.dfs
61	s 3 : //Vertica/52a/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a5d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a5d_0_dfdfd.df
131	s 3 : //Vertica/5d2/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a19/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a19_0_0.dfs

对象大小(字节)	存储分段/对象密钥完整路径
91	s 3 : //Vertica/5F7/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a11/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a11_0_0.dfs
118	s 3 : //Vertica/82d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a15/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a15_0_0.dfs
115	s 3 : //Vertica/9a2/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a61/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a61_0_0.dfs
33	s 3 : //Vertica/ACD/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021a29-026d63ae9d4a33237bf0e2c2cf2a794a00a000021a29_0_0.dfs
133	s 3 : //Vertica/b98/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a4d/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a4d_0_dfdfd.df
38	s 3 : //Vertica/db3/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a49-026d63ae9d4a33237bf0e2c2cf2a794a00a000021a49_0_0.dfs
38	s 3 : //Vertica/EBA/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a599/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a59_0_0.dfs
21521920	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a000000002152/026d63ae9d4a33237bf0e2c2cf2a794a00a00002152.tar

对象大小(字节)	存储分段/对象密钥完整路径
6865408	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021602/026d63ae9d4a33237bf0e2c2cf2a794a00a00002162.tar
204217344	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021610/026d63ae9d4a33237bf0e2c2cf2a794a00a000021610.tar
16109056	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000217e0/026d63ae9d4a33237bf0e2c2cf2a794a00a0000217e0.tar
12853248	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021800/026d63ae9d4a33237bf0e2c2cf2a794a00a00002180.tar
8937984	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000002187a/026d63ae9d4a33237bf0e2c2cf2a794a00a00002187a.tar
56260608	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000218b2/026d63ae9d4a33237bf0e2c2cf2a794a00a0000218b2.tar
53947904	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000219ba/026d63ae9d4a33237bf0e2c2cf2a794a00a0000219ba.tar

对象大小(字节)	存储分段/对象密钥完整路径
44932608	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000219de/026d63ae9d4a33237bf0e2c2cf2a794a00a0000219de.tar
256306688	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021a6e/026d63ae9d4a33237bf0e2c2cf2a794a00a000021a6e.tar
8062464	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021e34-026d63ae9d4a33237bf0e2c2cf2a794a00a000021e34.tar
20024832	s 3 : //Vertica/metadata/VMart/Libraries/026d63ae9d4a33237bf0e2c2cf2a794a00a00000000021e70/026d63ae9d4a33237bf0e2c2cf2a794a00a000021e70.tar
10444	s 3 : //Vertica/metadata/VMart/cluster_config.json
823266	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0016/Catalog/859703b06a3456d95d0be28575a673/checkpoints/c13_chkpt_1.cat.gz
254	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0016/Catalog/859703b06a3456d95d0be28575a673/checkpoints/c13/已完成
2958	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0016/Catalog/859703b06a3456d95d0be28575a673/checkpoints/c2_chkpt_1.cat.gz

对象大小(字节)	存储分段/对象密钥完整路径
231	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/checkpoints/c2_completed
822521	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/checkpoints/c4_chkpt_1.cat.gz
231	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/checkpoints/c4_4/completed
746513	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_14_g14.cat
2596	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_3_g3.cat.gz
821065	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_4_g4.cat.gz
6440	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_5_g5.cat
8518	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_8_g8.cat
0	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0016/Catalog/859703b06a3456d95d0be2 8575a673/tiered_catalog.cat

对象大小(字节)	存储分段/对象密钥完整路径
822922	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0017/Catalog/859703b06a3456d95d0be28575a673/checkpoint/C14_7/chkpt_1.cat.gz
232	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0017/Catalog/859703b06a3456d95d0be28575a673/checkpoint/C14_7/completed
822930	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0017/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat
0	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0017/Catalog/859703b06a3456d95d0be28575a673/tiered_catalog.cat
822922	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0018/Catalog/859703b06a3456d95d0be28575a673/checkpoint/C14_7/chkpt_1.cat.gz
232	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0018/Catalog/859703b06a3456d95d0be28575a673/checkpoint/C14_7/completed
822930	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_14_g7.cat.gz
755033	s 3 : //Vertica/metadata/VMart/nodes/v_vmartnode0018/Catalog/859703b06a3456d95d0be28575a673/Txnlogs/txn_15_g8.cat

对象大小(字节)	存储分段/对象密钥完整路径
0	s 3 ：//Vertica/metadata/VMart/nodes/v_vmart node0018/Catalog/859703b06a3456d95d0be2 8575a673/tiered_catalog.cat

禁用流限制

此操作步骤 基于适用于其他内部对象存储的Vertica指南、应适用于StorageGRID。

1. 创建数据库后、通过将`AWSStreamingConnectionPercentage`配置参数设置为`0`来禁用该参数。对于使用公共存储的Eon模式内部安装、不需要此设置。此配置参数用于控制Vertica用于流式读取的对象存储连接数。在云环境中、此设置有助于避免对象存储中的流式数据占用所有可用的文件句柄。它会使某些文件句柄可用于其他对象存储操作。由于内部对象存储的延迟较低、因此没有必要使用此选项。
2. 使用`vsql`语句更新参数值。此密码是您在"创建Eon内部数据库"中设置的数据库密码。例如、请参见以下示例输出：

```
[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
```

验证返厂设置

已为读写操作启用Vertica数据库默认存储库设置(值= 1)。NetApp强烈建议保持启用这些仓库设置以提高性能。

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

加载示例数据(可选)

如果此数据库用于测试并将被删除、您可以将样本数据加载到此数据库以进行测试。Vertica随附了示例数据集VMart、位于每个Vertica/node/opt/Vertica/Examples/VMart_Schema/``下。有关此示例数据集的详细信息、请参见 "此处"。

按照以下步骤加载示例数据：

1. 以DBadmin身份登录到Vertica节点之一：cd /opt/vertica/examples/VMart_Schemas/

2. 将示例数据加载到数据库中、并在子步骤c和d中出现提示时输入数据库密码：
   a. `cd /opt/vertica/examples/VMart_Schema`
   b. 。`/vmart根`
   c. `vsql< vmart定义架构.sql`
   d. `vsql < vmart load_data.sql`
3. 有多个预定义的SQL查询、您可以运行其中一些查询、以确认测试数据已成功加载到数据库中。例如：`vsql < vmart queries1.sql`

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- "NetApp StorageGRID 11.7产品文档"
- "StorageGRID 数据表"
- "Vertica 10.1产品文档"

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2021年9月	初始版本。

作者：郑安杰

使用ELK堆栈进行StorageGRID 日志分析

作者：郑安杰

通过StorageGRID系统日志转发功能、您可以配置外部系统日志服务器来收集和分析StorageGRID日志消息。ELK (Elasticsearch、Logstash、Kibana)已成为最受欢迎的日志分析解决方案之一。观看以查看示例的 "使用ELK视频进行StorageGRID 日志分析" 模拟配置、以及如何使用它来识别失败的S3请求并对其进行故障排除。StorageGRID均衡器支持将负载平衡器端点访问日志导出到外部系统日志服务器。观看此视频 "YouTube视频"、了解有关此新功能的更多信息。本文提供了Logstash配置、Kibana查询、图表和信息板的示例文件、可帮助您快速开始StorageGRID 日志管理和分析。

要求

- StorageGRID 11.6.0.2或更高版本
- ELK (Elasticsearch、Logstash和Kibana)已安装并运行7.1x或更高版本

示例文件

- "下载Logstash 7.x示例文件包" +* MD5 checksum* 148c23d0021d9a4bb4a6c0287464deab +* SHA256 checksum* f5ec9e2e3f842d5a7861566b167a561b4373038b4e7bb3b3d522adf2d6

- "下载Logstash 8.x示例文件包" +* MD5 checksum* e11ba3a662f87c3ef363d0fe06835 +* SHA256 checksum* 5c670755742cfdf5aa723a596b087e0153a65bcaef3934afdb682f61cd278d
- "下载适用于StorageGRID 11.9的Logstash 8.x示例文件包"+* md5校验和* 41272857c4a54600f95995f6ed74800d +* SHA256校验和* 77048ee86610527 19990851e1ad960d4902fe537a6e135e8600177188da677c9

假设

读者熟悉StorageGRID 和ELK的术语和操作。

说明

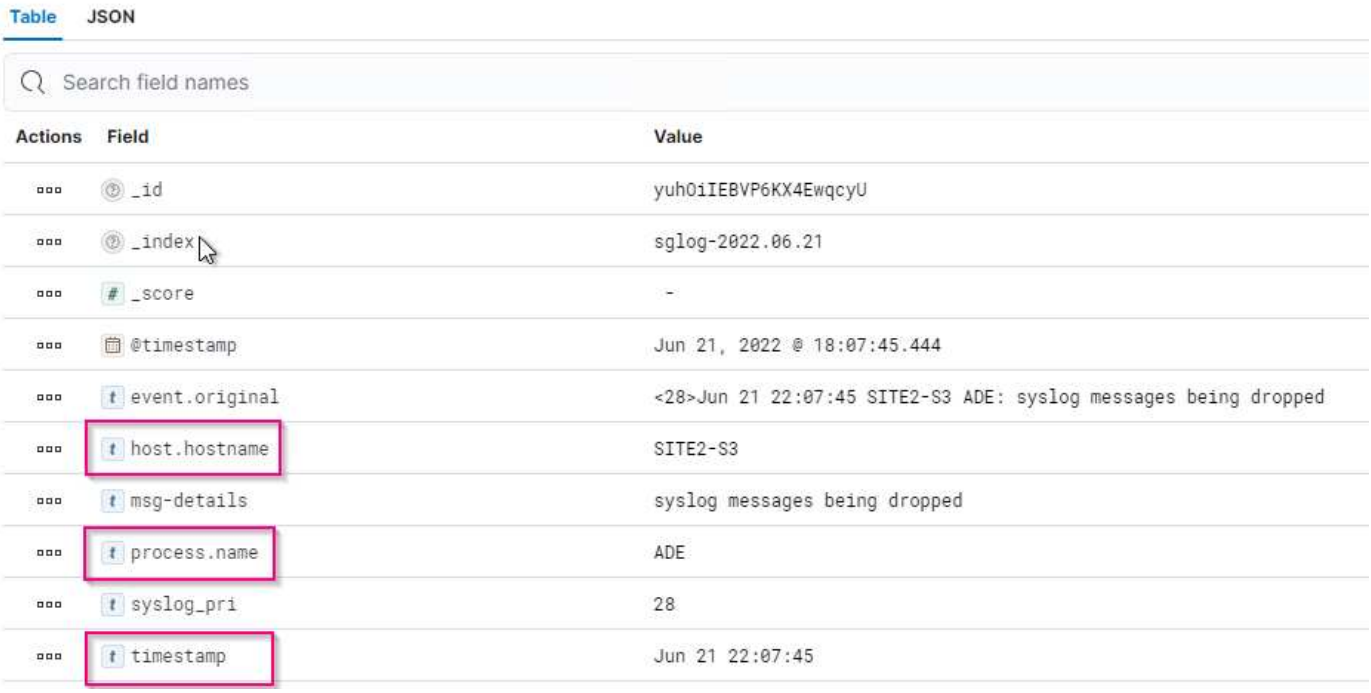
由于Grok模式定义的名称不同、因此提供了两个示例版本。+例如、Logstash配置文件中的SYSLOGBASE格式根据安装的Logstash版本定义不同的字段名称。

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

- Logstash 7.17示例*

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示例*



- 步骤 *

1. 根据您安装的ELK版本解压缩提供的示例。此示例文件夹包含两个Logstash配置示例：* sglog-2-file.conf：此配置文件会将**StorageGRID** 日志消息输出到**Logstash**上的文件中、而不会进行数据转换。您可以使用此命令来确认**Logstash**正在接收**StorageGRID** 消息、或者帮助了解**StorageGRID** 日志模式。+ sglog-2-es.conf：*此配置文件使用各种模式和筛选器转换StorageGRID 日志消息。其中包括示例drop语句、这些语句根据模式或筛选器丢弃消息。输出将发送到Elasticsearch以编制索引。+根据文件中的说明自定义选定的配置文件。
2. 测试自定义的配置文件：

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

如果返回的最后一行与以下行类似、则此配置文件没有语法错误：

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

3. 将自定义的conf文件复制到Logstash服务器的配置：/etc/logstash/conf.d+如果尚未在/etc/logstash/logstash.yml中启用config.reload.automatic、请重新启动Logstash服务。否则、请等待配置重新加载间隔过。

```
 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
```

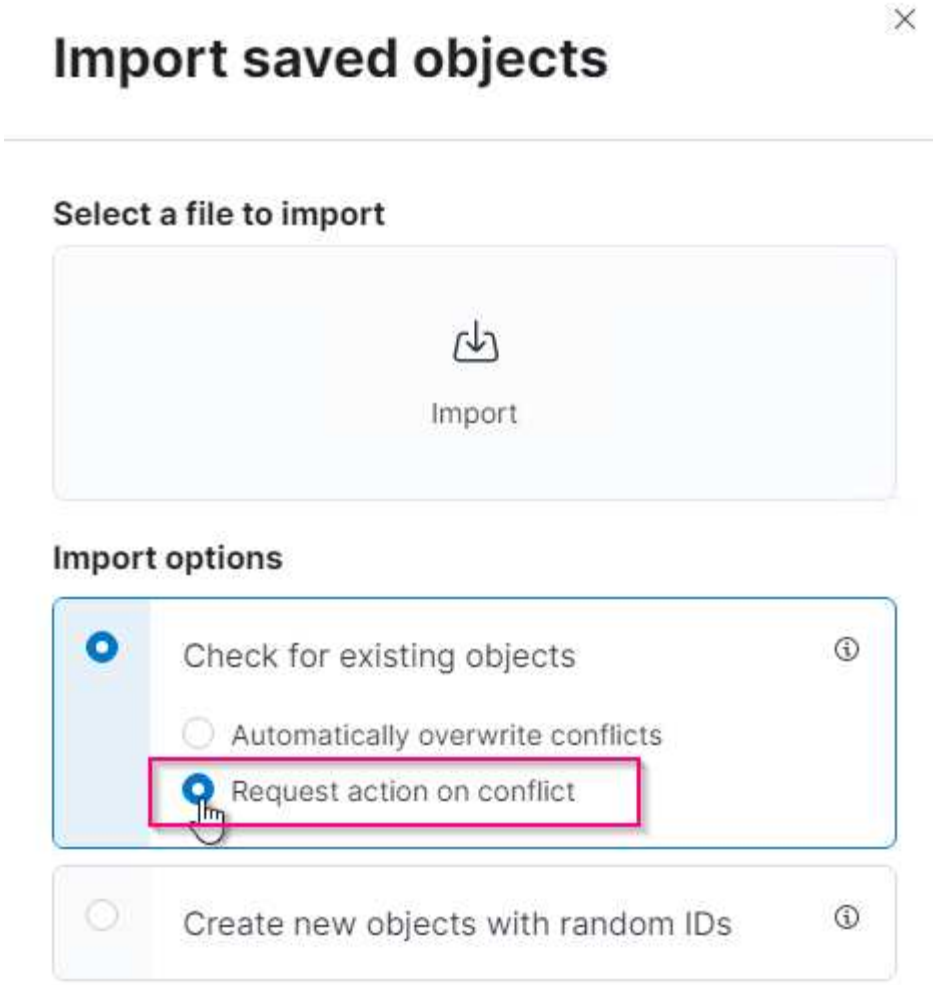
4. 检查/var/log/logstash/logstash-plain.log并确认在使用新配置文件启动Logstash时没有错误。
5. 确认TCP端口已启动并正在侦听。+在此示例中、使用TCP端口5000。

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

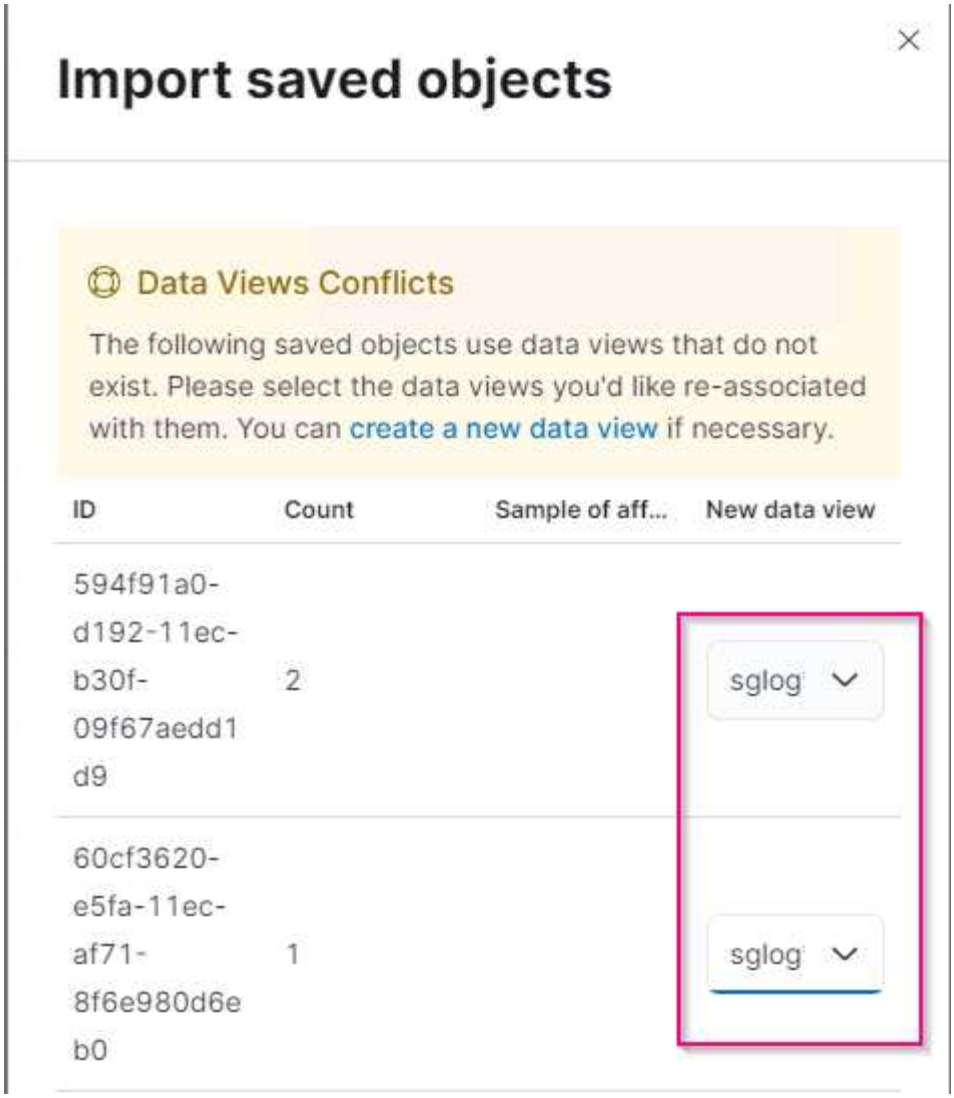
6. 在StorageGRID 管理器图形用户界面中、配置外部系统日志服务器以向Logstash发送日志消息。有关详细信息、请参见 "演示视频" 。
7. 您需要在Logstash服务器上配置或禁用防火墙、以允许StorageGRID 节点连接到定义的TCP端口。
8. 在Kibana GUI中、选择Management → Dev Tools。在控制台页面上、运行此get命令以确认已在Elasticsearch上创建新索引。

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

9. 在Kibana GUI中、创建索引模式(ELK 7.x)或数据视图(ELK 8.x)。
10. 在Kibana GUI的顶部中间的搜索框中输入"saved objects"。+在已保存对象页面上、选择导入。在导入选项下、选择"请求冲突操作"



导入ELK <version>-query-chart -sample.ndjson。+当系统提示您解决冲突时、请选择您在第8步中创建的索引模式或数据视图。



导入了以下基巴纳对象：* Query** audy-msg-s3rq-orln * bycast log S3相关消息* loglevel WARNING或 以上+失败的安全事件**+** NGINS-GW端点访问日志(仅在elk8-sSample—for-sg119.zip中提供)* Chart** S3请求计数(基于bycast.log * HTTP状态)按审核类型分类**)+ S3***信息板**+**审核请求的平均响应时间**)**。

现在、您可以使用Kibana执行StorageGRID 日志分析了。

其他资源

- "系统日志101"
- "什么是ELK堆栈"
- "Grok模式列表"
- "Logstash入门指南：Grok"
- "Logstash实用指南：系统日志深度剖析"
- "Kibana指南—浏览文档"
- "StorageGRID 审核日志消息参考"

使用Prometheus和Grafana延长指标保留期限

作者：*Aron Klein*

本技术报告详细说明了如何为NetApp StorageGRID 11.6配置外部Prometheus和Grafana服务。

简介

StorageGRID 使用Prometheus存储指标、并通过内置的Grafana信息板对这些指标进行可视化。通过配置客户端访问证书并为指定客户端启用Prometheus访问、可以从StorageGRID 安全地访问Prometheus指标。目前、此指标数据的保留受管理节点存储容量的限制。为了获得更长的持续时间并能够创建这些指标的自定义可视化效果、我们将部署一个新的Prometheus和Grafana服务器、配置我们的新服务器以从StorageGRID实例中擦除这些指标、并使用对我们重要的指标构建一个信息板。您可以获取有关在中收集的Prometheus指标的详细信息 "StorageGRID 文档"。

联合**Prometheus**

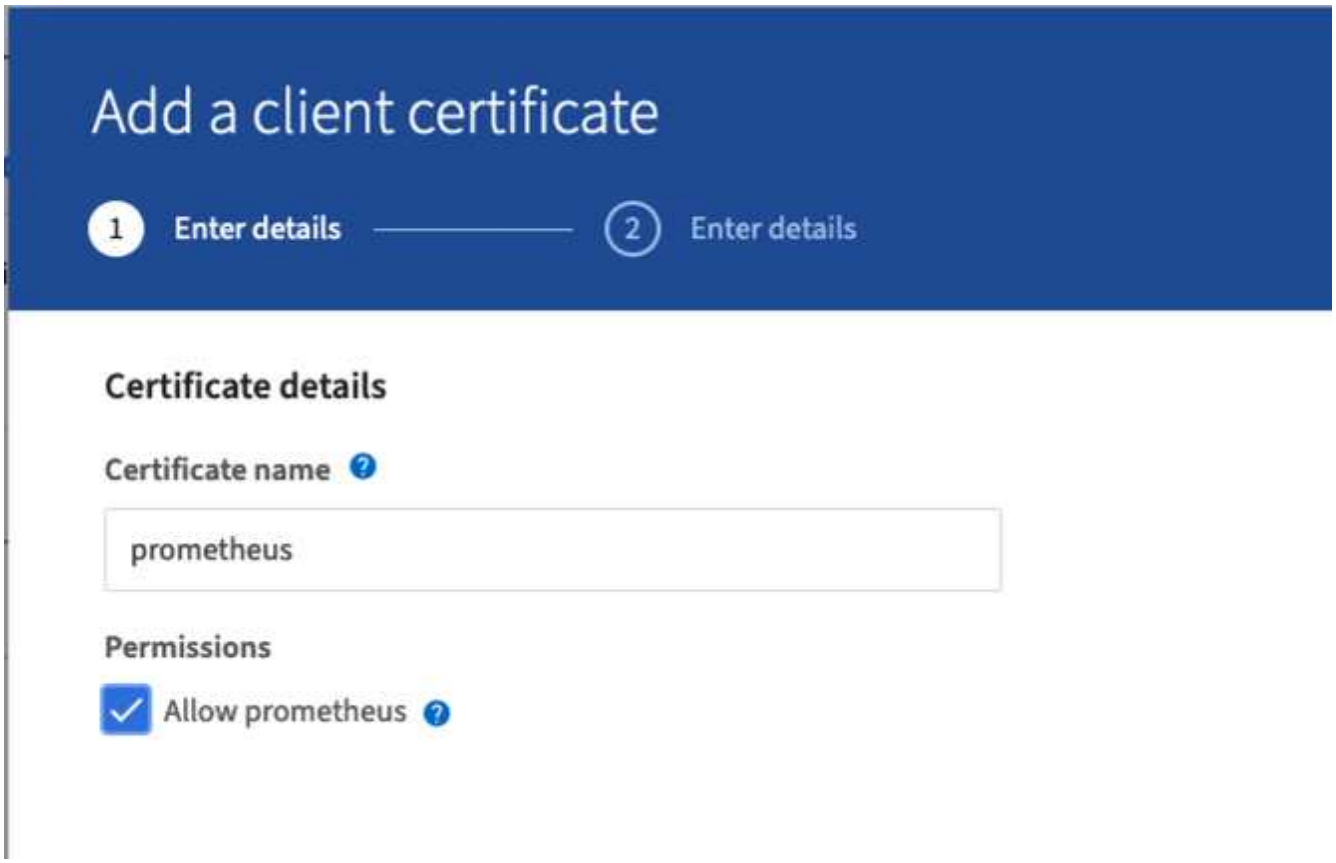
实验室详细信息

在本示例中、我将使用StorageGRID 11.6节点的所有虚拟机以及Debian 11服务器。StorageGRID 管理界面配置了一个公共信任的CA证书。本示例将不会介绍StorageGRID 系统或Debian Linux安装的安装和配置过程。您可以使用Prometheus和Grafana支持的任何Linux模式。Prometheus和Grafana都可以安装为Docker容器、从源代码构建或预编译的二进制文件。在此示例中、我将直接在同一Debian服务器上安装Prometheus和Grafana二进制文件。从下载并按照基本安装说明进行操作 https://prometheus.io 和 https://grafana.com/grafana/ 。

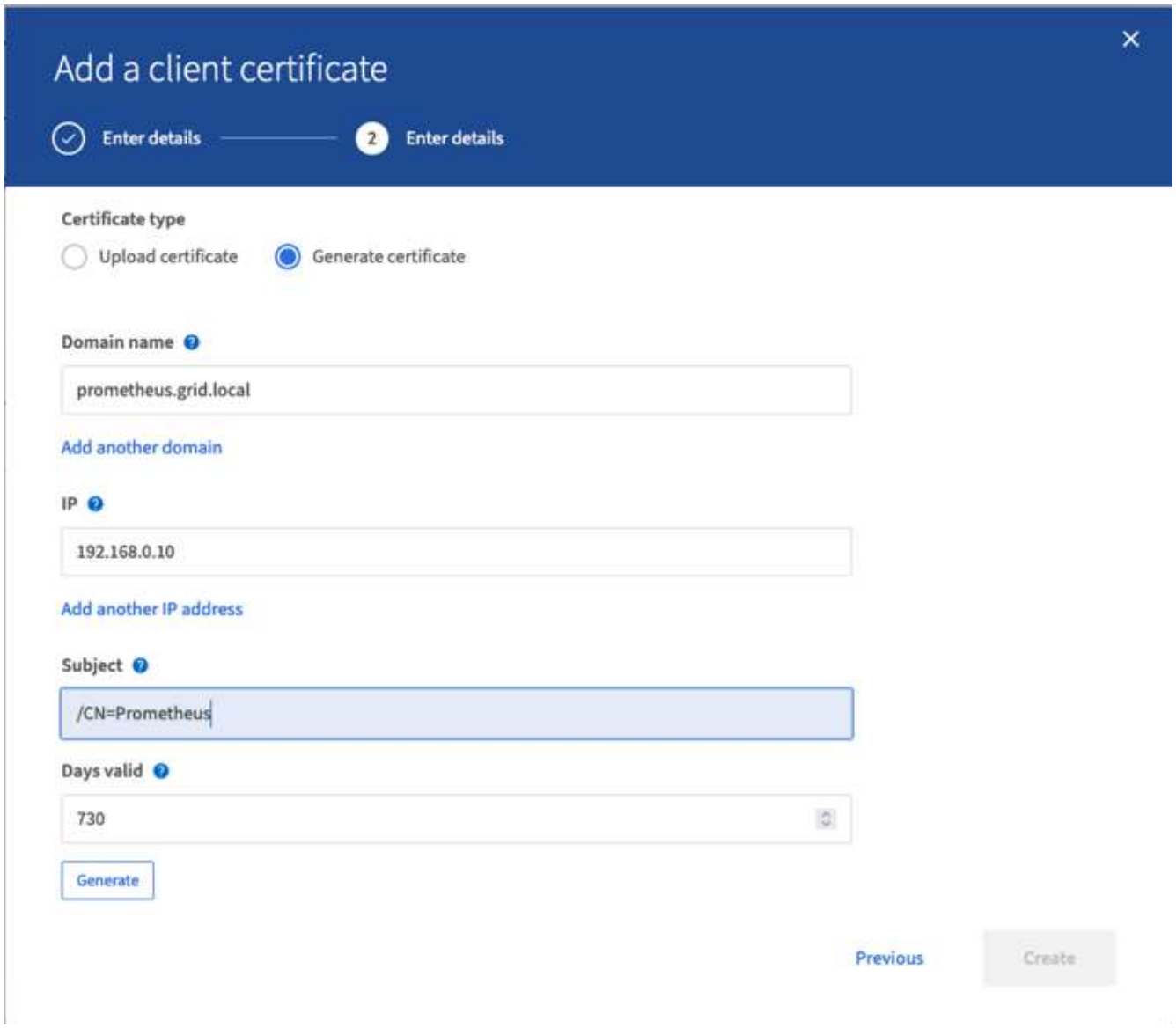
为**Prometheus**客户端访问配置**StorageGRID**

要访问StorageGRID Stored Prometheus指标、您必须生成或上传具有专用密钥的客户端证书、并为客户端启用权限。StorageGRID 管理接口必须具有SSL证书。此证书必须由Prometheus服务器信任、或者由可信CA信任、如果是自签名证书、则此证书必须手动受信任。要了解更多信息、请访问 "StorageGRID 文档"。

1. 在StorageGRID 管理界面中、选择左下方的"configuration"、然后在第二列的"Security"下单击Certificates。
2. 在"证书"页面上、选择"客户端"选项卡、然后单击"添加"按钮。
3. 提供要授予访问权限的客户端的名称并使用此证书。单击"允许用户"前面的"权限"下的框、然后单击"继续"按钮。

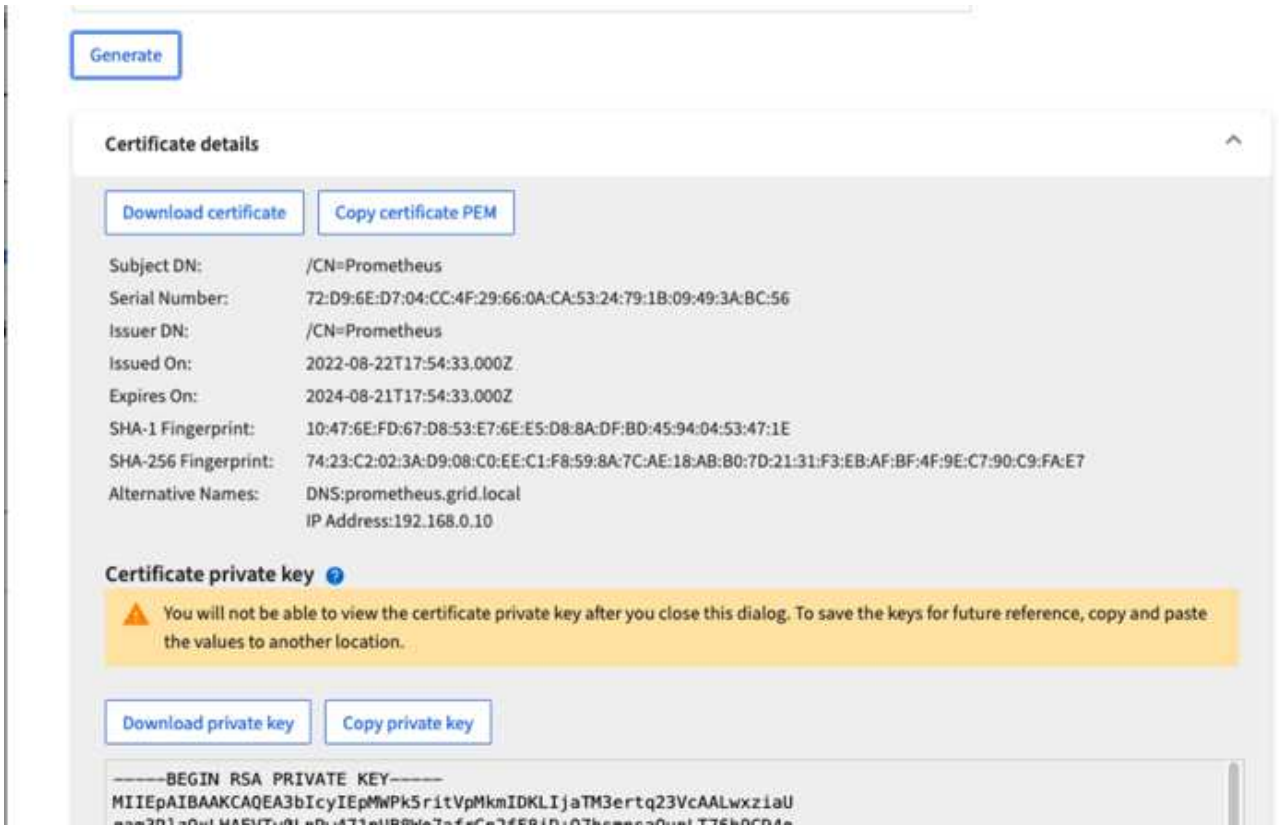


4. 如果您拥有CA签名的证书、则可以选择"上传证书"单选按钮、但在我们的情况下、我们将通过选择"生成证书"单选按钮让StorageGRID 生成客户端证书。此时将显示要填写的必填字段。输入客户端服务器的FQDN、服务器的IP、主题和有效天数。然后单击"生成"按钮。



> 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. 下载证书对等文件和专用密钥对等文件。



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

准备**Linux**服务器以安装**Prometheus**

在安装Prometheus之前、我希望为我的环境做好准备、让Prometheus用户、目录结构做好准备、并为指标存储位置配置容量。

1. 创建Prometheus用户。

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

2. 为Prometheus、客户端证书和指标数据创建目录。

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

3. 我使用ext4文件系统格式化了用于指标保留的磁盘。

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

4. 然后、我将文件系统挂载到Prometheus指标目录。

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

5. 获取用于指标数据的磁盘的UUID。

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

6. 在/etc/fstab/中添加一个条目、使挂载在重新启动后仍会使用/dev/sdb的uuid。

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

安装和配置**Prometheus**

现在、服务器已准备就绪、我可以开始安装Prometheus并配置此服务。

1. 提取Prometheus安装包

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

2. 将二进制文件复制到/usr/local/bin、并将所有权更改为先前创建的Prometheus用户

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

3. 将控制台和库复制到/etc/Prometheus

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

4. 将先前从StorageGRID 下载的客户端证书和专用密钥对等文件复制到/etc/Prometheus/Certs
5. 创建Prometheus配置YAML文件

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

6. 插入以下配置。作业名称可以是您所需的任何名称。将"-targets"更改为管理节点的FQDN、如果更改了证书名称和专用密钥文件名、请更新tls_config部分以使其匹配。然后保存文件。如果您的网格管理界面正在使用自签名证书、请下载此证书并将其与具有唯一名称的客户端证书一起放置、然后在tls_config部分中添加ca_file：/etc/Prometheus/Cert/UIcert.pem

   a. 在此示例中、我将收集以alertmanager、Cassandra、node和StorageGRID 开头的所有指标。您可以在中查看有关Prometheus指标的详细信息 "StorageGRID 文档"。

```
# 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']
```

如果网格管理界面使用的是自签名证书、请下载此证书并将其与具有唯一名称的客户端证书一起放置。在tls_config部分中、将证书添加到客户端证书和专用密钥行上方

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

1. 将/etc/Prometheus和/var/lib/Prometheus中所有文件和目录的所有权更改为Prometheus用户

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

2. 在/etc/systemd/system中创建一个Prometheus服务文件

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

3. 插入以下行、请注意#-storage.tsdb.retention.time=1y#、它会将指标数据的保留期限设置为1年。或者、您也可以使用#-storage.tsdb.retention.size=300GiB#根据存储限制确定保留期限。这是设置指标保留的唯一位置。

```
[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. 重新加载systemd服务以注册新的Prometheus服务。然后启动并启用Prometheus服务。

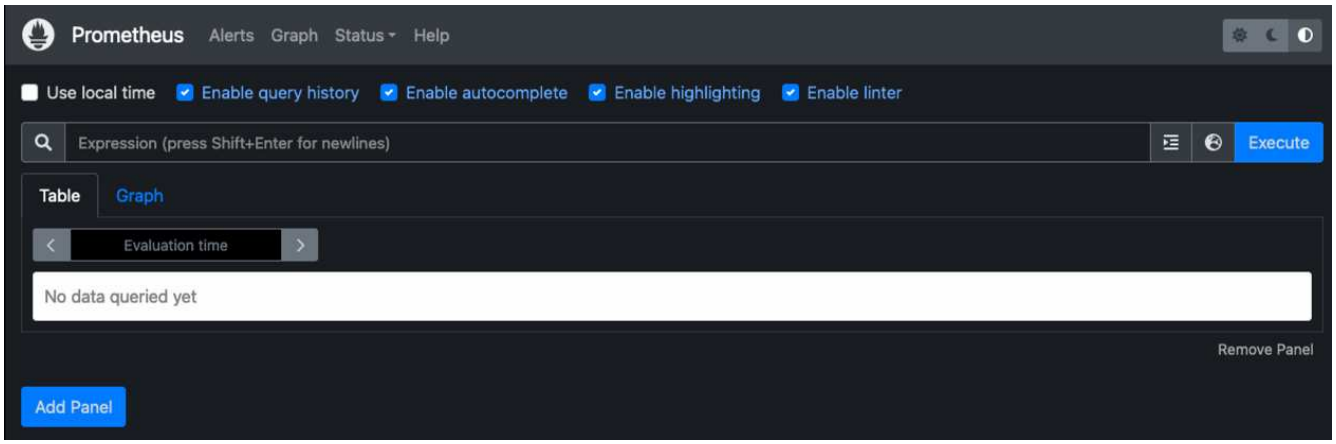
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. 检查服务是否运行正常

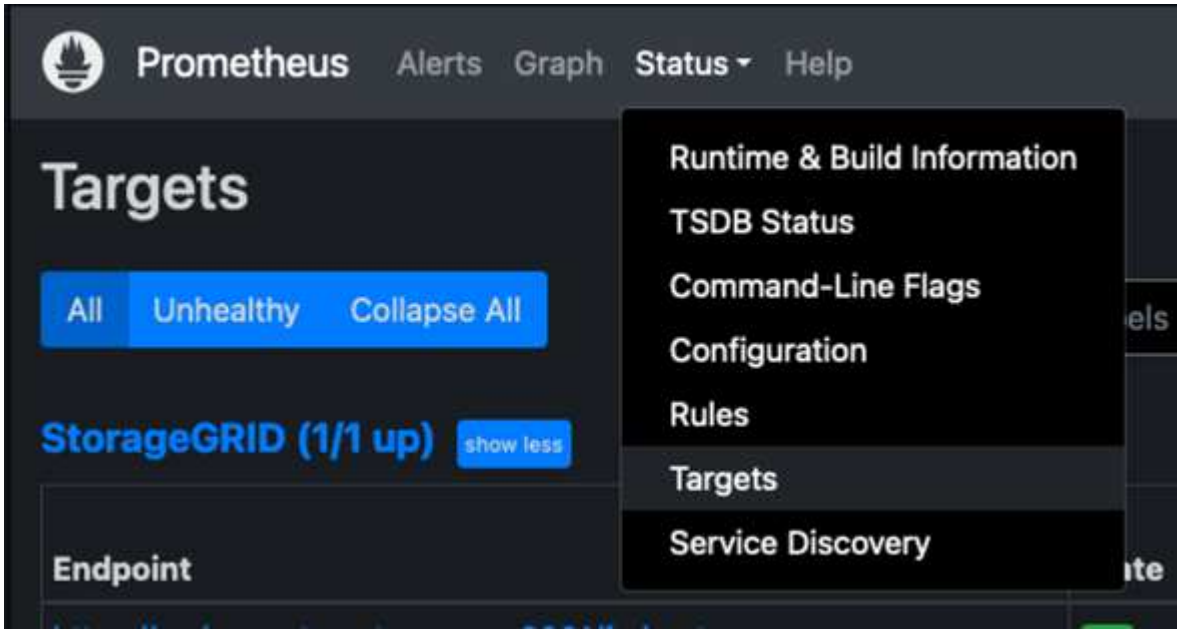
```
sudo systemctl status prometheus
```

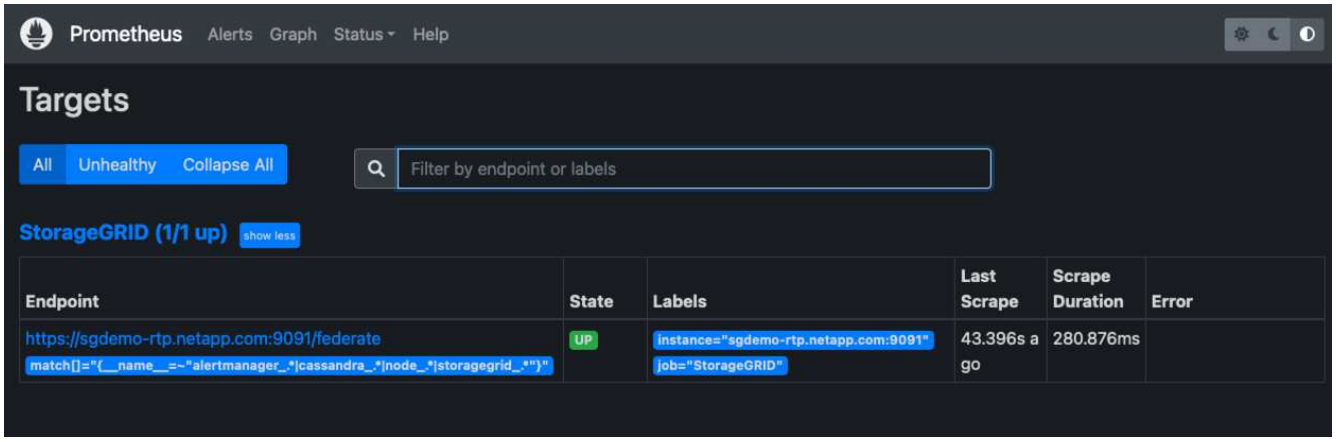
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: 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. 现在、您应该能够浏览到Prometheus服务器的UI http://Prometheus-server:9090 并查看UI

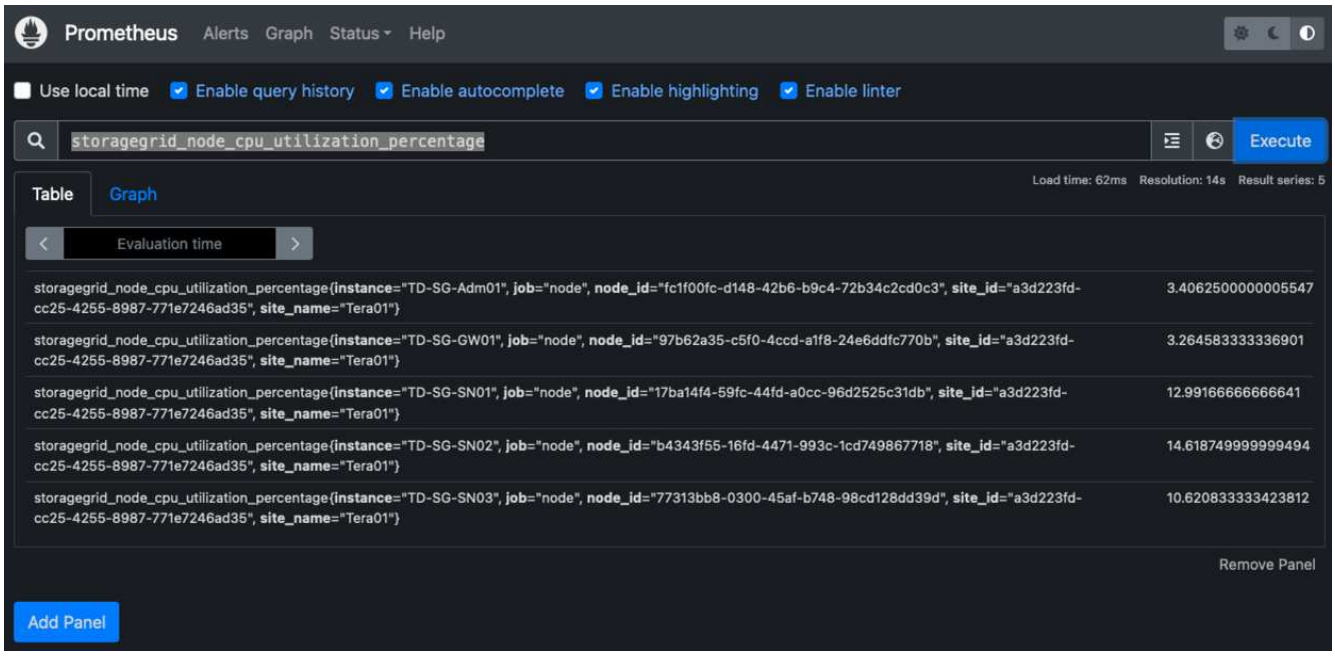


7. 在"Status" Targets下、您可以看到我们在Prometheus.yml中配置的StorageGRID 端点的状态





8. 在图形页面上、您可以执行测试查询并验证数据是否已成功擦除了。例如、在查询栏中输入"storagegRid_node_cpu_utilization_percentage "、然后单击执行按钮。



安装和配置Grafana

在Prometheus安装完毕并正常工作之后、我们可以继续安装Grafana并配置信息板

Grafana安装

1. 安装最新的企业版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. 为稳定版本添加此存储库：

```
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. 添加存储库后。

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

4. 重新加载systemd服务以注册新的grafana服务。然后启动并启用Grafana服务。

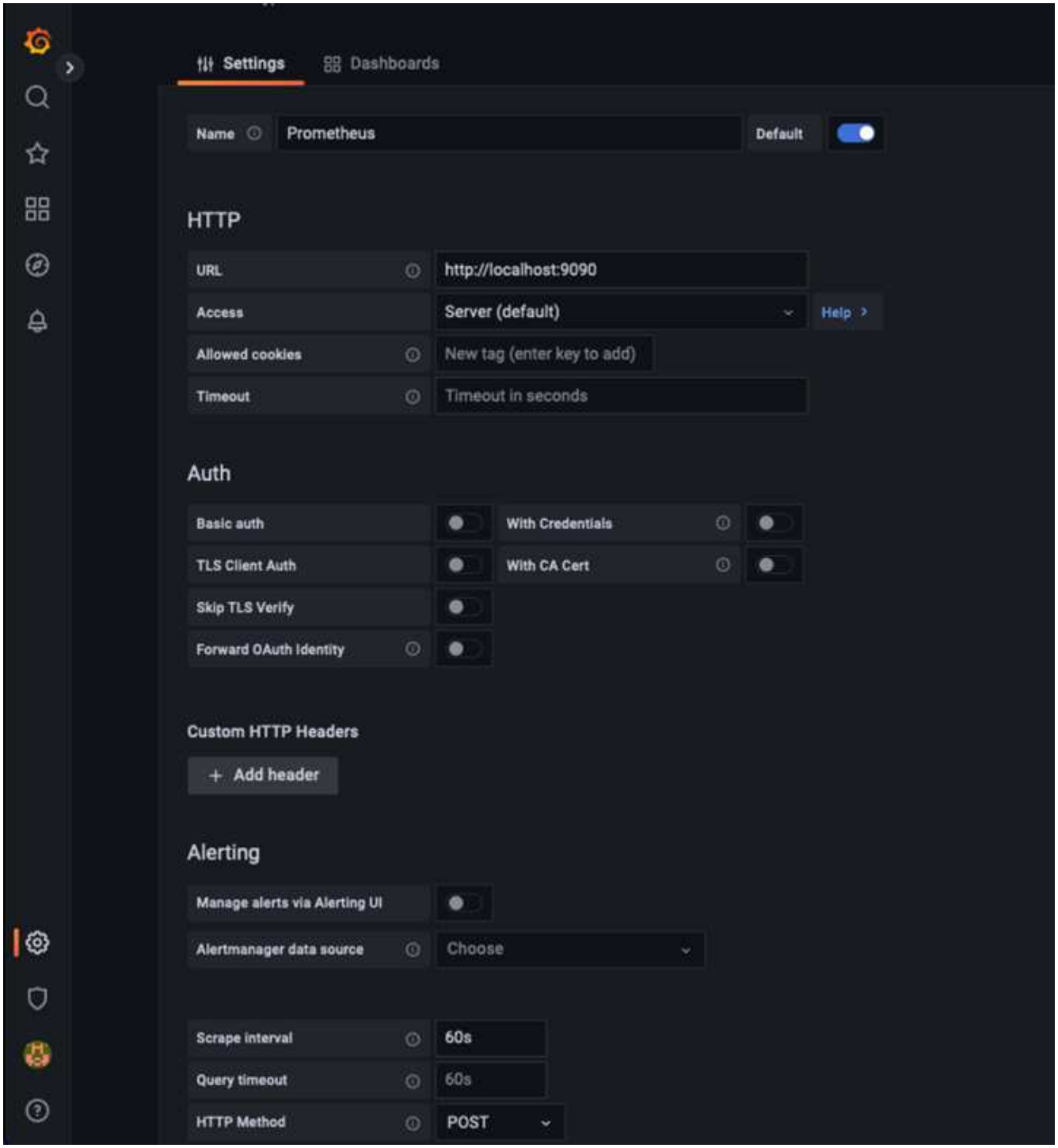
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

5. 现在、Grafana已安装并正在运行。打开浏览器访问HTTP：//Prometheus-server：3000时、您将看到Grafana登录页面。
6. 默认登录凭据为admin/admin、您应根据提示设置新密码。

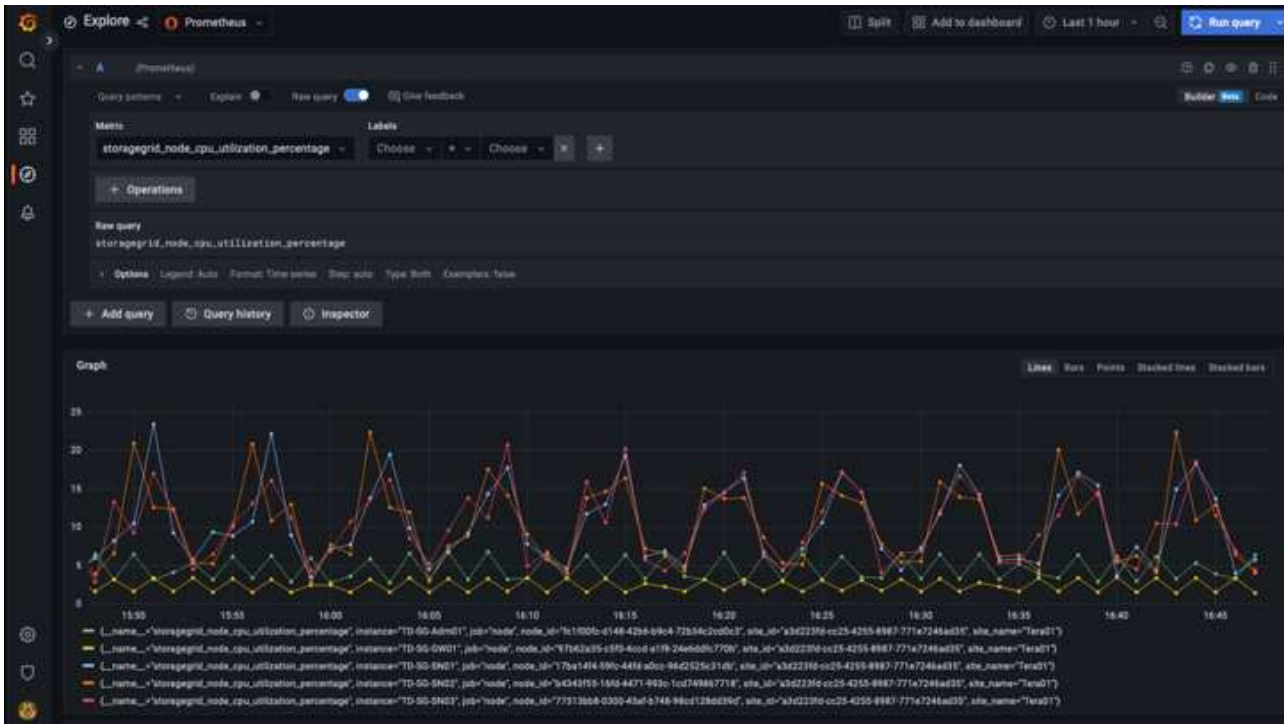
为**StorageGRID** 创建**Grafana**信息板

在Grafana和Prometheus安装并运行的情况下、现在是时候通过创建数据源和构建信息板来连接这两者了

1. 在左侧窗格中、展开"配置"并选择"数据源"、然后单击"添加数据源"按钮
2. Prometheus将是可供选择的顶级数据源之一。如果不是、请使用搜索栏找到"Prometheus"
3. 通过输入Prometheus实例的URL以及与Prometheus间隔匹配的擦除间隔来配置Prometheus源。我还禁用了警报部分、因为我未在Prometheus上配置警报管理器。



4. 输入所需设置后、向下滚动到底部、然后单击"Save & test"(保存并测试)
5. 配置测试成功后、单击Explore按钮。
   a. 在"浏览"窗口中、您可以使用我们使用"storagegrid node_cpu_utilization_percentage "测试的相同指标、然后单击"运行查询"按钮

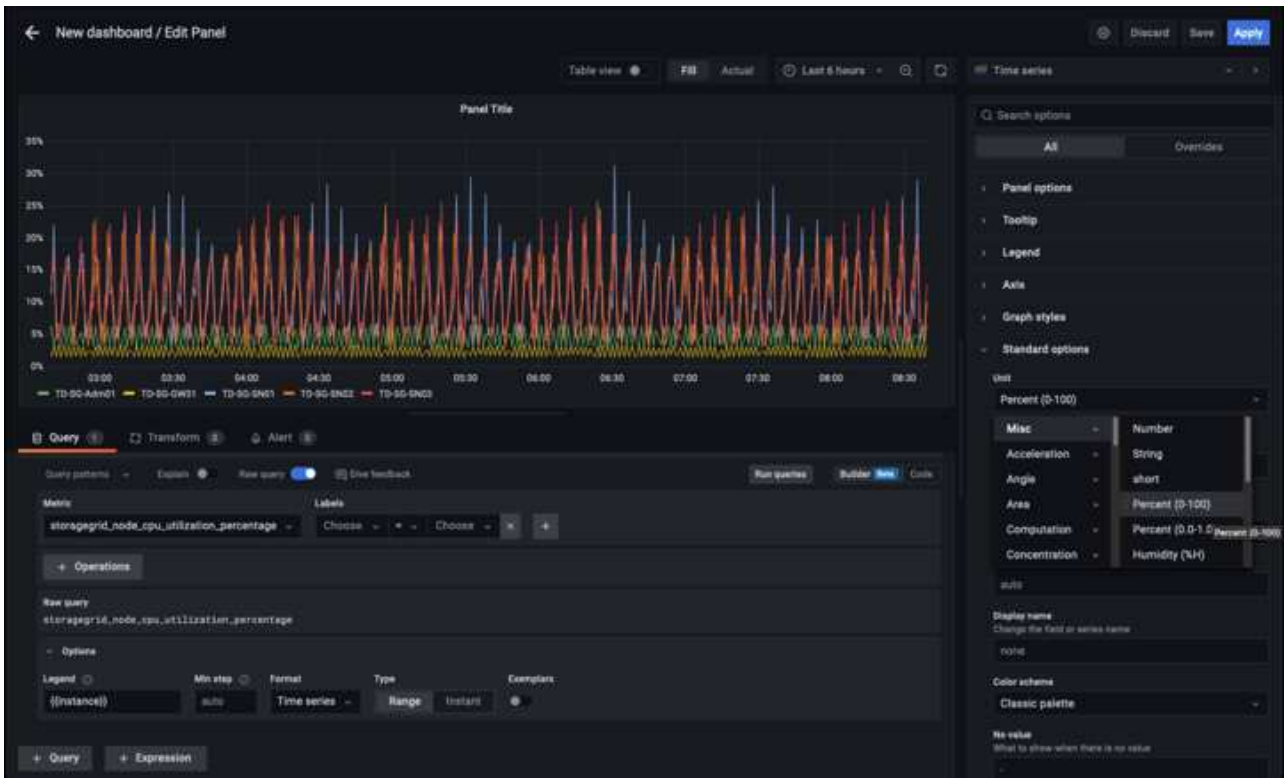


6. 现在、我们已配置数据源、可以创建一个信息板。

   a. 在左侧窗格中、展开Dashboards、然后选择"+" new Dashboard"

   b. 选择"添加新面板"

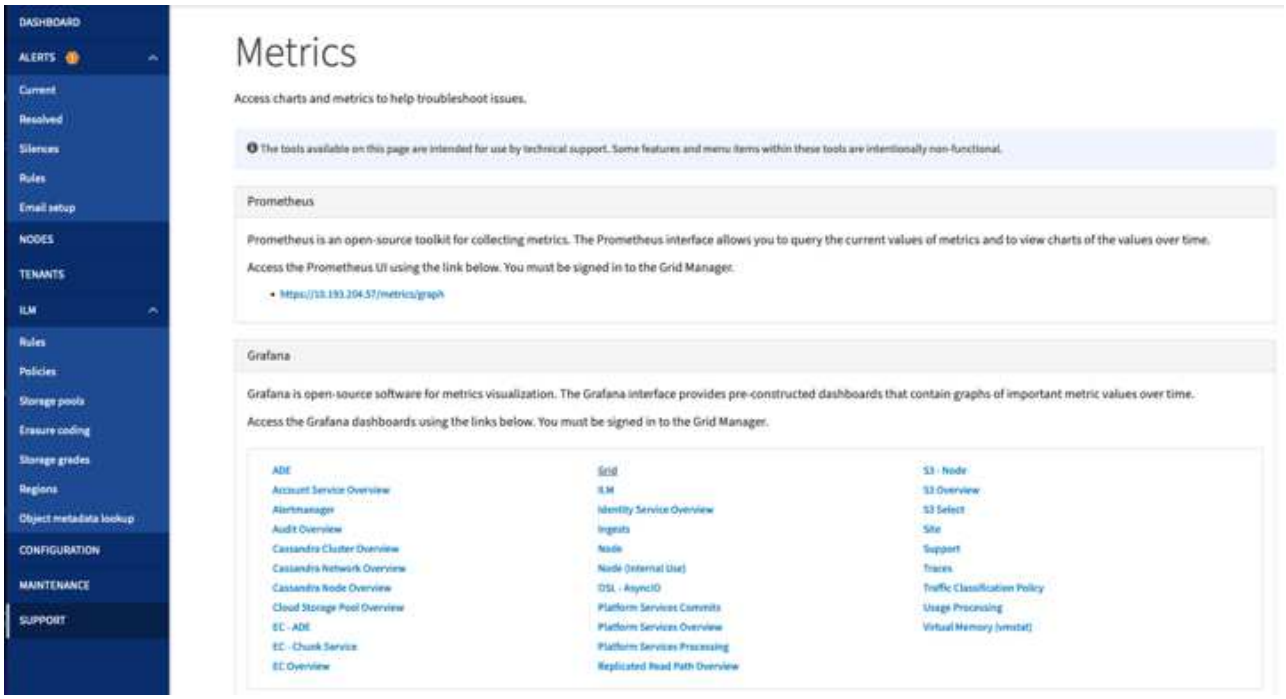
   c. 通过选择指标来配置新面板、我将再次使用"storagegrid node_cpu_utilization_percentage "、输入面板标题、展开底部的"选项"、并将图例更改为自定义、然后输入" ｛ {instance} ｝ "来定义节点名称、并在右侧窗格的"标准选项"下将"单元"设置为"Misc 100/percent (0%)"。然后单击"应用"将面板保存到信息板。



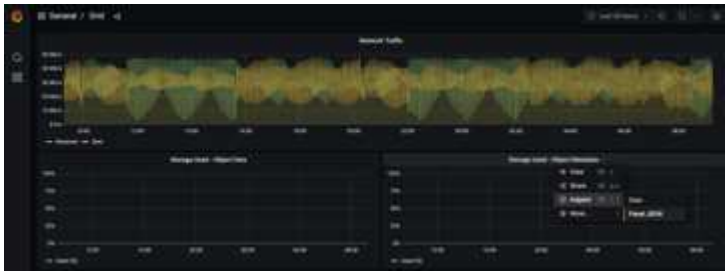
7. 我们可以继续为所需的每个指标构建这样的信息板、但幸运的是、StorageGRID 已经拥有包含面板的信息板、我们可以复制到自定义信息板中。

   a. 从StorageGRID 管理界面的左侧窗格中、选择"Support"、然后在"Tools"列的底部单击"Metrics "。

   b. 在指标中、我将选择中间列顶部的"网格"链接。

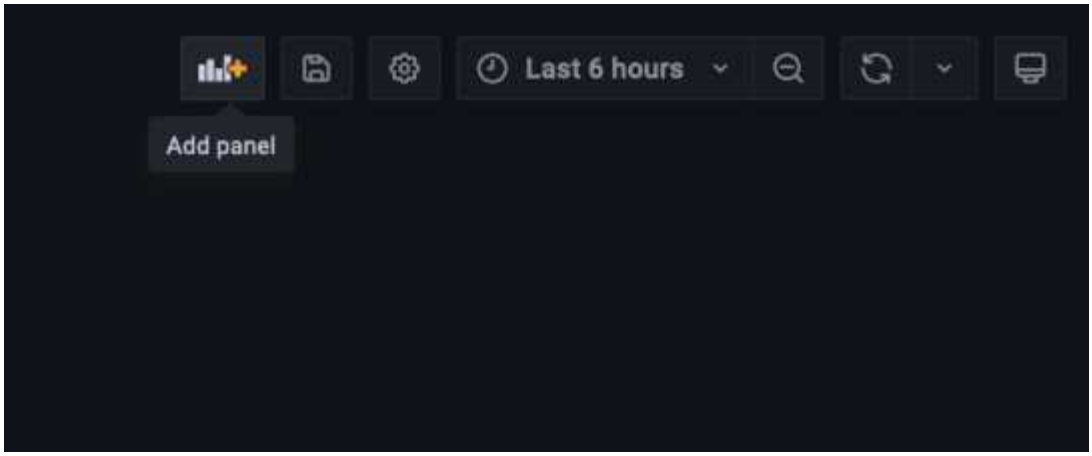


   c. 在网格信息板中、我们选择"已用存储-对象元数据"面板。单击小下箭头和面板标题的末尾以下拉菜单。从此菜单中选择"检查"和"面板JSON"。



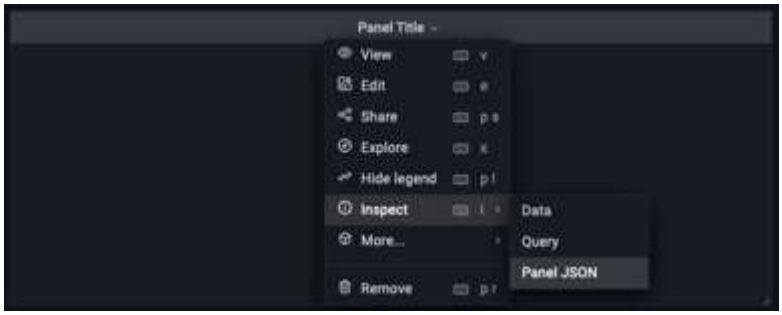
   d. 复制JSON代码并关闭窗口。

e. 在新信息板中、单击图标以添加新面板。

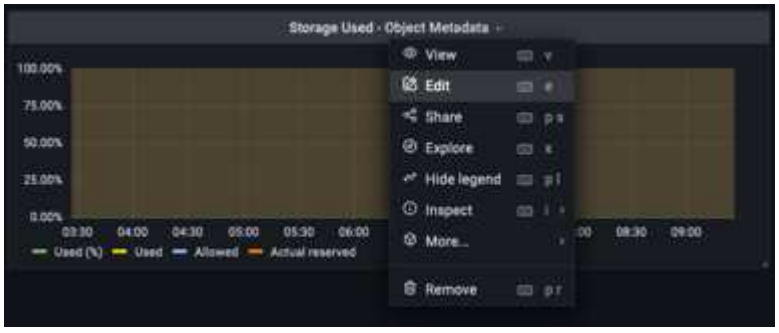


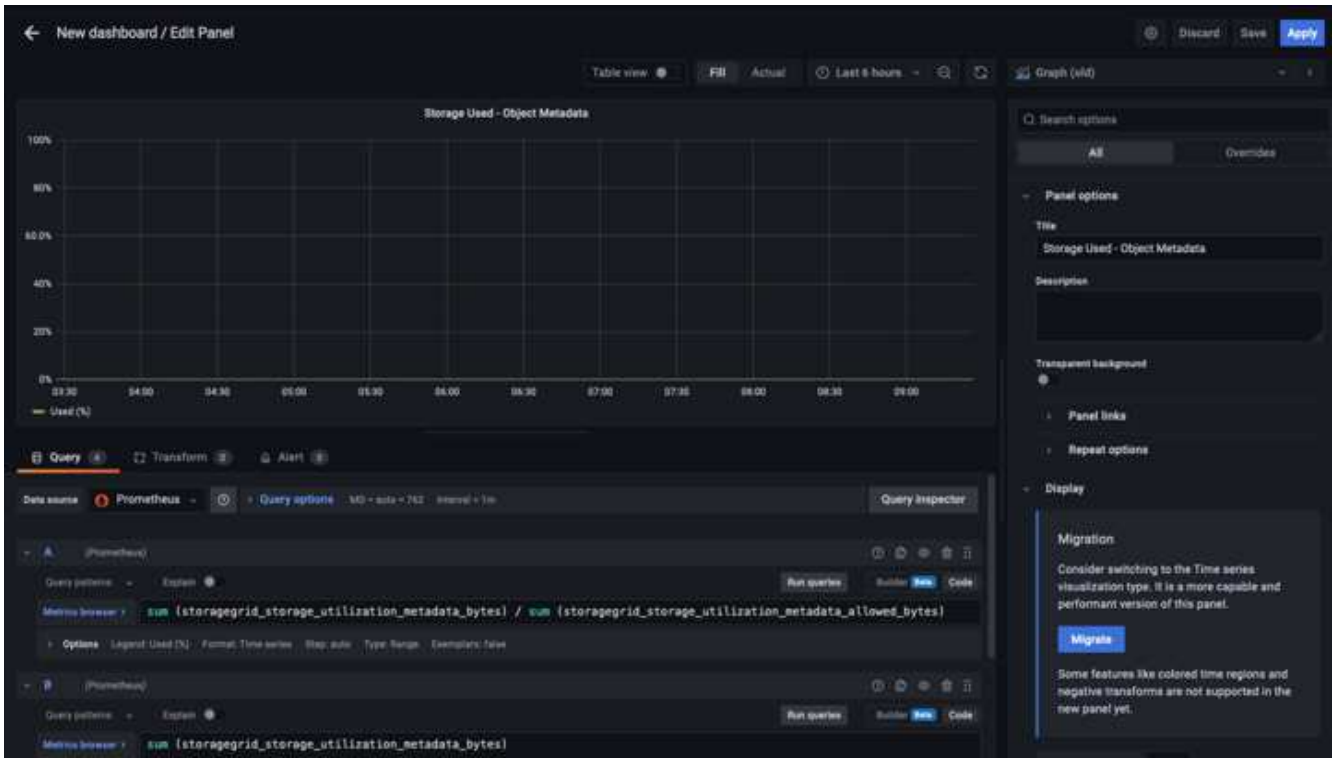
f. 应用新面板而不进行任何更改

g. 就像使用StorageGRID 面板一样、检查JSON。从StorageGRID 面板中删除所有JSON代码并将其替换为复制的代码。



h. 编辑新面板、在右侧、您将看到一条带有"迁移"按钮的迁移消息。单击按钮、然后单击"应用"按钮。





8. 将所有面板安装到位并根据需要进行配置后。单击右上角的磁盘图标以保存信息板、并为您的信息板指定一个名称。

结论

现在、我们推出了一款具有可自定义数据保留和存储容量的Prometheus服务器。这样、我们就可以继续构建自己的信息板、其中包含与我们的运营最相关的指标。您可以获取有关在中收集的Prometheus指标的详细信息 "StorageGRID 文档"。

Datadog SNMP配置

作者：*Aron Klein*

配置Datadog以收集StorageGRID SNMP指标和陷阱。

配置Datadog

Datadog是一种监控解决方案 、可提供指标、可视化和警报功能。以下配置是在StorageGRID 系统本地部署的Ubuntu 22.04.1主机上使用Linux代理版本7.43.1实施的。

从**StorageGRID MIB**文件生成的数据日志配置文件和陷阱文件

Datadog提供了一种将产品MIB文件转换为映射SNMP消息所需的数据日志参考文件的方法。

按照找到的说明生成用于数据日志陷阱解析映射的StorageGRID YAML文件 "此处"。+将此文件放在/etc/datadog-agent/conf.d/snmp.d/traps_db/+中

- "下载陷阱YAML文件" +

- * MD5校验和* 42e27e4210719945a46172b98c379517 +
- * SHA256校验和* d0fe5c8e6ca3c902d054f854b70a85f928cb8b7c76391d356f05d2cf73b6887 +

此StorageGRID 配置文件YAML文件用于数据日志指标映射、此文件是按照找到的说明生成的 "此处"。+将此文件放置在/etc/datadog-agent/conf.d/snmp.d/profiles/+中

- "下载配置文件YAML文件" +
  - * MD5校验和* 72bb7784f4801adda4e0c3ea77df19aa +
  - * SHA256校验和* b6b7fadd330 63422a8bb8e39b3ead8ab38349ee0229926eadc8585f0087b8cee +

用于衡量指标的**SNMP Datadog**配置

可以通过两种方式管理为指标配置SNMP。您可以通过提供包含StorageGRID 系统的网络地址范围来配置自动发现、也可以定义各个设备的IP。根据所做的决定、配置位置会有所不同。自动发现在数据日志代理YAML文件中定义。在SNMP配置YAML文件中配置显式设备定义。以下是同一StorageGRID 系统中的每个示例。

自动发现

配置位于/etc/datadog-agent/datadog.yaml中

```
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
```

单个设备

/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'
```

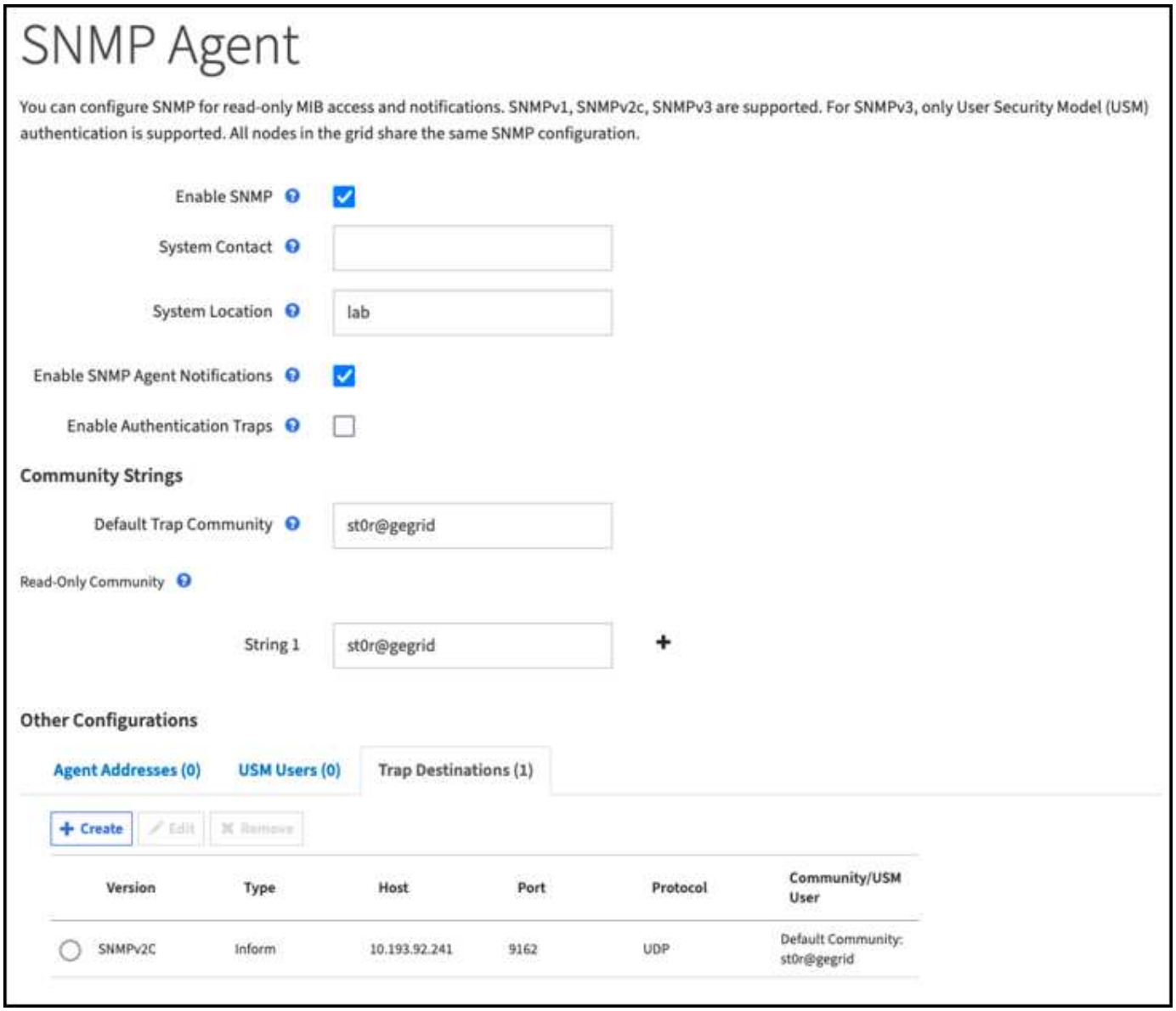
陷阱的**SNMP**配置

SNMP陷阱的配置在datadog配置yaml文件/etc/datadog-agent/datadog.yaml中定义

```
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
```

StorageGRID SNMP配置示例

StorageGRID 系统中的SNMP代理位于配置选项卡的监控列下。启用SNMP并输入所需信息。如果要配置陷阱、请选择"陷阱目标"并为包含陷阱配置的Datadog代理主机创建一个目标。



使用rclone在StorageGRID 上迁移、放置和删除对象

作者：Siegfried Hepp和Aron Klein_

rclone是一种用于S3操作的免费命令行工具和客户端。您可以使用rclone迁移、复制和删除StorageGRID 上的对象数据。rclone可以删除存储分段、即使不是空存储分段也可以使用"清除"功能、如以下示例所示。

安装和配置rclone

要在工作站或服务器上安装rclone、请从下载它 "rclone.org"。

初始配置步骤

1. 通过运行配置脚本或手动创建文件来创建rclone配置文件。
2. 在此示例中、我将使用sgdemo作为rclone配置中远程StorageGRID S3端点的名称。
   a. 创建配置文件~/.config/rclone/rclone.conf

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

b. 运行rclone config

rclone配置#

```
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
```

基本命令示例

- 创建存储分段：

  `rclone mkdir remote:bucket`

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

  如果需要忽略SSL证书、请使用-no-check-certificate。

- 列出所有分段：

```
rclone lsd remote:
```

rclone LSD sgdemo数：

- 列出特定分段中的对象：

```
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
```

- 删除分段：

```
rclone rmdir remote:bucket
```

rclone rmdir sgdemo：test02

- 放置对象：

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

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

- 获取对象：

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

rclone copy sgdemo：test01/testfile.txt ~/test/testfileS3.txt

- 删除对象：

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

rclone delete sgdemo：test01/testfile.txt

- 迁移存储分段中的对象

```
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
```

使用-progress或-P显示任务的进度。否则、不会显示任何输出。

- 删除分段和所有对象内容

```
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
```

使用Veeam备份和复制进行部署的StorageGRID最佳实践

作者：*Oliver Haensel*和*Aron Klein*

本指南重点介绍NetApp StorageGRID以及部分Veeam备份和复制的配置。本白皮书面向熟悉Linux系统并负责维护或实施NetApp StorageGRID系统与Veeam备份和复制的存储和网络管理员。

概述

存储管理员希望通过满足可用性、快速恢复目标、可扩展以满足其需求以及自动执行长期数据保留策略的解决方案来管理数据增长。这些解决方案还应提供保护、防止丢失或恶意攻击。Veeam和NetApp合作创建了一个将Veeam备份和恢复与NetApp StorageGRID相结合的数据保护解决方案、用于内部对象存储。

Veeam和NetApp StorageGRID提供了一个易于使用的解决方案、可协同工作、帮助满足全球数据快速增长和法规不断增长的需求。基于云的对象存储因其弹性、扩展能力、运营效率和成本效益而闻名、这使其成为备份目标的自然选择。本文档将为Veeam Backup解决方案和StorageGRID系统的配置提供指导和建议。

Veeam的对象工作负载会为小型对象创建大量并发放置、删除和列表操作。启用不可迁移性将增加对对象存储的请求数量、以设置保留和列出版本。备份作业的过程包括为每日更改写入对象、新写入完成后、该作业将根据备份的保留策略删除任何对象。备份作业的计划几乎总是重叠的。这种重叠将导致备份窗口的很大一部分在对象存储上包含50/50的放置/删除工作负载。在Veeam中调整任务插槽设置的并发操作数、通过增加备份作业块大小来增加对象大小、减少多对象删除请求中的对象数量、 选择完成作业的最长时间窗口将优化解决方案的性能和成本。

请务必阅读的产品文档 "Veeam备份和复制" 和 "StorageGRID" 开始之前。Veeam提供了一些计算器、用于了解Veeam基础架构的规模估算以及在调整StorageGRID 解决方案 规模之前应使用的容量要求。请始终访问Veeam Ready计划网站查看经Veeam-NetApp验证的配置 "Veeam Ready对象、对象不可变性和存储库"。

Veeam配置

建议版本

建议始终保持最新、并为Veeam Backup & Replication 12或12.1系统应用最新的修补程序。目前、我们建议至少安装Veeam 12修补程序P20230718。

S3存储库配置

横向扩展备份存储库(SOBR)是S3对象存储的容量层。容量层是主存储库的扩展、可提供更长的数据保留期限和更低的存储解决方案成本。Veeam能够通过S3对象锁定API提供不可变功能。Veeam 12可以在一个横向扩展存储库中使用多个分段。StorageGRID对单个存储分段中的对象数量或容量没有限制。使用多个分段可以提高备份非常大的数据集时的性能、在这些数据集中、对象中的备份数据可能会达到PB级。

可能需要限制并发任务、具体取决于特定解决方案的规模估算和要求。默认设置为每个CPU核心指定一个存储库任务插槽、并发任务插槽限制为64。例如，如果服务器有2个CPU核心，则对象存储总共将使用128个并发线程。这包括Put、GET和批删除。建议先为任务时隙选择一个保守限制、并在Veeam备份达到新备份和即将过期备份数据的稳定状态后调整此值。请与您的NetApp客户团队合作、适当估算StorageGRID系统的规模、以满足所需的时间窗口和性能要求。要提供最佳解决方案、可能需要调整任务插槽数量和每个插槽的任务限制。

备份作业配置

Veeam备份作业可以使用不同的块大小选项进行配置、应仔细考虑这些选项。默认块大小为1 MB、而Veeam具有数据压缩和重复数据删除功能、可为初始完整备份创建大约500 KB的对象大小、为增量作业创建100-200 KB的对象大小。通过选择更大的备份块大小、我们可以大幅提高性能并降低对象存储的要求。尽管较大的块大小可以显著提高对象存储的性能、但由于存储效率性能降低、可能会增加主存储容量需求。建议为备份作业配置4 MB的块大小、以便为完整备份创建大约2 MB的对象、并为增量备份创建大约700 kB-1 MB的对象大小。客户甚至可以考虑使用8 MB块大小配置备份作业、此功能可在Veeam支持人员的协助下启用。

实施不可配置备份时会使用对象存储上的S3对象锁定。不可更改性选项会生成更多的对象存储请求、以更新对象的列表和保留。

随着备份保留过期、备份作业将处理对象删除。Veeam以多对象删除请求的形式将删除请求发送到对象存储、每个请求1000个对象。对于小型解决方案、可能需要对此进行调整、以减少每个请求的对象数量。降低此值还可以更均匀地在StorageGRID系统中的节点之间分布删除请求。建议使用下表中的值作为配置多对象删除限制的起点。将表中的值乘以所选设备类型的节点数、即可获得Veeam中设置的值。如果此值等于或大于1000、则无需调整默认值。如果需要调整此值、请与Veeam支持部门合作进行更改。

设备型号	每个节点的**S3MultiObjectDeleteLimit**
SG5712	34.
SG5760	75
SG6060	200

请与您的NetApp客户团队合作、根据您的特定需求确定建议的配置。Veeam配置设置建议包括：

- 备份作业块大小= 4 MB
- SOBR任务插槽限制为2-16
- 多对象删除限制= 34 - 1000

StorageGRID配置

建议版本

对于Veeam部署、建议使用带有最新修补程序的NetApp StorageGRID 11.7或11.8.建议始终保持最新、并为StorageGRID系统应用最新的修补程序。

负载平衡器和**S3**端点配置

Veeam仅要求通过HTTPS连接端点。Veeam不支持非加密连接。SSL证书可以是自签名证书、专用可信证书颁发机构或公共可信证书颁发机构。为了确保持续访问S3存储库、建议在HA配置中至少使用两个负载平衡器。负载平衡器可以是位于每个管理节点和网关节点上的StorageGRID提供的集成负载平衡器服务、也可以是位于F5、Kemp、HAProxy、Loadbalancer.org等第三方解决方案上的集成负载平衡器服务 通过使用StorageGRID负载平衡器、可以设置流量划分器(QoS规则)、以便确定Veeam工作负载的优先级、或者限制Veeam、使其不会影响StorageGRID系统上优先级较高的工作负载。

S3 存储分段

StorageGRID是一种安全多租户存储系统。建议为Veeam工作负载创建一个专用租户。可以选择分配存储配额。作为最佳实践、请启用"使用自己的身份源"。使用适当的密码保护租户root管理用户的安全。Veeam Backup 12要求S3存储分段具有强大的一致性。StorageGRID提供了在存储分段级别配置的多个一致性选项。对于使用Veeam从多个位置访问数据的多站点部署、请选择"strong-globation"。如果Veeam备份和还原仅在单个站点上进行、则一致性级别应设置为"strong-site"。有关存储分段一致性级别的详细信息、请查看 "文档。"。要使用StorageGRID进行Veeam不可变备份、必须在创建存储分段期间全局启用S3对象锁定并在存储分段上进行配置。

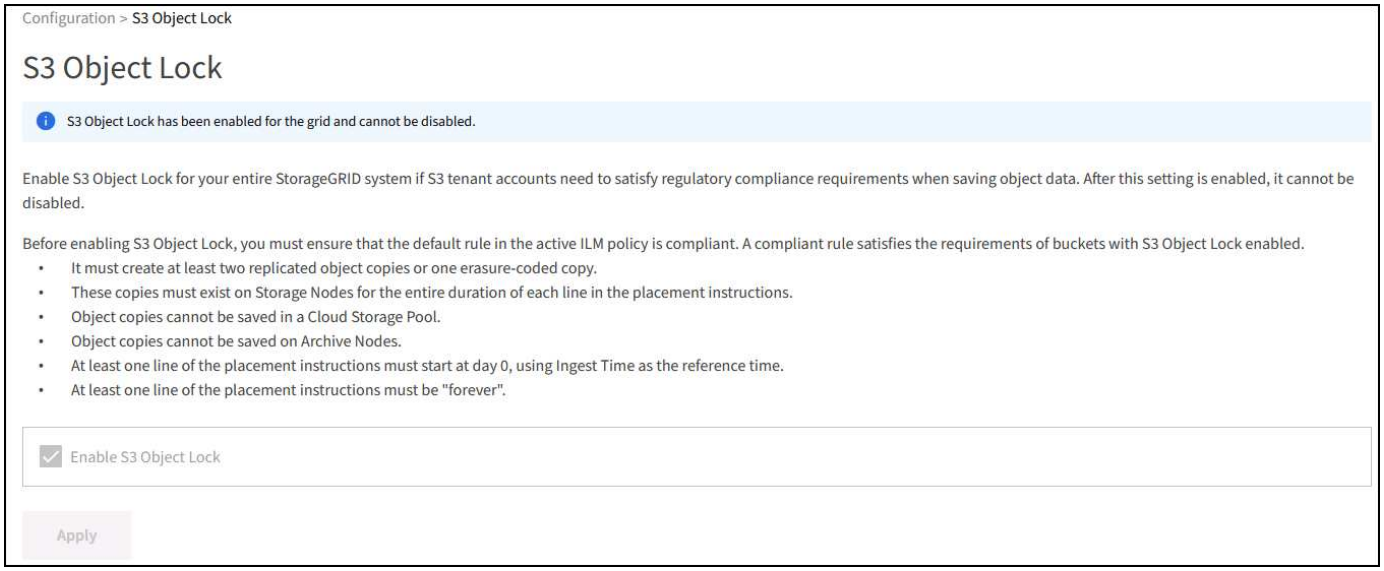
生命周期管理

StorageGRID支持在StorageGRID节点和站点之间进行复制和纠删编码、以实现对象级保护。纠删编码至少需要200 KB的对象大小。Veeam的默认块大小为1 MB、所产生的对象大小通常会低于Veeam存储效率后建议的200 KB最小大小。为了提高解决方案的性能、建议不要使用跨越多个站点的纠删编码配置文件、除非这些站点之间的连接足以避免增加延迟或限制StorageGRID系统的带宽。在多站点StorageGRID系统中、可以将ILM规则配置为在每个站点存储一个副本。为了获得最佳持久性、可以配置一条规则、以便在每个站点上存储一个经过删除的编码副本。对于此工作负载、最建议使用Veeam备份服务器本地的两个副本。

实施要点

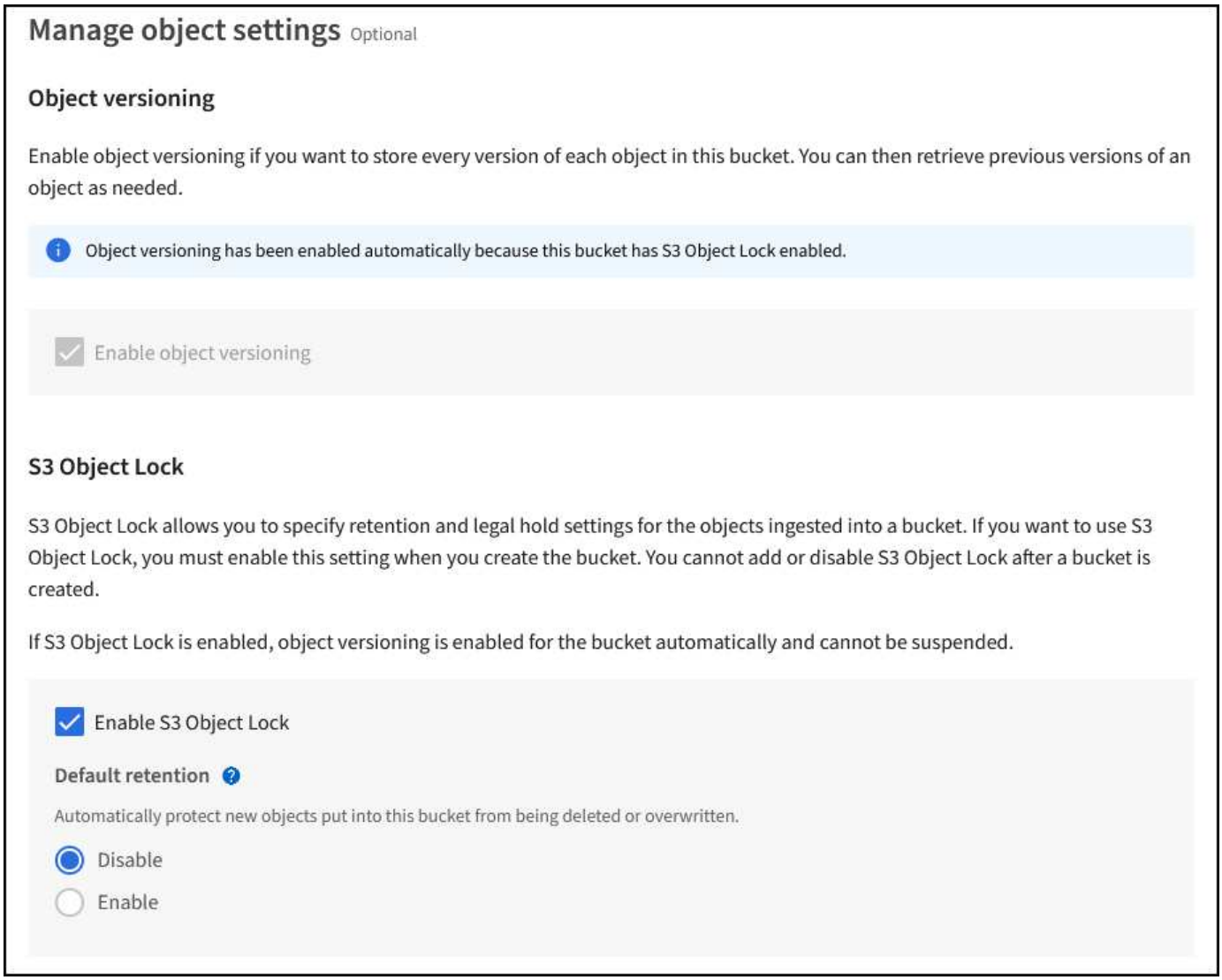
StorageGRID

如果需要不可破坏性、请确保在StorageGRID系统上启用对象锁定。在管理UI中的"Configuration/S3 Object Lock"(配置/S3对象锁定)下找到相应选项。

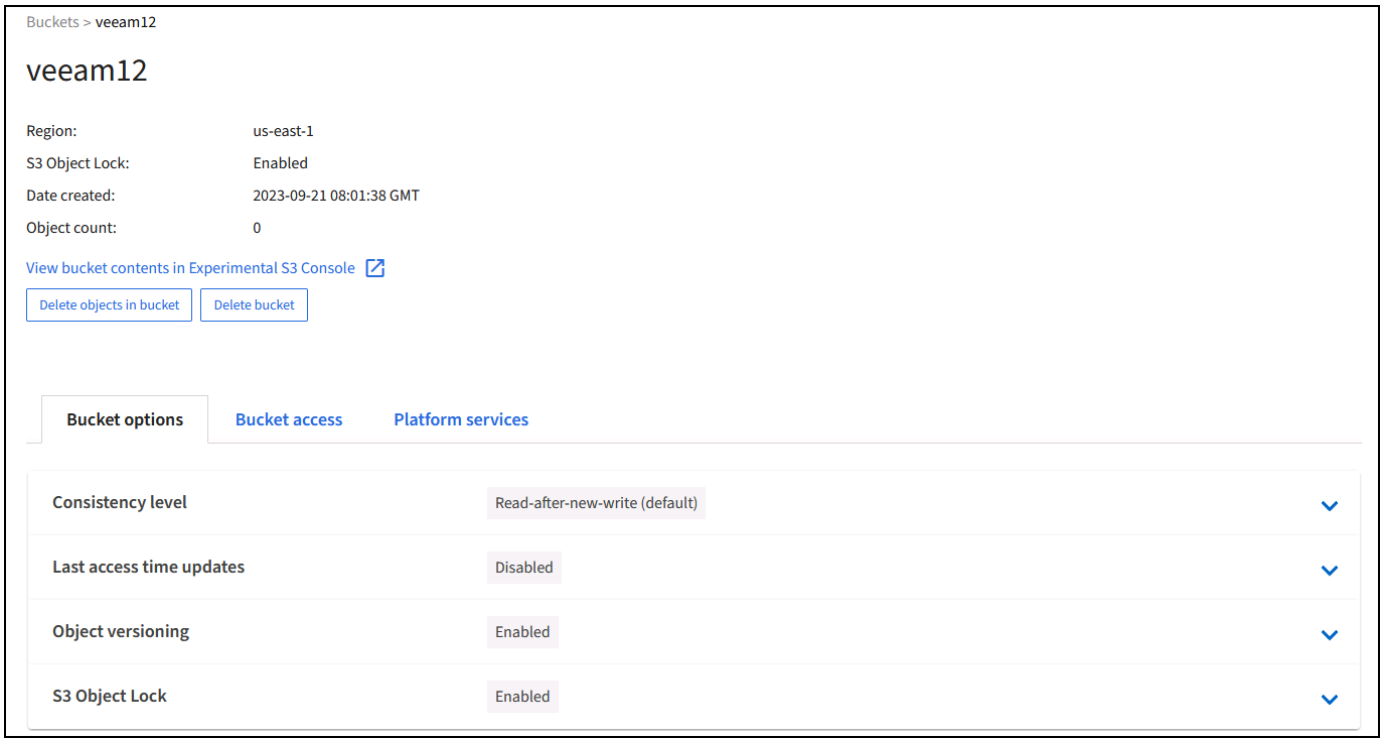


创建存储分段时、如果要将此存储分段用于不可移动备份、请选择"Enable S3 Object Lock"(启用S3对象锁定)。

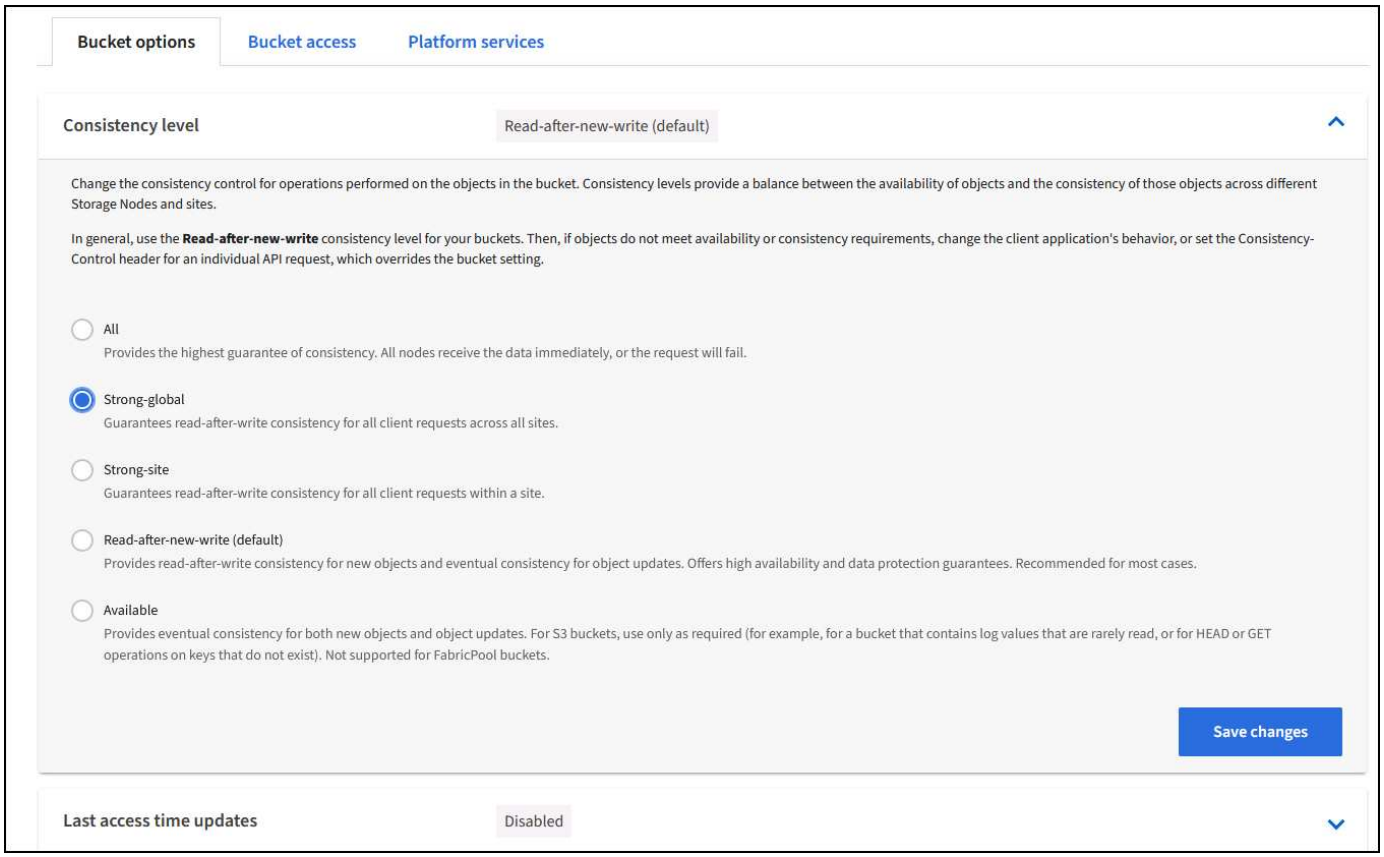
这将自动启用存储分段版本控制。保持禁用默认保留、因为Veeam将明确设置对象保留。如果Veeam不创建不可变备份、则不应选择版本控制和S3对象锁定。



创建存储分段后、转到所创建存储分段的详细信息页面。选择一致性级别。



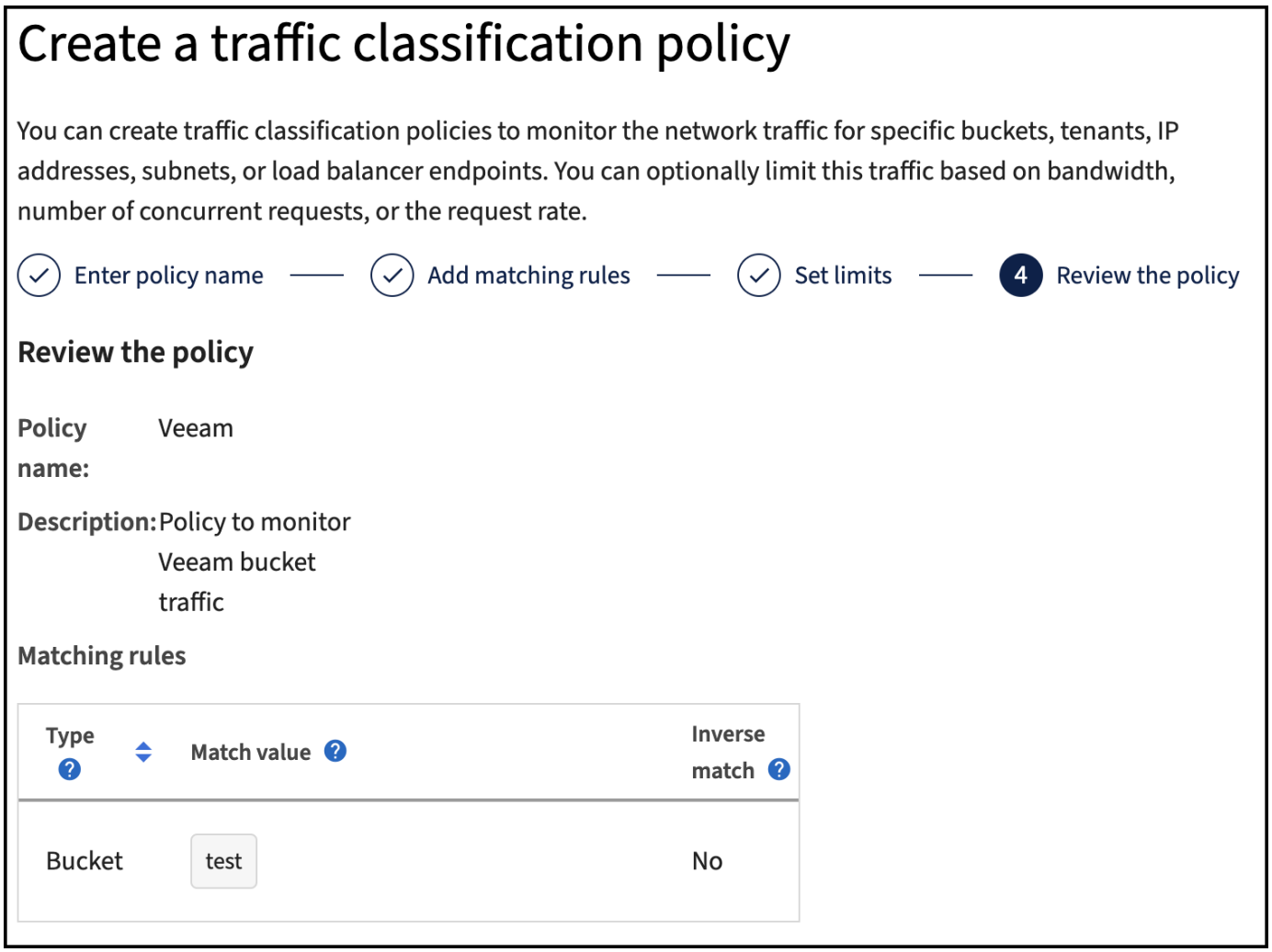
Veeam要求S3存储分段具有强大的一致性。因此、对于Veeam从多个位置访问数据的多站点部署、请选择"strong-globation"。如果Veeam备份和还原仅在单个站点上进行、则一致性级别应设置为"strong-site"。保存更改。



StorageGRID在每个管理节点和专用网关节点上提供集成负载平衡器服务。使用此负载平衡器的众多优势之一是能够配置流量分类策略(QoS)。虽然这些指标主要用于限制应用程序对其他客户端工作负载的影响或将工作负载

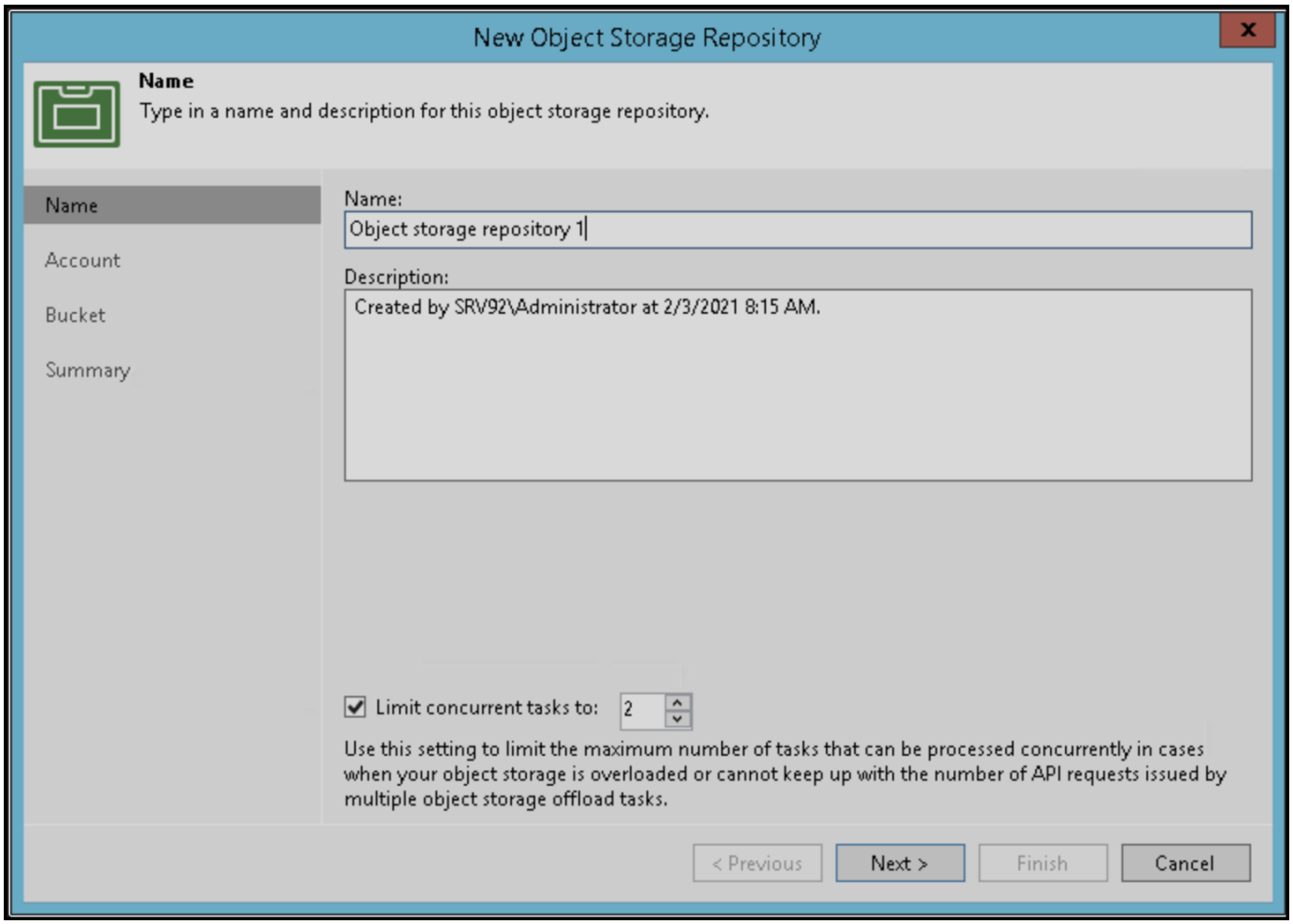
划分为优先级、但它们还提供了额外的指标收集功能、以协助监控。

在配置选项卡中、选择"Traffic Classification"(流量分类)并创建新策略。命名规则并选择存储分段或租户作为类型。输入存储分段或租户的名称。如果需要QoS、请设置限制、但对于大多数实施、我们只希望添加此功能提供的监控优势、因此不要设置限制。

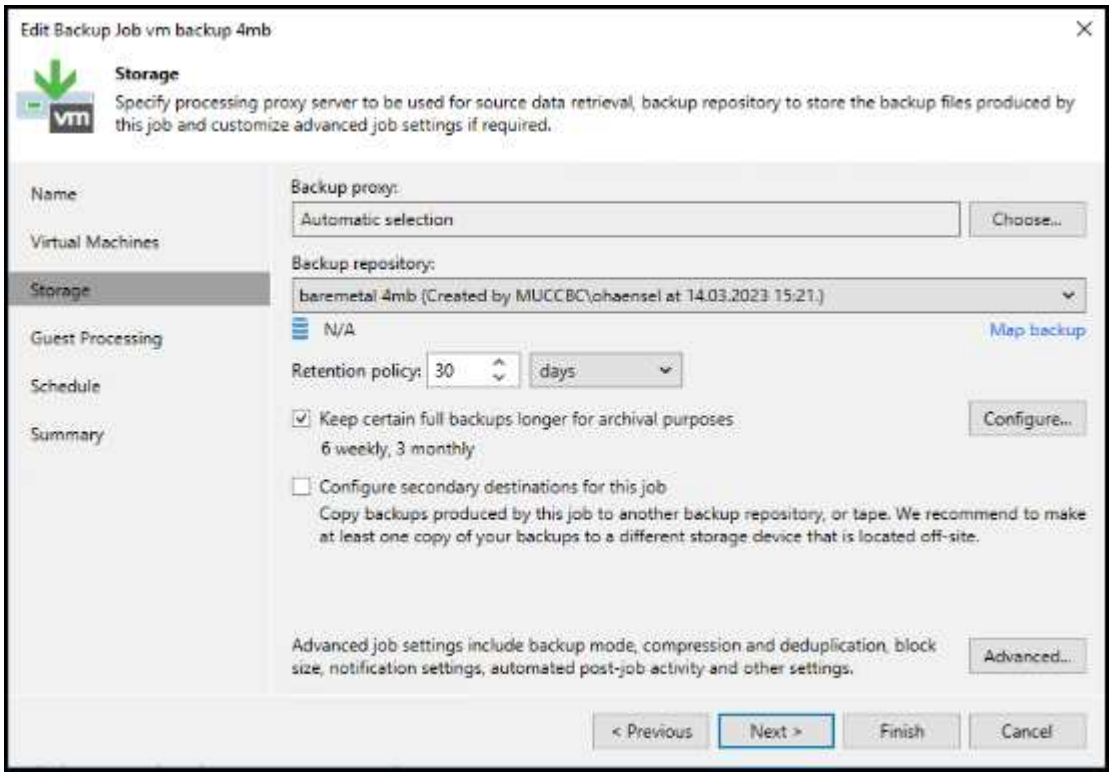


Veeam

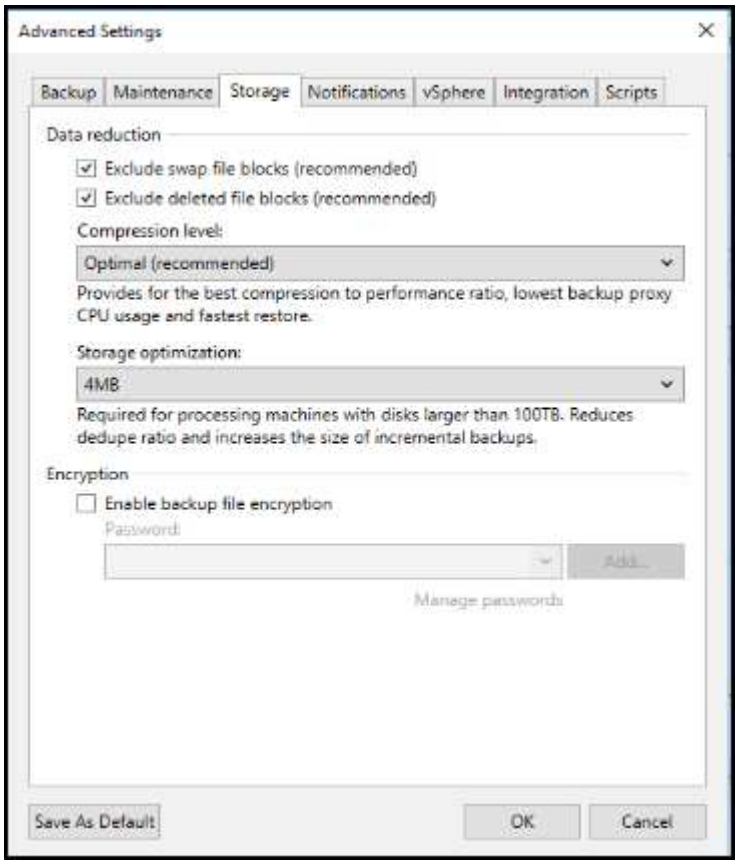
根据StorageGRID设备的型号和数量、可能需要选择并配置对存储分段上的并发操作数的限制。



按照Veeam控制台中有关备份作业配置的Veeam文档启动向导。添加VM后、选择SOBR存储库。



单击高级设置并将存储优化设置更改为4 MB或更大。应启用数据压缩和重复数据删除。根据需要更改子系统设置并配置备份作业计划。



监控StorageGRID

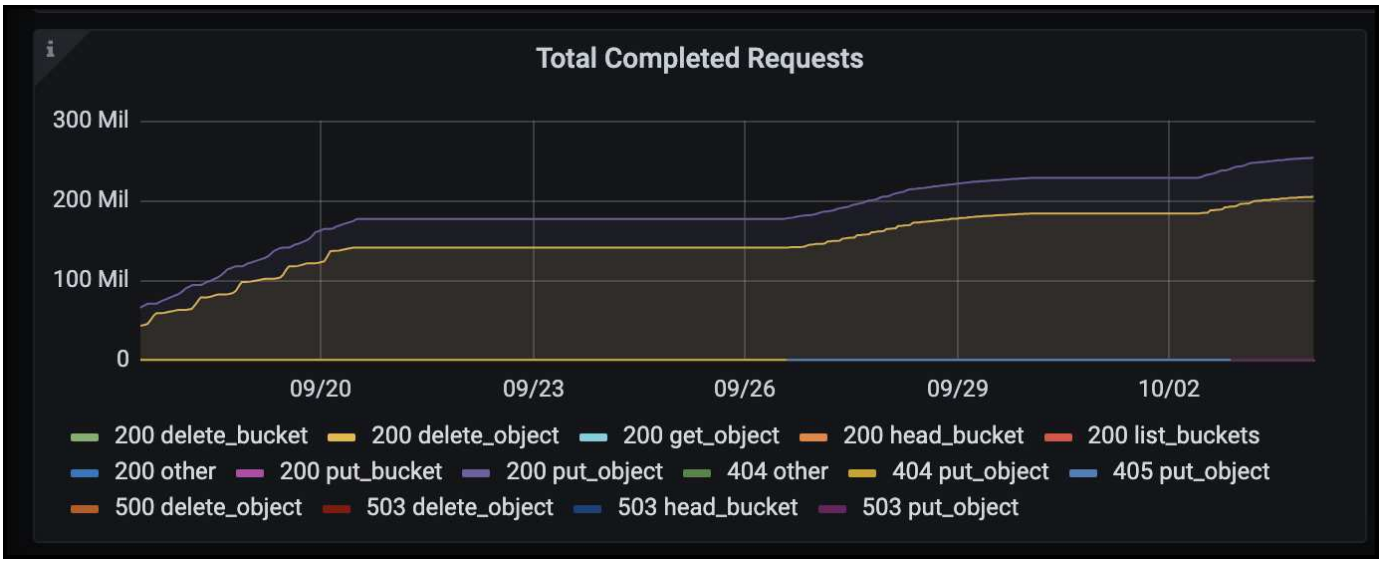
要全面了解Veeam和StorageGRID的协同运行情况、您需要等待第一个备份的保留时间到期。到目前为止、Veeam工作负载主要由Put操作组成、尚未执行任何删除操作。备份数据过期并进行清理后、您现在可以在对象存储中看到完全一致的使用情况、并根据需要调整Veeam中的设置。

StorageGRID在"Support"(支持)选项卡"Metrics (指标)"页面中提供了方便的图表来监控系统的运行。要查看的主要信息板是S3概述、ILM和流量分类策略(如果已创建策略)。在"S3概述"信息板中、您可以找到有关S3操作速率、延期和请求响应的信息。

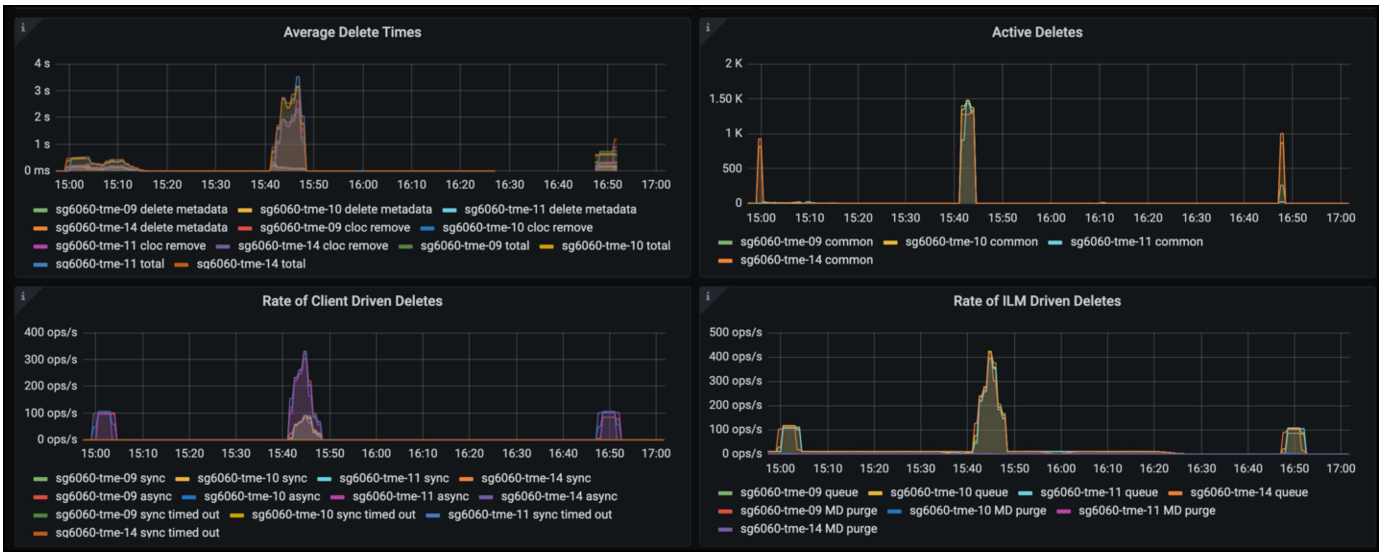
通过查看S3速率和活动请求、您可以按类型查看每个节点正在处理的负载以及请求总数。

"平均持续时间"图表显示每个节点针对每种请求类型花费的平均时间。这是请求的平均延迟、可能很好地指示可能需要进行额外调整、或者StorageGRID系统有承担更多负载的空间。

在“已完成请求总数”图表中，您可以按类型和响应代码查看请求。如果您看到的响应不是200 (OK)、则可能表示问题描述(如StorageGRID系统)负载过重、正在发送503 (减慢)响应、可能需要进行一些额外调整、或者现在是扩展系统以应对增加的负载的时候了。



在ILM信息板中、您可以监控StorageGRID系统的删除性能。StorageGRID会在每个节点上同时执行同步和异步删除、以尝试优化所有请求的整体性能。



通过流量分类策略、我们可以查看有关负载平衡器请求吞吐量、速率、持续时间以及Veeam正在发送和接收的对象大小的指标。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- "NetApp StorageGRID 11.9产品文档"
- "Veeam备份和复制"

使用StorageGRID配置d不良 数据源

作者：郑安杰

多米奥支持多种数据源、包括基于云的或内部对象存储。 您可以将d不良 配置为使用StorageGRID作为对象存储数据源。

配置d不良 数据源

前提条件

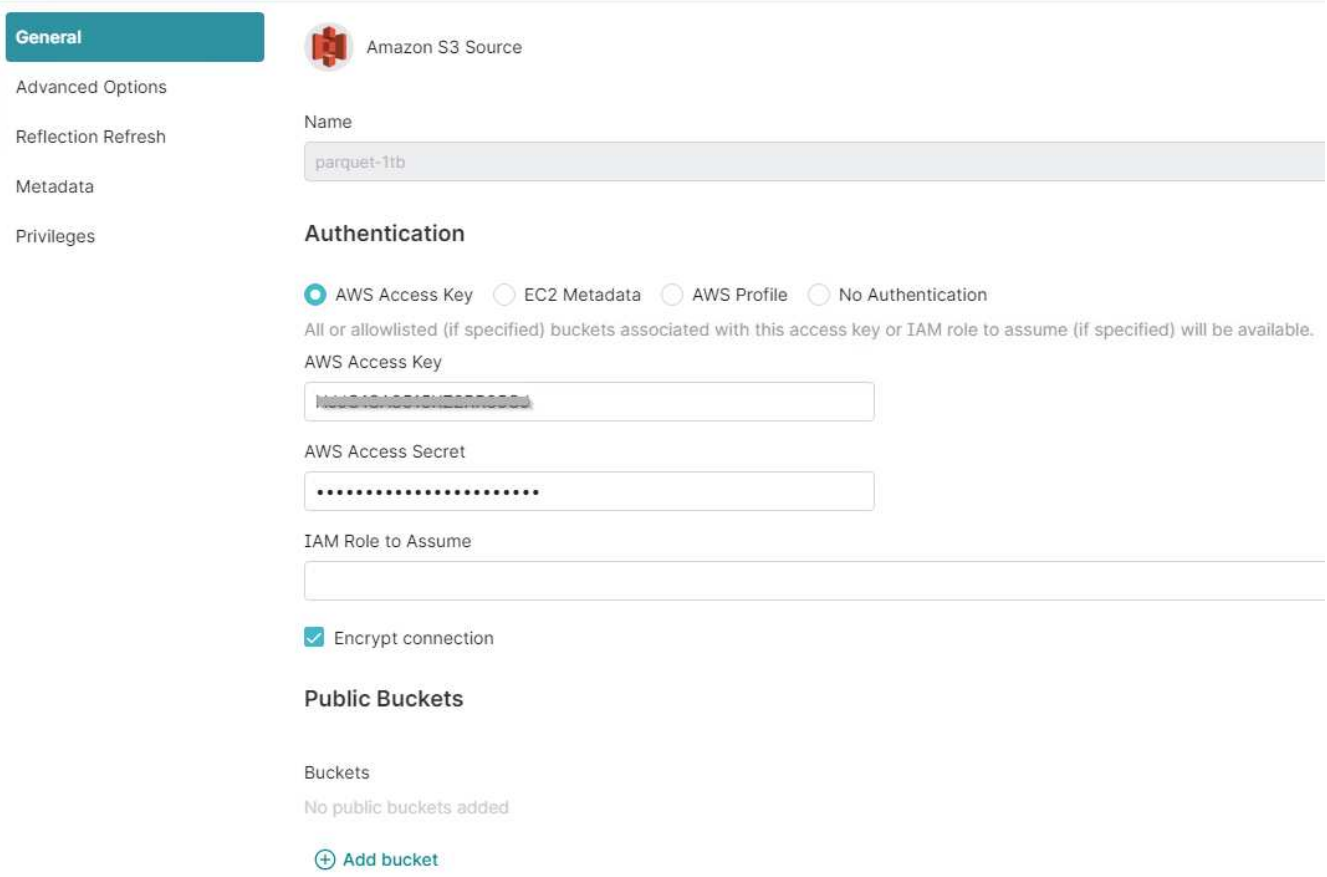
- StorageGRID S3端点URL、租户S3访问密钥ID和机密访问密钥。
- StorageGRID配置建议：禁用数据压缩(默认情况下处于禁用状态)。
  DERMIO使用字节范围GET在查询期间同时从同一对象中提取不同的字节范围。 字节范围请求的典型大小为1 MB。经过压缩的对象会降低字节范围GET性能。

d不良 指南

"连接到Amazon S3 -配置S3兼容存储"。

说明

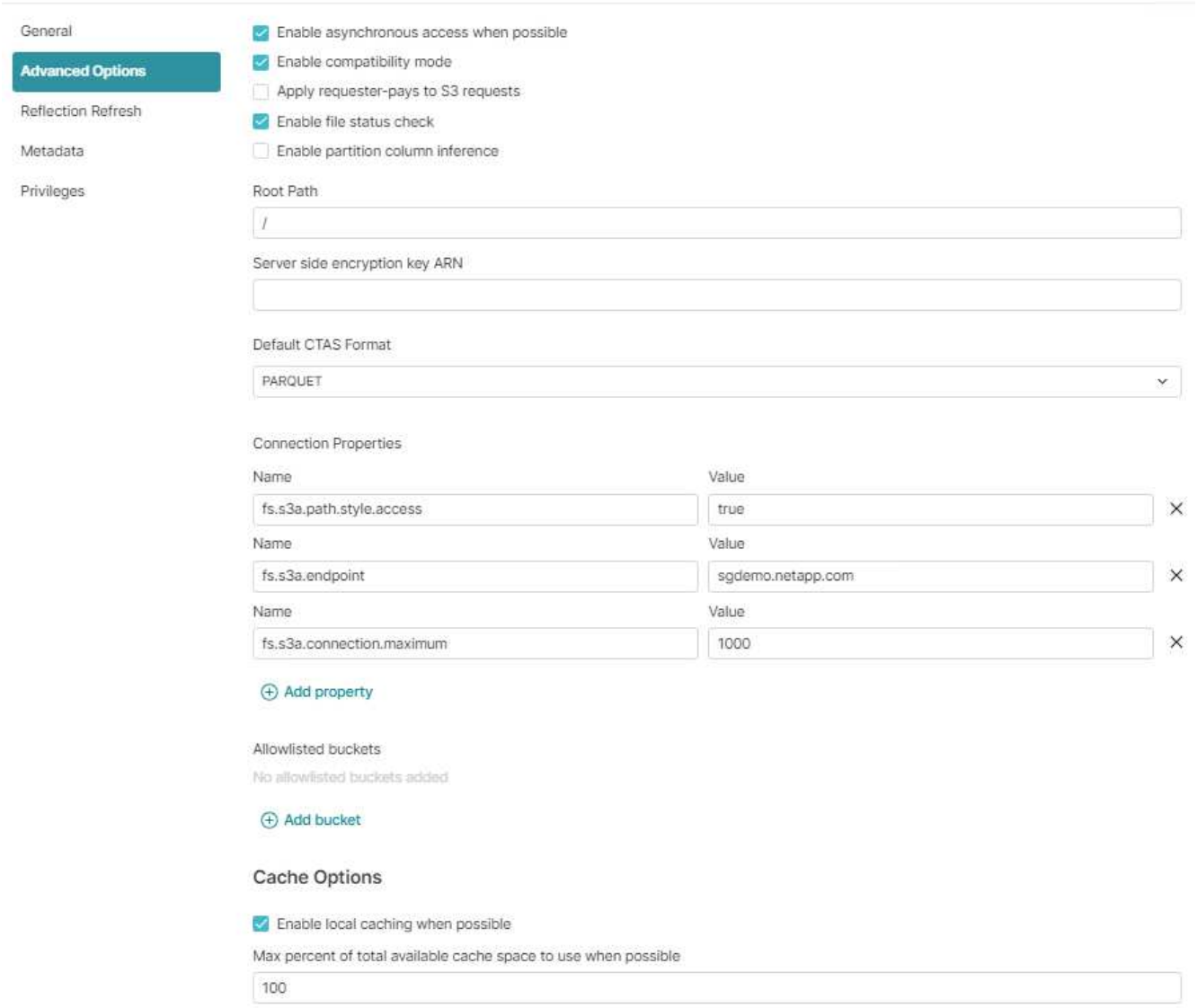
1. 在"Desmio数据集"页面上、单击+符号以添加源、然后选择"Amazon S3"。
2. 输入此新数据源的名称、StorageGRID S3租户访问密钥ID和机密访问密钥。
3. 如果使用https连接到StorageGRID S3端点、请选中"加密连接"复选框。+
   如果对此S3端点使用自签名CA证书、请按照dremio指南说明将此CA证书添加到<JAVA_HOME>服务器的dre/jre/lib/security +中
   屏幕截图示例



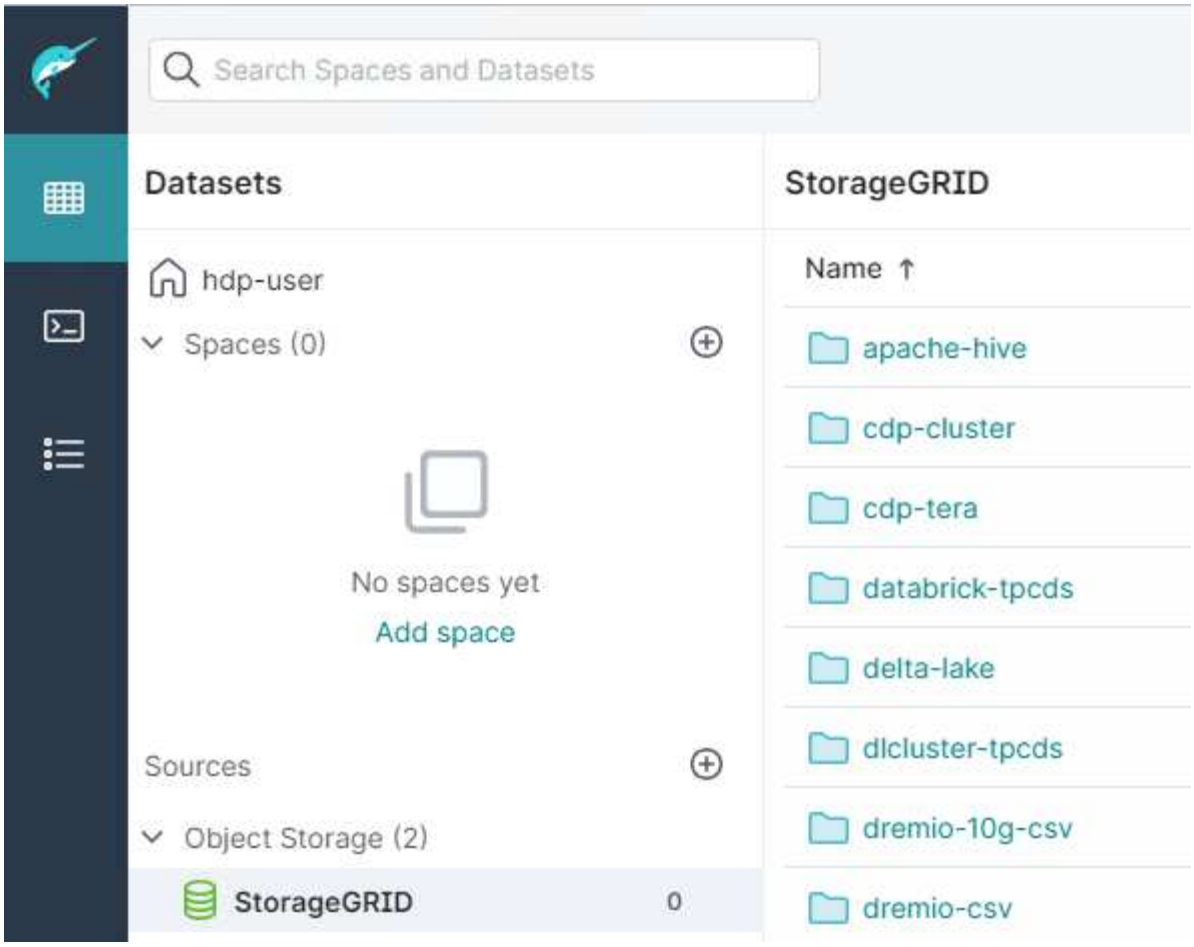
4. 单击"高级选项"、选中"启用兼容模式"
5. 在连接属性下、单击+添加属性并添加这些S3A属性。
6. fs.s3a.connection．maximum默认值为100。 如果S3数据集包含具有100个或更多列的大型镶木地板文件、则必须输入一个大于100的值。 有关此设置的信息、请参见《drefio指南》。

Name	价值
fs.s3a.endpoint	StorageGRID S3端点：端口>_
fs.s3a.path.style.access	true
FS.S3A.CONNECTION。最大值	_<大于100>_的值

屏幕截图示例



7. 根据您的组织或应用程序要求配置其他的多米奥选项。
8. 单击保存按钮以创建此新数据源。
9. 成功添加StorageGRID数据源后、左侧面板将显示存储分段列表。+
屏幕截图示例



NetApp StorageGRID与GitLab

作者：郑安杰

NetApp已使用GitLab对StorageGRID进行了测试。请参见下面的GitLab配置示例。 请参见 "GitLab对象存储配置指南" 了解详细信息。

对象存储连接示例

对于Linux软件包安装、这是的一个示例 `connection` 在合并表单中设置。编辑 `/etc/gitlab/gitlab.rb` 并添加以下行、替换所需的值：

```
# 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'
```

过程和API示例

在StorageGRID 上测试和演示S3加密选项

作者：*Aron Klein*

StorageGRID 和S3 API提供了多种不同的方法来加密空闲数据。要了解更多信息，请参见 "查看 StorageGRID 加密方法"。

本指南将演示S3 API加密方法。

服务器端加密(SSR)

使用SSE、客户端可以存储对象、并使用由StorageGRID 管理的唯一密钥对其进行加密。请求对象时、该对象将通过存储在StorageGRID 中的密钥进行解密。

SS一 示例

- 使用SSR放置对象

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

- 对对象执行HEAD以验证加密

```
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": {}
}
```

- 获取对象

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

使用客户提供的密钥(SSI-C)进行服务器端加密

通过"SSE "、客户端可以存储对象、并使用客户端随对象提供的唯一密钥对其进行加密。请求对象时、必须提供相同的密钥才能解密并返回对象。

SSI-C示例

- 出于测试或演示目的、您可以创建加密密钥
  - 创建加密密钥

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

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

- 放置具有生成密钥的对象

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

- 为对象设置头

```
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=="
            }
```

如果不提供加密密钥、则会收到错误"An error occurred (404) when calling the HeadObject operation：not found"(调用HeadObject操作时出错(404)：未找到)

- 获取对象

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

如果不提供加密密钥、则在调用GetObject操作时将收到错误"An error occurred (InvalidRequest)：The object was stored using a form of Server side Encryption"。要检索对象、必须提供正确的参数。"

存储分段服务器端加密(SSI-S3)

SSI-S3允许客户端为存储在存储在存储分段中的所有对象定义默认加密行为。这些对象使用由StorageGRID 管理的唯一密钥进行加密。请求对象时、该对象将通过存储在StorageGRID 中的密钥进行解密。

存储分段**SSI-S3**示例

- 创建新存储分段并设置默认加密策略
  - 创建新存储分段

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

  - 放入存储分段加密

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

- 将对象放入存储分段中

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

- 为对象设置头

```
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": {}
}
```

- 获取对象

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

测试并演示StorageGRID 上的S3对象锁定

作者：*Aron Klein*

对象锁定提供了一个WORM模型、用于防止删除或覆盖对象。对StorageGRID 对象锁定实施情况进行了评估、以帮助满足法规要求、支持对象保留的合法保留和合规模式以及默认存储分段保留策略。

本指南将演示S3对象锁定API。

合法保留

- 对象锁定合法保持是应用于对象的简单开/关状态。

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

- 使用GET操作对其进行验证。

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

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

- 关闭合法保留

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

- 使用GET操作对其进行验证。

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

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

合规模式

- 对象保留是使用"保留到"时间戳完成的。

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

- 验证保留状态

```
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"
    }
}
```

默认保留

- 将保留期限设置为天数和年数以及使用每个对象API定义的保留截止日期。

```
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
```

- 验证保留状态

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

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

- 将对象放入存储分段中

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

- 存储分段上设置的保留持续时间将转换为对象上的保留时间戳。

```
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"
    }
}
```

测试删除已定义保留的对象

对象锁定基于版本控制构建。保留是在对象的某个版本上定义的。如果尝试删除定义了保留的对象、但未指定版本、则会创建一个删除标记作为对象的当前版本。

- 删除定义了保留的对象

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

- 列出存储分段中的对象

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

  - 请注意、此对象未列出。

- 列出可查看删除标记的版本以及原始锁定版本

```
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"
        }
    ]
}
```

- 删除对象的锁定版本

```
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
```

分段和组(IAM)策略示例

下面是StorageGRID S3中的策略和权限示例。

策略的结构

在StorageGRID中、组策略与AWS用户(IAM) S3服务策略相同。

StorageGRID中需要使用组策略。具有S3访问密钥但未分配给用户组或分配给组但策略未授予某些权限的用户将无法访问任何数据。

存储分段和组策略共享大多数相同的元素。策略以json格式构建、可使用生成 "AWS策略生成器"

所有策略都将定义效果、操作和资源。存储分段策略还将定义主体。

其*效果*是允许或拒绝请求。Principal*是指被授予或拒绝这些能力的帐户/用户。可以将其定义为通配符*"、存储分段所在租户中的本地或联合用户或组、或者网格中的其他租户。用户或组可通过名称或ID字符串进行标识。“操作”是授予或拒绝给用户的一组S3操作。

用户需要执行S3：ListBucket"操作才能执行任何S3操作。

资源*是指被授予或拒绝对其执行操作的主体的一个或多个分段。(可选)策略操作的有效时间可以是一个*条件*。

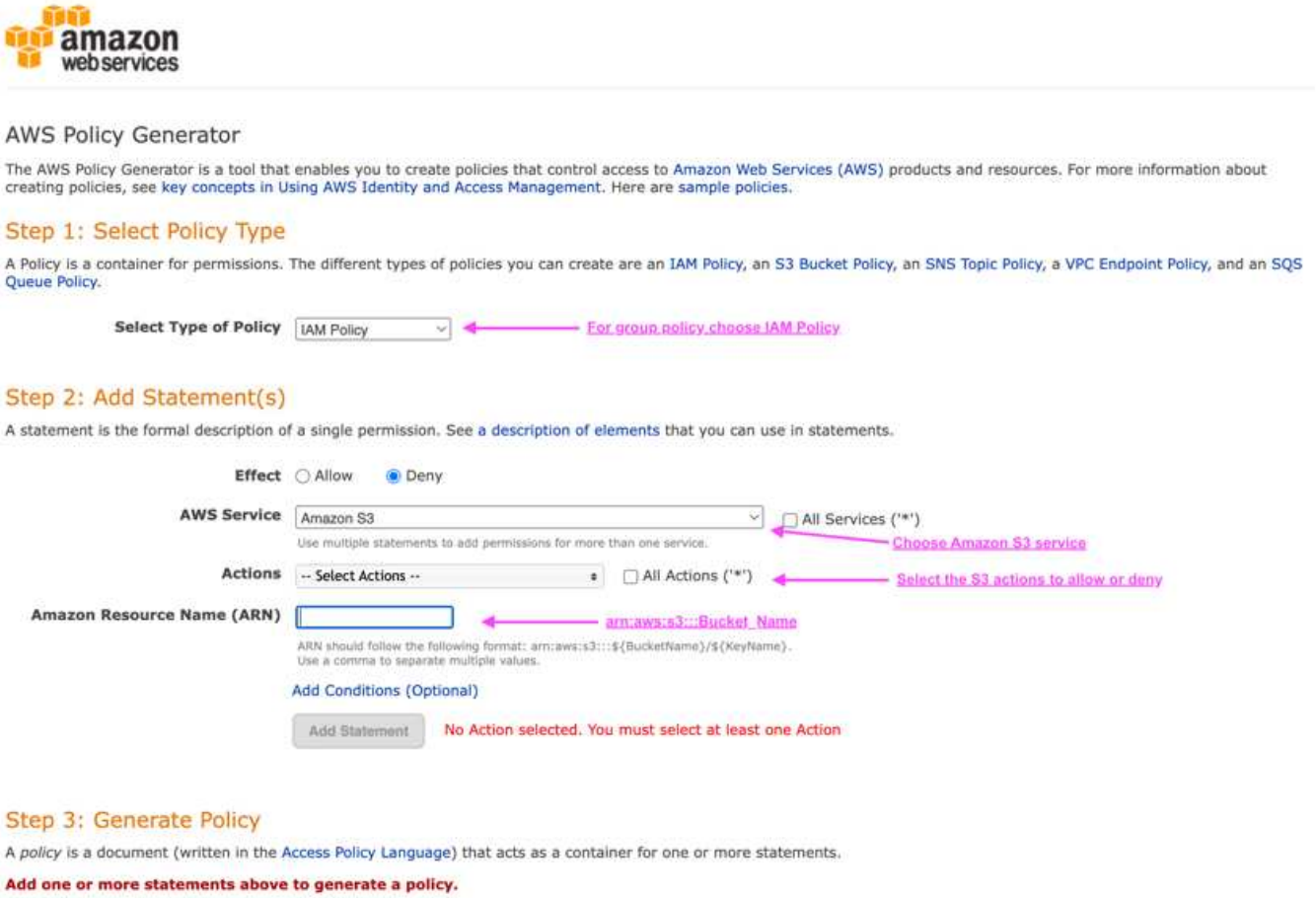
JSON策略的格式如下所示：

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

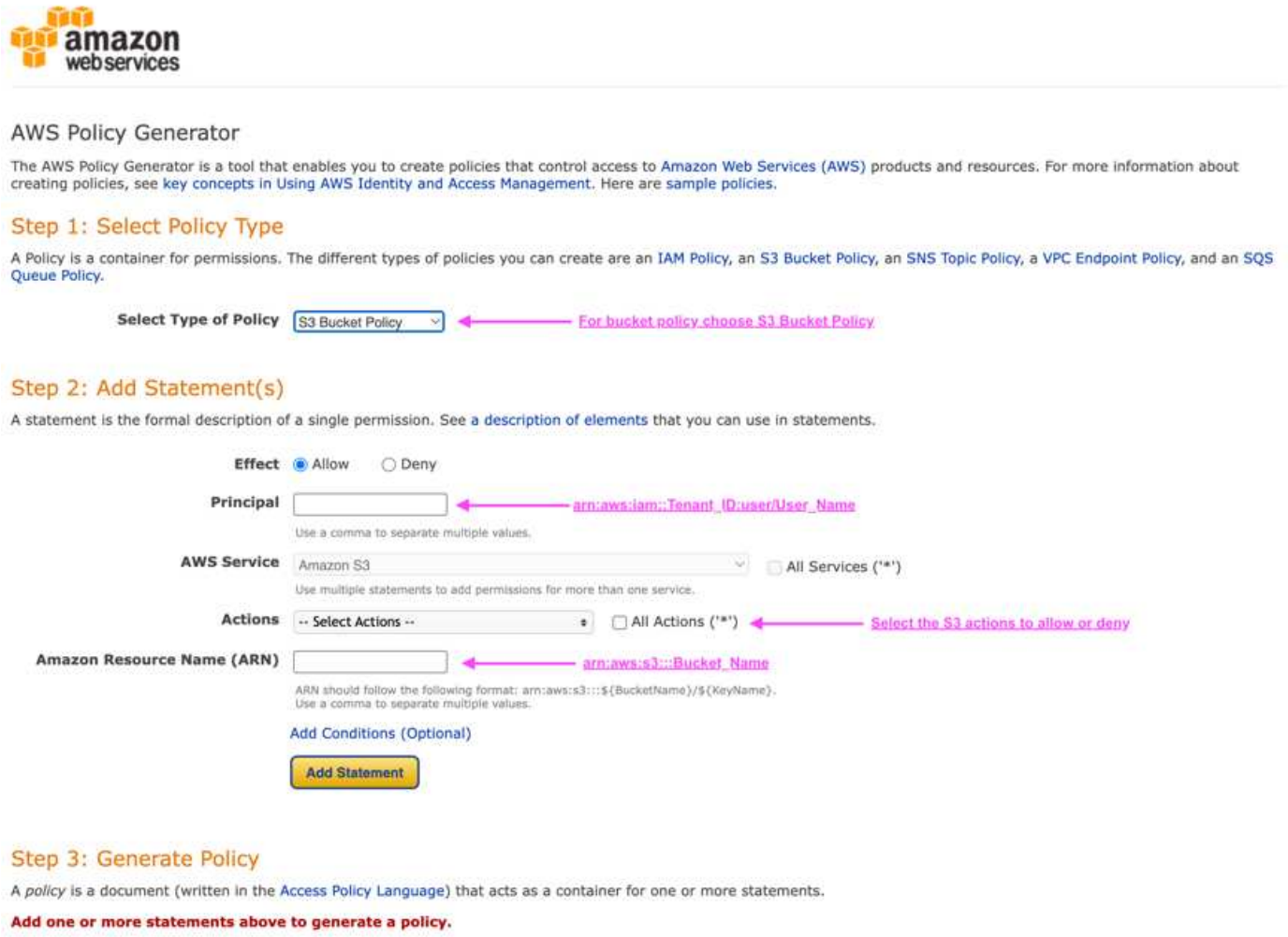
使用**AWS**策略生成器

AWS策略生成器是一个很好的工具、可帮助您获取具有正确格式的json代码以及您尝试实施的信息。

要为StorageGRID组策略生成权限、请执行以下操作：*为策略类型选择IAM策略。*选择所需效果的按钮-允许或拒绝。最好先使用拒绝权限启动策略、然后在操作下拉列表中添加允许权限*单击要包含在此权限中的尽可能多的S3操作旁边的框或"所有操作"框。*在Amazon资源名称(ARN)框中键入存储分段路径。在存储分段名称前包括"arn：aws：s3：：：："。例如、"ARN：AWS：S3：：：exple_bket"

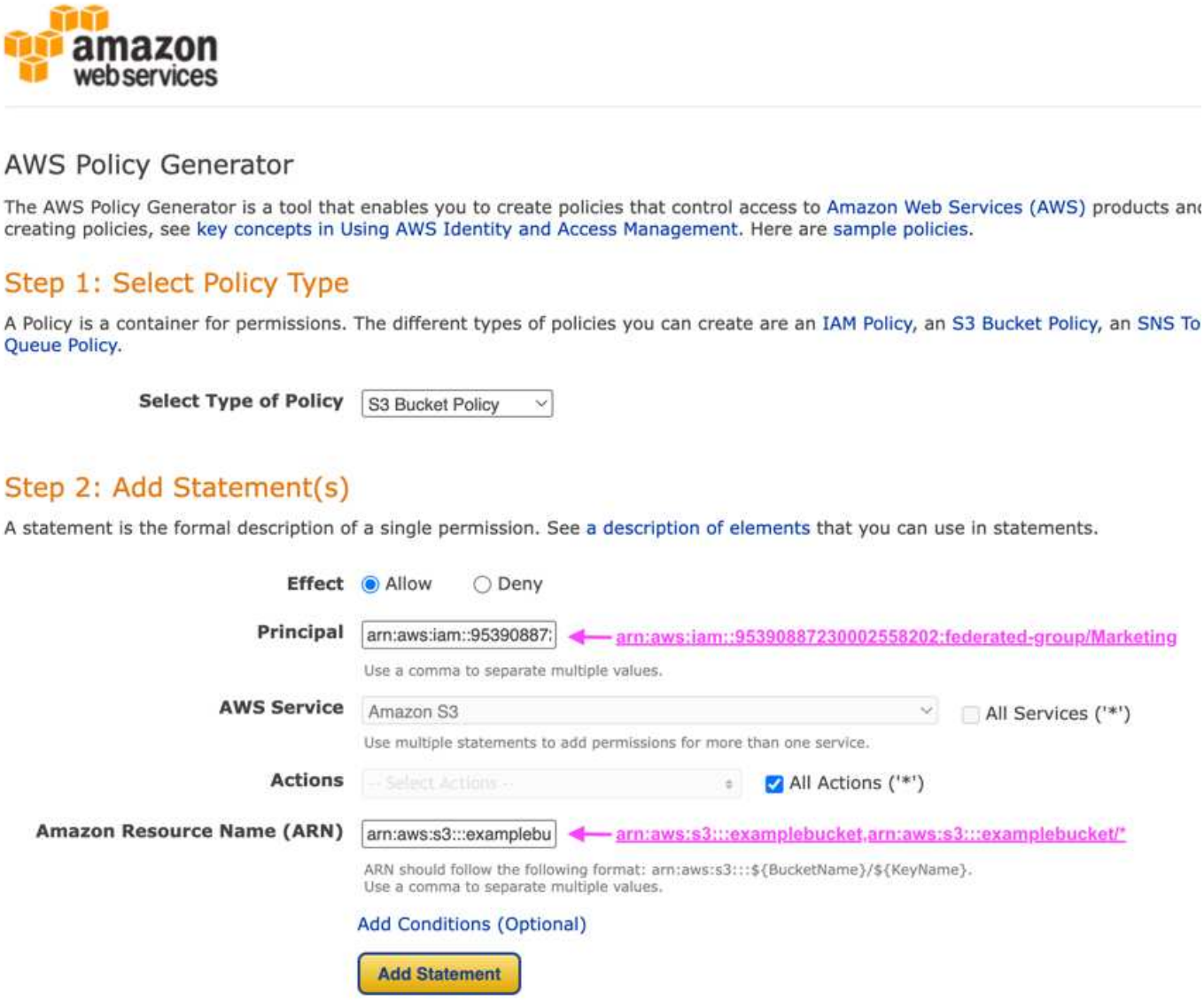


要为存储分段策略生成权限、请执行以下操作：*为策略类型选择S3存储分段策略。*选择所需效果的按钮-允许或拒绝。最好先使用拒绝权限启动策略、然后在主体的用户或组信息中添加允许权限*键入。*在操作下拉列表中、单击要包含在此权限中的S3操作旁边的框或"所有操作"框。*在Amazon资源名称(ARN)框中键入存储分段路径。在存储分段名称前包括"arn：aws：s3：：：："。例如、"ARN：AWS：S3：：：exple_bket"



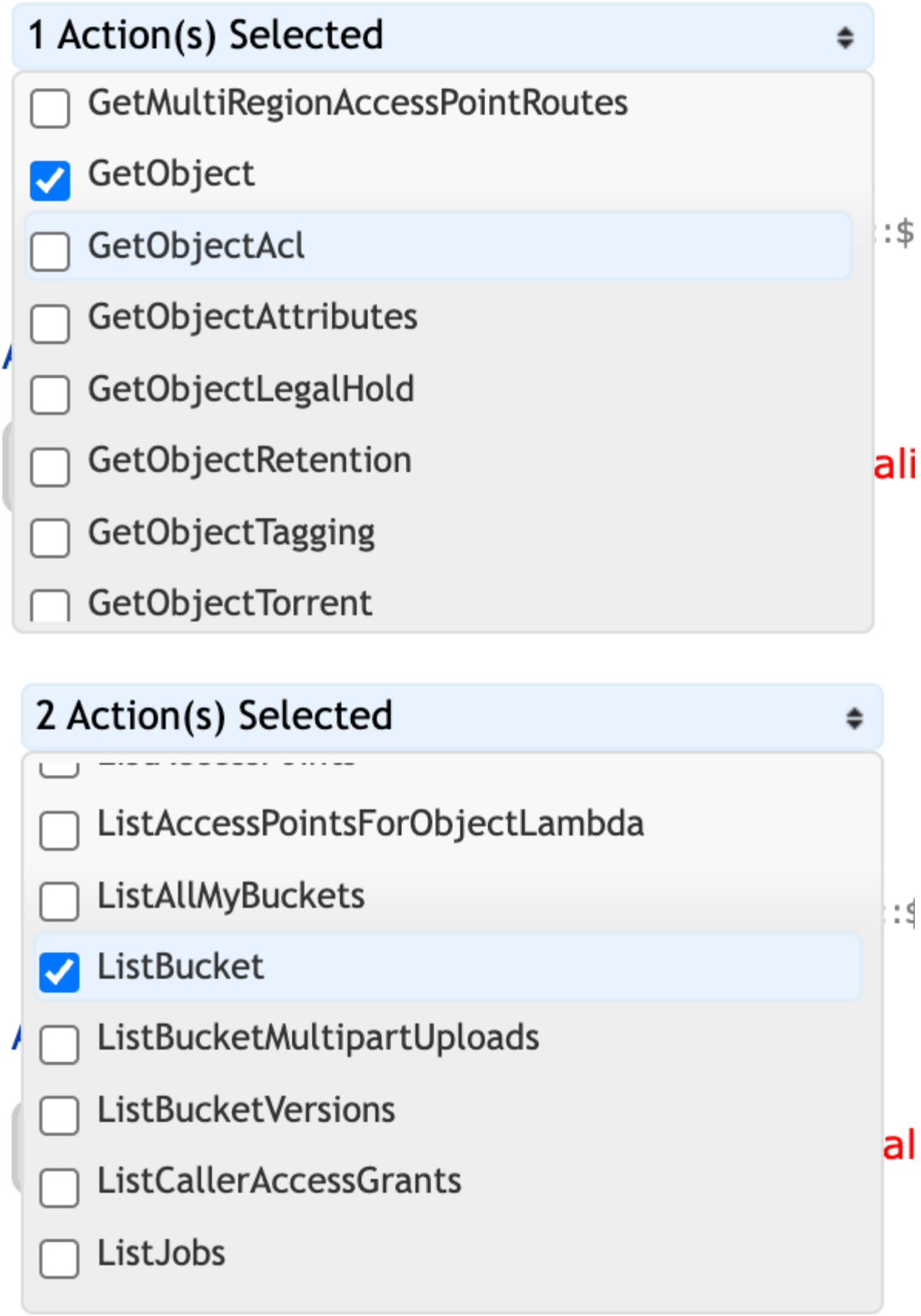
例如、如果要生成存储分段策略、以允许所有用户对存储分段中的所有对象执行GetObject操作、而仅允许指定帐户中属于组"Marketing"的用户进行完全访问。

- 选择S3存储分段策略作为策略类型。
- 选择允许效果
- 输入Marketing组信息：arn：aws：iam：：95390887230002558202：联合组/营销
- 单击"所有操作"框
- 输入存储分段信息—arn：aws：s3：：：exple_bket,arn：aws：s3：：：exple_bket/*



- 单击"Add Statement"(添加诊断代码)按钮

- 选择允许效果
- 为每个人输入星号*
- 单击GetObject和ListBucket"旁边的框



• 输入存储分段信息—arn：aws：s3：：：：exple_bket,arn：aws：s3：：：：exple_bket/*

amazon web services

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products an creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS To Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 2 Action(s) Selected All Actions ('*')

Amazon Resource Name (ARN) arn:aws:s3:::examplebu ← arn:aws:s3:::examplebucket,arn:aws:s3:::examplebucket/*

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

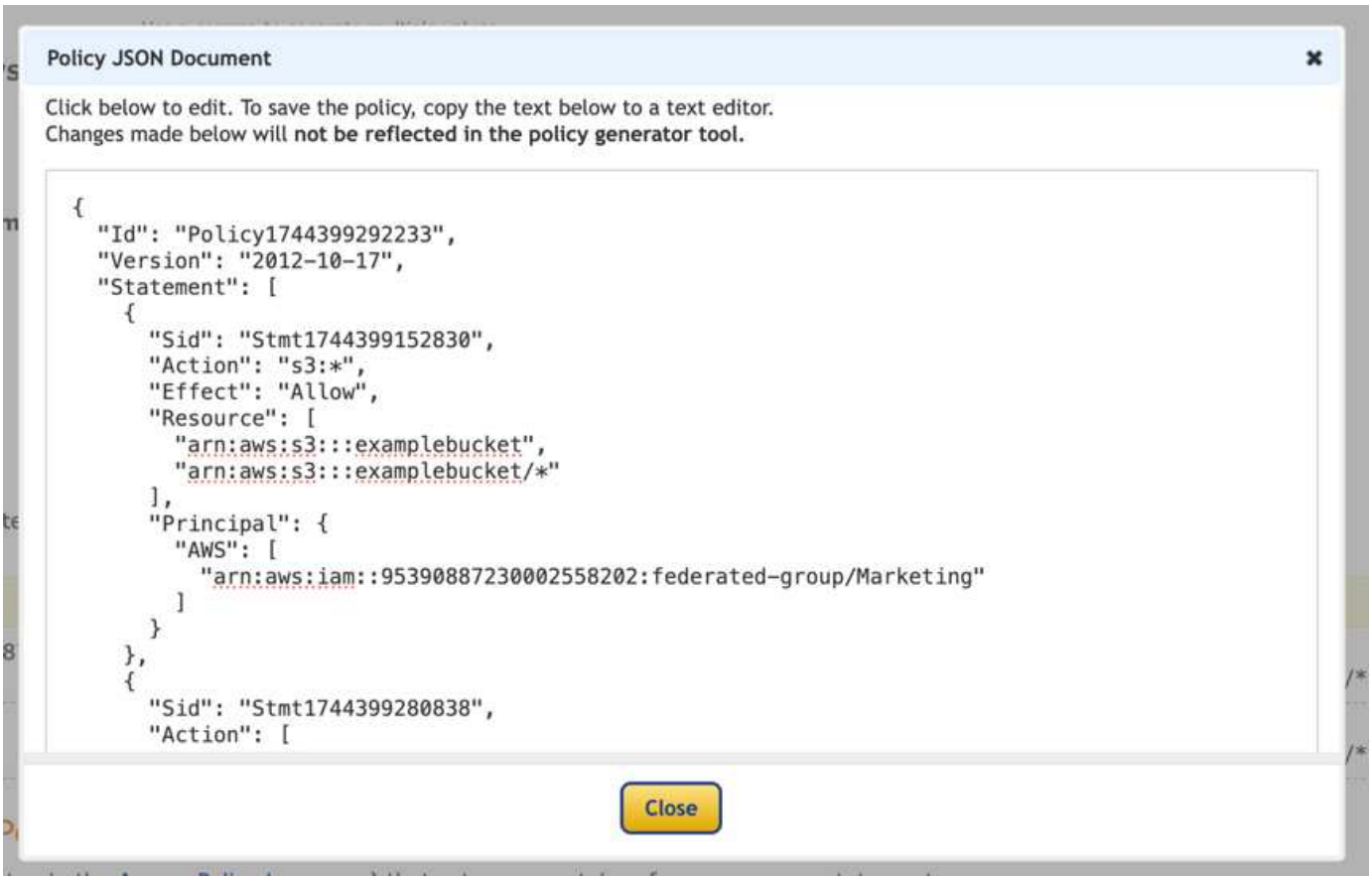
Add Statement

- 单击"Add Statement"(添加诊断代码)按钮

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• arn:aws:iam::953908872300025582O2:federated-group/Marketing	Allow	s3:*	• arn:aws:s3:::examplebucket • arn:aws:s3:::examplebucket/*	*None*
• *	Allow	• s3:GetObject • s3:ListBucket	• arn:aws:s3:::examplebucket • arn:aws:s3:::examplebucket/*	*None*

- 单击"生成策略"按钮、此时将显示一个弹出窗口、其中会显示您生成的策略。



- 复制完整的json文本、如下所示：

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

此json可以按原样使用、也可以删除"Statement"行上方的ID和版本行、您可以自定义每个权限的Sid、并为每个权限指定更有意义的标题、也可以删除这些内容。

例如：

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

组策略(IAM)

主目录模式的存储分段访问

此组策略仅允许用户访问名为Users username的分段中的对象。

```
{
"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}/*"
    }

  ]
}
```

拒绝创建对象锁定分段

此组策略将限制用户创建在存储分段上启用了对象锁定的存储分段。

此策略不会在StorageGRID UI中强制实施、而是仅通过S3 API强制实施。

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

对象锁定保留限制

此存储分段策略会将对象锁定保留期限限制为10天或更短

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

按版本ID限制用户删除对象

此组策略将限制用户按版本ID删除受版本控制的对象

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

存储分段策略

限制用户删除分段中受版本控制的对象

此存储分段策略将限制用户(由用户ID "56622399308951294926"标识)按版本ID删除版本控制的对象

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

将存储分段限制为具有只读访问权限的单个用户

此策略允许单个用户对某个存储分段拥有只读访问权限、并明确授予所有其他用户的访问权限。将deny语句分组在策略顶部是一种较好的做法、可以加快评估速度。

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

将组限制为具有只读访问权限的单个子目录(前缀)

此策略允许组成员对分段中的子目录(前缀)具有只读访问权限。分段名称为"study"、子目录为"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/*"
            ]
        }
    ]
}
```

技术报告

StorageGRID技术报告简介

NetApp StorageGRID 是一款软件定义的对象存储套件、支持公共、私有和混合多云环境中的各种用例。StorageGRID 为Amazon S3 API提供本机支持、并提供行业领先的创新技术、例如自动化生命周期管理、以便长期经济高效地存储、保护和保留非结构化数据。

StorageGRID提供的文档涵盖了有关多种StorageGRID功能和集成的最佳实践和建议。

NetApp StorageGRID和大数据分析

NetApp StorageGRID用例

NetApp StorageGRID对象存储解决方案可提供可扩展性、数据可用性、安全性和高性能。各种规模和各行各业的组织都在广泛的使用情形中使用StorageGRID S3。让我们来了解一些典型场景：

大数据分析： StorageGRID S3常用作数据湖、企业可在其中存储大量结构化和非结构化数据、以便使用Apache Spark、Splunk Smartstore和DREMIO等工具进行分析。

数据分层： NetApp客户使用ONTAP的FabricPool功能在高性能本地层之间自动将数据移动到StorageGRID。在将冷数据保留在低成本对象存储上的同时、将昂贵的闪存存储释放出来、以存储热数据。这样可以最大限度地提高性能并节省成本。

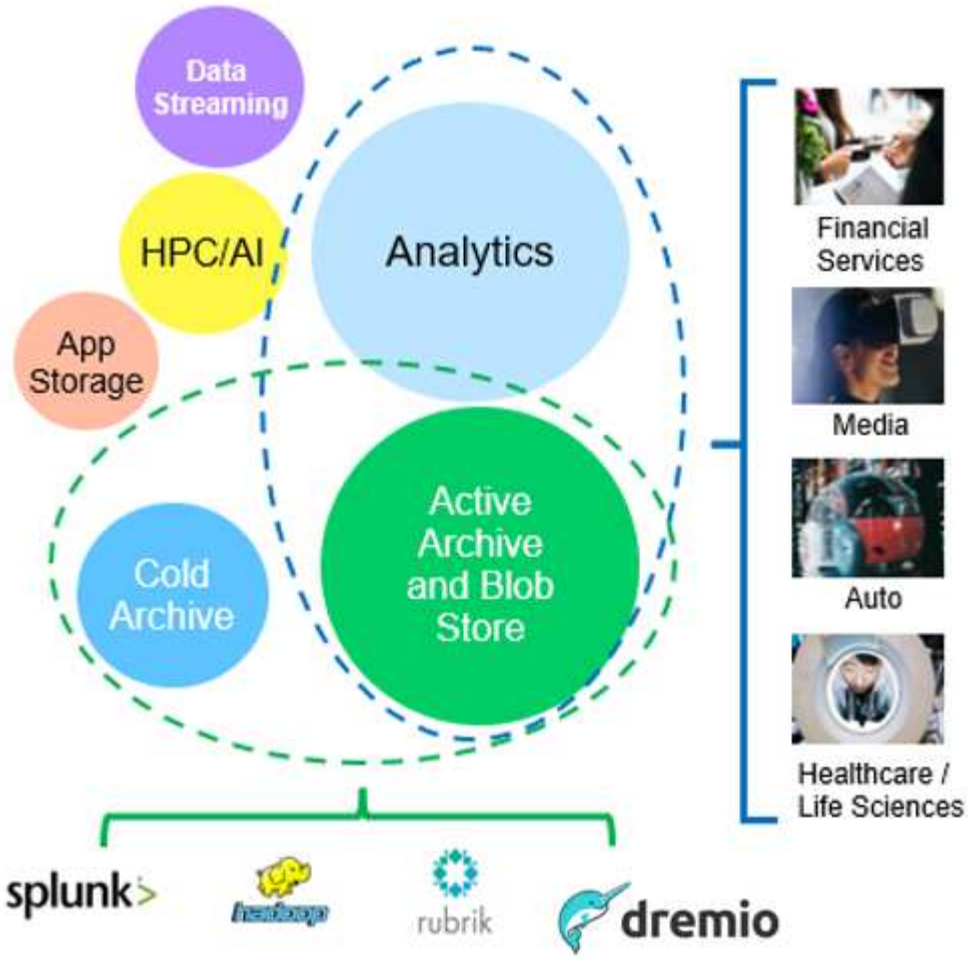
*数据备份和灾难恢复：*企业可以使用StorageGRID S3作为可靠且经济高效的解决方案来备份关键数据并在发生灾难时进行恢复。

应用程序的数据存储： StorageGRID S3可用作应用程序的存储后端，使开发人员能够轻松地存储和检索文件、图像、视频和其他类型的数据。

内容交付： StorageGRID S3可用于存储静态网站内容、媒体文件和软件下载并提供给全球用户、利用StorageGRID的地区分布和全局命名空间实现快速可靠的内容交付。

数据归档： StorageGRID提供不同的存储类型、并支持分层到公共长期低成本存储选项、使其成为出于合规性或历史目的需要保留的数据归档和长期保留的理想解决方案。

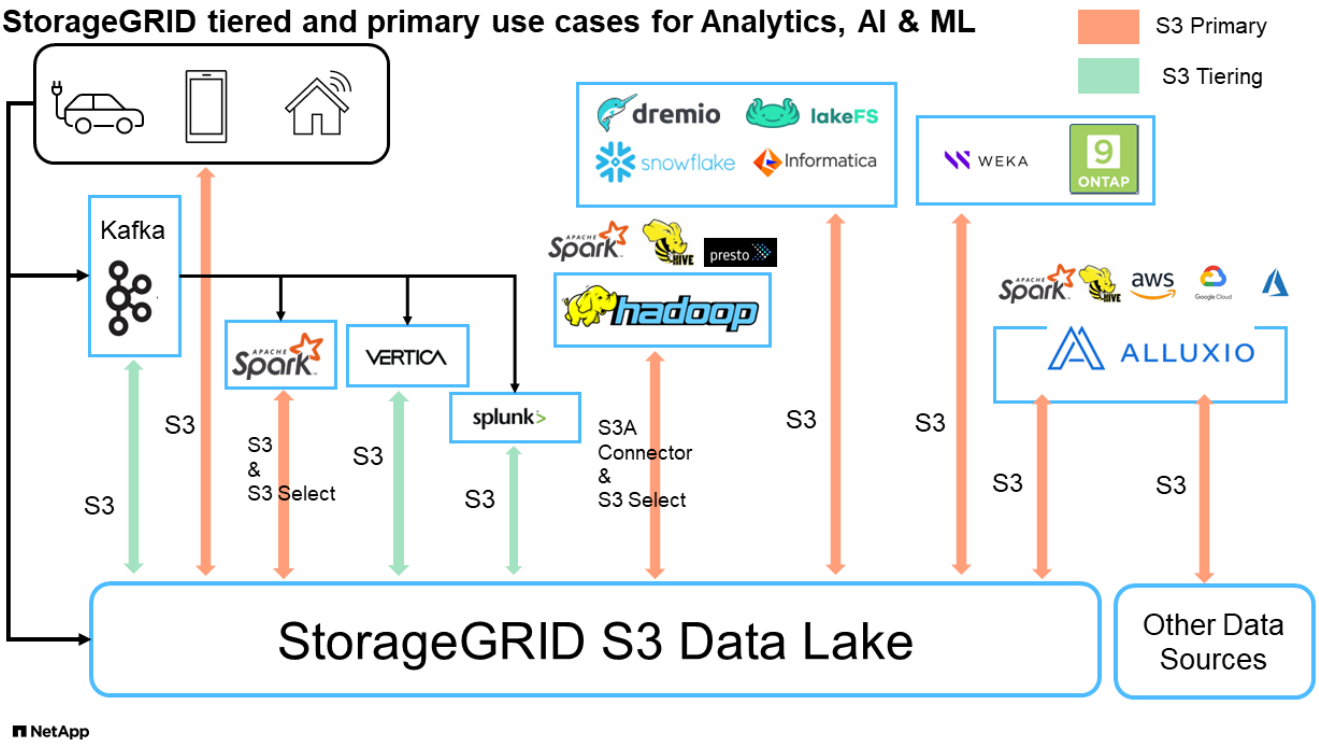
对象存储用例



在上述情形中、大数据分析是最热门的使用情形之一、其使用量呈上升趋势。

为什么选择**StorageGRID**解决数据湖问题?

- 增强协作—利用行业标准API访问实现大规模共享多站点、多租户
- 降低运营成本—通过一个自我修复型自动化横向扩展架构简化运营
- 可扩展性—与传统的Hadoop和数据仓库解决方案不同、StorageGRID S3对象存储可将存储与计算和数据分离、从而使企业能够随着增长扩展存储需求。
- 耐用性和可靠性—StorageGRID的耐用性高达99.9999999%、这意味着存储的数据能够高度抵御数据丢失。它还提供高可用性、确保数据始终可访问。
- 安全性—StorageGRID提供各种安全功能、包括加密、访问控制策略、数据生命周期管理、对象锁定和版本控制、以保护S3存储分段中存储的数据
- StorageGRID S3数据湖*



《使用S3对象存储对数据仓库和湖屋进行基准测试：比较研究》

本文介绍了使用NetApp StorageGRID的各种数据仓库和温室生态系统的综合基准。其目标是确定哪个系统在使用S3对象存储时性能最佳。请参阅此内容https://www.dremio.com/wp-content/uploads/2023/02/apache-Iceberg-TDG_ER1.pdf?aliId=eyJpIjoieDRUYjFKN2ZMbXhTRnFRWCIsInQiOiJIUUw0djJsWnlJa21iNUsyQURRalNnPT0ifQ%253D%253D["Apache iceberg：权威指南"]、了解有关数据存储/数据库架构和表格格式(镶木地板和冰山一角)的更多信息。

- 基准测试工具- TPC-DS - https://www.tpc.org/tpcds/
- 大数据生态系统
  - VM集群、每个VM具有128 G RAM和24个vCPU、用于系统磁盘的SSD存储
  - 采用Hive 3.1.3的Hadoop 3.3.5 (1个名称节点+ 4个数据节点)
  - 采用Spark 3.2.0 (1个主服务器+ 4个员工)和Hadoop 3.3.5的Delta Lake
  - d不良 者v25.2 (1名协调员+ 5名执行者)
  - Trino v438 (1名协调员+ 5名工作人员)
  - Starburst v453 (1名协调员+ 5名员工)
- 对象存储
  - NetApp® StorageGRID® 11.8(3 x SG6060+1x SG1000负载平衡器)
  - 对象保护-2个副本(结果与EC 2+1类似)
- 数据库大小为1000 GB
- 对于使用镶木地板格式的每个查询测试、在所有生态系统中禁用了缓存。对于icerberg格式、我们比较了禁用缓存和启用缓存的情形之间的S3获取请求数量和总查询时间。

TPC-DS包括99个为基准测试而设计的复杂SQL查询。我们测量了执行所有99个查询所需的总时间、并通过检查S3请求的类型和数量进行了详细分析。我们的测试对两种常见的表格格式(镶木地板和冰山一角)的效率进行了比较。

镶木地板表格式的**TPC-DS**查询结果

生态系统	配置	三角洲湖	**Dremio**	**Trino**	星突发
TPCDS 99查询+总分钟数	1084 [1]	55	36	32	28
S3请求细分	获取	1、117184	2、074、610	3,939,690	1,504,212
1,495,039	观察：+ 所有范围GET	从32 MB对象中获取2 KB到2 MB的80%范围、每秒50到100个请求	73%的范围从32 MB对象开始低于100 KB、每秒1000到1400个请求	从256MB对象获取90% 1M字节范围、2500到3000个请求/秒	范围获取大小：100 KB以下50%、1 MB左右16%、27% 2 MB到9 MB、3500到4000次请求/秒
范围获取大小：100 KB以下50%、1 MB左右16%、27% 2 MB到9 MB、4000到5000个请求/秒	列出对象	312、053	24、158	120	509
512	头部+ (不存在的对象)	156、027	12、103	96	0
0	头部+ (存在的对象)	982、126	922732	0	0
0	请求总数	2.	3、033、603	3,939.906	1,504,721

[1] Hive无法完成查询编号72

TPC-DS查询结果，带**icerberg**表格格式

生态系统	**Dremio**	**Trino**	星突发
TPCDS 99查询+总分钟数(缓存已禁用)	22	28	22
TPCDS 99次查询+总分钟数[2](启用缓存)	16.	28	21.5
S3请求细分	GET (缓存已禁用)	1,985,922	938,639

生态系统	Dremio	Trino	星突发
931,582	GET (已启用缓存)	611,347	30,158
3,281	观察：+ 所有范围GET	范围获取大小：67% 1MB、15% 100KB、10% 500KB、3500 - 4500次请求/秒	范围获取大小：100 KB以下42%、1 MB左右17%、33% 2 MB到9 MB、3500到4000次请求/秒
范围获取大小：100 KB以下43%、1 MB左右17%、33% 2 MB到9 MB、4000到5000个请求/秒	列出对象	1465	0
0	头部+ (不存在的对象)	1464	0
0	头部+ (存在的对象)	3,702	509
509	请求总数(缓存已禁用)	1,992,553	939,148

[2] Trino/Starburst性能会因计算资源而出现瓶颈；向集群添加更多RAM可缩短总查询时间。

如第一个表所示、Hive的速度明显低于其他现代数据数据库生态系统。我们发现、Hive发送了大量S3列表对象请求、这些请求在所有对象存储平台上通常都很慢、尤其是在处理包含许多对象的分段时。这会显著增加整体查询持续时间。此外、现代的温室生态系统可以并行发送大量GET请求、每秒从2000到5、000个不等、而Hive的每秒请求数为50到100个。Hive和Hadoop S3A的标准文件系统模拟导致Hive在与S3对象存储交互时运行的很小。

要将Hadoop (无论是在HDFS还是S3对象存储上)与Hive或Spark结合使用、需要掌握Hadoop和Hive或Spark的丰富知识、并了解每个服务的设置如何进行交互。它们共有1、000多种设置、其中许多设置相互关联、无法单独更改。要找到设置和值的最佳组合、需要花费大量时间和精力。

通过比较镶木地板和冰山一角的结果、我们发现表格格式是一个主要的性能因素。在S3请求数量方面、iciceberg表格格式比镶木地板更高效、与镶木地板格式相比、请求数量减少了35%到50%。

但是、集群的性能主要取决于集群的计算能力。虽然这三个系统都使用S3A连接器建立S3对象存储连接、但它们不需要Hadoop、并且这些系统不会使用Hadoop的大多数FS.S3A设置。这样可以简化性能调整、无需学习和测试各种Hadoop S3A设置。

根据此基准测试结果、我们可以得出结论、针对基于S3的工作负载优化的大数据分析系统是一个主要性能因素。现代的温室可优化查询执行、高效利用元数据并提供对S3数据的无缝访问、从而在使用S3存储时获得比Hive更高的性能。

请参见此指南 "页面。"以使用StorageGRID配置drefio S3数据源。

请访问以下链接、详细了解StorageGRID和德莱米奥如何协同工作来提供现代化且高效的数据湖基础架构、以及NetApp如何从Hive + HDFS迁移到德莱米奥+ StorageGRID来显著提高大数据分析效率。

- "借助NetApp StorageGRID提升大数据的性能"
- "借助StorageGRID和d处 米奥打造现代化、功能强大且高效的数据湖基础架构"
- "NetApp如何利用产品分析重新定义客户体验"

Hadoop S3A调整

作者：郑安杰

Hadoop S3A连接器有助于在基于Hadoop的应用程序和S3对象存储之间实现无缝交互。在使用S3对象存储时、要优化性能、必须调整Hadoop S3A Connector。在深入介绍调整详细信息之前、我们先大致了解一下Hadoop及其组件。

什么是Hadoop?

Hadoop 是一个功能强大的开源框架，专为处理大规模数据处理和存储而设计。它支持跨多个计算机集群进行分布式存储和并行处理。

Hadoop的三个核心组件是：

- **Hadoop HDFS (Hadoop**分布式文件系统)：用于处理存储、将数据拆分为块并在节点之间分布。
- **Hadoop MapReredget**：负责将任务划分为较小的区块并并行执行来处理数据。
- **Hadoop yar (Yet Another Resource Neotiator)**： "高效管理资源并计划任务"

Hadoop HDFS和S3A连接器

HDFS是Hadoop生态系统的重要组成部分、在高效处理大数据方面发挥着关键作用。HDFS可实现可靠的存储和管理。它可确保并行处理和优化数据存储、从而加快数据访问和分析速度。

在大数据处理方面、HDFS在为大型数据集提供容错存储方面表现出色。它通过数据复制来实现这一点。它可以在数据仓库环境中存储和管理大量结构化和非结构化数据。此外、它还可以与领先的大数据处理框架无缝集成、例如Apache Spark、Hive、Pig和Flink、从而实现可扩展的高效数据处理。它与基于Unix (Linux)的操作系统兼容、因此对于更喜欢使用基于Linux的环境进行大数据处理的组织来说、它是理想的选择。

随着数据量逐渐增长、使用自己的计算和存储向Hadoop集群添加新计算机的方法变得效率低下。线性扩展为高效使用资源和管理基础架构带来了挑战。

为了应对这些挑战、Hadoop S3A连接器可针对S3对象存储提供高性能I/O。使用S3A实施Hadoop工作流有助于将对象存储用作数据存储库、并将计算和存储分开、进而使您能够独立扩展计算和存储。分离计算和存储还可以让您将适当数量的资源专用于计算作业、并根据数据集大小提供容量。因此、您可以降低Hadoop工作流的总体TCO。

Hadoop S3A连接器调整

S3的行为与HDFS不同、某些尝试保留文件系统外观的行为也明显欠佳。要最高效地利用S3资源、必须仔细调整/测试/试验。

本文档中的Hadoop选项基于Hadoop 3.3.5、请参见 "Hadoop 3.3.5 core-site.xml" 所有可用选项。

注意—某些Hadoop FS.S3a设置的默认值在每个Hadoop版本中都不同。请务必查看特定于当前Hadoop版本的默认值。如果未在Hadoop core-site.xml中指定这些设置、则会使用默认值。您可以使用Spark或Hive配置选项在运行时覆盖此值。

您必须访问此页面 "Apache Hadoop页面" 了解每个FS.S3A选项。如果可能、请在非生产Hadoop集群中对其进行测试、以查找最佳值。

您应阅读 "在使用S3A连接器时最大限度地提高性能" 了解其他调整建议。

让我们来探讨一些关键注意事项：

- 。数据压缩*

请勿启用StorageGRID数据压缩。大多数大数据系统都使用字节范围GET、而不是检索整个对象。对压缩对象使用字节范围GET会显著降低GET性能。

- 。S3a提交人*

一般情况下、建议使用magic S3A提交器。请参见此部分 "通用S3A提交器选项页面" 更好地了解Magic committer及其相关的S3A设置。

魔力委员会：

Magic Commonter特别依靠S3Guard在S3对象存储上提供一致的目录列表。

借助一致的S3 (现在是这种情况)、Magic Comm矽 鴸 昆 可以安全地与任何S3存储分段配合使用。

选择和实验：

根据您的使用情形、您可以在Staging Commenter (依赖于集群HDFS文件系统)和Magic Commenter之间进行选择。

尝试这两种方法、确定哪种方法最适合您的工作负载和要求。

总之、S3A委员会为应对持续、高性能和可靠的S3输出承诺这一根本性挑战提供了解决方案。其内部设计可确保高效的数据传输、同时保持数据完整性。

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.线程、连接池大小和块大小

- 与单个存储分段交互的每个*S3A*客户端都有自己的专用池，其中包含用于上传和复制操作的开放HTTP 1.1连接和线程。
- "您可以调整这些池大小、以便在性能与内存/线程使用量之间取得平衡"。
- 将数据上传到S3时、数据会划分为多个块。默认块大小为32 MB。您可以通过设置FS.S3a.block.size属性来自定义此值。
- 较大的块大小可通过减少上传期间管理多部件的开销来提高大型数据上传的性能。对于大型数据集、建议值为256 MB或以上。

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.多部分上传

S3A提交者*始终*使用MPU (多部分上传)将数据上传到S3存储分段。这是在以下情况下所必需的：任务失败、任务的推测性执行以及提交前作业中止。以下是与多部件上传相关的一些关键规格：

- 最大对象大小：5 TiB (TB)。
- 每次上传的最大部件数：10、000。
- 部件号：范围为1到10、000 (含1到10、000)。
- 部件大小：介于5 MiB和5 GiB之间。值得注意的是、多部分上传的最后一部分没有最小大小限制。

对S3多部件上传使用较小的部件大小既有优点也有缺点。

优势：

- 从网络问题中快速恢复：当您上传较小的部分时、由于网络错误而重新启动失败的上传所产生的影响将降至最低。如果某个部件出现故障、您只需要重新上传该特定部件、而不是整个对象。
- 更好的并行处理：利用多线程或并发连接、可以并行上传更多部件。这种并行处理可提高性能、尤其是在处理大型文件时。

缺点：

- 网络开销：部件较小意味着要上传的部件较多、每个部件都需要自己的HTTP请求。HTTP请求越多、启动和完成单个请求的开销就越大。管理大量小部件可能会影响性能。
- 复杂性：管理订单、跟踪部件和确保上传成功可能会非常繁琐。如果需要中止上传、则需要跟踪并清除已上传的所有部件。

对于Hadoop、建议对fs.s3a.multipart.size使用256MB或以上的部件大小。请始终将FS.S3a.mutlpart.threshold"值设置为2 x FS.S3a.multipart.size值。例如、如果fs.s3a.multipart.size = 256M、则fs.s3a.mutlifpart.threshold"应为512M。

对大型数据集使用较大的零件大小。根据您的特定使用情形和网络条件、选择一个能够平衡这些因素的部件大小非常重要。

多部分上传是 "三步流程"：

1. 上传已启动、StorageGRID将返回一个上传ID.
2. 对象部件将使用上载-id进行上载。
3. 上传所有对象部件后、发送包含上传id的完整多部分上传请求。StorageGRID根据上传的部分构建对象、客户端可以访问该对象。

如果未成功发送完整的多部件上传请求、则这些部件将保留在StorageGRID中、不会创建任何对象。作业中断、失败或中止时会发生这种情况。这些部件将保留在网格中、直到多部件上传完成或中止、或者如果上传启动后15天、StorageGRID会清除这些部件。如果一个存储分段中有许多(几百到几百万个)正在进行的多部分上传、则当Hadoop发送'list-multipart-Uploads'(此请求不按上传ID筛选)时、此请求可能需要很长时间才能完成、或者最终超时。您可以考虑使用适当的FS.S3a.mutlpart.purge值将FS.S3a.multipart.purge.age设置为true (例如、5到7天、不要使用默认值86400、即1天)。或者联系NetApp支持部门调查情况。

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.缓冲区写入数据存储在内存中

为了提高性能、您可以在将写入数据上传到S3之前将其缓冲在内存中。这样可以减少小型写入次数并提高效率。

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

请记住、S3和HDFS的工作方式各不相同。要最有效地利用S3资源、必须仔细调整/测试/实验。

TR-4871：使用Commvault.配置StorageGRID以进行备份和恢复

使用StorageGRID和Commvault.备份和恢复数据

Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Recovery for NetApp软件与NetApp NetApp StorageGRID云存储软件相结合、共同创建了一个联合数据保护解决方案Commvault"完整备份和恢复"和NetApp StorageGRID提供独特且易于使用的解决方案、这些解决方案可以协同工作、帮助您满足全球数据快速增长和法规不断增长的需求。

许多企业希望将存储迁移到云、扩展系统并自动执行长期保留数据的策略。基于云的对象存储因其弹性、扩展能力以及运营和成本效益而闻名、这使其成为备份目标的自然选择。Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commvault/Commv NetApp解决方案全球所有类型的客户都采用了Commvault完 整备份和恢复以及StorageGRID组合解决方案。

关于Commvault和StorageGRID

Commvault"完整备份和恢复"软件是一款企业级集成数据和信息管理解决方案、在单一平台上从头构建、并具有统一的代码库。它的所有功能都共享后端技术、从而在保护、管理和访问数据方面提供完全集成的方法所带来的无与伦比的优势和优势。该软件包含用于保护、归档、分析、复制和搜索数据的模块。这些模块共享一组通用的后端服务和高级功能、这些服务和功能可以彼此无缝交互。解决方案可解决企业中数据管理的所有方面、同时提供无限可扩展性以及前所未有的数据和信息控制。

NetApp StorageGRID作为Commvault云层 是一种企业级混合云对象存储解决方案。您可以将其部署在多个站点上、无论是专用设备还是软件定义的部署。通过StorageGRID、您可以建立数据管理策略、以确定如何存储和保护数据。StorageGRID会收集您制定和实施策略所需的信息。它分析了广泛的特性和需求、包括性能、持久性、可用性、地理位置、 寿命和成本。随着数据在不同位置之间移动以及数据老化、数据将得到全面维护和保护。

StorageGRID智能策略引擎可帮助您选择以下选项之一：

- 使用纠删编码跨多个站点备份数据、以提高故障恢复能力。
- 将对象复制到远程站点、以最大程度地降低WAN延迟和成本。

当StorageGRID存储对象时、无论该对象位于何处或存在多少副本、您都可以将其作为一个对象进行访问。这种行为对于灾难恢复至关重要、因为借助这种行为、即使数据的一个备份副本损坏、StorageGRID也能够还原数据。

将备份数据保留在主存储中的成本可能很高。使用NetApp StorageGRID时、您可以通过将非活动备份数据迁移到StorageGRID来释放主存储上的空间、同时还可以从StorageGRID的众多功能中受益。备份数据的价值会随着时间的推移而变化、存储成本也会随之变化。StorageGRID可以最大限度地降低主存储的成本、同时提高数据的持久性。

主要功能：

CommVault软件平台的主要功能包括：

- 完整的数据保护解决方案、支持虚拟和物理服务器、NAS系统、基于云的基础架构和移动设备上的所有主要操作系统、应用程序和数据库。

- 通过单一控制台简化管理：您可以查看、管理和访问整个企业的所有功能以及所有数据和信息。
- 多种保护方法、包括用于电子发现的数据备份和归档、快照管理、数据复制和内容索引。
- 对磁盘和云存储使用重复数据删除、实现高效存储管理。
- 与NetApp存储阵列(例如AFF、FAS、NetApp HCI和E系列阵列)以及NetApp SolidFire®横向扩展存储系统集成。此外，还可以与NetApp Cloud Volumes ONTAP软件集成，在NetApp存储产品组合中自动创建索引化的应用程序感知型NetApp Snapshot™副本。
- 全面的虚拟基础架构管理、可支持领先的内部虚拟虚拟机管理程序和公共云超规模平台。
- 高级安全功能、可限制对关键数据的访问、提供精细管理功能、并为Active Directory用户提供单点登录访问。
- 基于策略的数据管理、支持您根据业务需求(而不是物理位置)管理数据。
- 提供最先进的最终用户体验、让您的用户能够保护、查找和恢复自己的数据。
- API驱动的自动化、支持您使用第三方工具(如vReise Automation或Service Now)来管理数据保护和恢复操作。

有关支持的工作负载的详细信息，请访问 "CommVault支持的技术"。

备份选项

在云存储上实施CommvaultComplete Backup and Recovery软件时、您有两种备份选项：

- 备份到主磁盘目标、同时将辅助副本备份到云存储。
- 将备份到云存储作为主要目标。

过去、人们认为云或对象存储的性能太低、无法用于主备份。使用主磁盘目标可以加快备份和还原过程、并将辅助副本作为冷备份保留在云上。StorageGRID代表下一代对象存储。StorageGRID的高性能、海量吞吐量以及性能和灵活性远超其他对象存储供应商。

下表列出了StorageGRID中每个备份选项的优势：

	主备份到磁盘和辅助副本到**StorageGRID**	主备份到**StorageGRID**
性能	使用实时挂载或实时恢复时恢复速度最快：最适合第0层/第1层工作负载。	不能用于实时挂载或实时恢复操作。非常适合流式恢复操作和长期保留。
部署架构	使用全闪存或旋转磁盘作为第一个备份登录层。StorageGRID用作二级层。	使用StorageGRID作为全面的备份目标、简化部署。
高级功能(实时还原)	supported	不支持

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- StorageGRID 11．11文档中心+https://docs.netapp.com/us-en/storagegrid-119/[]
- NetApp产品文档+
  https://docs.netapp.com
- CommVault文档+
  https://documentation.commvault.com/2024/essential/index.html

经过测试的解决方案概述

经过测试的解决方案将NetApp解决方案相结合、打造出功能强大的联合解决方案。

解决方案设置

在实验室设置中、StorageGRID环境包含四个NetApp StorageGRID SG5712设备、一个虚拟主管理节点和一个虚拟网关节点。SG5712设备是入门级选项—一种基线配置。选择NetApp StorageGRID SG5760或SG6060等性能更高的设备选项可以显著提高性能。请咨询NetApp StorageGRID 解决方案 架构师以获得规模估算帮助。

对于其数据保护策略、StorageGRID使用集成生命周期管理(ILM)策略来管理和保护数据。在策略中自上而下评估ILM规则。我们实施了下表所示的ILM策略：

ILM规则	限定符	载入行为
纠删编码2+1	超过200 KB的对象	平衡
2副本	所有对象	双提交

默认规则为ILM 2复制规则。在此测试中、对任何200 KB或更大的对象应用了纠删编码2+1规则。默认规则应用于小于200 KB的对象。以这种方式应用规则是StorageGRID的最佳实践。

有关此测试环境的技术详细信息、请阅读中的解决方案设计和最佳实践一节 "借助Commvault,实现NetApp横向扩展数据保护" 技术报告。

StorageGRID硬件规格

下表介绍了此测试中使用的NetApp StorageGRID硬件。采用10Gbps网络连接的StorageGRID SG5712设备是入门级选项、代表了一种基线配置。也可以为SG5712配置25 Gbps网络连接。

硬件	数量	**Disk**	可用容量	网络
StorageGRID SG5712设备	4.	48个4 TB (近线SAS HDD)	136 TB	10 Gbps

选择NetApp StorageGRID SG5760、SG6060或全闪存SGF6112设备等性能更高的设备选项可以显著提升性能。请咨询NetApp StorageGRID 解决方案 架构师以获得规模估算帮助。

Commvault"和**StorageGRID**软件要求

下表列出了在我们的测试中安装在VMware软件上的Commvell和NetApp StorageGRID软件的软件要求。安装了四个MediaAgent数据传输管理器和一个CommServe服务器。在测试中、我们为VMware基础架构实施了10 Gbps网络连接。下表

下表列出了Commvaults软件的总体系统要求：

组件	数量	数据存储库	**Size**	总计	所需的总**IOPS**
CommServe服务器	1.	os	500 GB	500 GB	不适用
		SQL/	500 GB	500 GB	不适用
MediaAgent	4.	虚拟CPU (vCPU)	16.	64	不适用
		RAM	128 GB	512	不适用
		os	500 GB	2 TB	不适用
		索引缓存	2 TB	8 TB	200多个
		DDB	2 TB	8 TB	200-80000 K

在测试环境中、VMware上的NetApp E系列E2812存储阵列上部署了一个虚拟主管理节点和一个虚拟网关节点。每个节点都位于一台单独的服务器上、具有下表所述的最低生产环境要求：

下表列出了StorageGRID虚拟管理节点和网关节点的要求：

节点类型	数量	**vCPU**	**RAM**	存储
网关节点	1.	8.	24 GB	100 GB LUN、用于操作系统
管理节点	1.	8.	24 GB	100 GB LUN、用于操作系统 200 GB LUN、用于管理节点表 200 GB LUN、用于管理节点审核日志

StorageGRID规模估算指南

有关适用于您环境的特定规模估算、请咨询NetApp数据保护专家。NetApp数据保护专家可以使用CommvaultTotal Backup Storage Calculator工具来估计备份基础架构需求。该工具需要CommvaultPartner Portal访问权限。如果需要、请注册访问权限。

Commvaults规模估算输入

可以使用以下任务来执行发现以调整数据保护解决方案的大小：

- 确定需要保护的系统或应用程序/数据库工作负载以及相应的前端容量(以TB为单位)。
- 确定需要保护的虚拟机/文件工作负载和类似前端容量(TB)。
- 确定短期和长期保留要求。
- 确定已确定的数据集/工作负载的每日变更率百分比。
- 确定未来12、24和36个月的预计数据增长。
- 根据业务需求定义用于数据保护/恢复的RTO和RPO。

获得此信息后、便可完成备份基础架构规模估算、从而细分所需的存储容量。

StorageGRID规模估算指南

在执行NetApp StorageGRID规模估算之前、请考虑工作负载的以下方面：

- 可用容量
- WORm模式
- 平均对象大小
- 性能要求
- 已应用ILM策略

可用容量需要满足您已分层到StorageGRID的备份工作负载的大小以及保留计划。

WORM模式是否启用？在Commvault"中启用WORM后、此操作将在StorageGRID上配置对象锁定。这将增加所需的对象存储容量。所需的容量因保留期限和每次备份的对象更改数而异。

平均对象大小是一个输入参数、用于帮助估算StorageGRID环境中的性能规模。Commvault"工作负载使用的平均对象大小取决于备份类型。

下表按备份类型列出了平均对象大小、并说明了还原过程从对象存储中读取的内容：

备份类型	平均对象大小	还原行为
在StorageGRID中创建辅助副本	32 MB	完全读取32 MB对象
将备份定向到StorageGRID (已启用重复数据删除)	8MB	1 MB随机范围读取
将备份定向到StorageGRID (已禁用重复数据删除)	32 MB	完全读取32 MB对象

此外、了解完整备份和增量备份的性能要求有助于确定StorageGRID存储节点的规模估算。StorageGRID信息生命周期管理(ILM)策略数据保护方法可确定存储Commvaults备份所需的容量、并影响网格的规模估算。

StorageGRID ILM复制是StorageGRID用于存储对象数据的两种机制之一。当StorageGRID将对象分配给复制数据的ILM规则时、系统会为对象的数据创建精确副本、并将这些副本存储在存储节点上。

纠删编码是 StorageGRID 存储对象数据的第二种方法。当StorageGRID将对象分配给配置为创建经过删除编码的副本的ILM规则时、它会将对象数据分区为数据片段。然后、它会额外地对奇偶校验片段进行运算、并将每个片段存储在不同的存储节点上。访问某个对象时，系统会使用存储的片段重新组合该对象。如果数据片段或奇偶校验片段损坏或丢失、纠删编码算法可以使用剩余数据和奇偶校验片段的一部分重新创建该片段。

这两种机制需要不同的存储量、如以下示例所示：

- 如果存储两个复制副本、则存储开销会增加一倍。
- 如果您存储的是2+1经过删除的副本、则存储开销会增加1.5倍。

对于测试的解决方案、我们使用了单个站点上的入门级StorageGRID部署：

- 管理节点：VMware虚拟机(VM)
- 负载平衡器：VMware VM
- 存储节点：4个SG5712、带有4 TB驱动器
- 主管理节点和网关节点：具有最低生产工作负载要求的VMware VM

StorageGRID还支持第三方负载平衡器。

StorageGRID通常部署在两个或更多站点中、并采用数据保护策略来复制数据、以防止发生节点和站点级故障。通过将数据备份到StorageGRID、您的数据将受到多个副本或通过纠删编码的保护、这些编码可通过一种算法可靠地分隔和重新组合数据。

您可以使用规模估算工具 "Fusion" 调整网格大小。

扩展

您可以通过向存储节点添加存储、向现有站点添加新网格节点或添加新数据中心站点来扩展NetApp StorageGRID系统。您可以在不中断当前系统运行的情况下执行扩展。
StorageGRID可以通过为存储节点或运行负载平衡器和管理节点的物理设备使用性能更高的节点来扩展性能、也可以通过简单地添加更多节点来扩展性能。

有关扩展StorageGRID系统的详细信息，请参阅 "《StorageGRID 11.9."。

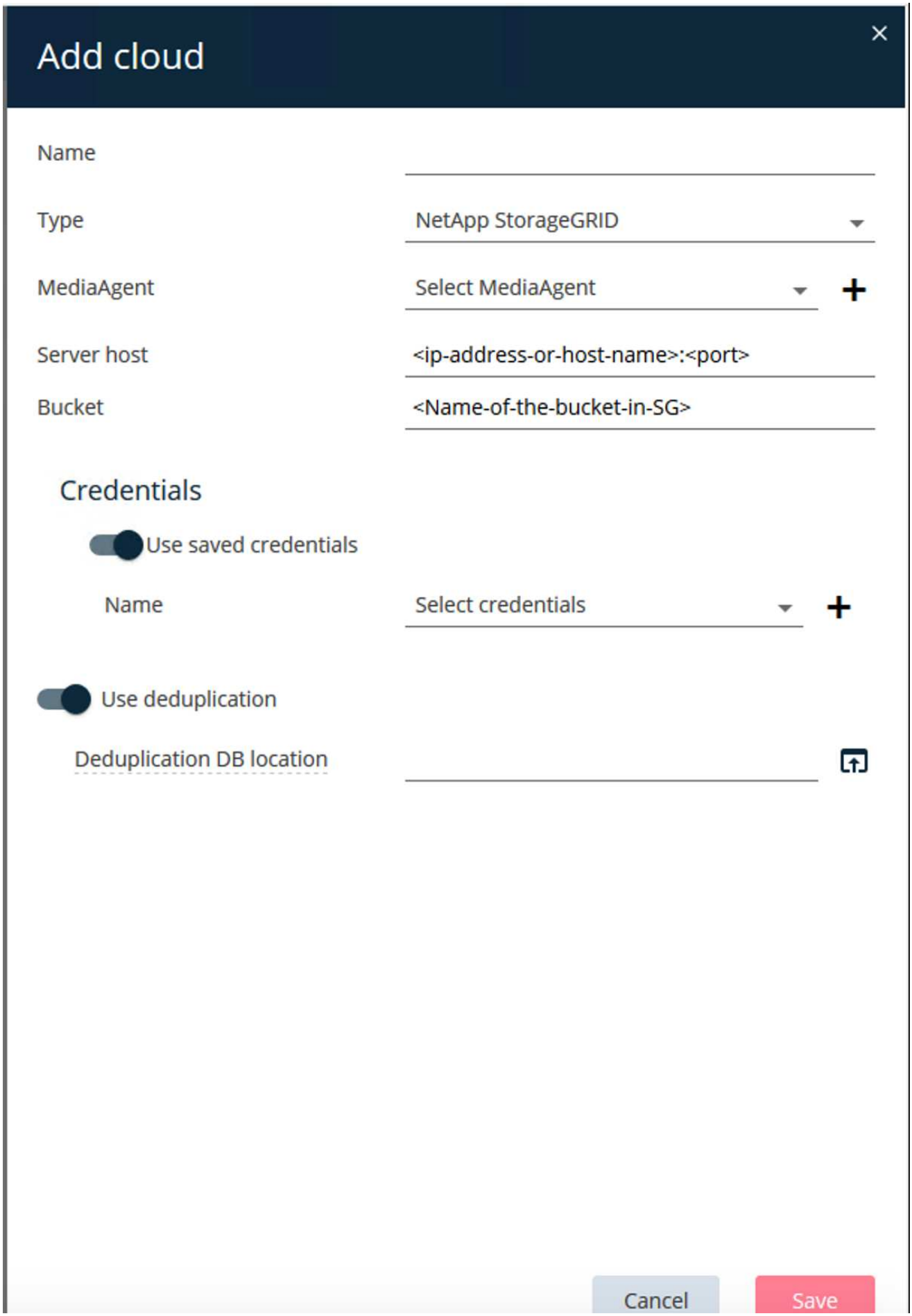
运行数据保护作业

要为StorageGRID配置适用于NetApp的Commvault完 整备份和恢复、请执行以下步骤、以便在Commvault软件 中将StorageGRID添加为云库。

第1步：使用StorageGRID配置Commvault

步骤

1. 登录到CommvaultCommand Center。在左侧面板上、单击"存储">"云">"添加"以查看并响应"添加云"对话框：


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. 对于类型、选择NetApp StorageGRID。
3. 对于MediaAgent、选择与云库关联的所有。
4. 对于服务器主机、输入StorageGRID端点的IP地址或主机名以及端口号。

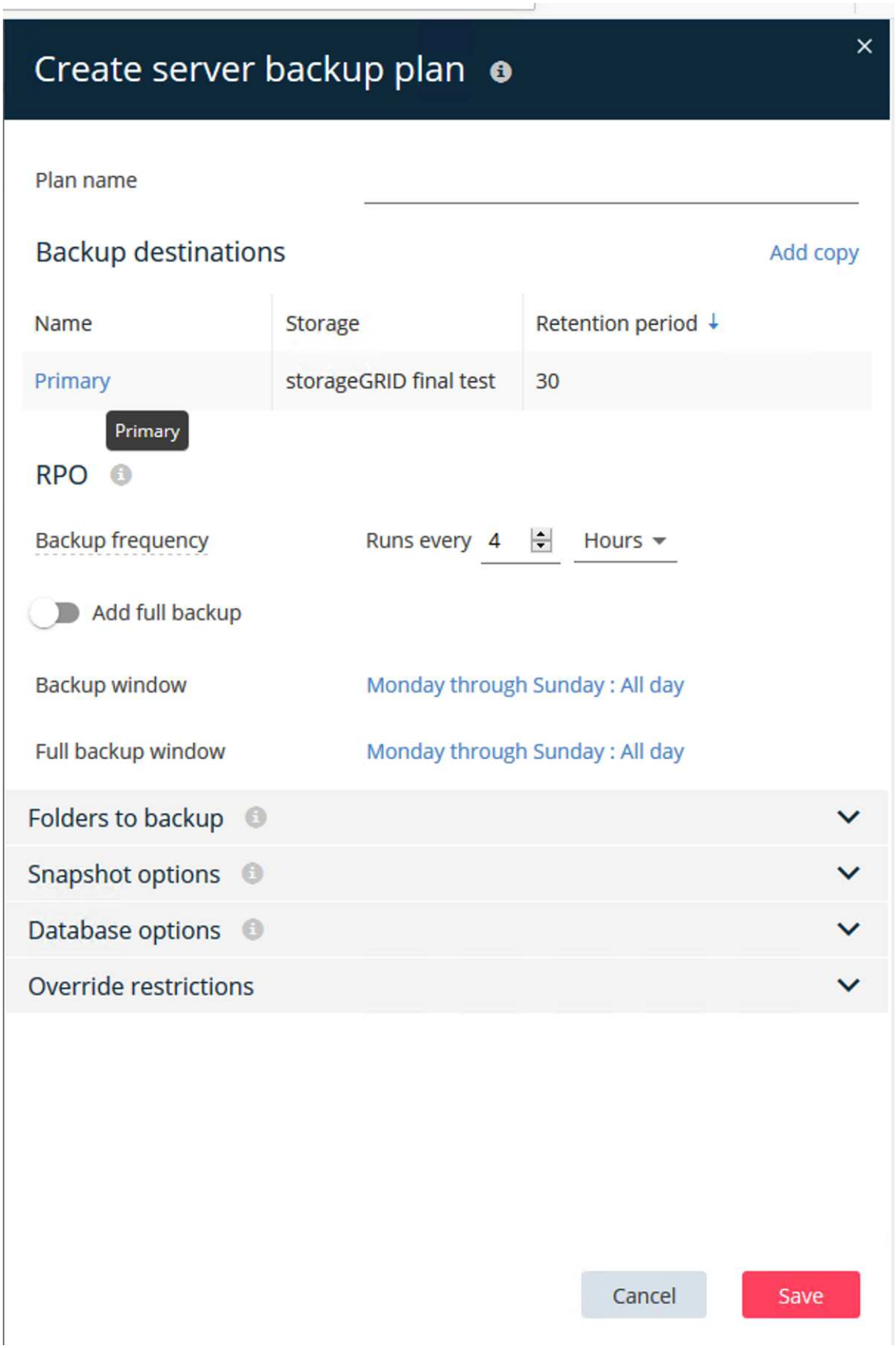
   按照上的StorageGRID文档中的步骤进行操作 "如何配置负载平衡器端点(端口)"。确保您有一个HTTPS端口、其中包含自签名证书以及StorageGRID端点的IP地址或域名。

5. 如果要使用重复数据删除、请启用此选项并提供指向重复数据删除数据库位置的路径。
6. 单击保存。

第**2**步：创建以**StorageGRID**为主要目标的备份计划

步骤

1. 在左侧面板上、选择Manage > Plans以查看并响应Create Server Backup Plan对话框。

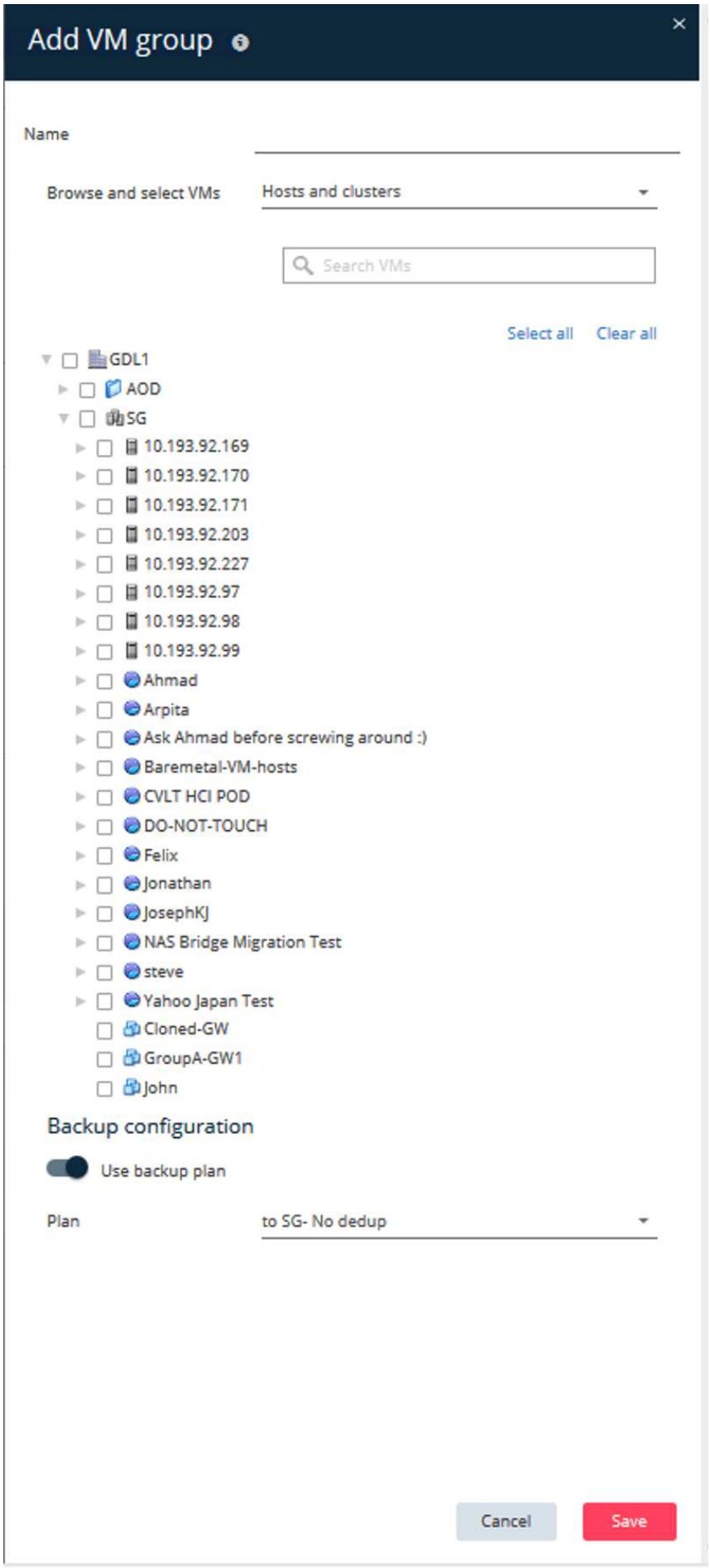

Create server backup plan
Plan name
Backup destinations
Add copy
Name
Storage
Retention period
Primary
storageGRID final test
30
Primary
RPO
Backup frequency
Runs every 4
Hours
Add full backup
Backup window
Monday through Sunday : All day
Full backup window
Monday through Sunday : All day
Folders to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

2. 输入计划名称。
3. 选择先前创建的StorageGRID简单存储服务(S3)存储备份目标。
4. 输入所需的备份保留期限和恢复点目标(RPO)。
5. 单击保存。

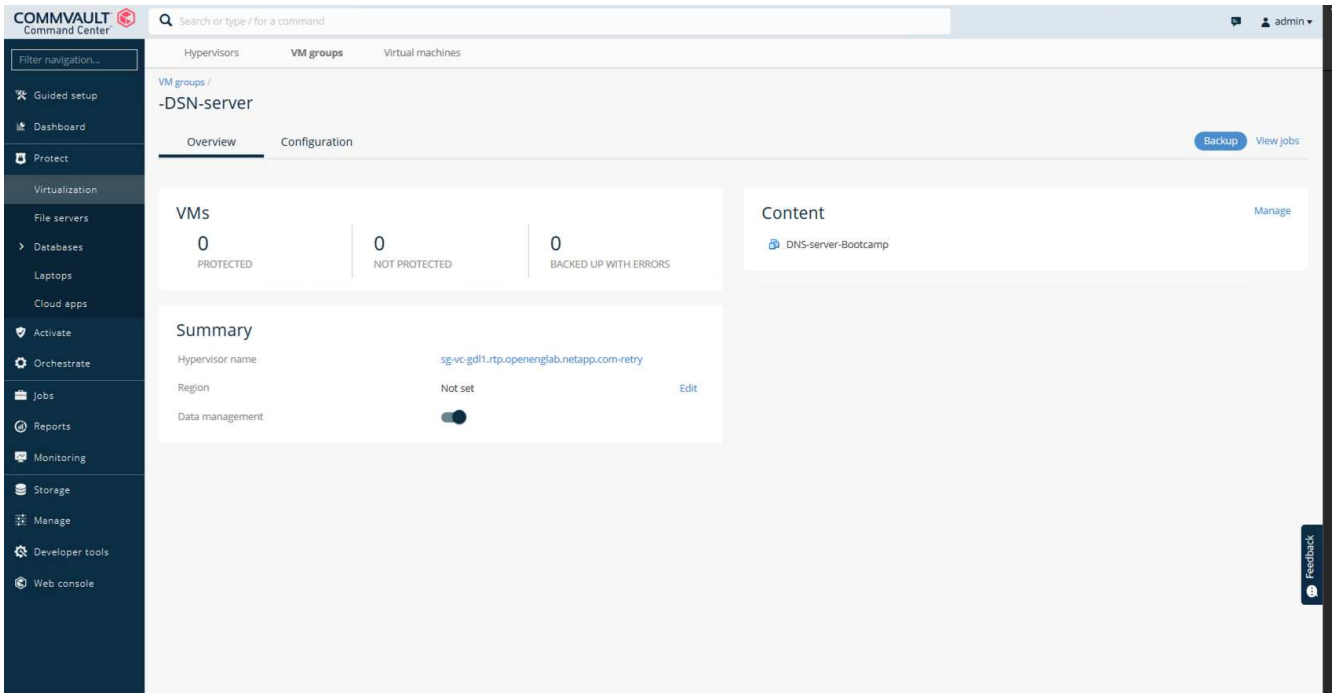
第**3**步：启动备份作业以保护工作负载

步骤

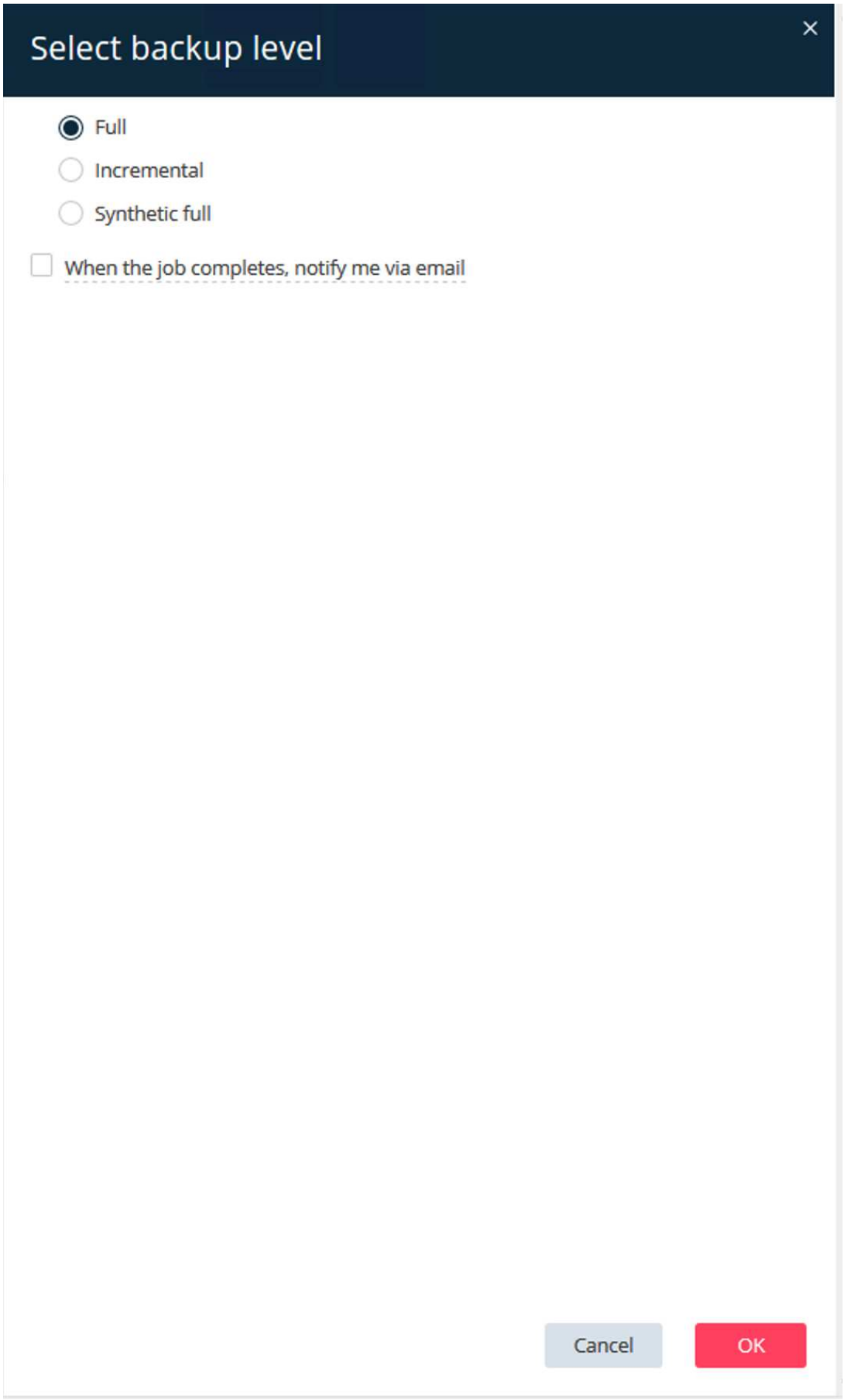
1. 在CommVault Command Center上、导航到"Protect">"Virtualization (保护>虚拟化)"。
2. 添加VMware vCenter Server虚拟机管理程序。
3. 单击刚刚添加的虚拟机管理程序。
4. 单击添加VM组以响应添加VM组对话框、以便您可以查看计划保护的vCenter环境。


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

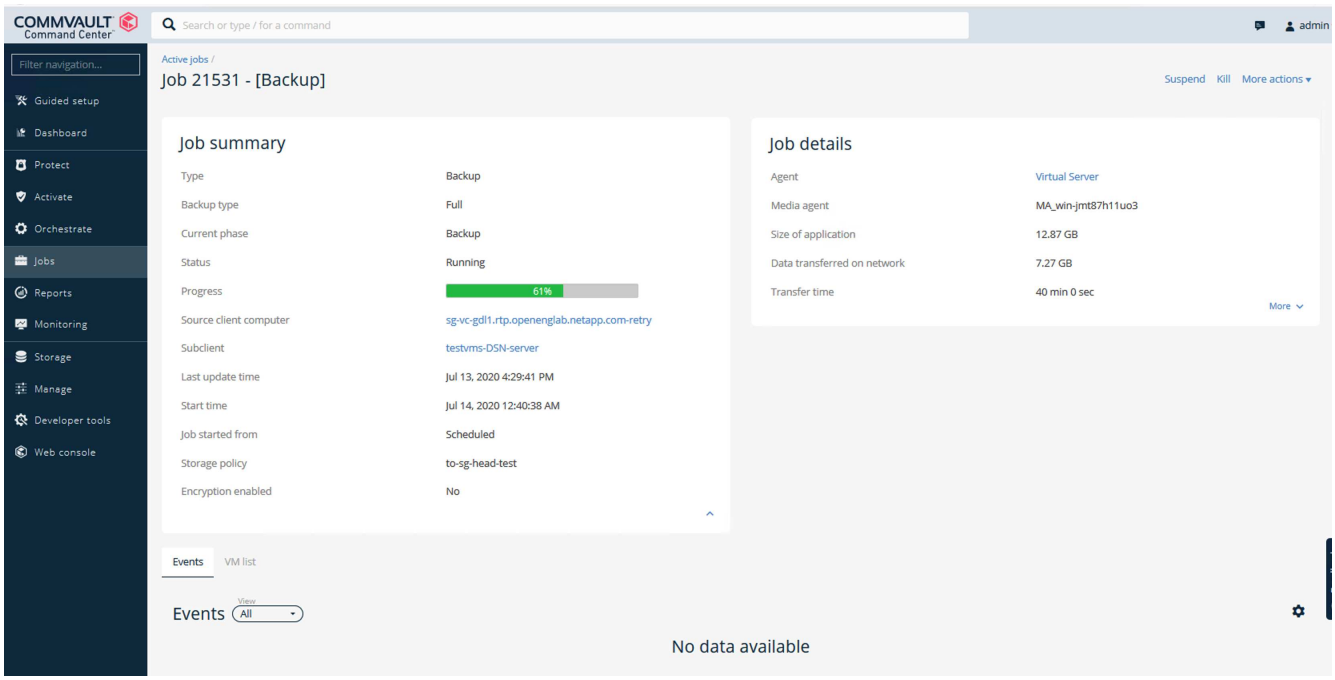
5. 选择一个数据存储库、一个VM或一组VM、然后为其输入一个名称。
6. 选择您在上一任务中创建的备份计划。
7. 单击保存以查看您创建的VM组。
8. 在虚拟机组窗口的右上角、选择备份：



9. 选择完整作为备份级别、(可选)备份完成后请求电子邮件、然后单击确定启动备份作业：


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

10. 导航到作业摘要页面以查看作业指标：



查看基线性能测试

在辅助副本操作中、四个CommvaultMediaAgent将数据备份到NetApp AFF A300系统、并在NetApp StorageGRID上创建了一个辅助副本。有关测试设置环境的详细信息、请阅读技术报告中的"解决方案设计和最佳实践"一节 "借助Commvault,实现NetApp横向扩展数据保护" 。

测试涉及100个VM和1000个VM、这两个测试都包含50/50的Windows和CentOS VM。下表显示了基线性能测试的结果：

操作	备份速度	恢复速度
辅助复印	2 TB/小时	1.27 TB/小时
直接与对象连接和从对象连接(启用重复数据删除)	2.2 TB/小时	1.22 TB/小时

为了测试过期性能、删除了250万个对象。如图2和图3所示、删除操作在3小时内完成、并释放了80 TB以上的空间。删除运行于上午10：30开始。

图**1**：在不到**3**小时的时间内删除**250**万**(80 TB)**对象。

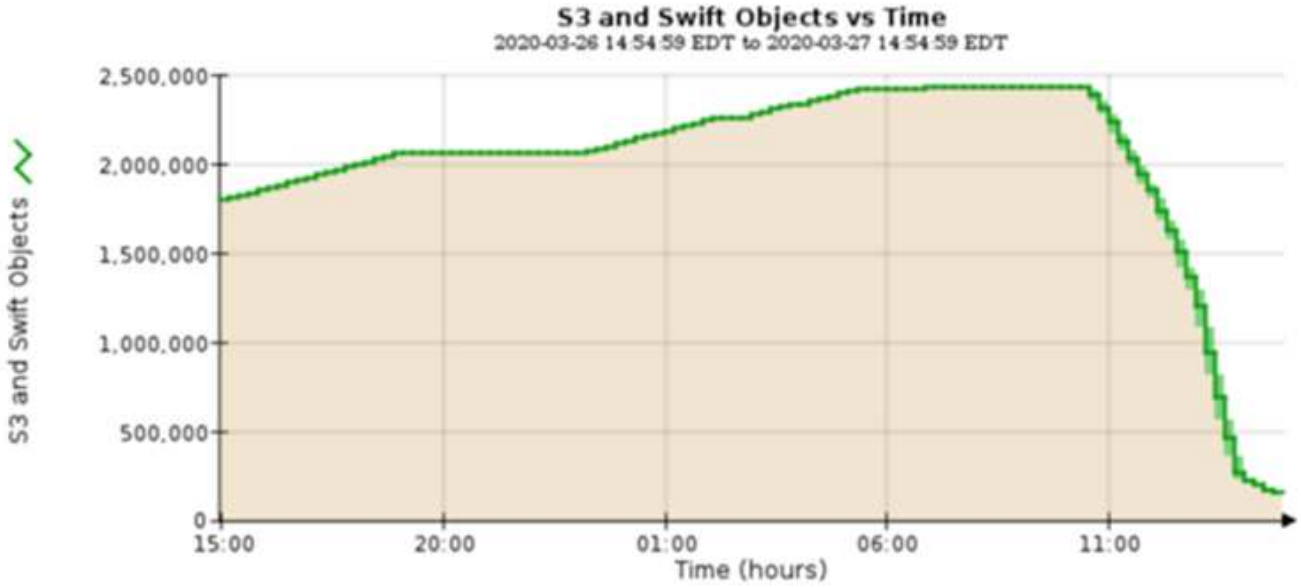
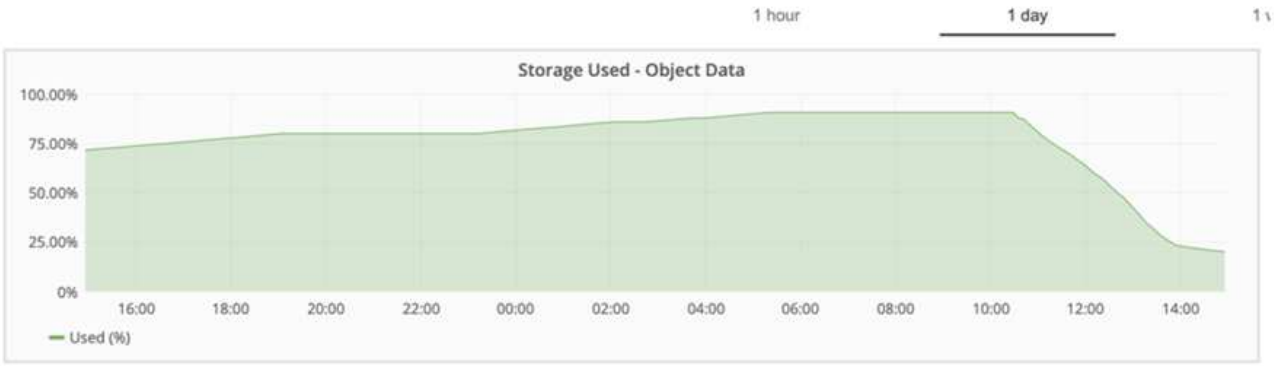


图**2**：在不到**3**小时的时间内释放**80 TB**的存储。



存储分段一致性级别建议

通过NetApp StorageGRID、最终用户可以为对简单存储服务(S3)分段中的对象执行的操作选择一致性级别。

CommVault MediaAgent是CommVault环境中的数据迁移程序。大多数情况下，MediaAgent配置为在本地写入主StorageGRID站点。因此、建议在本地主站点中使用高一致性级别。在StorageGRID中创建的Commvault"分段上设置一致性级别时、请遵循以下准则。

如果您的CommVault版本早于11.0.0 - Service Pack 16、请考虑将CommVault升级到最新版本。如果不能这样做、请务必遵循适用于您的版本的准则。

- Commvault11.0.0之前的版本- Service Pack 16.*在11.0.0之前的版本- Service Pack 16中，Commvault"会在还原和删减过程中对不存在的对象执行S3 head和GET操作。将存储分段一致性级别设置为强站点、以便为Commvaultvault"备份到StorageGRID实现最佳一致性级别。
- Commvault11.0.0版- Service Pack 16及更高版本。*在11.0.0版- Service Pack 16及更高版本中、对不存在的对象执行S3机头和GET操作的数量将降至最低。将默认分段一致性级别设置为read-after-new-write、以确保StorageGRID环境中的高一致性级别。

TR-4626：负载平衡器

将第三方负载平衡器与**StorageGRID**结合使用

了解第三方和全局负载平衡器在StorageGRID等对象存储系统中的作用。

使用第三方负载平衡器实施NetApp®StorageGRID®的一般指导。

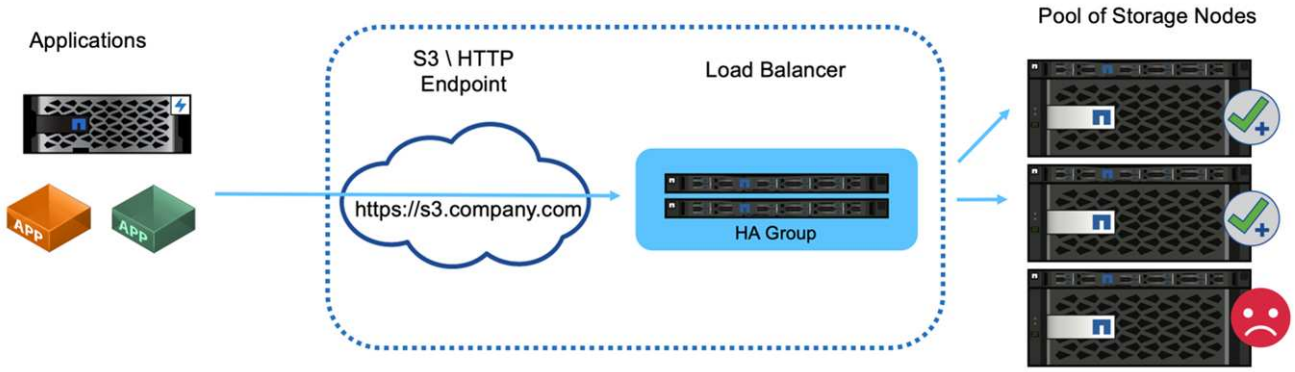
对象存储与"云存储"一词同义、正如您所期望的那样、利用云存储的应用程序会通过URL为该存储寻址。在这一简单URL的支持下、StorageGRID可以在单个站点或分布在不同地理位置的站点上扩展容量、性能和持久性。负载平衡器是实现这种精简性的组件。

本文档的目的是向StorageGRID客户介绍负载平衡器选项、并提供配置第三方负载平衡器的一般指导。

负载平衡器基础知识

负载平衡器是StorageGRID等企业级对象存储系统的基本组件。StorageGRID由多个存储节点组成、每个存储节点都可以为给定StorageGRID实例提供整个简单存储服务(Simple Storage Service、S3)名称空间。负载平衡器会创建一个高度可用的端点、我们可以将StorageGRID节点放置在该端点的后面。StorageGRID在与S3兼容的对象存储系统中是独一无二的、因为它提供自己的负载平衡器、但它也支持第三方或通用负载平衡器、例如F5、Citrix NetScaler、HA代理、NGINX等。

下图使用示例URL/完全限定域名(FQDN) s3.company.com”。负载平衡器会创建一个虚拟IP (VIP)、该IP可通过DNS解析为FQDN、然后将应用程序的任何请求定向到StorageGRID节点池。负载平衡器会对每个节点执行运行状况检查、并仅与运行状况良好的节点建立连接。



此图显示了StorageGRID提供的负载平衡器、但第三方负载平衡器的概念相同。应用程序使用负载平衡器上的VIP建立HTTP会话、流量将通过负载平衡器传输到存储节点。默认情况下、从应用程序到负载平衡器以及从负载平衡器到存储节点的所有流量都会通过HTTPS进行加密。HTTP是一个受支持的选项。

本地和全局负载平衡器

负载平衡器有两种类型：

- 本地交通管理系统**(LTM)**。将连接分布在单个站点的一个节点池中。
- 全局服务负载平衡器**(GSLB)**。将连接分布在多个站点上、从而有效地对LTM负载平衡器进行负载平衡。可以将GSLB视为智能DNS服务器。当客户端请求StorageGRID端点URL时、GSLB会根据可用性或其他因素(例如、哪个站点可以为应用程序提供更低的延迟)将其解析为LTM的VIP。虽然LTM始终是必需的、但GSLB是可选的、具体取决于StorageGRID站点数量和应用程序要求。

在与S3兼容的对象存储供应商中、StorageGRID是独一无二的、因为它提供了一个本机负载平衡器、可用作专用设备、VM或容器。StorageGRID提供的负载平衡器也称为网关节点。

对于尚未拥有F5、Citrix等负载平衡器的客户、实施第三方负载平衡器可能非常复杂。StorageGRID负载平衡器可显著简化负载平衡器操作。

网关节点是一种高可用性、高性能的企业级负载平衡器。客户可以选择在同一网格中实施网关节点、第三方负载平衡器甚至两者。网关节点是本地流量管理器、而不是GSLB。

StorageGRID负载平衡器具有以下优势：

- 精简性。自动配置资源池、运行状况检查、修补和维护、所有这些都由StorageGRID进行管理。
- 性能。StorageGRID负载平衡器专用于StorageGRID、您不会与其他应用程序争用带宽。
- 成本。虚拟机(VM)和容器版本免费提供。
- 交通分类。高级流量分类功能支持StorageGRID专用的QoS规则以及工作负载分析。
- 未来的**StorageGRID**特定功能。在即将发布的版本中、StorageGRID将继续优化负载平衡器并为其添加创新功能。

有关部署StorageGRID网关节点的详细信息，请参见 "StorageGRID 文档"。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- NetApp StorageGRID文档中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID支持 https://docs.netapp.com/us-en/storagegrid-enable/
- StorageGRID F5负载平衡器设计注意事项 https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load平衡NetApp StorageGRID https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- KEMP—负载平衡NetApp StorageGRID https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

了解如何在StorageGRID中为HTTPS实施SSL证书

了解在StorageGRID中实施SSL证书的重要性和步骤。

如果您使用的是HTTPS、则必须具有安全套接字层(SSL)证书。SSL协议可识别客户端和端点、并验证它们是否可信。SSL还可对流量进行加密。客户端必须信任SSL证书。为此、SSL证书可以来自全局受信任的证书颁发机构(CA)、例如、数码证书、在基础架构中运行的私有CA或主机生成的自签名证书。

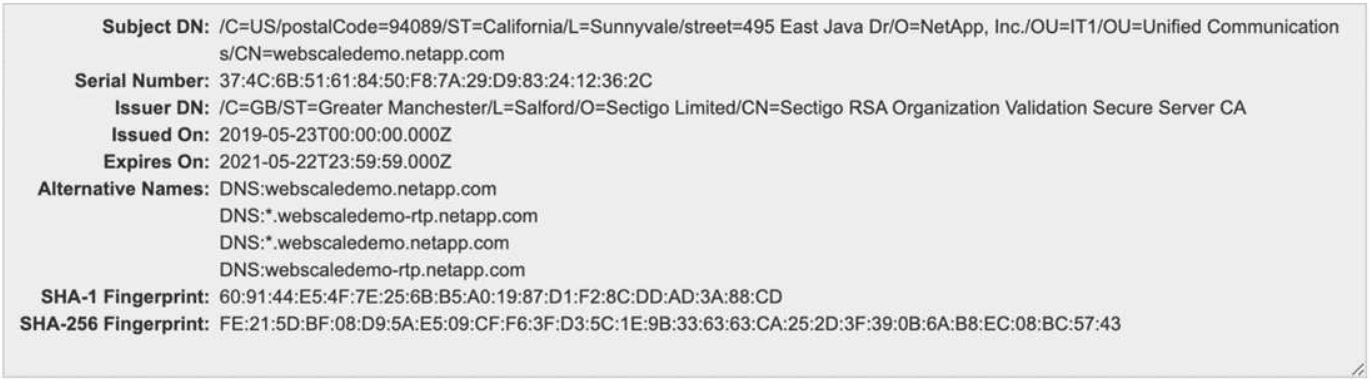
首选方法是使用全局受信任的CA证书、因为无需执行其他客户端操作。证书将加载到负载平衡器或StorageGRID中、客户端信任并连接到端点。

使用私有CA要求将根证书和所有从属证书添加到客户端。信任专用CA证书的过程可能因客户端操作系统和应用程序而异。例如、在ONTAP for FabricPool中、您必须单独将链中的每个证书(根证书、从属证书、端点证书)上

传到ONTAP集群。

使用自签名证书要求客户端信任提供的证书、而不使用任何CA来验证其真实性。某些应用程序可能不接受自签名证书、并且无法忽略验证。

SSL证书在客户端负载平衡器StorageGRID路径中的放置取决于您需要SSL终止的位置。您可以将负载平衡器配置为客户端的终止端点、然后使用新的SSL证书对负载平衡器与StorageGRID的连接进行重新加密或热加密。或者、您也可以通过此流量并让StorageGRID成为SSL终止端点。如果负载平衡器是SSL终止端点、则此证书将安装在负载平衡器上、并包含DNS名称/URL的使用者名称以及客户端配置为通过负载平衡器连接到StorageGRID目标的任何备用URL/DNS名称。 包括任何通配符名称。如果为负载平衡器配置了直通、则必须在StorageGRID中安装SSL证书。同样、证书必须包含DNS名称/URL的使用者名称、以及客户端配置为通过负载平衡器连接到StorageGRID目标的任何备用URL/DNS名称、包括任何通配符名称。证书中无需包含单个存储节点名称、只需包含端点URL即可。



在**StorageGRID**中配置受信任的第三方负载平衡器

了解如何在StorageGRID中配置受信任的第三方负载平衡器。

如果使用的是一个或多个外部第7层负载平衡器以及基于IP的S3分段或组策略、则StorageGRID必须确定实际发送方的IP地址。它通过查看负载平衡器插入到请求中的X-Forwarded-for (XFF)标头来执行此操作。由于在直接发送到存储节点的请求中、XFF标头很容易受到保护、因此StorageGRID必须确认每个请求都由可信的第7层负载平衡器路由。如果StorageGRID无法信任请求源、则会忽略XFF标头。有一个网格管理API允许配置受信任的外部第7层负载平衡器列表。此新API为专用API、未来的StorageGRID版本可能会有所更改。有关最新信息，请参见知识库文章 "如何配置StorageGRID以使用第三方第7层负载平衡器"。

了解本地流量管理器负载平衡器

浏览有关本地流量管理器负载平衡器的指导、并确定最佳配置。

下面介绍了配置第三方负载平衡器的一般指导。与负载平衡器管理员一起确定适合您环境的最佳配置。

创建存储节点的资源组

将StorageGRID存储节点分组到资源池或服务组中(术语可能因特定负载平衡器而异)。StorageGRID存储节点会在以下端口上提供S3 API：

- S3 HTTPS：18082
- S3 HTTP：18084

大多数客户选择通过标准HTTPS和HTTP端口(443和80)在虚拟服务器上提供API。

每个StorageGRID站点默认需要三个存储节点、其中两个节点必须运行状况良好。

运行状况检查

第三方负载平衡器需要一种方法来确定每个节点的运行状况及其接收流量的资格。NetApp建议使用HTTP `OPTIONS` 方法执行运行状况检查。负载平衡器会向每个存储节点发出HTTP `OPTIONS` 请求、并需要 `200` 状态响应。

如果任何存储节点未提供 `200` 响应、则该节点将无法处理存储请求。您的应用程序和业务要求应确定这些检查的超时时间以及负载平衡器所执行的操作。

例如、如果数据中心1中的四个存储节点中有三个已关闭、您可以将所有流量定向到数据中心2。

建议的轮询间隔为每秒一次、在三次检查失败后将节点标记为脱机。

S3运行状况检查示例

在以下示例中，我们会发送 `OPTIONS` 并检查 `200 OK`。我们使用 `OPTIONS` 、因为Amazon S3)不支持未经授权的请求。

```
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
```

基于文件或内容的运行状况检查

通常、NetApp不建议执行基于文件的运行状况检查。例如，通常在具有只读策略的存储分段中创建一个小文件—`healthcheck.htm`。然后、负载平衡器会提取并评估此文件。这种方法有几个缺点：

- *取决于单个帐户。*如果禁用了拥有该文件的帐户、则运行状况检查将失败、并且不会处理任何存储请求。

- *数据保护规则。*默认数据保护方案采用双副本方法。在这种情况下、如果托管运行状况检查文件的两个存储节点不可用、则运行状况检查将失败、并且存储请求不会发送到运行状况良好的存储节点、从而使网格脱机。
- *审核日志膨胀。*负载平衡器每X分钟从每个存储节点提取一次文件、从而创建许多审核日志条目。
- *资源密集型。*每隔几秒钟从每个节点提取运行状况检查文件会占用网格和网络资源。

如果需要执行基于内容的运行状况检查、请使用具有专用S3存储分段的专用租户。

会话持久性

会话持久性(即、保持性)是指允许给定HTTP会话持续的时间。默认情况下、存储节点会在10分钟后丢弃会话。持久性越长、性能越好、因为应用程序不必为每个操作重新建立会话；但是、保持这些会话处于打开状态会占用资源。如果您确定工作负载将受益、则可以减少第三方负载平衡器上的会话持久性。

虚拟托管模式寻址

现在、虚拟托管模式已成为AWS S3的默认方法、虽然StorageGRID和许多应用程序仍支持路径模式、但最佳做法是实施虚拟托管模式支持。虚拟托管模式请求的主机名包含分段。

要支持虚拟托管模式、请执行以下操作：

- 支持通配符DNS查找：*。.s3.company.com
- 使用带有主题可选名称的SSL证书支持通配符：*。.s3.company.com一些客户已经表达了有关使用通配符证书的安全问题。StorageGRID继续支持路径模式访问、FabricPool等关键应用程序也是如此。也就是说、如果没有虚拟托管支持、某些S3 API调用会失败或行为不正确。

SSL终止

第三方负载平衡器上的SSL终止具有安全优势。如果负载平衡器受损、网格将被分割。

支持三种配置：

- *SSL传递。*SSL证书作为自定义服务器证书安装在StorageGRID上。
- *SSL终止和重新加密(建议)。*如果您已经在负载平衡器上执行SSL证书管理、而不是在StorageGRID上安装SSL证书、则这可能会很有用。此配置还具有将攻击面限制在负载平衡器上的其他安全优势。
- *使用HTTP终止SSL。*在此配置中、SSL将在第三方负载平衡器上终止、负载平衡器与StorageGRID之间的通信将不进行加密、以利用SSL卸载功能(由于SSL库嵌入在现代处理器中、因此优势有限)。

直通配置

如果您要为负载平衡器配置直通、则必须在StorageGRID上安装证书。转到菜单：配置[服务器证书>对象存储API服务端点服务器证书]。

源客户端**IP**可见性

StorageGRID 11.4引入了可信第三方负载平衡器的概念。要将客户端应用程序IP转发到StorageGRID、必须配置此功能。有关详细信息、请参见 "如何配置StorageGRID以使用第三方第7层负载平衡器。"

要启用XFF标头以查看客户端应用程序的IP、请执行以下步骤：

步骤

1. 在审核日志中记录客户端IP。
2. 使用 `aws:SourceIp` S3存储分段或组策略。

负载平衡策略

大多数负载平衡解决方案都提供多种负载平衡策略。以下是常见策略：

- *循环*通用配置、但节点较少且传输量较大、从而使单个节点堵塞。
- *最少连接。*非常适合小型对象工作负载和混合对象工作负载、从而使连接平等分布到所有节点。

随着可供选择的存储节点数量不断增加、算法的选择就不再那么重要了。

数据路径

所有数据流经本地流量管理器负载平衡器。StorageGRID不支持直接服务器路由(DSR)。

验证连接分布

要验证您的方法是否在存储节点之间均匀分布负载、请检查给定站点中每个节点上已建立的会话：

- *用户界面方法。*转到菜单：Support[Metrics > S3 Overview > LDR HTTP S语]
- *Metrics API.*使用 `storagegrid_http_sessions_incoming_currently_established`

了解**StorageGRID**配置的几个用例

了解客户和NetApp IT实施的StorageGRID配置的少数用例。

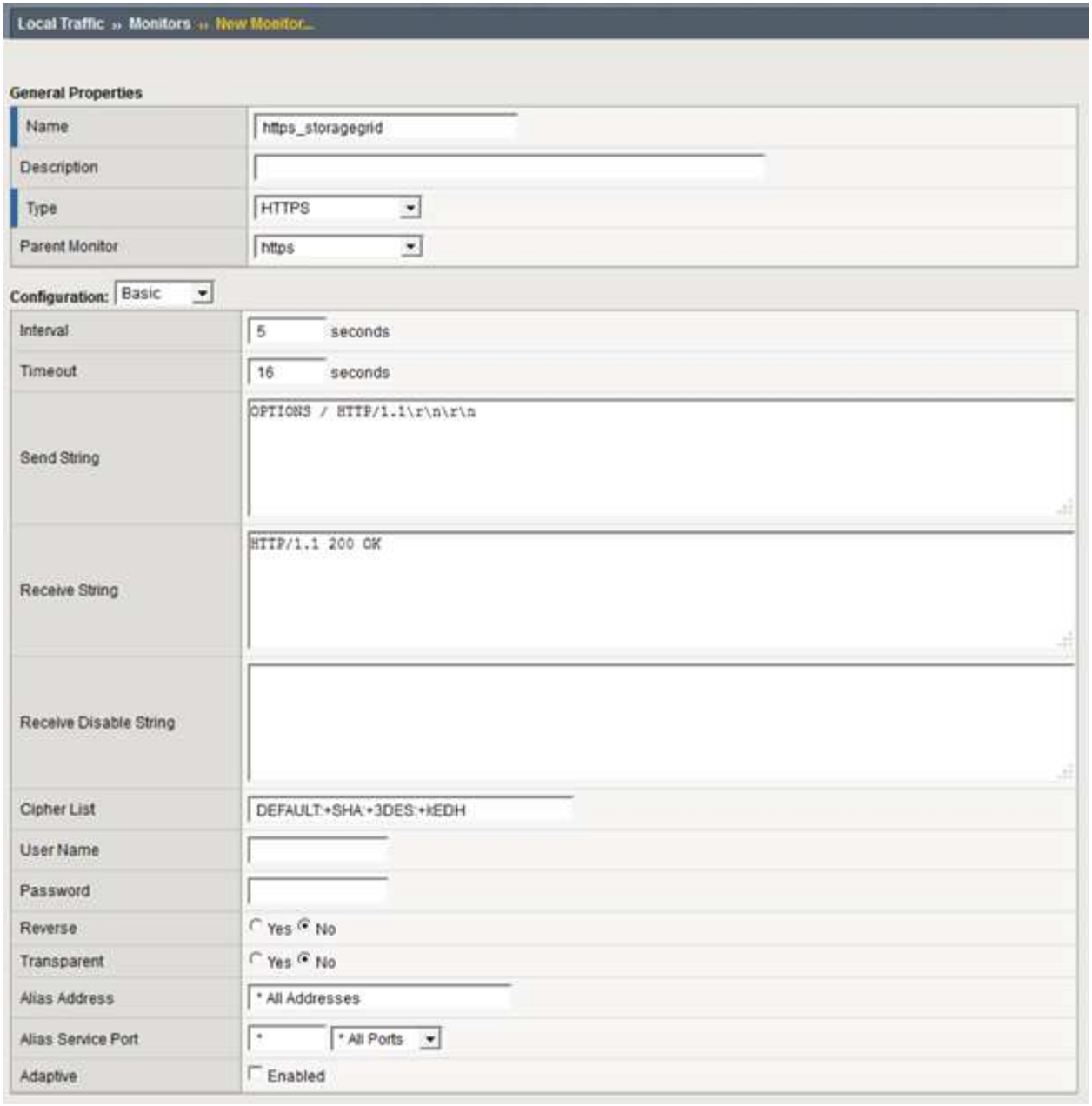
以下示例说明了StorageGRID客户(包括NetApp IT)实施的配置。

用于**S3**存储分段的**F5 BIG-IP**本地流量管理器运行状况检查监控器

要配置F5 BIG-IP本地流量管理器运行状况检查监控器、请执行以下步骤：

步骤

1. 创建新显示器。
   a. 在Type字段中，输入 `HTTPS`。
   b. 根据需要配置时间间隔和超时。
   c. 在发送字符串字段中，输入 `OPTIONS / HTTP/1.1\r\n\r\n`. \r\n表示回车；不同版本的大IP软件需要零个、一个或两组\r\n序列。有关详细信息，请参见 https://support.f5.com/csp/article/K10655。
   d. 在Receive String (接收字符串)字段中，输入： `HTTP/1.1 200 OK`。



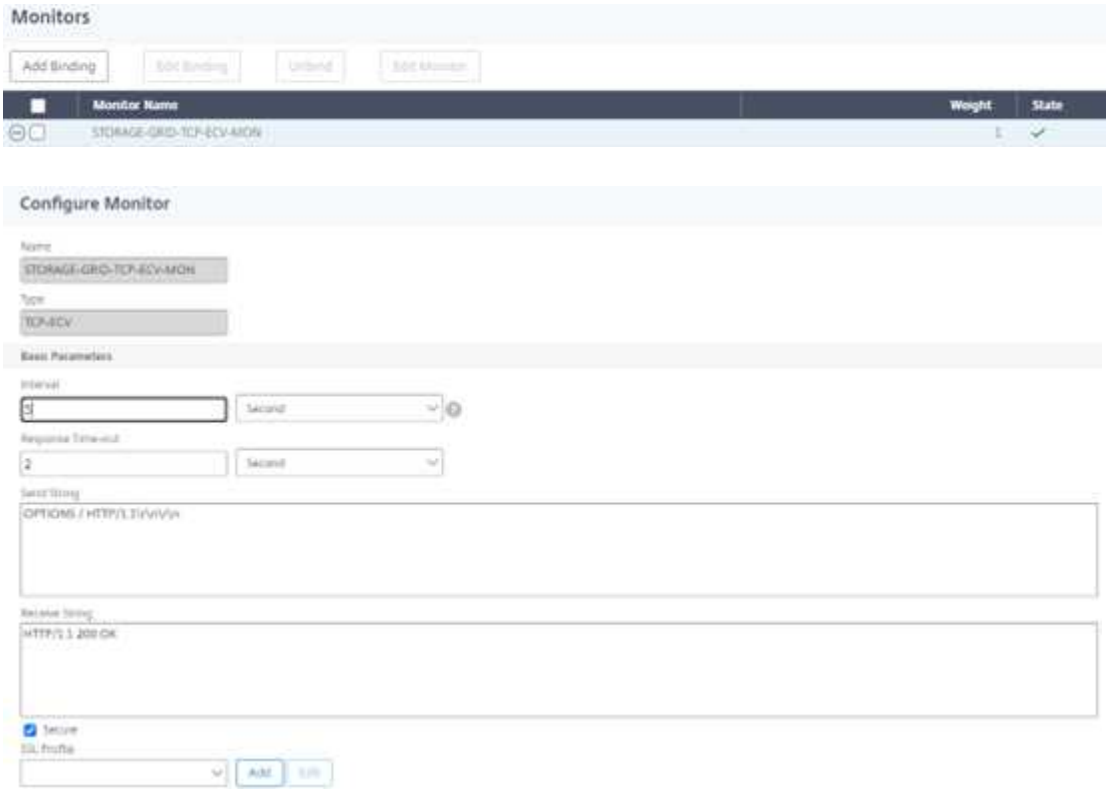
2. 在创建池中、为所需的每个端口创建一个池。
   a. 分配在上一步中创建的运行状况监控器。
   b. 选择负载平衡方法。
   c. 选择服务端口：18082 (S3)。
   d. 添加节点。

Citrix NetScaler

Citrix NetScaler为存储端点创建一个虚拟服务器，并将StorageGRID存储节点称为应用程序服务器，然后将其分组到“服务”中。

使用HTTP-ECV运行状况检查监控器创建自定义监控器，以便通过选项请求和接收来执行建议的运行状况检查 `200`。为HTTP-ECV配置了发送字符串并验证接收字符串。

有关详细信息，请参阅Citrix文档 "HTTP-ECV运行状况检查监控器的配置示例"。



Loadbalancer.org

Loadbalancer.org已对StorageGRID进行了自己的集成测试，并提供了大量的配置指南：https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf。

凯普

KEMP已对StorageGRID进行了自己的集成测试，并提供了大量的配置指南： https://kemptechnologies.com/solutions/netapp/。

HA 代理

将HAProxy配置为使用options request、并在haproxy.cfg中检查运行状况检查的200状态响应。您可以将前端的绑定端口更改为其他端口、例如443。

以下是在HAProxy上终止SSL的示例：

```
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
```

以下是SSL直通示例：

```
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
```

有关StorageGRID配置的完整示例、请参见 "HAProxy配置示例" GitHub上的。

验证StorageGRID中的SSL连接

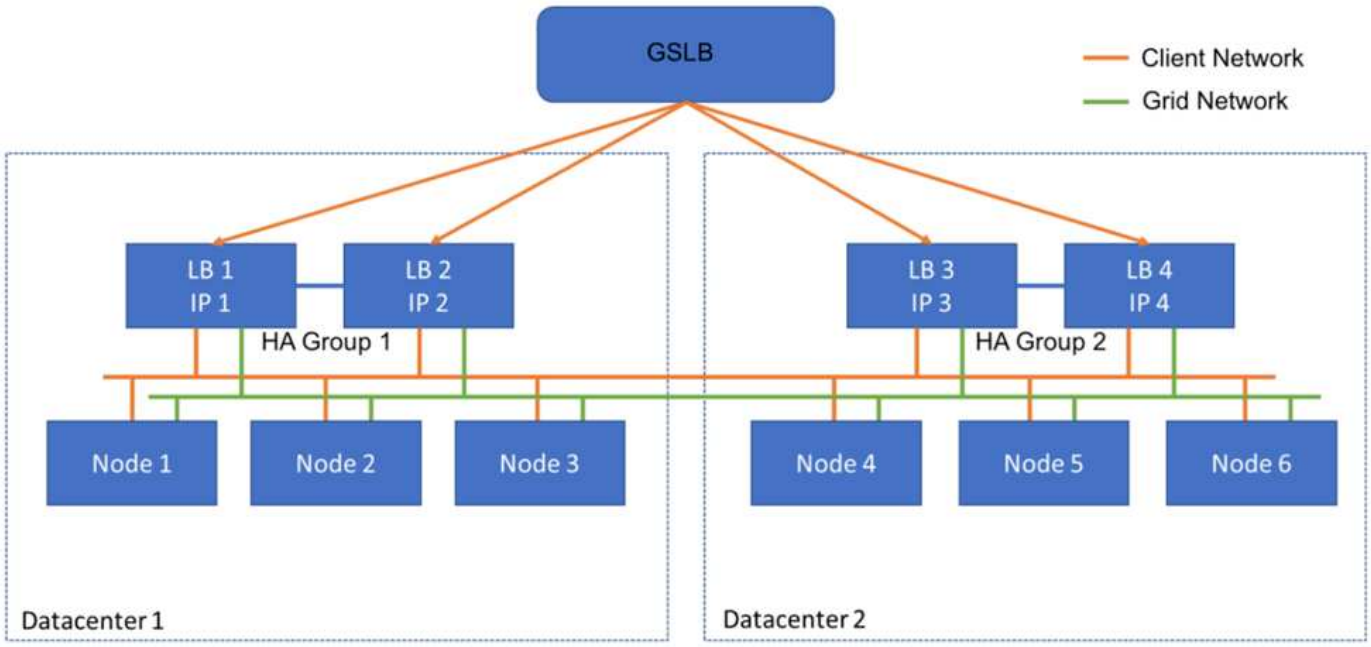
了解如何在StorageGRID中验证SSL连接。

配置负载平衡器后、您应使用OpenSSL和AWS命令行界面等工具验证连接。S3浏览器等其他应用程序可能会忽略SSL配置不当。

了解StorageGRID的全局负载平衡要求

了解StorageGRID中全局负载平衡的设计注意事项和要求。

全局负载平衡需要与DNS集成、以便在多个StorageGRID站点之间提供智能路由。此功能不在StorageGRID域中、必须由第三方解决方案(如上文讨论的负载平衡器产品)和/或DNS流量控制解决方案(如Infoblox)提供。此顶级负载平衡可提供到命名空间中最近的目标站点的智能路由、以及中断检测和重定向到命名空间中的下一个站点。典型的GSLB实施由顶级GSLB组成、其中站点池包含站点本地负载平衡器。站点负载平衡器包含本地站点存储节点的池。这可能包括用于GSLB功能的第三方负载平衡器和提供站点本地负载平衡的StorageGRID的组合、或者第三方的组合、或者前面讨论的许多第三方的组合可以同时提供GSLB和站点本地负载平衡。



TR-4645：安全功能

保护对象存储中的**StorageGRID**数据和元数据的安全

了解StorageGRID对象存储解决方案不可或缺的安全功能。

本文档概述了NetApp®StorageGRID®中的许多安全功能，包括数据访问、对象和元数据、管理访问和平台安全性。它已进行更新、加入了随StorageGRID 11.9.

安全性是NetApp StorageGRID对象存储解决方案不可或缺的一部分。安全性尤为重要、因为非常适合对象存储的许多类型的富内容数据在本质上也是敏感的、并受法规和合规性的约束。随着StorageGRID功能的不断发展、该软件提供了许多安全功能、这些功能对于保护组织的安全防护以及帮助组织遵守行业最佳实践至关重要。

本文概述了StorageGRID 11.9中的许多安全功能、分为五类：

- 数据访问安全功能
- 对象和元数据安全功能
- 管理安全性功能
- 平台安全功能
- 云集成

本白皮书旨在提供一个安全产品规格、其中并未详细说明如何配置系统以支持中枚举的默认未配置的安全功能。"《StorageGRID加强指南》"可在官方页面上找到 "StorageGRID 文档" 。

除了本报告中介绍的功能之外，StorageGRID还遵循 "NetApp产品安全漏洞响应和通知策略"。根据产品安全事件响应流程、对报告的漏洞进行验证和响应。

NetApp StorageGRID可为要求苛刻的企业对象存储用例提供高级安全功能。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- NetApp StorageGRID：SEC 17a-4 (f)、FIRA 4511 (c)和CFTC 1.31 (c)-(d)合规性评估 https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- StorageGRID 11．11文档页 https://docs.netapp.com/us-en/storagegrid-119/
- NetApp产品文档 https://www.netapp.com/support-and-training/documentation/

术语和首字母缩略语

本节提供了文档中所用术语的定义。

术语或首字母缩略语	定义
S3	Simple Storage Service。
客户端	一种可以通过S3协议(用于数据访问)或HTTP协议(用于管理)与StorageGRID连接的应用程序。
租户管理员	StorageGRID租户帐户的管理员
租户用户	StorageGRID租户帐户中的用户
TLS	传输层安全性
ILM	信息生命周期管理
LAN	局域网
网格管理员	StorageGRID系统的管理员
网格	StorageGRID系统
存储分段	存储在S3中的对象的容器
LDAP	轻型目录访问协议
秒	证券和交易委员会；管理交易所成员、经纪人或交易商
这是	金融行业监管机构；遵守SEC规则17a-4 (f)的格式和媒体要求
CFTC	商品期货交易委员会；管理商品期货交易
NIST	国家标准和技术研究所

数据访问安全功能

了解StorageGRID中的数据访问安全功能。

功能	功能	影响	合规性
可配置传输层安全(TLS)	TLS会为客户端与StorageGRID网关节点、存储节点或负载平衡器端点之间的通信建立握手协议。 StorageGRID支持以下TLS密码套件： • 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 支持TLS v1.2和1.3。 不再支持SSLv3、TLS v1.1及更早版本。	使客户端和StorageGRID能够相互识别和身份验证、并在保密和数据完整性的情况下进行通信。确保使用最新的TLS版本。现在、您可以在"配置/安全"设置下配置这些用户的用户	—

功能	功能	影响	合规性
可配置的服务器证书(负载平衡器端点)	网格管理员可以将负载平衡器端点配置为生成或使用服务器证书。	允许使用由其标准可信证书颁发机构(Certificate Authority、CA)签名的数字证书、对每个负载平衡器端点的网格和客户端之间的对象API操作进行身份验证。	—
可配置的服务器证书(API端点)	网格管理员可以集中配置所有StorageGRID API端点、以使用由其组织的受信任CA签名的服务器证书。	允许使用由其标准可信CA签名的数字证书对客户端和网格之间的对象API操作进行身份验证。	—
多租户	StorageGRID支持每个网格包含多个租户；每个租户都有自己的命名空间。租户提供S3协议；默认情况下、对分段/容器和对象的访问仅限于帐户中的用户。租户可以拥有一个用户(例如、一个企业部署、其中每个用户都有自己的帐户)或多个用户(例如、一个服务提供商部署、其中每个帐户都是服务提供商的一家公司和一个客户)。用户可以是本地用户、也可以是联合用户；联合用户由Active Directory或轻型目录访问协议(Lightweight-Directory Access Protocol、LDAP)定义。StorageGRID提供了一个按租户显示的信息板、用户可在其中使用其本地或联合帐户凭据登录。用户可以根据网格管理员分配的配额访问有关租户使用情况的可视化报告、包括分段存储的数据和对象中的使用情况信息。具有管理权限的用户可以执行租户级别的系统管理任务、例如管理用户和组以及访问密钥。	允许StorageGRID管理员托管来自多个租户的数据、同时隔离租户访问、并通过将用户与外部身份提供程序(如Active Directory或LDAP)联盟来建立用户身份。	SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
访问凭据的不可否认性	每个S3操作都使用唯一的租户帐户、用户和访问密钥进行标识和记录。	允许网格管理员确定由哪些个人执行哪些API操作。	—
已禁用匿名访问	默认情况下、S3帐户禁用匿名访问。请求者必须拥有租户帐户中有效用户的有效访问凭据、才能访问帐户中的分段、容器或对象。可以使用显式IAM策略启用对S3存储分段或对象的匿名访问。	允许网格管理员禁用或控制对分段/容器和对象的匿名访问。	—

功能	功能	影响	合规性
合规性WORM	旨在满足SEC规则17a-4 (f)的要求、并经过Cohasset验证。客户可以在存储分段级别实现合规性。保留期限可以延长、但绝不能减少。 信息生命周期管理(ILM)规则强制实施最低数据保护级别。	允许具有法规数据保留要求的租户对存储的对象和对象元数据启用WORM保护。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
WORm	网格管理员可以通过启用禁用客户端修改选项来启用网格范围的WORM、此选项可防止客户端覆盖或删除所有租户帐户中的对象或对象元数据。 S3租户管理员还可以通过指定IAM策略按租户、存储分段或对象前缀启用WORM、此策略包括自定义的对象和元数据覆盖S3：PutOverwriteObject权限。	允许网格管理员和租户管理员控制对已存储对象和对象元数据的WORM保护。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
Kms主机服务器加密密钥管理	网格管理员可以在网格管理器中配置一个或多个外部密钥管理服务器(KMS)、以便为StorageGRID服务和存储设备提供加密密钥。每个KMS主机服务器或KMS主机服务器集群都使用密钥管理互操作性协议(Key Management互操作性协议、KMIP)为关联StorageGRID站点上的设备节点提供加密密钥。	实现空闲数据加密。对设备卷进行加密后、您将无法访问设备上的任何数据、除非节点可以与KMS主机服务器进行通信。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
自动故障转移	StorageGRID提供内置冗余和自动故障转移功能。即使从磁盘或节点到整个站点发生多个故障、也可以继续访问租户帐户、分段和对象。StorageGRID具有资源感知能力、可自动将请求重定向到可用节点和数据位置。StorageGRID站点甚至可以在隔离模式下运行；如果WAN中断使站点与系统的其余部分断开连接、则可以使用本地资源继续执行读取和写入操作、并在WAN还原后自动恢复复制。	支持网格管理员解决正常运行时间、SLA和其他合同义务问题、并实施业务连续性计划。	—

功能	功能	影响	合规性
特定于**S3**的数据访问安全功能	AWS签名版本2和版本4	对API请求签名可为S3 API操作提供身份验证。Amazon支持签名版本2和版本4的两个版本。签名过程可验证请求者的身份、保护传输中的数据并防止潜在的重放攻击。	符合AWS对签名版本4的建议、并支持与签名版本2中的旧应用程序向后兼容。
—	S3 对象锁定	StorageGRID中的S3对象锁定功能是一种对象保护解决方案、相当于Amazon S3中的S3对象锁定。	允许租户在启用S3对象锁定的情况下创建分段、以符合要求将某些对象保留固定时间或无限期的法规要求。
SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)	S3凭据的安全存储	S3访问密钥以受密码哈希功能(SHA-2)保护的格式存储。	通过组合使用密钥长度(10^{31}随机生成的数字)和密码哈希算法来安全存储访问密钥。
—	有时间限制的S3访问密钥	在为用户创建S3访问密钥时、客户可以设置访问密钥的到期日期和时间。	为网格管理员提供配置临时S3访问密钥的选项。
—	每个用户帐户具有多个访问密钥	通过StorageGRID、可以为一个用户帐户创建多个访问密钥、并使其同时处于活动状态。由于每个API操作都使用租户用户帐户和访问密钥进行记录、因此、即使多个密钥处于活动状态、也会保留不可否认性。	使客户端能够无干扰地轮换访问密钥、并允许每个客户端都有自己的密钥、从而避免在客户端之间共享密钥。
—	S3 IAM访问策略	StorageGRID支持S3 IAM策略、支持网格管理员按租户、分段或对象前缀指定精细访问控制。StorageGRID还支持IAM策略条件和变量、从而支持更动态的访问控制策略。	允许网格管理员按用户组为整个租户指定访问控制；还允许租户用户为自己的分段和对象指定访问控制。
—	使用StorageGRID托管密钥(SSE)进行服务器端加密	StorageGRID支持SSE、可使用StorageGRID管理的加密密钥对空闲数据进行多租户保护。	允许租户对对象进行加密。要写入和检索这些对象、需要使用加密密钥。

功能	功能	影响	合规性
SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)	使用客户提供的加密密钥(SSE-C)进行服务器端加密	StorageGRID支持SSE-C、可使用客户端管理的加密密钥对空闲数据进行多租户保护。 虽然StorageGRID负责管理所有对象加密和解密操作、但使用SSE-C时、客户端必须自行管理加密密钥。	使客户端能够使用其控制的密钥对对象进行加密。要写入和检索这些对象、需要使用加密密钥。

对象和元数据安全性

了解StorageGRID中的对象和元数据安全功能。

功能	功能	影响	合规性
高级加密标准(Advanced Encryption Standard、AES)服务器端对象加密	StorageGRID可为对象提供基于AES 128和AES 256的服务器端加密。网格管理员可以启用加密作为全局默认设置。StorageGRID还支持S3 x-AMZ-server-side加密标头、以允许按对象启用或禁用加密。启用后、对象在存储时或在网格节点之间传输时会进行加密。	有助于保护对象的存储和传输、不受底层存储硬件的限制。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
内置密钥管理	启用加密后、每个对象都会使用随机生成的唯一对称密钥进行加密、该密钥存储在StorageGRID中、无需外部访问。	无需外部密钥管理即可启用对象加密。	
符合联邦信息处理标准(Federal Information Processing Standard、FIPS) 140-2的加密磁盘	SG5812、SG5860、SG6160和SGF6024 StorageGRID设备可提供符合FIPS 140-2的加密磁盘选项。磁盘的加密密钥可以选择由外部KMIP服务器管理。	支持安全存储系统数据、元数据和对象。此外、还提供基于StorageGRID软件的对象加密功能、可保护对象的存储和传输安全。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
后台完整性扫描和自我修复	StorageGRID在对象和子对象级别使用哈希、校验和和和循环冗余校验(CrC)的互斥机制、以防止在对象存储和传输过程中出现数据不一致、篡改或修改。StorageGRID会自动检测损坏和被篡改的对象并进行替换、同时隔离更改后的数据并向管理员发出警报。	支持网格管理员满足SLA、法规和其他有关数据持久性的义务。帮助客户检测尝试加密、篡改或修改数据的勒索软件或病毒。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)

功能	功能	影响	合规性
基于策略的对象放置和保留	StorageGRID支持网格管理员配置ILM规则、用于指定对象保留、放置、保护、过渡和到期时间。网格管理员可以将StorageGRID配置为按对象的元数据筛选对象、并在各种粒度级别应用规则、包括网格范围、租户、存储分段、密钥前缀、和用户定义的元数据键值对。StorageGRID有助于确保在对象的整个生命周期内根据ILM规则存储对象、除非客户端明确删除这些对象。	有助于强制实施数据放置、保护和保留。帮助客户在持久性、可用性和性能方面实现SLA。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
后台元数据扫描	StorageGRID会定期扫描后台的对象元数据、以应用ILM指定的对象数据放置或保护更改。	帮助发现损坏的对象。	
可调一致性	租户可以在存储分段级别选择一致性级别、以确保多站点连接等资源可用。	仅当提供所需数量的可用站点或资源时、才可选择向网格提交写入。	

管理安全性功能

了解StorageGRID中的管理安全功能。

功能	功能	影响	合规性
服务器证书(网格管理接口)	网格管理员可以将网格管理界面配置为使用由其组织的受信任CA签名的服务器证书。	允许使用由其标准可信CA签名的数字证书对管理客户端和网格之间的管理UI和API访问进行身份验证。	—
管理用户身份验证	管理用户使用用户名和密码进行身份验证。管理用户和组可以是本地用户或联合用户、也可以是从客户的Active Directory或LDAP导入的用户和组。本地帐户密码以bcrypt保护的格式存储；命令行密码以SHA-2保护的格式存储。	对管理UI和API的管理访问进行身份验证。	—

功能	功能	影响	合规性
SAML支持	StorageGRID支持使用安全断言标记语言2.0 (SAML 2.0)标准的单点登录(SSO)。启用 SSO 后，所有用户都必须经过外部身份提供程序的身份验证，然后才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。本地用户无法登录到 StorageGRID 。	为网格和租户管理员提供更高级别的安全性、例如SSO和多因素身份验证(MFA)。	NIST SP800-63
精细的权限控制	网格管理员可以为角色分配权限、并为管理用户组分配角色、这样可以使用管理UI和API强制执行允许管理客户端执行的任务。	允许网格管理员管理管理员用户和组的访问控制。	—
分布式审核日志记录	StorageGRID提供内置的分布式审核日志记录基础架构、可扩展到多达16个站点上的数百个节点。StorageGRID软件节点会生成审核消息、这些消息通过冗余审核中继系统传输、并最终捕获到一个或多个审核日志存储库中。审核消息可捕获对象级别粒度的事件、例如客户端启动的S3 API操作、ILM对象生命周期事件、后台对象运行状况检查以及通过管理UI或API进行的配置更改。 可以通过CIFS或NFS从管理节点导出审核日志、从而可以使用Splunk和PEK等工具挖掘审核消息。审核消息有四种类型： • 系统审核消息 • 对象存储审核消息 • HTTP协议审核消息 • 管理审核消息	为网格管理员提供经验证的可扩展审计服务、使他们能够为各种目标挖掘审计数据。此类目标包括故障排除、审核SLA性能、客户端数据访问API操作以及管理配置更改。	—
系统审核	系统审核消息可捕获与系统相关的事件、例如网格节点状态、损坏对象检测、根据ILM规则在所有指定位置提交的对象以及系统范围维护任务(网格任务)的进度。	帮助客户解决系统问题、并提供根据其SLA存储对象的证据。SLA通过StorageGRID ILM规则实施、并受到完整性保护。	—

功能	功能	影响	合规性
对象存储审核	对象存储审核消息可捕获对象API事务和生命周期相关事件。这些事件包括对象存储和检索、网格节点到网格节点的传输以及验证。	帮助客户审核系统中的数据进度以及是否正在交付SLA (指定为StorageGRID ILM)。	—
HTTP协议审核	HTTP协议审核消息可捕获与客户端应用程序和StorageGRID节点相关的HTTP协议交互。此外，客户还可以捕获特定的HTTP请求标头(例如X-Forwarded-for和用户元数据[x-AMZ-meta-*])以进行审核。	帮助客户审核客户端和StorageGRID之间的数据访问API操作、并跟踪单个用户帐户和访问密钥的操作。客户还可以将用户元数据记录到审核中、并使用日志挖掘工具(例如Splunk或ETK)搜索对象元数据。	—
管理审计	管理审核消息会记录管理员用户对管理UI (网格管理接口)或API的请求。对于 API ，并非 GET 或 HEAD 请求的每个请求都会记录一个响应，其中包含 API 的用户名， IP 和请求类型。	帮助网格管理员建立系统配置更改记录、记录由哪个用户在哪个时间从哪个源IP进行更改、以及从哪个目标IP进行更改。	—
TLS 1.3支持管理UI和API访问	TLS会为管理客户端与StorageGRID管理节点之间的通信建立握手协议。	使管理客户端和StorageGRID能够相互识别和身份验证、并在机密性和数据完整性的情况下进行通信。	—
SNMPv3、用于StorageGRID监控	SNMPv3通过提供强身份验证和数据加密来保护隐私、从而提供安全性。对于v3、协议数据单元将使用CBC-DES作为加密协议进行加密。 发送协议数据单元的用户身份验证由HMAC-SHA或HMAC-MD5身份验证协议提供。 SNMPv2和v1仍受支持。	通过在管理节点上启用SNMP代理、帮助网格管理员监控StorageGRID系统。	—
Prometheus指标导出的客户端证书	网格管理员可以上传或生成客户端证书、这些证书可用于提供对StorageGRID Prometheus数据库的安全、经过身份验证的访问。	网格管理员可以使用客户端证书通过Grafana等应用程序在外部监控StorageGRID。	—

平台安全功能

了解StorageGRID中的平台安全功能。

功能	功能	影响	合规性
内部公共密钥基础架构(PKI)、节点证书和TLS	StorageGRID使用内部PKI和节点证书对节点间通信进行身份验证和加密。节点间通信受TLS保护。	有助于保护LAN或WAN上的系统流量、尤其是在多站点部署中。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
节点防火墙	StorageGRID会自动配置IP表和防火墙规则、以控制传入和传出网络流量、并关闭未使用的端口。	帮助保护StorageGRID系统、数据和元数据免受未经请求的网络流量的影响。	—
OS强化	StorageGRID物理设备和虚拟节点的基本操作系统得到了强化；不相关的软件包将被删除。	有助于最大限度地减少潜在攻击面。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
定期更新平台和软件	StorageGRID提供常规软件版本、其中包括操作系统、应用程序二进制文件和软件更新。	有助于使用最新的软件和应用程序二进制文件保持StorageGRID系统最新。	—
已禁用通过安全Shell (SSH)进行root登录	已在所有StorageGRID节点上禁用通过SSH进行root登录。SSH访问使用证书身份验证。	帮助客户防止root登录的潜在远程密码破解。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
自动时间同步	StorageGRID会自动将每个节点的系统时钟与多个外部时间网络时间协议(NTP)服务器同步。至少需要四个Stratum 3或更高版本的NTP服务器。	确保所有节点的时间参考相同。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
为客户端、管理和内部网格流量分隔网络	StorageGRID软件节点和硬件设备支持多个虚拟和物理网络接口、因此客户可以通过不同的网络隔离客户端、管理和内部网格流量。	允许网格管理员隔离内部和外部网络流量、并通过具有不同SLA的网络交付流量。	—
多个虚拟LAN (VLAN)接口	StorageGRID支持在StorageGRID客户端和网格网络上配置VLAN接口。	网格管理员可以对应用程序流量进行分区和隔离、以提高安全性、灵活性和性能。	
不可信客户端网络	不可信客户端网络接口仅接受已显式配置为负载平衡器端点的端口上的入站连接。	确保暴露给不可信网络的接口安全。	—
可配置防火墙	管理管理管理、网格和客户端网络的开放和关闭端口。	允许网格管理员控制端口访问、并管理经过批准的设备对端口的访问。	

功能	功能	影响	合规性
增强的SSH行为	将节点升级到StorageGRID 11.5时、系统会生成新的SSH主机证书和主机密钥。	增强中间人攻击防护。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
节点加密	作为新的KMS主机服务器加密功能的一部分、StorageGRID设备安装程序会添加一个新的节点加密设置。	必须在设备安装的硬件配置阶段启用此设置。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)

云集成

了解StorageGRID如何与云服务集成。

功能	功能	影响
基于通知的病毒扫描	StorageGRID平台服务支持事件通知。事件通知可与外部云计算服务结合使用、用于对数据触发病毒扫描工作流。	允许租户管理员使用外部云计算服务触发数据病毒扫描。

TR-4921：勒索软件防御

保护**StorageGRID S3**对象免遭勒索软件的攻击

了解勒索软件攻击以及如何利用StorageGRID安全最佳实践保护数据。

勒索软件攻击呈上升趋势。本文档就如何保护StorageGRID上的对象数据提供了一些建议。

如今、勒索软件已成为数据中心面临的一个始终存在的威胁。勒索软件旨在对数据进行加密、使依赖该数据的用户和应用程序无法使用该数据。保护从强化网络和可靠用户安全实践的常规防御开始、我们需要遵循数据访问安全实践。

勒索软件是当今最大的安全威胁之一。NetApp StorageGRID团队正在与我们的客户合作、以防范这些威胁。通过使用对象锁定和版本控制、您可以防止不必要的更改并从恶意攻击中恢复。数据安全是一项多层风险、您的对象存储只是数据中心的一部分。

StorageGRID最佳实践

对于StorageGRID、安全最佳实践应包括使用HTTPS和签名证书进行管理和对象访问。为应用程序和个人创建专用用户帐户、不要使用租户root帐户进行应用程序访问或用户数据访问。换言之、遵循最小特权原则。使用具有定义的身份和访问管理(IAM)策略的安全组来管理用户权限以及特定于应用程序和用户的访问帐户。实施这些措施后、您仍然必须确保数据受到保护。对于简单存储服务(S3)、在修改对象以对其进行加密时、可以通过覆盖原始对象来实现。

辩护方法

S3 API中的主要勒索软件保护机制是实施对象锁定。并非所有应用程序都与对象锁定兼容、因此本报告中介绍

了另外两个保护对象的选项：复制到启用了版本控制的另一个存储分段以及使用IAM策略进行版本控制。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- NetApp StorageGRID文档中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID支持 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp产品文档 https://www.netapp.com/support-and-training/documentation/

使用对象锁定进行勒索软件防护

了解StorageGRID中的对象锁定如何提供WORM模型来防止数据删除或覆盖、以及如何满足法规要求。

对象锁定提供了WORM模型、可防止删除或覆盖对象。StorageGRID实施对象锁定 "评估的协资产" 有助于满足法规要求、支持合法保留、合规模式和对象保留监管模式以及默认分段保留策略。您必须在创建分段和版本控制过程中启用对象锁定。对象的特定版本被锁定、如果未定义版本ID、则保留将放置在对象的当前版本上。如果当前版本配置了保留、并且尝试删除、修改或覆盖对象、则会创建一个新版本、其中包含删除标记、或者对象的新修订版作为当前版本。 锁定的版本将保留为非当前版本。对于尚不兼容的应用程序、您仍可以使用对象锁定以及存储分段上的默认保留配置。定义配置后、此操作会对放入存储分段的每个新对象应用对象保留。只要将应用程序配置为在保留时间过去之前不删除或覆盖对象、此操作就有效。

以下是使用对象锁定API的几个示例：

对象锁定合法保留是应用于对象的简单开/关状态。

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

设置合法保留状态成功后不会返回任何值、因此可以通过GET操作进行验证。

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

要关闭合法保留、请应用关闭状态。

```
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"
    }
}
```

设置对象保留时、会使用保留到时间戳。

```
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
```

同样、成功时也不返回任何值、因此您可以通过GET调用来验证保留状态。

```
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"
    }
```

为启用了对象锁定的存储分段设置默认保留期限时、保留期限以天和年为单位。

```
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
```

与大多数操作一样、成功后不会返回任何响应、因此、我们可以执行GET以验证配置。

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

接下来、您可以在应用保留配置的情况下将对象放入存储分段中。

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

Put操作确实会返回响应。

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

在保留对象上、上例中为分段设置的保留持续时间将转换为对象上的保留时间戳。

```
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"
    }
}
```

使用具有版本控制的复制存储分段进行勒索软件防护

了解如何使用StorageGRID CloudMirror将对象复制到二级存储分段。

并非所有应用程序和工作负载都能与对象锁定兼容。另一种方法是、将对象复制到同一网格中的二级存储分段(最好是访问受限的不同租户)、或者使用StorageGRID平台服务CloudMirror的任何其他S3端点。

StorageGRID CloudMirror是StorageGRID的一个组件、可以配置为在将某个存储分段的对象移入源存储分段时将其复制到定义的目标、而不会复制删除。由于CloudMirror是StorageGRID的一个集成组件、因此不能关闭它、也不能被基于S3 API的攻击所操纵。您可以在启用版本控制的情况下配置此复制分段。在这种情况下、您

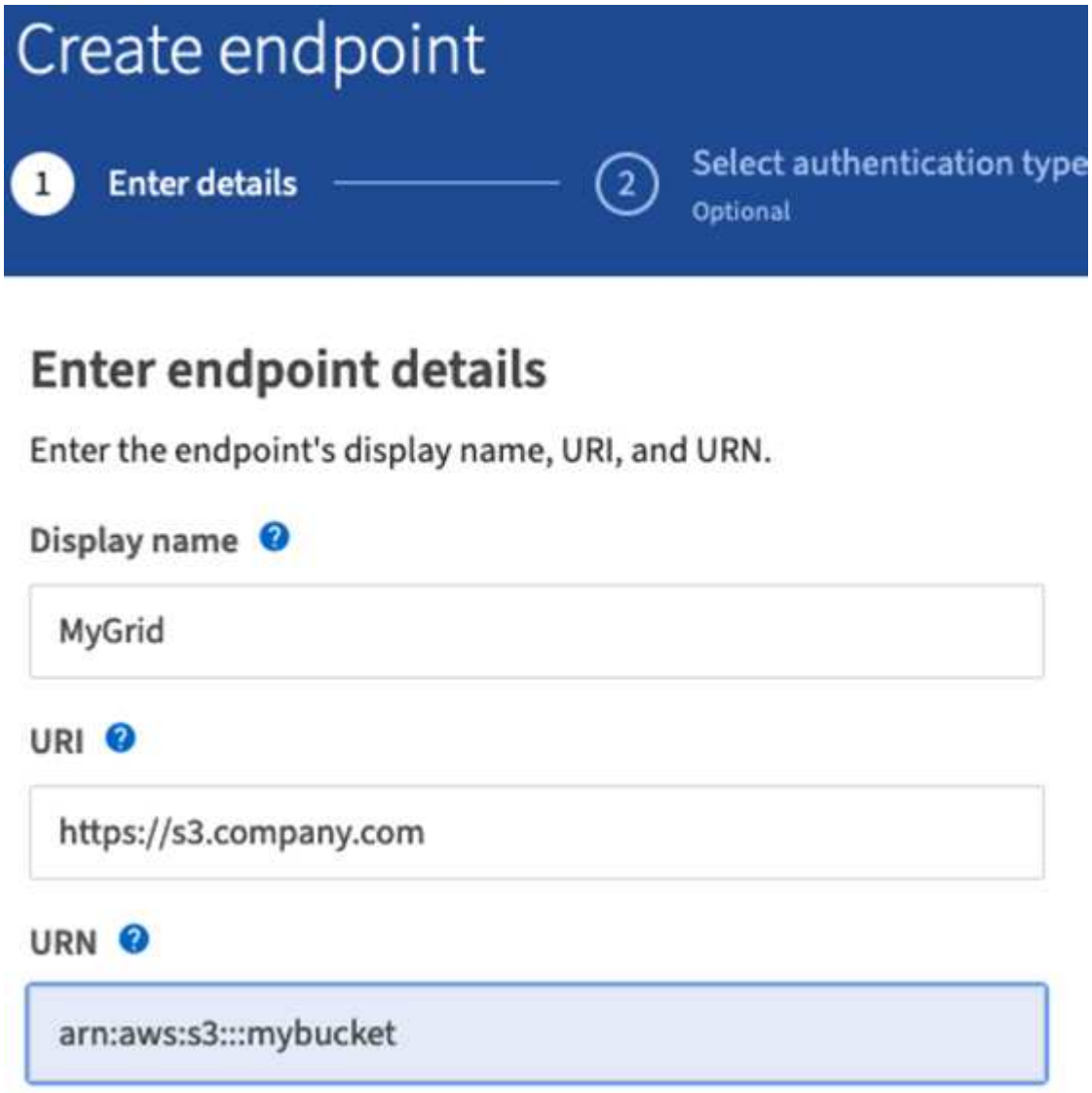
需要对复制的存储分段的旧版本进行一些可安全丢弃的自动清理。为此、您可以使用StorageGRID ILM策略引擎。创建规则、根据非当前时间管理对象放置、持续数天、足以识别攻击并从攻击中恢复。

这种方法的一个缺点是、它会通过保留存储分段的完整第二个副本以及多个版本的对象一段时间来消耗更多存储。此外、必须从复制的存储分段中手动删除主存储分段中特意删除的对象。产品之外还有其他复制选项、例如NetApp CloudSync、可以为类似的解决方案复制删除。二级存储分段启用了版本控制而未启用对象锁定的另一个缺点是、存在许多特权帐户、这些帐户可能会导致二级位置损坏。其优势在于、它应该是该端点或租户存储分段的唯一帐户、而这种损害可能不包括对主位置上的帐户的访问、反之亦然。

创建源分段和目标分段并为目标配置版本控制后、您可以按如下所示配置和启用复制：

步骤

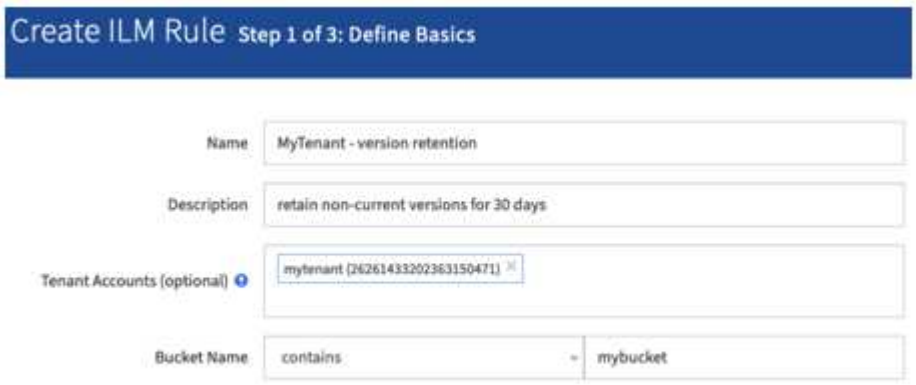
1. 要配置CloudMirror、请为S3目标创建一个平台服务端点。

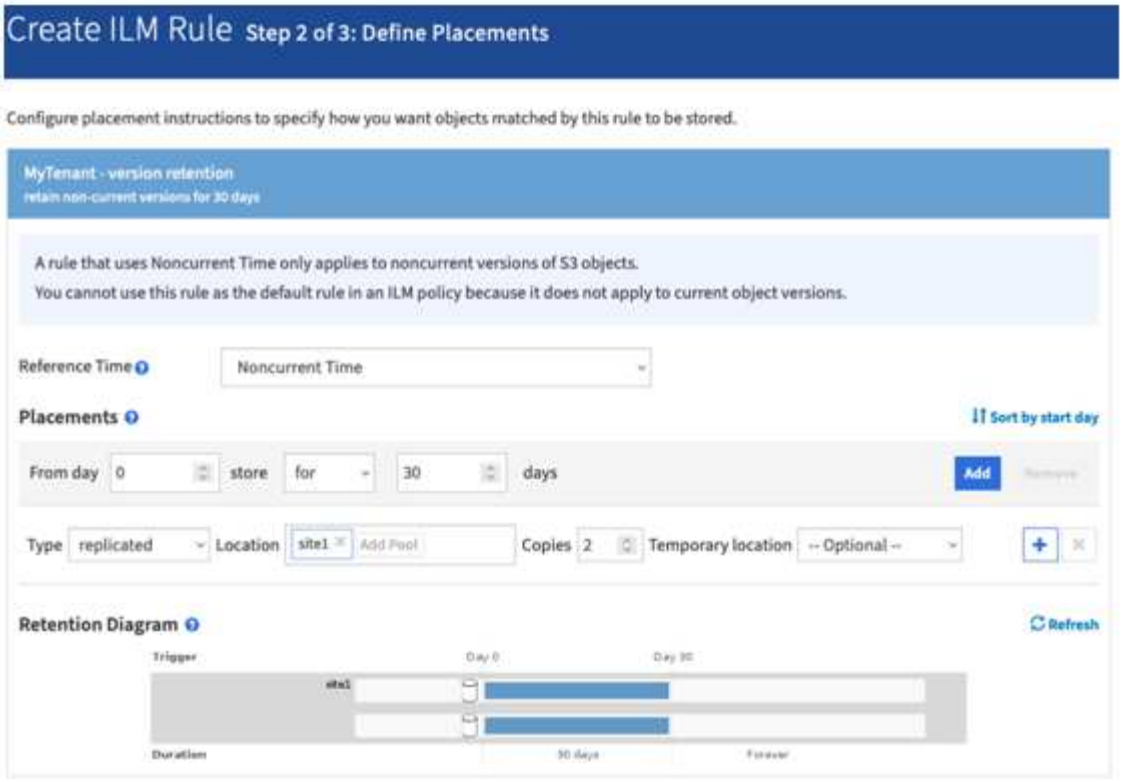


2. 在源存储分段上、配置复制以使用配置的端点。

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

3. 创建ILM规则以管理存储放置和版本存储持续时间管理。在此示例中、配置了要存储的对象的非最新版本。





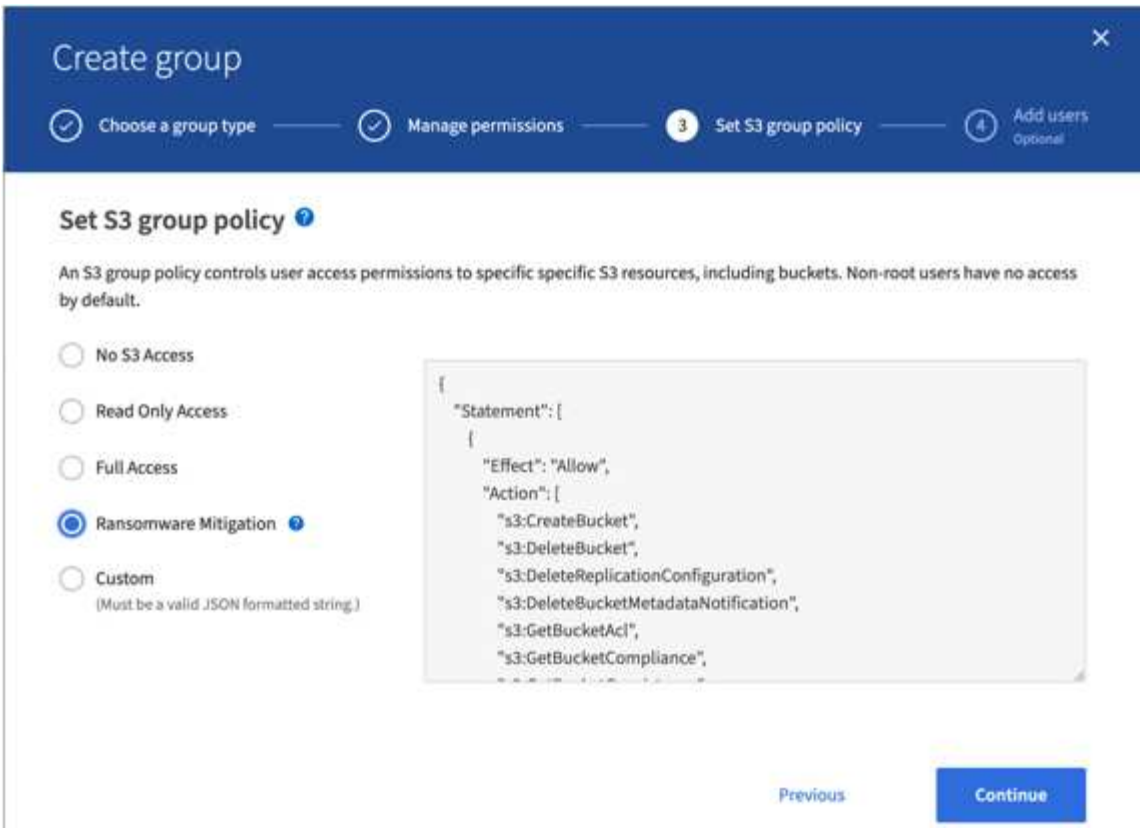
站点1中有两个副本、保留30天。此外、您还可以根据在ILM规则中使用加载时间作为参考时间来为当前版本的对象配置规则、以匹配源存储分段存储持续时间。可以对对象版本的存储放置进行卷或复制。

使用版本控制和保护性**IAM**策略进行勒索软件防御

了解如何通过在StorageGRID中对存储分段启用版本控制并对用户安全组实施IAM策略来保护您的数据。

在不使用对象锁定或复制的情况下保护数据的一种方法是、在存储分段上启用版本控制、并在用户安全组上实施IAM策略、以限制用户管理对象版本的能力。在发生攻击时、系统会创建新的错误数据版本作为当前版本、而最新的非最新版本是安全清理数据。为获得数据访问权限而泄露的帐户无权删除或以其他方式更改用于保护数据以供日后还原操作的非最新版本。与上一种情形一样、ILM规则可在您选择的持续时间内管理非最新版本的保留。缺点是、仍然可能存在针对恶意攻击者攻击的特权帐户、但必须为所有应用程序服务帐户和用户配置限制性更强的访问。限制性组策略必须明确允许您希望用户或应用程序能够执行的每个操作、并明确拒绝您不希望用户或应用程序能够执行的任何操作。NetApp建议不要使用通配符allow、因为将来可能会引入新的操作、您需要控制是允许还是拒绝该操作。对于此解决方案、拒绝列表必须包括DeleteObjectVersion、PutBucketPolicy、DeleteBucketPolicy、PutLifecycleConfiguration和PutketVersioning、以防止用户或编程更改分段和对象版本的版本控制配置。

在StorageGRID 11.7中、引入了一个新的S3组策略选项"Ransmans要 缓解"、以便于实施此解决方案。在租户中创建用户组时、在选择组权限后、您可以看到此新的可选策略。



下面是组策略的内容、其中包括显式允许的大多数可用操作以及所需的最小拒绝值。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
```

```
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
```

```
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

TR-4765：《监控StorageGRID》

StorageGRID监控简介

了解如何使用外部应用程序(例如Splunk)监控StorageGRID系统。

通过有效监控NetApp StorageGRID基于对象的存储、管理员可以快速响应紧急问题、并主动添加资源来处理不断增长的工作负载。本报告提供了有关如何监控关键指标以及如何利用外部监控应用程序的一般性指导。本文档旨在补充现有的"监控和故障排除"指南。

NetApp StorageGRID部署通常由多个站点和多个节点组成、这些站点和节点用于创建分布式容错对象存储系统。在StorageGRID等分布式弹性存储系统中、出现错误情况是正常的、而网格仍正常运行。作为管理员、您面临的挑战是、了解错误条件(例如节点关闭)出现问题时应立即解决的阈值、以及应分析的信息。通过分析StorageGRID提供的数据、您可以了解自己的工作负载并做出明智的决策、例如何时添加更多资源。

StorageGRID提供了深入探讨监控主题的出色文档。本报告假设您熟悉StorageGRID、并且已阅读有关它的文档。我们不会重复这些信息、而是参阅本指南中的产品文档。StorageGRID产品文档以PDF格式在线提供。

本文档旨在对产品文档进行补充、并讨论如何使用外部应用程序(例如Splunk)监控StorageGRID系统。

数据源

要成功监控NetApp StorageGRID、请务必了解从何处收集有关StorageGRID系统运行状况和操作的数据。

- *Web UI和信息板。*StorageGRID网格管理器提供了一个顶级视图、可显示管理员在逻辑演示文稿中需要查看的信息。作为管理员、您还可以深入了解服务级别信息、以便进行故障排除和收集日志。
- *审核日志。*StorageGRID会保留有关放置、获取和删除等租户操作的精细审核日志。您还可以跟踪对象从数据管理规则的加热到应用的整个生命周期。
- *Metrics API.*StorageGRID GMI的底层是开放式API、因为UI是API驱动的。通过这种方法、您可以使用外部监控和分析工具提取数据。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

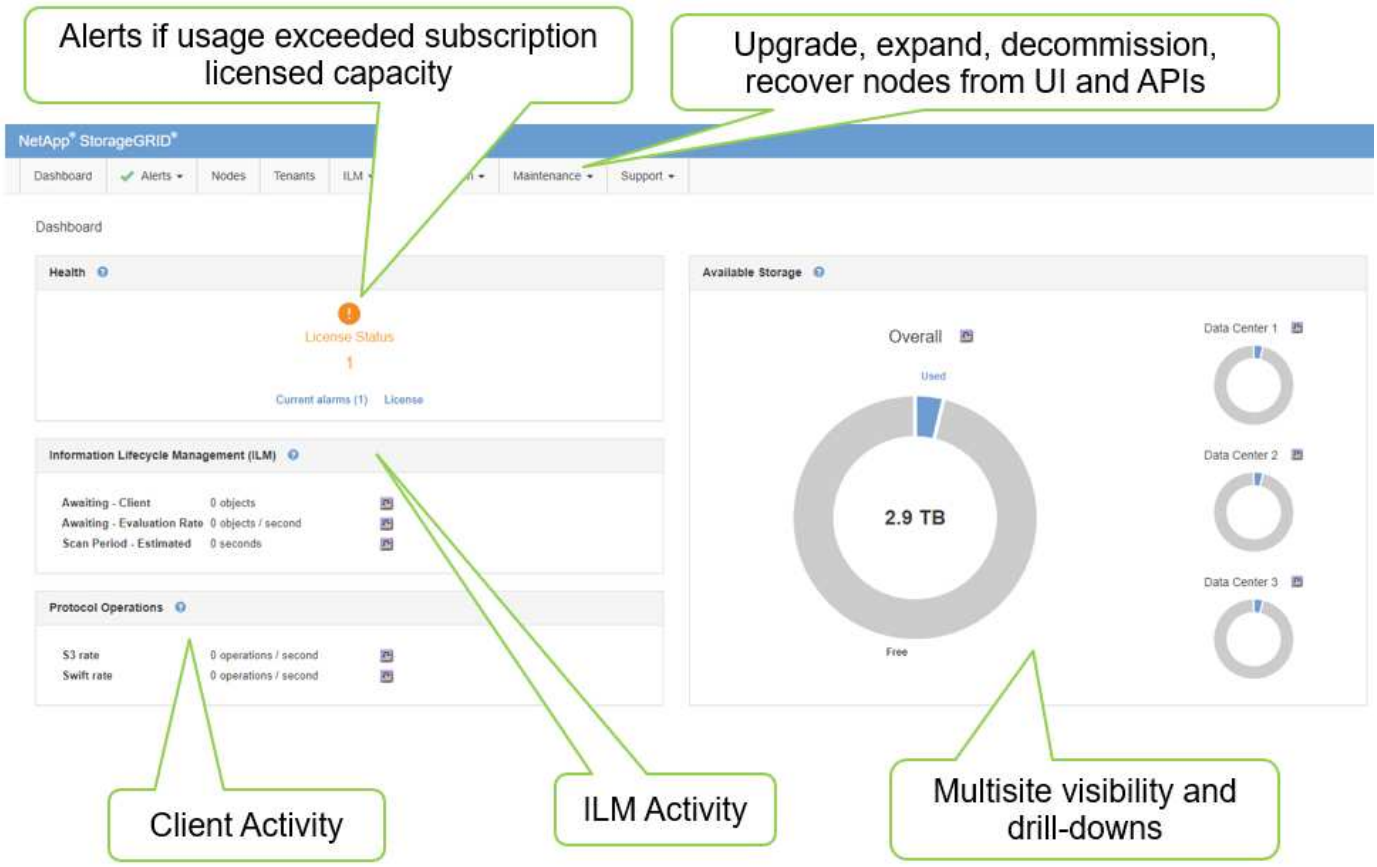
- NetApp StorageGRID文档中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID支持 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp产品文档 https://www.netapp.com/support-and-training/documentation/

- 适用于Splunk的NetApp StorageGRID应用程序 https://splunkbase.splunk.com/app/3898/#/details

使用GMI信息板监控StorageGRID

StorageGRID网格管理界面(GMI)信息板提供了StorageGRID基础架构的集中视图、可用于监控整个网格的运行状况、性能和容量。

使用GMI信息板检查网格的每个核心组件。



您应定期监控的信息

本技术报告的上一版本列出了要定期检查的指标与趋势。该信息现在包含在中 "监控和故障排除指南"。

监控存储

本技术报告的先前版本列出了监控重要指标的位置、例如对象存储空间、元数据空间、网络资源等。该信息现在包含在中 "监控和故障排除指南"。

使用警报监控StorageGRID

了解如何使用StorageGRID中的警报系统监控问题、管理自定义警报以及使用SNMP或电子邮件扩展警报通知。

警报提供了重要信息、可用于监控StorageGRID系统中的各种事件和状况。

警报系统是用于监控StorageGRID系统中可能发生的任何问题的主要工具。警报系统侧重于系统中可操作的问题、并提供一个易于使用的界面。

我们提供了各种默认警报规则、旨在帮助您监控系统并对其进行故障排除。您可以通过创建自定义警报、编辑或禁用默认警报以及静音警报通知来进一步管理警报。

警报也可通过SNMP或电子邮件通知进行扩展。

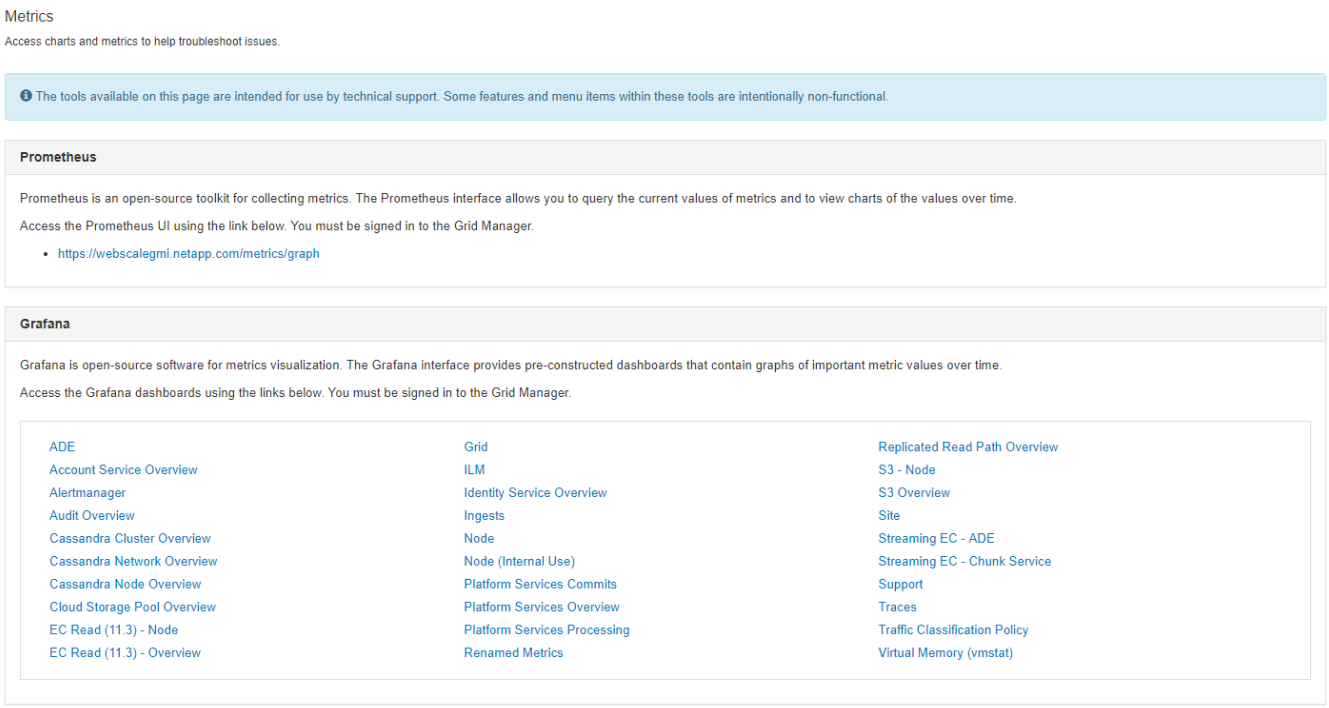
有关警报的详细信息、请参见在线提供的PDF格式的 "产品文档" 。

StorageGRID中的高级监控

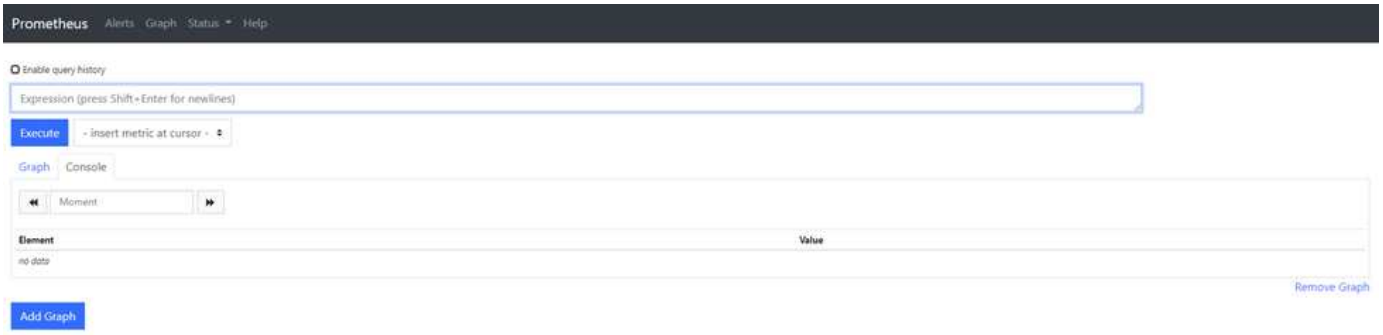
了解如何访问和导出指标以帮助解决问题。

通过Prometheus查询查看指标API

Prometheus是一款用于收集指标的开源软件。要通过GMI访问StorageGRID的嵌入式ProMetheus、请转到菜单：Support[Metrics]。



或者、您也可以直接导航到该链接。

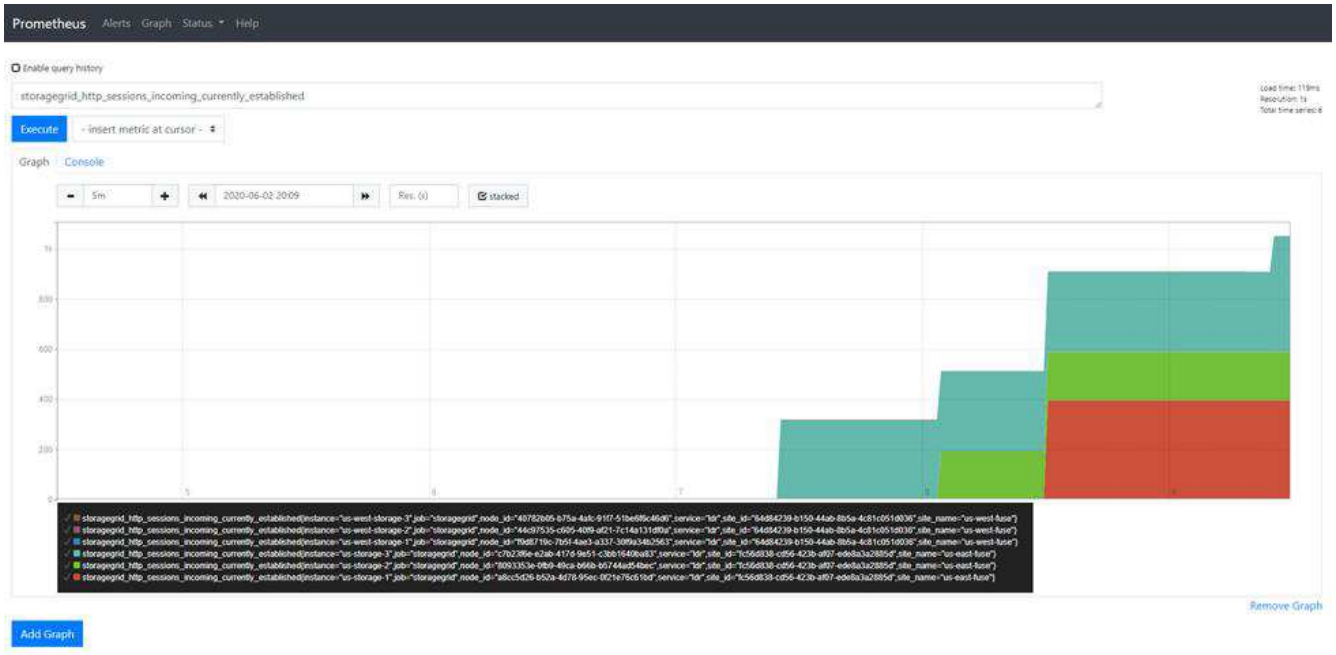


通过此视图、您可以访问Prometheus界面。您可以从此处搜索可用指标、甚至可以尝试查询。

要进行Prometheus URL查询、请按照以下步骤操作：

步骤

1. 在查询文本框中开始键入。键入时、将列出指标。对于我们而言、只有以StorageGRID和Node开头的指标才很重要。
2. 要查看每个节点的HTTP会话数，请键入 `storagegrid_http` ，然后选择 `storagegrid_http_sessions_incoming_currently_established`。单击Execute、并以图形或控制台格式显示信息。



通过此URL构建的查询和图表不会持久保留。复杂查询会占用管理节点上的资源。NetApp建议您使用此视图来浏览可用指标。

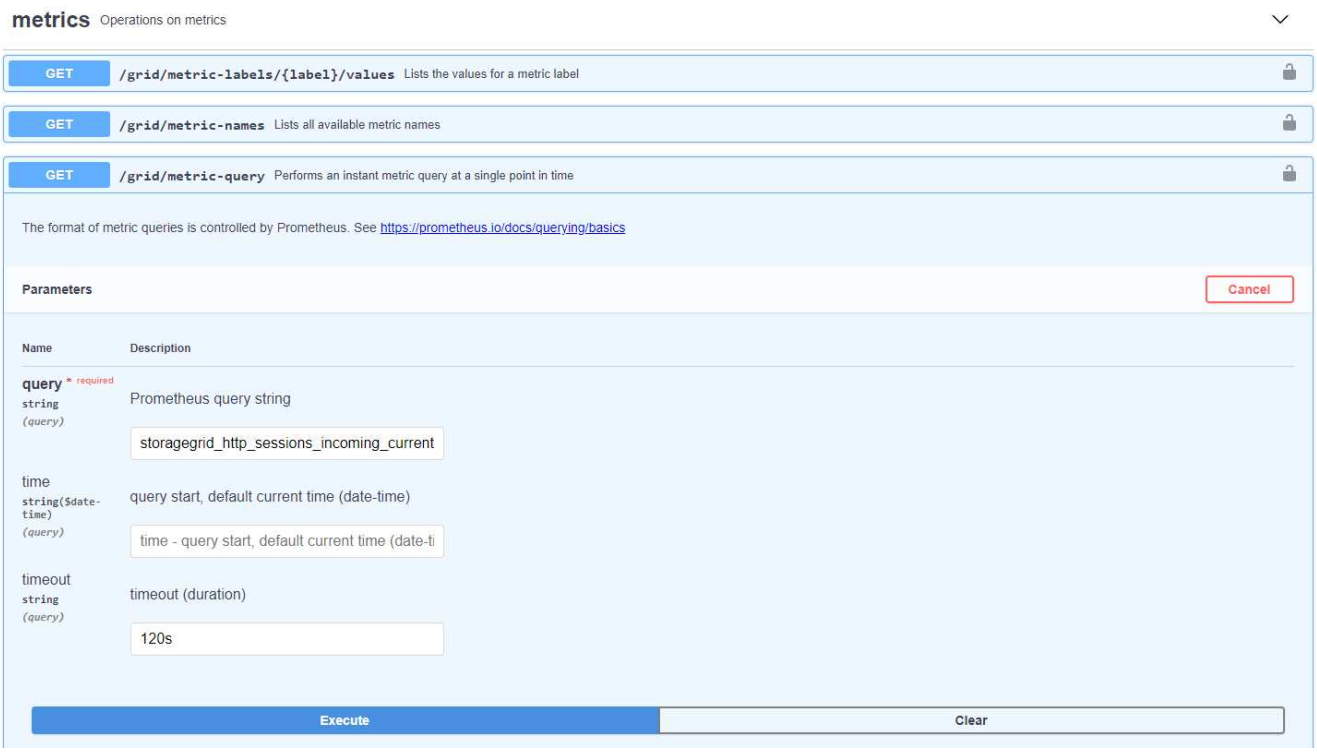
建议不要直接连接到Prometheus实例、因为这需要打开其他端口。建议使用安全的方法通过API访问指标。

通过**API**导出指标

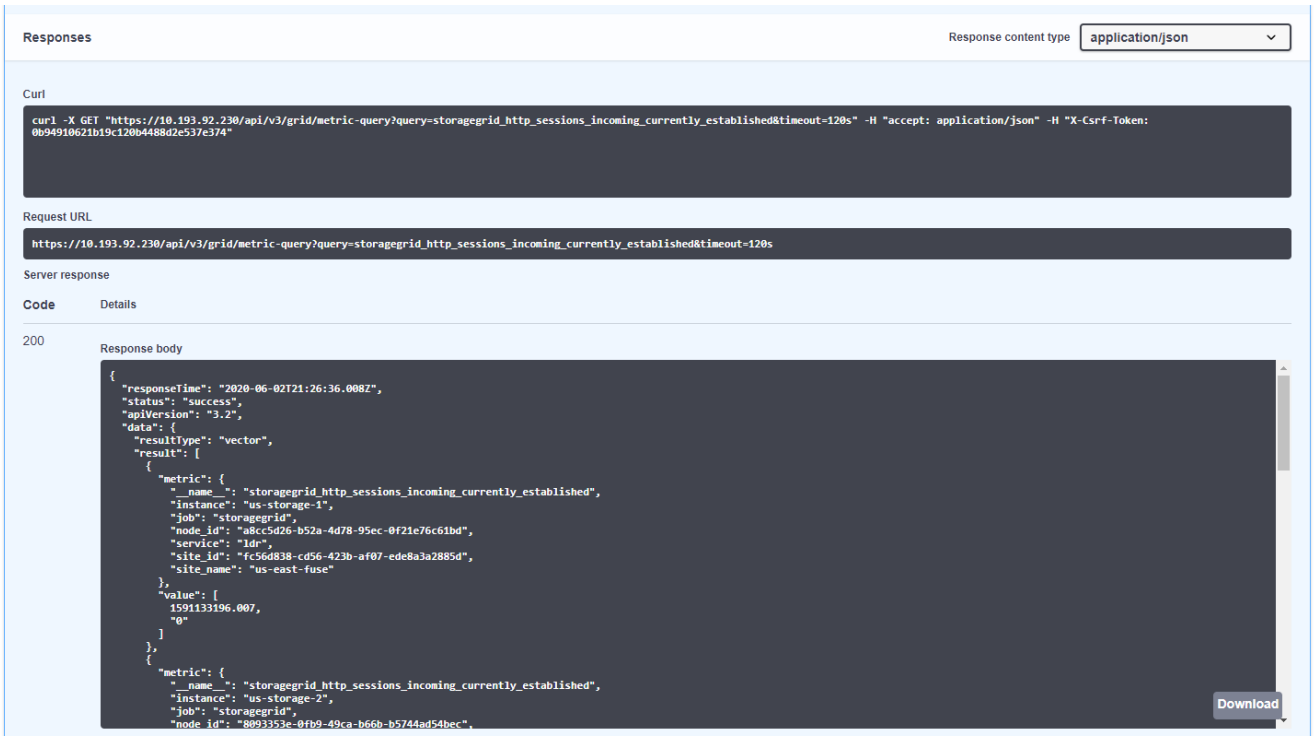
您还可以通过StorageGRID管理API访问相同的数据。

要通过API导出指标、请执行以下步骤：

1. 从GMI中、选择菜单：帮助[API文档]。
2. 向下滚动到Metrics、然后选择GET /grid / metric-query-。



此响应包含可通过Prometheus URL查询获取的相同信息。您可以再次查看当前在每个存储节点上建立的HTTP会话的数量。您还可以下载JSON格式的响应以供阅读。下图显示了Prometheus查询响应示例。



使用API的优势在于、它可以执行经过身份验证的查询

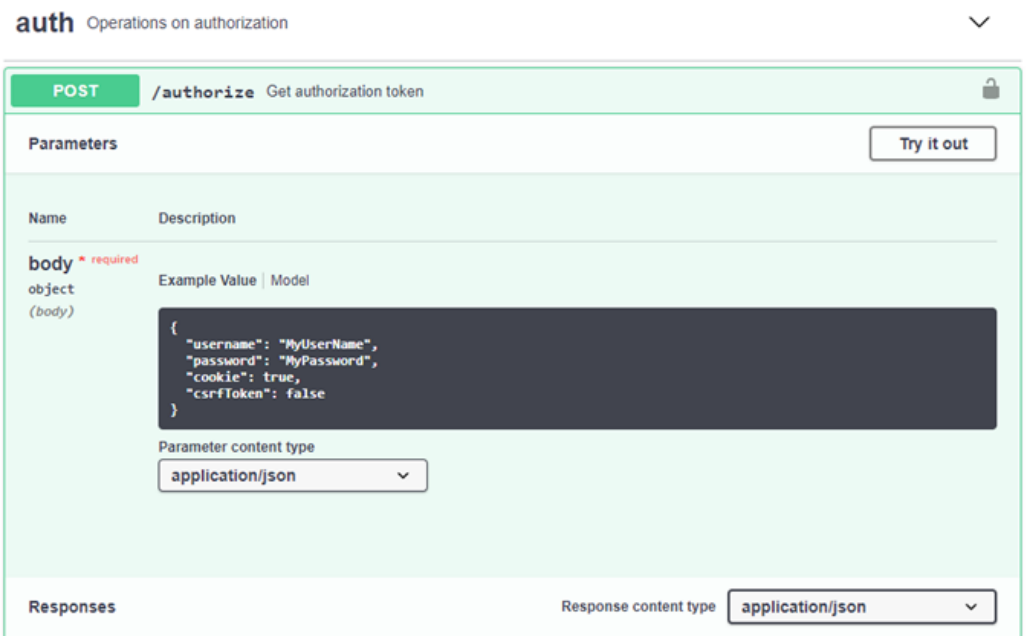
在StorageGRID中使用CURL访问指标

了解如何使用CURL通过命令行界面访问指标。

要执行此操作、您必须先获取授权令牌。要请求令牌、请执行以下步骤：

步骤

1. 从GMI中、选择菜单：帮助[API文档]。
2. 向下滚动到身份验证以查找授权操作。以下屏幕截图显示了POST方法的参数。



3. 单击试用并使用您的GMI用户名和密码编辑正文。
4. 单击“执行”。
5. 复制在卷曲部分中提供的卷曲命令、并将其粘贴到终端窗口中。此命令如下所示：

```
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
```

如果您的GMI密码包含特殊字符、请记得使用\转义特殊字符。例如，替换! 使用\!

6. 运行上述URL命令后、输出将为您提供一个授权令牌、如下例所示：

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

现在、您可以使用授权令牌字符串通过CURL访问指标。访问度量指标的过程与第节中的步骤类似"StorageGRID中的高级监控"。但是、出于演示目的、我们显示了一个示例、其中在"指标"类别中选择了GET /grid /metric-labels/ {label"} /values。

7. 例如、以下带有上述授权令牌的URL命令将在StorageGRID中列出站点名称。

```
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"
```

Curl命令将生成以下输出：

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

使用StorageGRID中的Grafana信息板查看指标

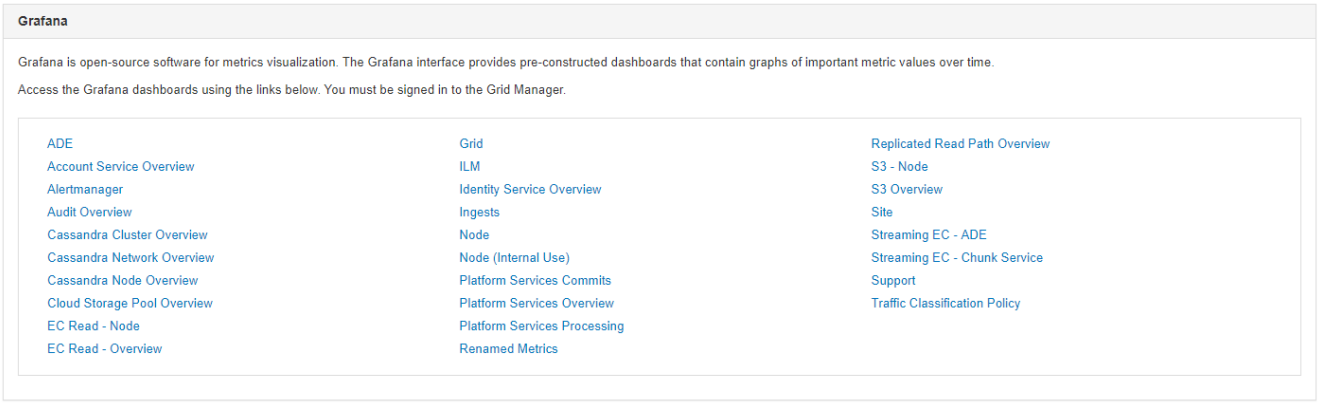
了解如何使用Grafana界面可视化和监控StorageGRID数据。

Grafana是一款用于度量可视化的开源软件。默认情况下、我们预先构建了信息板、可提供有关StorageGRID系统的有用而强大的信息。

这些预先构建的信息板不仅可用于监控、还可用于对问题进行故障排除。有些供技术支持使用。例如、要查看存储节点的指标、请执行以下步骤。

步骤

1. 在GMI中、菜单：Support[Metrics]。
2. 在Grafana部分下、选择Node信息板。



3. 在Grafana中、将主机设置为要查看指标的任何节点。在这种情况下、将选择一个存储节点。提供的信息比以下屏幕截图所示的信息要多。

在StorageGRID中使用流量分类策略

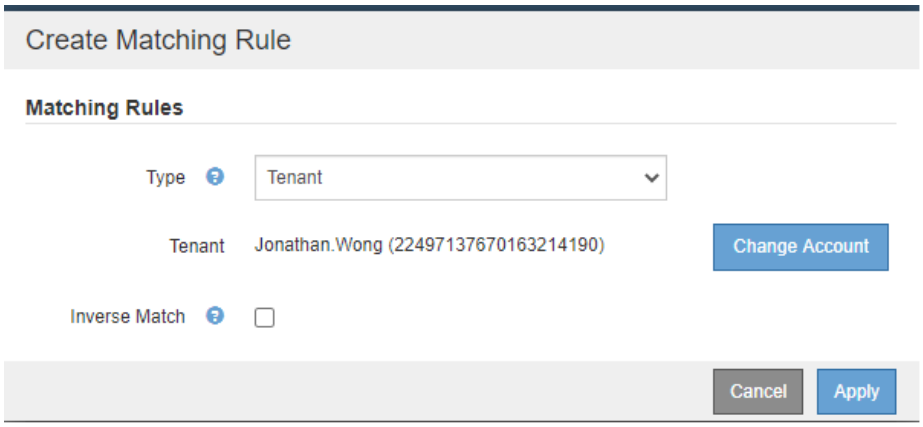
了解如何设置和配置流量分类策略、以管理和优化StorageGRID中的网络流量。

流量分类策略提供了一种根据特定租户、分段、IP子网或负载平衡器端点监控和/或限制流量的方法。网络连接和带宽是StorageGRID的特别重要的衡量指标。

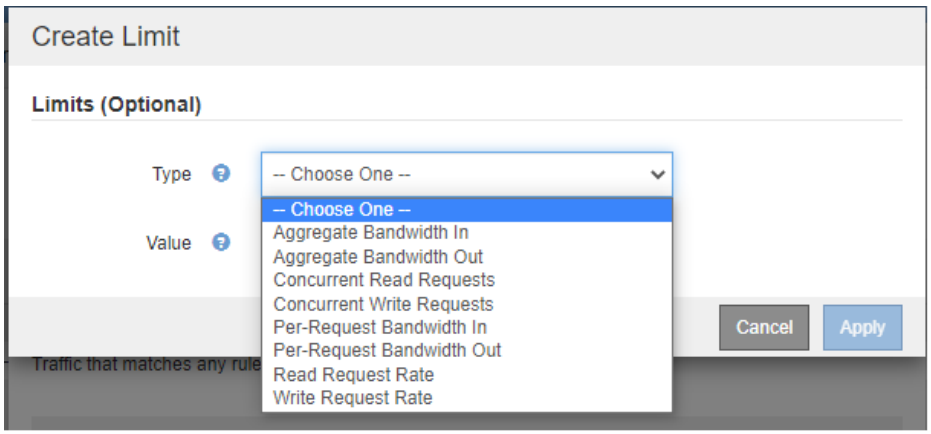
要配置流量分类策略、请执行以下步骤：

步骤

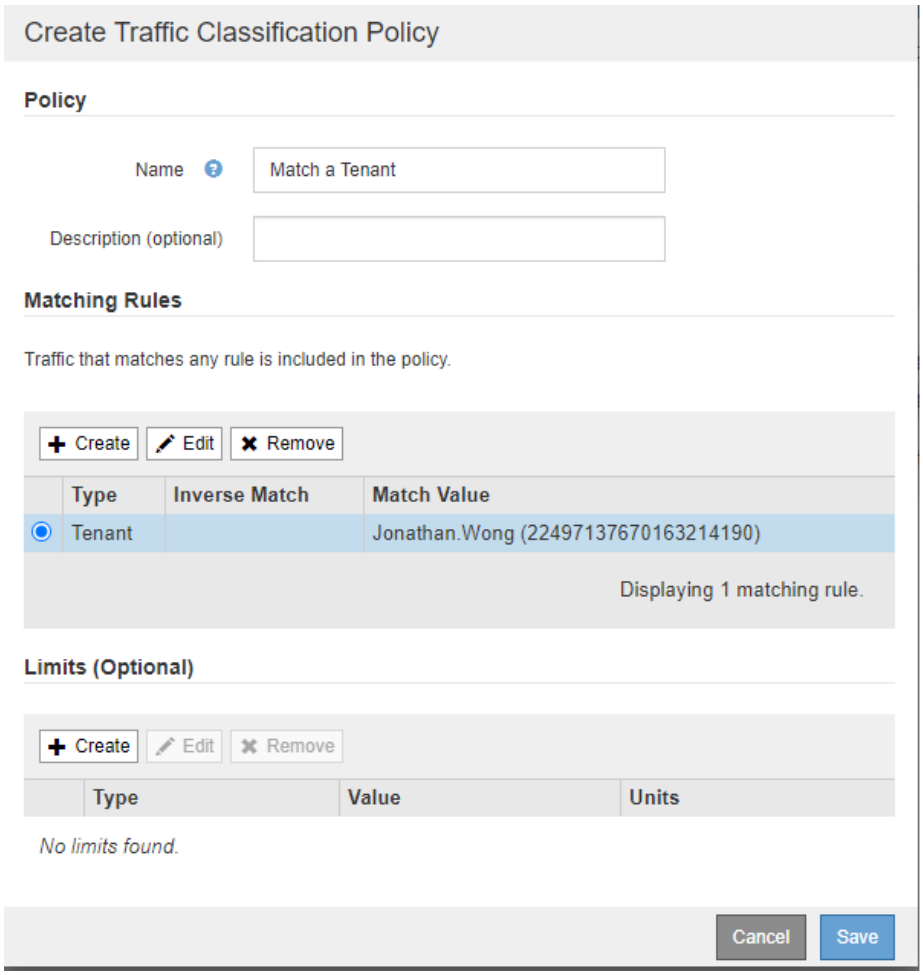
1. 在GMI上、导航到菜单：配置[系统设置>交通分类]。
2. 单击创建+
3. 输入策略的名称和说明。
4. 创建匹配规则。



5. 设置限制(可选)。



6. 保存策略



要查看与您的流量分类策略关联的指标、请选择您的策略、然后单击指标。此时将生成Grafana信息板、其中显示负载平衡器请求流量和平均请求持续时间等信息。

使用审核日志监控**StorageGRID**

了解如何使用StorageGRID审核日志详细了解租户和网格活动、以及如何利用Splunk等工具进行日志分析。

通过StorageGRID审核日志、您可以收集有关租户和网格活动的详细信息。可以通过NFS公开审核日志以供分析。有关如何导出审核日志的详细说明，请参阅《管理员指南》。

导出审核后、您可以使用Splunk或Logstash + ElashSearch等日志分析工具了解租户活动或创建详细的计费和成本分摊报告。

有关审核消息的详细信息、请参见StorageGRID文档。请参阅。 "审核消息"

使用适用于**Splunk**的**StorageGRID**应用程序

了解适用于Splunk的NetApp StorageGRID应用程序、该应用程序允许您在Splunk平台中监控和分析StorageGRID环境。

Splunk是一个软件平台、用于导入计算机数据并为其编制索引、以提供强大的搜索和分析功能。NetApp StorageGRID应用程序是适用于Splunk的附加软件、用于导入和丰富从StorageGRID利用的数据。

有关如何安装、升级和配置StorageGRID加载项的说明、请参见： https://splunkbase.splunk.com/app/3895/#/details

TR-4882：安装StorageGRID裸机网格

StorageGRID安装简介

了解如何在裸机主机上安装StorageGRID。

TR-4882提供了一组实用的分步说明、用于生成可正常工作的NetApp StorageGRID安装。此安装可以安装在裸机上、也可以安装在运行Red Hat Enterprise Linux (RHEL)的虚拟机(VM)上。该方法是、在三台物理(或虚拟)计算机上以建议的布局和存储配置执行六个StorageGRID容器化服务的"确定性"安装。一些客户可能会发现按照本技术报告中的示例部署更容易理解部署过程。

有关StorageGRID和安装过程的更深入的了解、请参见 https://docs.netapp.com/us-en/storagegrid-118/landing-install-upgrade/index.html 产品文档中的[安装、升级和修补程序StorageGRID]。

在开始部署之前、让我们先了解一下NetApp StorageGRID软件的计算、存储和网络连接要求。StorageGRID在Podman或Docker中作为容器化服务运行。在此模型中、某些要求是指主机操作系统(托管Docker且运行StorageGRID软件的操作系统)。某些资源会直接分配给每个主机中运行的Docker容器。在此部署中、为了最大程度地提高硬件利用率、我们会为每个物理主机部署两项服务。有关详细信息，请继续下一节， "安装StorageGRID的前提条件"。

本技术报告中概述的步骤可在六个裸机主机上正常安装StorageGRID。现在、您已拥有一个工作网格和客户端网络、这在大多数测试场景中都很有用。

从何处查找追加信息

要详细了解本技术报告中介绍的信息、请查看以下文档资源：

- NetApp StorageGRID文档中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID支持 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp产品文档 https://www.netapp.com/support-and-training/documentation/

安装StorageGRID的前提条件

了解部署StorageGRID所需的计算、存储、网络、Docker和节点采购。

计算要求

下表列出了每种类型的StorageGRID节点支持的最低资源要求。这是StorageGRID节点所需的最低资源。

节点类型	CPU核心	RAM
管理员	8.	24 GB
存储	8.	24 GB
网关	8.	24 GB

此外、每个物理Docker主机至少应分配16 GB RAM、以便正常运行。因此、例如、要在一个物理Docker主机上同时托管表中所述的任意两项服务、应执行以下计算：

24 + 24 + 16 = 64 GB RAM、8 + 8 = 16核

由于许多现代服务器都超过了这些要求、因此我们将六种服务(StorageGRID容器)组合到三个物理服务器上。

网络要求

三种类型的StorageGRID流量包括：

- *网格流量(必需)。*网格中所有节点之间传输的内部 StorageGRID 流量。
- *管理员流量(可选)。*用于系统管理和维护的流量。
- *客户端流量(可选)。*在外部客户端应用程序和网格之间传输的流量，包括来自 S3 和 Swift 客户端的所有对象存储请求。

您最多可以配置三个网络以用于StorageGRID系统。每种网络类型都必须位于一个单独的子网上、不能重叠。如果所有节点都位于同一子网上、则不需要网关地址。

在此评估中、我们将部署在两个网络上、其中包含网格和客户端流量。可以稍后添加一个管理网络来执行该附加功能。

将网络一致地映射到所有主机中的接口非常重要。例如、如果每个节点上有两个接口、即ens192和ens224、则它们都应映射到所有主机上的同一网络或VLAN。在此安装中、安装程序会将这些映像映射到Docker容器中、并将其映射为eth0@if2和eth2@if3 (因为环回是容器内的IF1)、因此、一致的模型非常重要。

有关**Docker**网络连接的说明

StorageGRID使用网络的方式与某些Docker容器实施方式不同。它不使用Docker (或Kubnetes或Swarm)提供的网络。相反、StorageGRID实际上会将容器生成为—net=none、这样、Docker就不会对容器执行任何网络连接操作。StorageGRID服务生成容器后、将从节点配置文件中定义的接口创建一个新的macvlan设备。该设备具有一个新的MAC地址、并作为一个单独的网络设备、可以从物理接口接收数据包。然后、macvlan设备将移至容器命名空间、并重命名为容器中的eth0、eth1或eth2之一。此时、此网络设备将在主机操作系统中不再可见。在本示例中、Docker容器中的网格网络设备为eth0、客户端网络为eth2。如果我们有一个管理网络、则此设备在容器中将为eth1。

> 在某些网络和虚拟环境中、容器网络设备的新MAC地址可能需要启用混杂模式。此模式允许物理设备接收和发送与已知物理MAC地址不同的MAC地址的数据包。+如果在VMware vSphere中运行、则在运行RHEL时、必须在提供StorageGRID流量的端口组中接受混杂模式、MAC地址更改和伪传输。在大多数情况下、Ubuntu或Debian都可以在不进行这些更改的情况下运行。+

存储要求

每个节点都需要下表所示大小的基于SAN的磁盘设备或本地磁盘设备。

> 表中的数字适用于每种StorageGRID服务类型、而不适用于整个网格或每个物理主机。根据部署选项，我们将在本文档后面的中计算每个物理主机的数量 "物理主机布局和要求"。+安装程序将在StorageGRID容器中创建标有星号的路径或文件系统。管理员不需要手动配置或创建文件系统、但主机需要块设备来满足这些要求。换言之、块设备应使用命令显示 `lsblk` 、但不能在主机操作系统中进行格式化或挂载。+

节点类型	**LUN** 用途	**LUN** 数量	**LUN**的最小大小	需要手动文件系统	建议的节点配置条目
全部	管理节点系统空间 `/var/local` (此处的SSD非常有用)	每个管理节点一个	90GB	否	`BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/ADM-VAR-LOCAL`

节点类型	**LUN** 用途	**LUN** 数量	**LUN**的最小大小	需要手动文件系统	建议的节点配置条目
所有节点	Docker存储池、位于 `/var/lib/docker for container pool`	每个主机(物理或VM)一个	每个容器100 GB	是—etx4	不适用—格式化并挂载为主机文件系统(未映射到容器)
管理员	管理节点审核日志(管理容器中的系统数据) `/var/local/audit/export`	每个管理节点一个	200GB	否	`BLOCK_DEVICE_AUDIT_LOGS =/dev/mapper/ADM-OS`
管理员	管理节点表(管理容器中的系统数据) `/var/local/mysql_ibdata`	每个管理节点一个	200GB	否	`BLOCK_DEVICE_TABLES = /dev/mapper/ADM-MySQL`
存储节点	对象存储(块设备) `/var/local/rangedb0` (此处的SSD非常有用) `/var/local/rangedb1` `/var/local/rangedb2`	每个存储容器三个	4000GB	否	`BLOCK_DEVICE_RANGEDB_000 = /dev/mapper/SN-Db00` `BLOCK_DEVICE_RANGEDB_001 = /dev/mapper/SN-Db01` `BLOCK_DEVICE_RANGEDB_002 = /dev/mapper/SN-Db02`

在此示例中、每种容器类型都需要下表中显示的磁盘大小。每个物理主机的要求将在本文档后面的中进行介绍 "物理主机布局和要求"。

每个容器类型的磁盘大小

管理容器

Name	大小 **(GiB)**
Docker存储	100 (每个容器)
ADM-OS	90
ADM-Audit	200
ADM-MySQL	200

存储容器

Name	大小 **(GiB)**
Docker存储	100 (每个容器)
SN-OS	90

Name	大小 (GiB)
Rangedb-0	4096
Rangedb-1	4096
Rangedb-2	4096

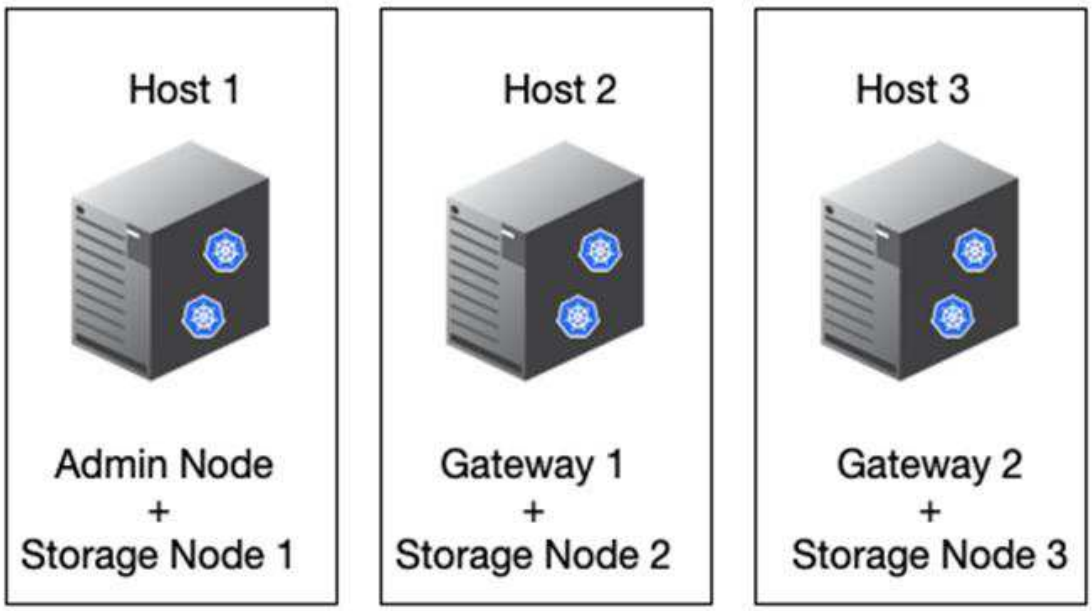
网关容器

Name	大小 (GiB)
Docker存储	100 (每个容器)
/var/local	90

物理主机布局和要求

通过将上表所示的计算和网络要求相结合、您可以获得此安装所需的一组基本硬件、其中包括三个物理(或虚拟)服务器、16核、64 GB RAM和两个网络接口。如果需要更高的吞吐量、可以在网格或客户端网络上绑定两个或更多接口、并在节点配置文件中使用带VLAN标记的接口、例如bond0.520。如果您希望工作负载更密集、则为主机和容器提供更多内存会更好。

如下图所示、这些服务器将托管六个Docker容器、每个主机两个。RAM的计算方法是、为每个容器提供24 GB、为主机操作系统本身提供16 GB。



每个物理主机(或VM)所需的总RAM为24 x 2 + 16 = 64 GB。下表列出了主机1、2和3所需的磁盘存储。

主机 **1**	大小 **(GiB)**
Docker存储	`/var/lib/docker` (文件系统)
200 (100 x 2)	管理容器
`BLOCK_DEVICE_VAR_LOCAL`	90
`BLOCK_DEVICE_AUDIT_LOGS`	200
`BLOCK_DEVICE_TABLES`	200
存储容器	SN-OS `/var/local` (设备)
90	Rangedb-0(设备)
4096	Rangedb-1 (设备)
4096	Rangedb-2 (设备)

主机 **2**	大小 **(GiB)**
Docker存储	`/var/lib/docker` (共享)
200 (100 x 2)	网关容器
GW-OS */var/local	100
存储容器	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

主机 **3**	大小 **(GiB)**
Docker存储	`/var/lib/docker` (共享)
200 (100 x 2)	网关容器
*/var/local	100
存储容器	*/var/local
100	Rangedb-0
4096	Rangedb-1
4096	Rangedb-2

Docker存储的计算方法是、每个/var/local (每个容器)允许100 GB x两个容器= 200 GB。

准备节点

要为StorageGRID的初始安装做准备、请先安装RHEL 9.2版并启用SSH。根据最佳实践设置网络接口、网络时间协议(NTP)、DNS和主机名。您需要在网格网络上至少启用一个网络接口、而在客户端网络上至少启用另一个网络接口。如果您使用的是带VLAN标记的接口、请按照以下示例进行配置。否则、只需简单的标准网络接口配置即可。

如果您需要在网格网络接口上使用VLAN标记、则您的配置应具有以下格式的两个文件 `/etc/sysconfig/network-scripts/`：

```
# 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
```

此示例假设网格网络的物理网络设备为enp67s0。它也可以是绑定的设备、例如、绑定0。无论是使用绑定还是标准网络接口、如果网络端口没有默认VLAN或默认VLAN未与网格网络关联、则必须在节点配置文件中使用带VLAN标记的接口。StorageGRID容器本身不会取消标记以太网帧、因此必须由父操作系统处理。

使用**iSCSI**设置可选存储

如果不使用iSCSI存储、则必须确保host1、host2和host3包含足够大的块设备、以满足其要求。有关host1、host2和host3的存储要求、请参见 "每个容器类型的磁盘大小" 。

要使用iSCSI设置存储、请完成以下步骤：

步骤

1. 如果使用外部iSCSI存储，如NetApp E系列或NetApp ONTAP®数据管理软件，请安装以下软件包：

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

2. 查找每个主机上的启动程序ID。

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

3. 使用步骤2中的启动程序名称、将存储设备上的LUN (即表中所示的数量和大小)映射到每个存储 "存储要求" 节点。
4. 使用发现并登录到新创建的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.
```

有关详细信息、请参见 "正在创建iSCSI启动程序" Red Hat客户门户上的。

5. 要显示多路径设备及其关联的LUN WWID、请运行以下命令：

```
# multipath -ll
```

如果您不对多路径设备使用iSCSI、只需使用唯一的路径名称挂载设备即可、该名称将保留设备更改并以类似方式重新启动。

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

如果稍后删除或添加设备、只需使用 `/dev/sdx` 设备名称可能会导致问题。+如果使用多路径设备、请按如下所示修改 `/etc/multipath.conf` 文件以使用别名。+

这些设备可能存在于所有节点上、也可能不存在于所有节点上、具体取决于布局。

```
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
}
}
```

在主机操作系统中安装Docker之前、请格式化并挂载LUN或磁盘备份 `/var/lib/docker`。其他LUN在节点配置文件中进行定义、并直接由StorageGRID容器使用。也就是说、它们不会显示在主机操作系统中、而是显示在容器本身中、这些文件系统由安装程序处理。

如果您使用的是iSCSI支持的LUN、请在fstab文件中放置类似于以下行的内容。如前所述、其他LUN不需要挂载到主机操作系统中、但必须显示为可用块设备。

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

准备安装Docker

要准备Docker安装、请完成以下步骤：

步骤

1. 在所有三台主机的Docker存储卷上创建文件系统。

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

如果使用的是具有多路径的iSCSI设备，请使用 `/dev/mapper/Docker-Store`。

2. 创建Docker存储卷挂载点：

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

3. 将Docker存储卷设备的类似条目添加到 `/etc/fstab`。

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

只有在使用iSCSI设备时、建议使用以下 `_netdev` 选项。如果您不需要使用本地块设备、则建议使用此设备 `_netdev defaults` 。

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

4. 挂载新文件系统并查看磁盘使用情况。

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

5. 出于性能原因、请关闭并禁用交换。

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

6. 要保留这些设置、请从/etc/fstab中删除所有交换条目、例如：

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

如果未完全禁用交换，则会严重降低性能。

7. 对节点执行测试重新启动、以确保 `/var/lib/docker` 卷持久存在且所有磁盘设备均返回。

安装适用于StorageGRID的Docker

了解如何安装适用于StorageGRID的Docker。

要安装Docker、请完成以下步骤：

步骤

1. 为Docker配置yum repo。

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

2. 安装所需的软件包。

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

3. 启动Docker。

```
sudo systemctl start docker
```

4. 测试Docker。

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

5. 确保Docker在系统启动时运行。

```
sudo systemctl enable docker
```

为StorageGRID准备节点配置文件

了解如何为StorageGRID准备节点配置文件。

总体而言、节点配置过程包括以下步骤：

步骤

1. 在所有主机上创建 `/etc/storagegrid/nodes` 目录。

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

2. 为每个物理主机创建所需的文件、以匹配容器/节点类型布局。在此示例中、我们在每台主机上的每个物理主机上创建了两个文件。

> 文件名用于定义实际的安装节点名称。例如， `dc1-adm1.conf` 将成为名为的节点 `dc1-adm1`。

--主机1：
`dc1-adm1.conf`
`dc1-sn1.conf`

--主机2：
`dc1-gw1.conf`
`dc1-sn2.conf`

--主机3：
`dc1-gw2.conf`
`dc1-sn3.conf`

正在准备节点配置文件

以下示例使用 `/dev/disk/by-path` 格式。您可以运行以下命令来验证路径是否正确：

```
[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
```

以及以下命令：

```
[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
```

主管理节点示例

示例文件名：

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

示例文件内容：

磁盘路径可以遵循以下示例或使用 `/dev/mapper/alias` 模式命名。请勿使用块设备名称(如) `/dev/sdb` 、因为它们可能会在重新启动时更改、并对网格造成严重损坏。

```
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
```

存储节点示例

示例文件名：

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

示例文件内容：

```
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
```

网关节点示例

示例文件名：

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

示例文件内容：

```
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
```

安装StorageGRID依赖关系和软件包

了解如何安装StorageGRID依赖关系和软件包。

要安装StorageGRID依赖关系和软件包、请运行以下命令：

```
[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
```

验证StorageGRID配置文件

了解如何验证StorageGRID的配置文件内容。

在中为每个StorageGRID节点创建配置文件后 `/etc/storagegrid/nodes` 、必须验证这些文件的内容。

要验证配置文件的内容，请在每个主机上运行以下命令：

```
sudo storagegrid node validate all
```

如果这些文件正确无误、则输出将显示每个配置文件均已通过：

```
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
```

如果配置文件不正确、问题将显示为警告和错误。如果发现任何配置错误，则必须先更正这些错误，然后再继续安装。

```
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
```

启动 StorageGRID 主机服务

了解如何启动StorageGRID主机服务。

要启动StorageGRID节点并确保它们在主机重新启动后重新启动、您必须启用并启动StorageGRID主机服务。

要启动StorageGRID主机服务、请完成以下步骤。

步骤

1. 在每个主机上运行以下命令：

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

> 初始运行时、启动过程可能需要一段时间。

2. 运行以下命令以确保部署正在进行：

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

3. 对于任何返回或状态的节点 `Not-Running` `Stopped`，请运行以下命令：

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

例如、根据以下输出、您应启动 `dc1-adm1` 节点：

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

4. 如果您之前已启用并启动StorageGRID主机服务(或者不确定该服务是否已启用并启动)、请同时运行以下命令：

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

在StorageGRID中配置网格管理器

了解如何在主管理节点上的StorageGRID中配置网格管理器。

通过主管理节点上的网格管理器用户界面配置StorageGRID系统来完成安装。

高级步骤

配置网格并完成安装涉及以下任务：

步骤

1. [导航到网格管理器]
2. "指定 StorageGRID 许可证信息"
3. "将站点添加到StorageGRID"
4. "指定网格网络子网"
5. "批准待定网格节点"
6. "指定NTP服务器信息"
7. "指定域名系统服务器信息"
8. "指定 StorageGRID 系统密码"
9. "查看您的配置并完成安装"

导航到网格管理器

使用网格管理器定义配置StorageGRID系统所需的所有信息。

开始之前、必须先部署主管理节点并完成初始启动序列。

要使用网格管理器定义信息、请完成以下步骤。

步骤

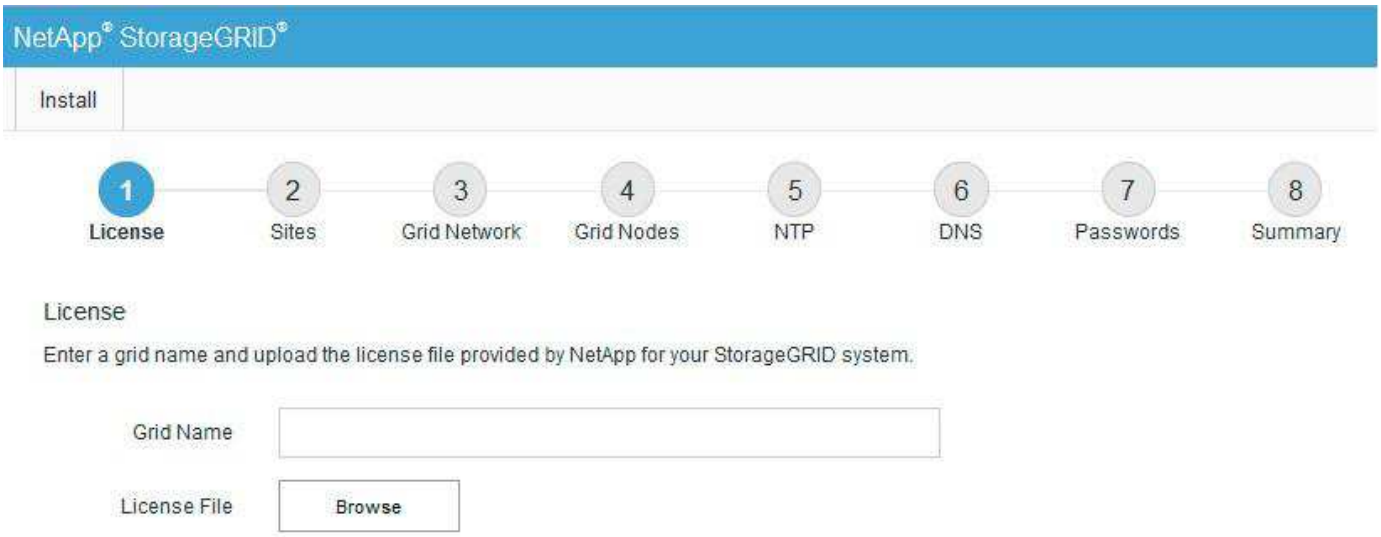
1. 通过以下地址访问网格管理器：

   ```
   https://primary_admin_node_grid_ip
   ```

   或者、您也可以通过端口8443访问Grid Manager。

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

2. 单击安装StorageGRID系统。此时将显示用于配置StorageGRID网格的页面。



添加**StorageGRID**许可证详细信息

了解如何上传StorageGRID许可证文件。

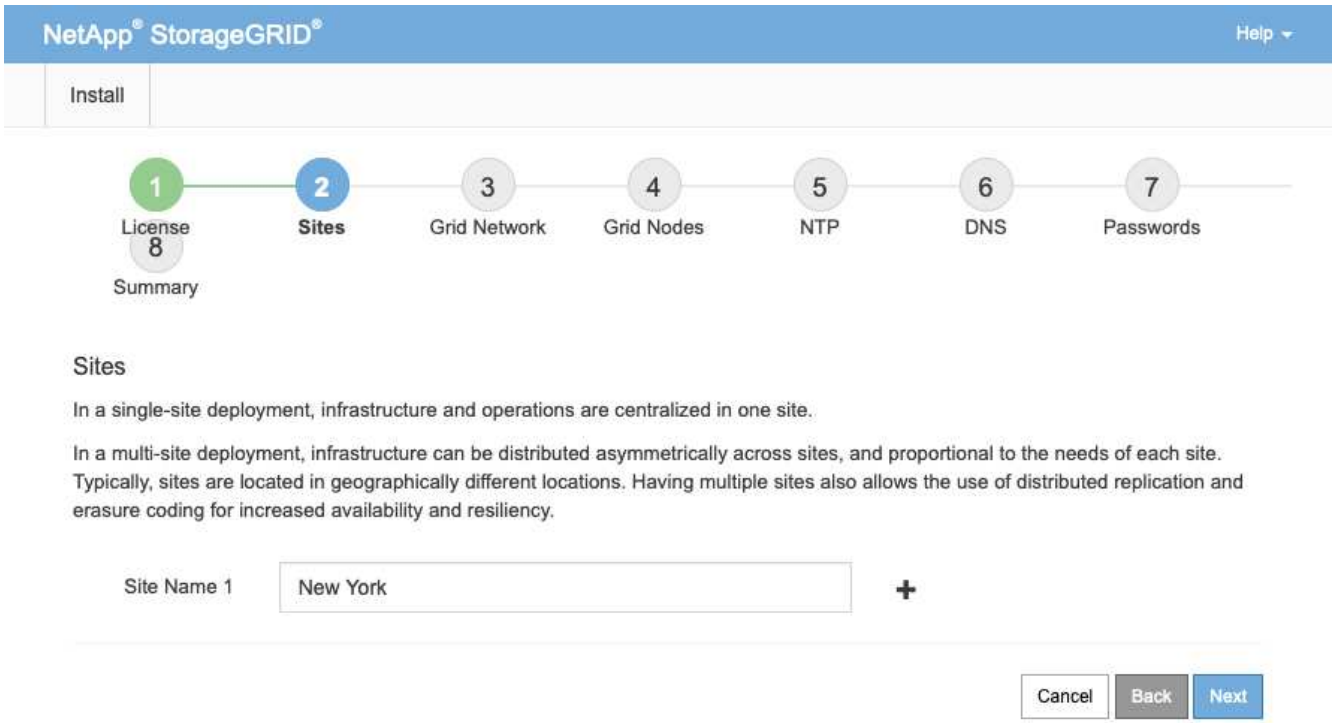
您必须指定 StorageGRID 系统的名称并上传 NetApp 提供的许可证文件。

要指定StorageGRID许可证信息、请完成以下步骤：

步骤

1. 在许可证页面的网格名称字段中、输入StorageGRID系统的名称。安装后、该名称将显示为网格拓扑树中的顶层。
2. 单击浏览，找到NetApp许可证文件 (`NLF-unique-id.txt`，然后单击打开。此时将验证许可证文件，并显示序列号和许可的存储容量。

> StorageGRID 安装归档包含一个免费许可证，不提供产品的任何支持授权。您可以在安装后更新为提供支持的许可证。



3. 单击下一步。

将站点添加到StorageGRID

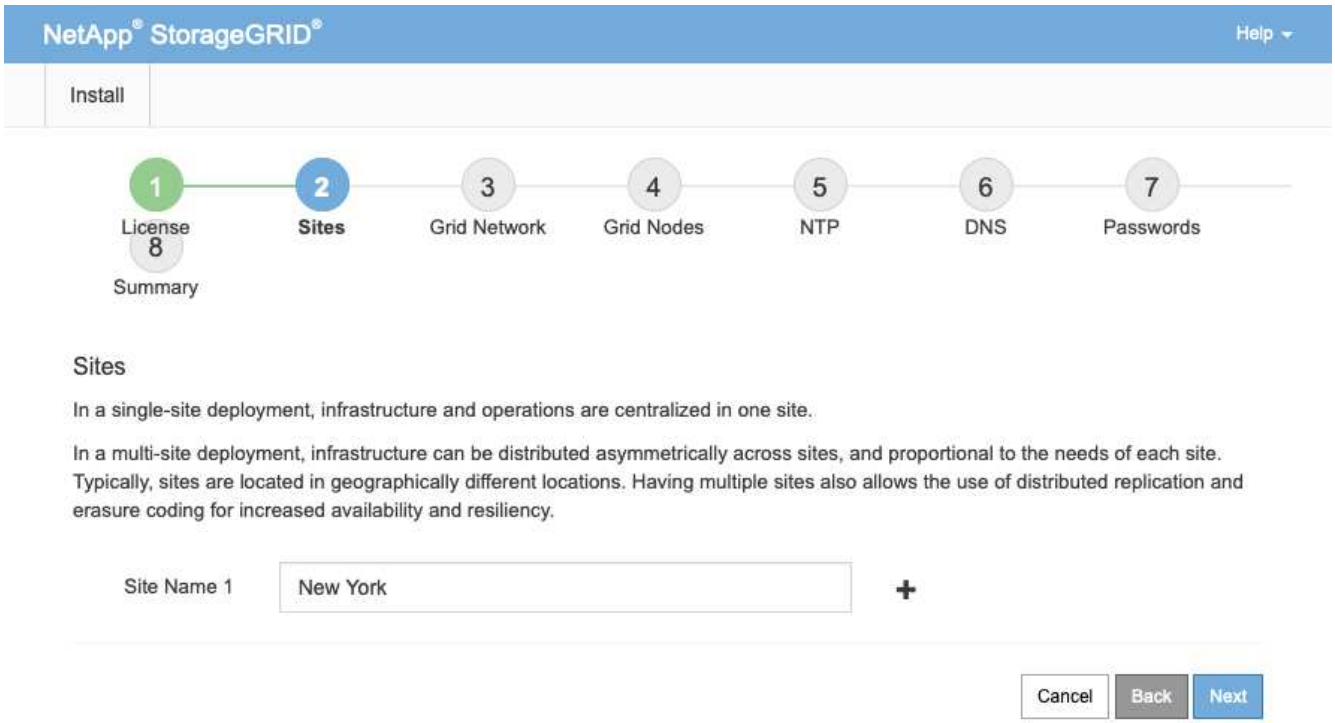
了解如何将站点添加到StorageGRID以提高可靠性和存储容量。

安装StorageGRID时、必须至少创建一个站点。您可以创建其他站点来提高 StorageGRID 系统的可靠性和存储容量。

要添加站点、请完成以下步骤：

步骤

1. 在Sites页面上、输入站点名称。
2. 要添加其他站点、请单击最后一个站点条目旁边的加号、然后在新站点名称文本框中输入该名称。根据需要为网格拓扑添加尽可能多的其他站点。您最多可以添加 16 个站点。



3. 单击下一步。

为StorageGRID指定网格网络子网

了解如何为StorageGRID配置网格网络子网。

您必须指定网格网络上使用的子网。

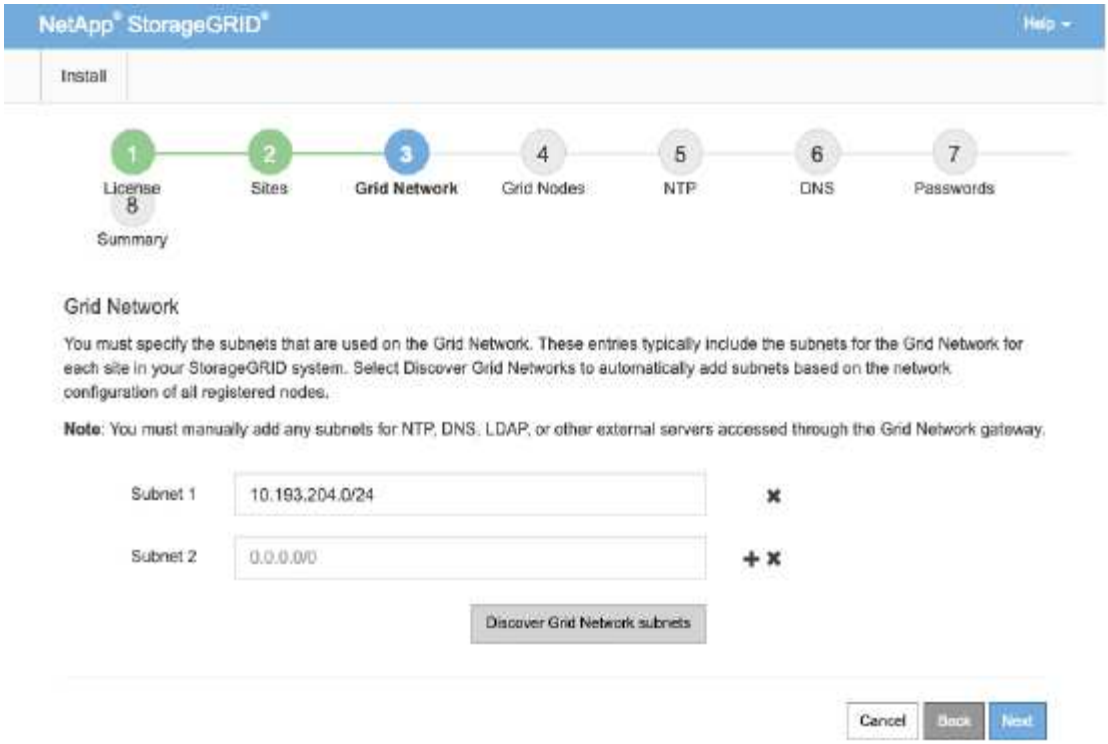
子网条目包括StorageGRID系统中每个站点的网格网络子网以及必须通过网格网络访问的任何子网(例如托管NTP服务器的子网)。

如果有多个网格子网、则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。

要指定网格网络子网、请完成以下步骤：

步骤

1. 在子网1文本框中、至少为一个网格网络指定CIDR网络地址。
2. 单击最后一个条目旁边的加号以添加其他网络条目。如果已部署至少一个节点、请单击发现网格网络子网以使用已向网格管理器注册的网格节点报告的子网自动填充网格网络子网列表。



3. 单击下一步。

批准StorageGRID的网格节点

了解如何审核和批准加入StorageGRID系统的任何待定网格节点。

您必须先批准每个网格节点、然后再将其加入StorageGRID系统。

开始之前、必须部署所有虚拟节点和StorageGRID设备网格节点。

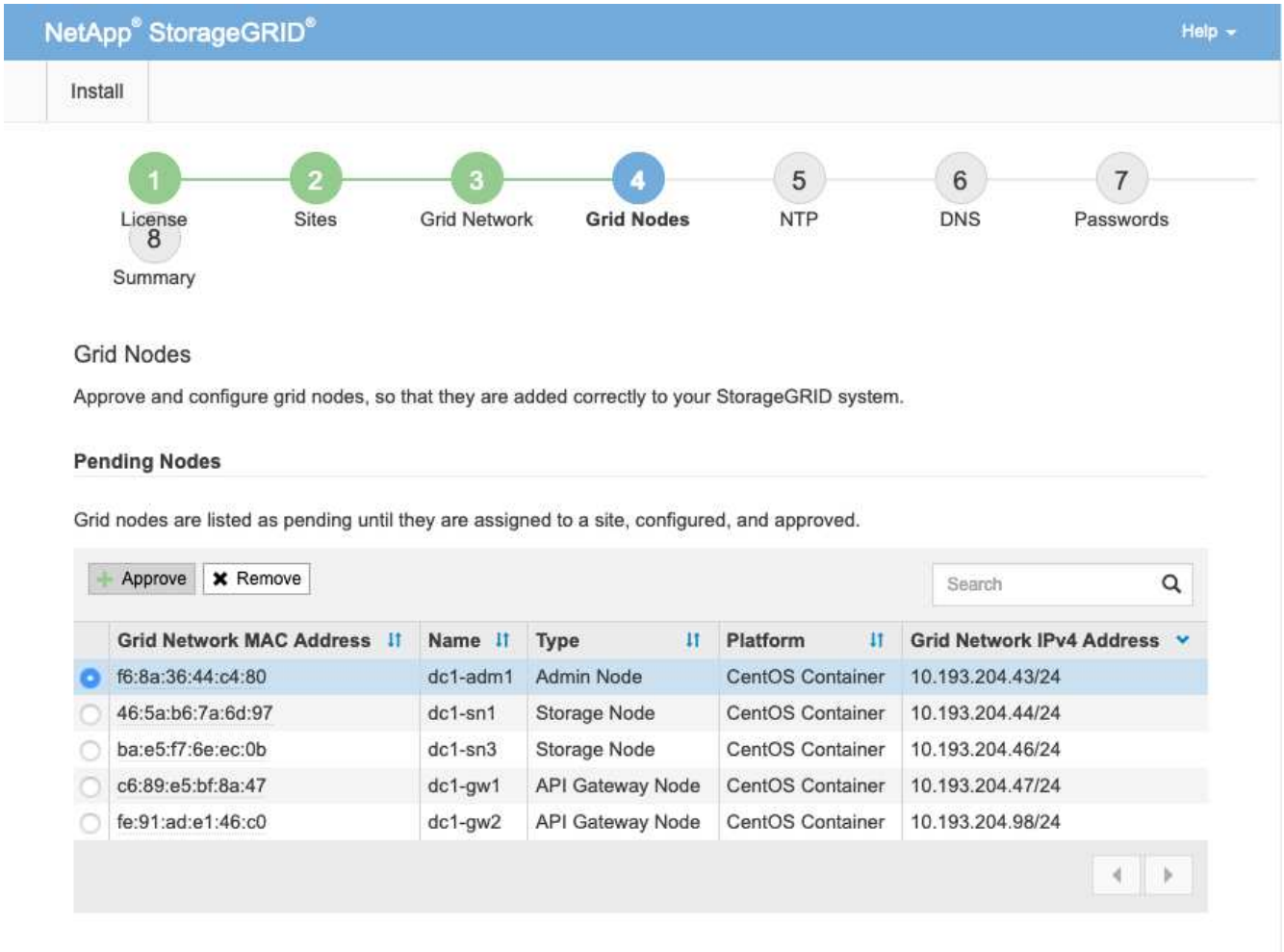
要批准待定网格节点、请完成以下步骤：

步骤

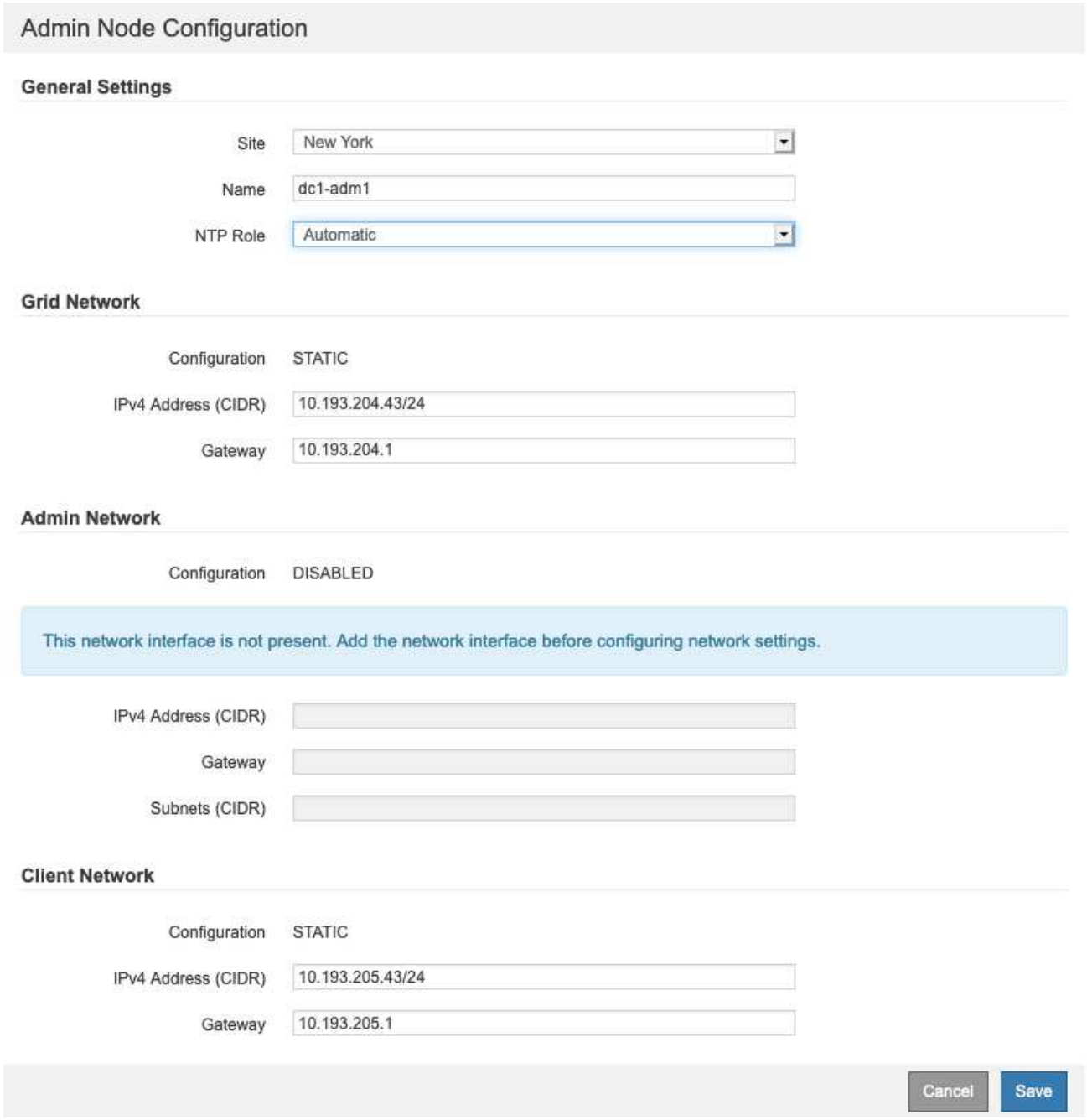
1. 查看Pending Node列表、并确认它显示了您部署的所有网格节点。

   如果缺少网格节点，请确认已成功部署该节点。

2. 单击要批准的待定节点旁边的单选按钮。



3. 单击批准。
4. 在常规设置中、根据需要修改以下属性的设置。



--**Site**:此网格节点的站点的系统名称。

--**Name**：要分配给节点的主机名，以及要在网格管理器中显示的名称。此名称默认为您在节点部署期间指定的名称、但您可以根据需要更改此名称。

--**NTP**角色:网格节点的NTP角色。选项包括"自动"、"主"和"客户端"。选择自动选项会将主要角色分配给管理节点、具有管理域控制器(ADC)服务的存储节点、网关节点以及具有非静态IP地址的任何网格节点。所有其他网格节点均分配有客户端角色。

确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

--**ADC**服务**(**仅限存储节点**)**:选择“自动”让系统确定节点是否需要ADC服务。此 ADA 服务可跟踪网格服务的位

置和可用性。每个站点上必须至少有三个存储节点包含ADC服务。在部署此节点后，您不能将此 ADC 服务添加到该节点中。

5. 在Grid Network中、根据需要修改以下属性的设置：

   --IPv4地址(CIDR)：网格网络接口(容器内的eth0)的CIDR网络地址。例如， `192.168.1.234/24`。

   --*Gateway：网格网络网关。例如， `192.168.0.1`。

   > 如果有多个网格子网、则需要网关。

   > 如果您为网格网络配置选择了DHCP、并更改了此处的值、则新值将配置为节点上的静态地址。确保生成的IP地址不在DHCP地址池中。

6. 要为网格节点配置管理网络、请根据需要在管理网络部分中添加或更新设置。

   在子网(CIDR)文本框中输入此接口之外的路由的目标子网。如果存在多个管理子网、则需要使用管理网关。

   > 如果您为管理网络配置选择了DHCP、并更改了此处的值、则新值将在节点上配置为静态地址。确保生成的IP地址不在DHCP地址池中。

   设备：对于StorageGRID设备，如果在初始安装期间未使用StorageGRID设备安装程序配置管理网络，则无法在此网格管理器对话框中配置管理网络。而是必须执行以下步骤：

   a. 重新启动设备：在设备安装程序中、选择菜单：高级[重新启动]。重新启动可能需要几分钟时间。
   b. 选择菜单：配置网络[链接配置]并启用相应的网络。
   c. 选择菜单：配置网络[IP配置]并配置已启用的网络。
   d. 返回主页页面、然后单击开始安装。
   e. 在网格管理器中：如果已批准节点表中列出了该节点、请重置该节点。
   f. 从 Pending Nodes 表中删除此节点。
   g. 等待节点重新出现在 "Pending Nodes" 列表中。
   h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。对于追加信息 ，请参见适用于您的设备型号的安装和维护说明。

7. 如果要为网格节点配置客户端网络，请根据需要在客户端网络部分中添加或更新设置。如果配置了客户端网络，则需要使用网关，安装后，它将成为节点的默认网关。

   设备：对于StorageGRID设备，如果在初始安装期间未使用StorageGRID设备安装程序配置客户端网络，则无法在此网格管理器对话框中配置客户端网络。而是必须执行以下步骤：

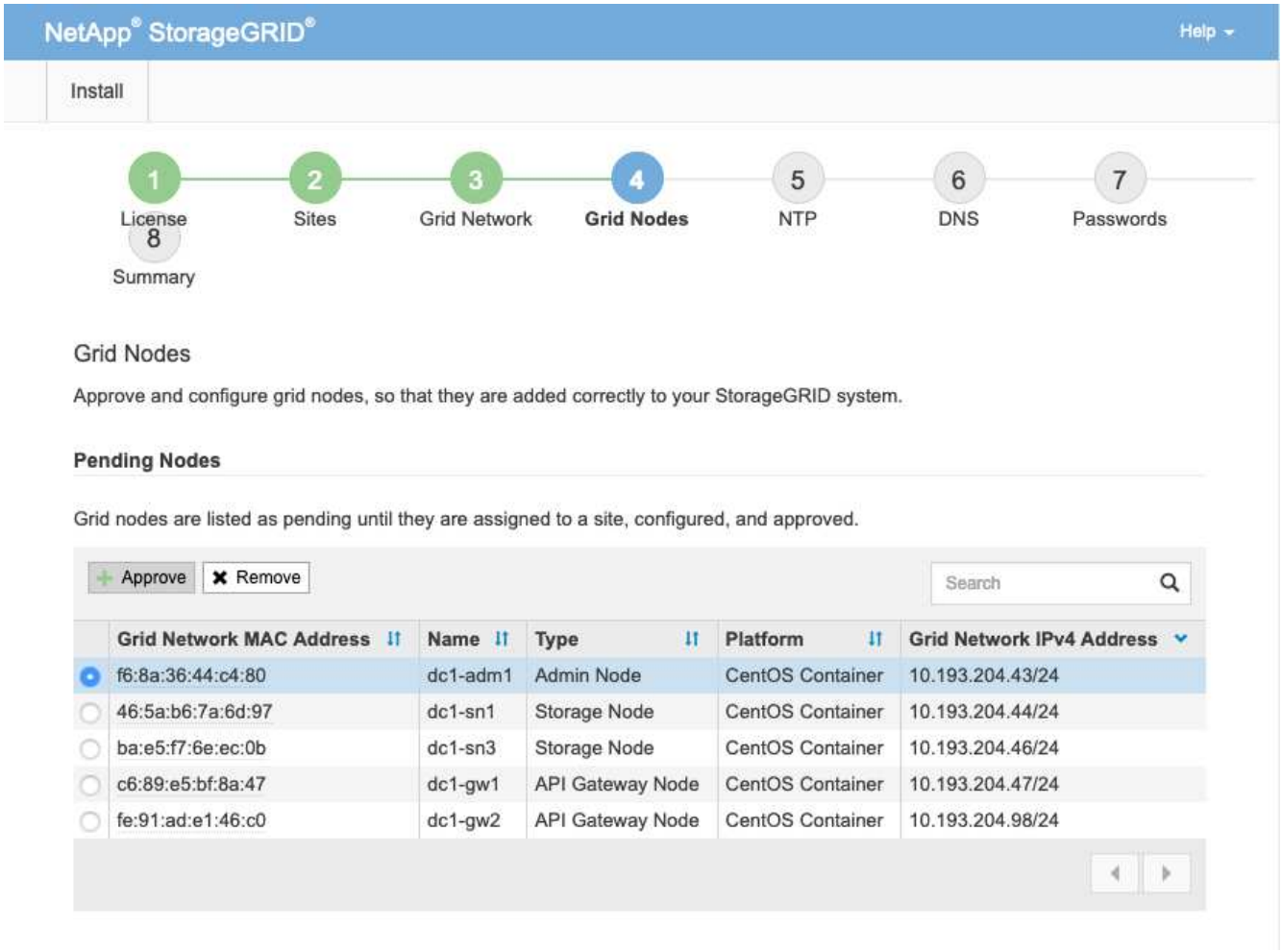
   a. 重新启动设备：在设备安装程序中、选择菜单：高级[重新启动]。重新启动可能需要几分钟时间。
   b. 选择菜单：配置网络[链接配置]并启用相应的网络。
   c. 选择菜单：配置网络[IP配置]并配置已启用的网络。
   d. 返回主页页面、然后单击开始安装。
   e. 在网格管理器中：如果已批准节点表中列出了该节点、请重置该节点。

f. 从 Pending Nodes 表中删除此节点。

g. 等待节点重新出现在 "Pending Nodes" 列表中。

h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。对于追加信息，请参见适用于您的设备的安装和维护说明。

8. 单击保存。网格节点条目将移至 "Approved Nodes" 列表。



9. 对要批准的每个待定网格节点重复步骤1-8。

   您必须批准网格中所需的所有节点。但是、您可以在单击"摘要"页面上的"安装"之前随时返回到此页面。要修改已批准的网格节点的属性、请单击其单选按钮、然后单击编辑。

10. 批准完网格节点后、单击下一步。

指定StorageGRID的NTP服务器详细信息

了解如何为StorageGRID系统指定NTP配置信息、以便在不同服务器上执行的操作可以保持同步。

为了防止出现时间漂移问题、您必须指定Stratum 3或更高版本的四个外部NTP服务器参考。

在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的Windows上的时间服务不够准确、Microsoft不支持在要求苛刻的环境(如StorageGRID)中使用此服务。

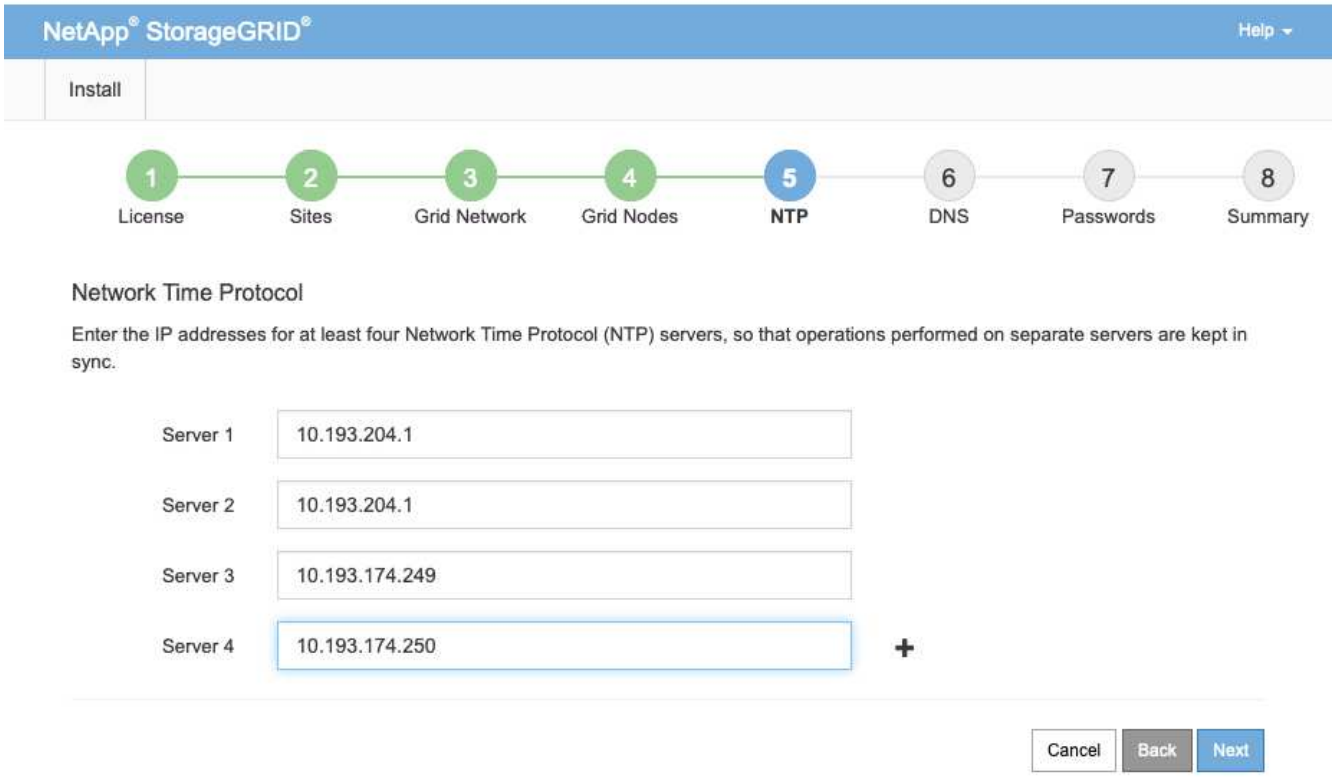
外部NTP服务器由先前分配了主要NTP角色的节点使用。

客户端网络未在安装过程中尽早启用、无法成为NTP服务器的唯一源。确保至少可以通过网格网络或管理网络访问一个NTP服务器。

要指定NTP服务器信息、请完成以下步骤：

步骤

1. 在服务器1到服务器4文本框中、指定至少四个NTP服务器的IP地址。
2. 如有必要、请单击最后一个条目旁边的加号以添加更多服务器条目。



3. 单击下一步。

指定StorageGRID的DNS服务器详细信息

了解如何为StorageGRID配置DNS服务器。

您必须为StorageGRID系统指定DNS信息、以便可以使用主机名而不是IP地址访问外部服务器。

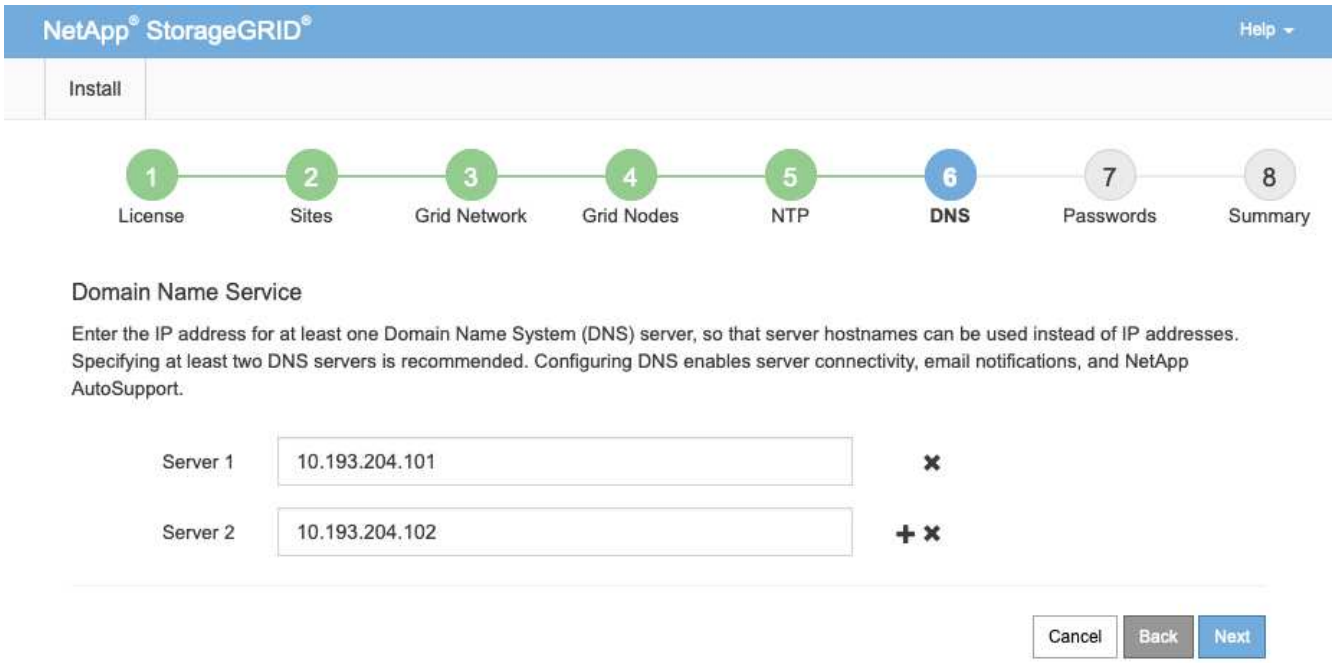
通过指定DNS服务器信息，您可以在电子邮件通知和NetApp AutoSupport®消息中使用完全限定域名(FFQDN)主机名，而不是IP地址。NetApp建议至少指定两个DNS服务器。

您应选择 DNS 服务器，以便在网络隔离时每个站点都可以在本地访问这些服务器。

要指定DNS服务器信息、请完成以下步骤：

步骤

1. 在服务器1文本框中、指定DNS服务器的IP地址。
2. 如有必要、请单击最后一个条目旁边的加号以添加更多服务器。



3. 单击下一步。

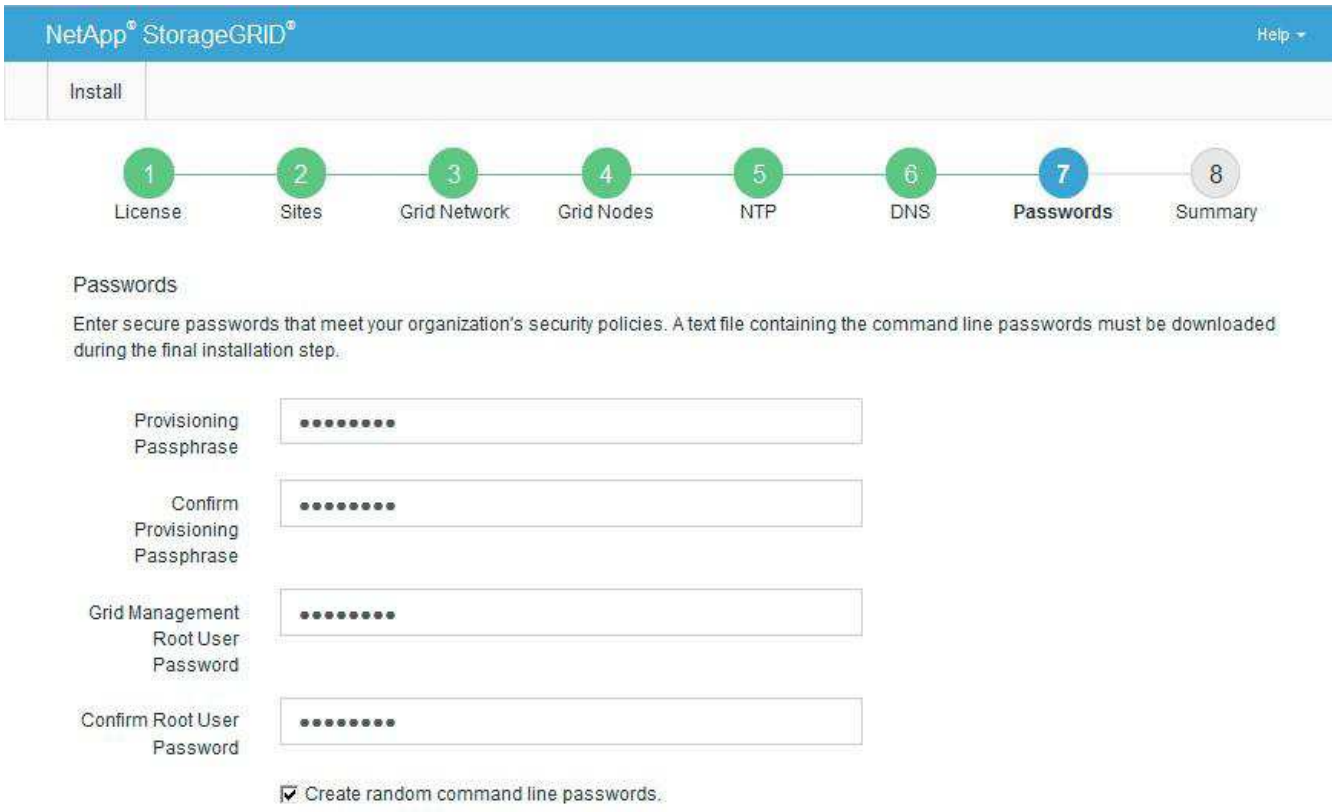
指定StorageGRID的系统密码

了解如何通过设置配置密码短语和网格管理root用户密码来保护StorageGRID系统。

要输入用于保护StorageGRID系统的密码、请按照以下步骤操作：

步骤

1. 在配置密码短语中、输入更改StorageGRID系统的网格拓扑所需的配置密码短语。您应将此密码记录在安全的位置。
2. 在确认配置密码短语中、重新输入配置密码短语。
3. 在网格管理root用户密码中、输入以root用户身份访问网格管理器所使用的密码。
4. 在确认root用户密码中、重新输入网格管理器密码。



5. 如果您要安装网格以进行概念验证或演示、请取消选择创建随机命令行密码选项。

   对于生产部署，出于安全原因，应始终使用随机密码。如果您要使用默认密码通过root或admin帐户从命令行访问网格节点、请取消选择仅适用于演示网格的创建随机命令行密码选项。

   > 单击“摘要”页面上的“安装”时，系统将提示您下载恢复软件包文件 (`sgws-recovery-packageid-revision.zip`)。您必须下载此文件才能完成安装。用于访问系统的密码存储在恢复软件包文件中的文件中 `Passwords.txt` 。

6. 单击下一步。

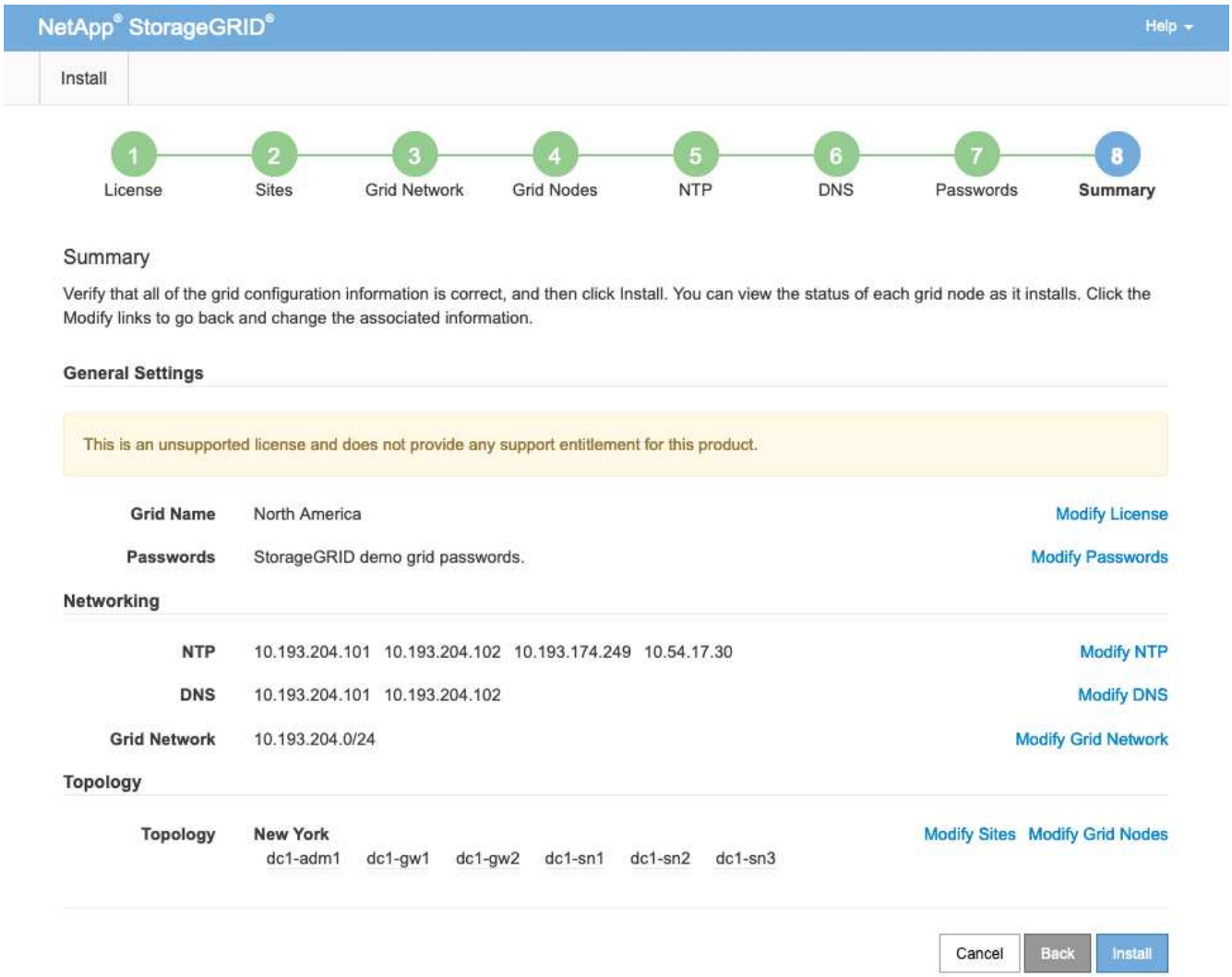
检查配置并完成StorageGRID安装

了解如何验证网格配置信息并完成StorageGRID安装过程。

要确保安装成功完成、请仔细查看您输入的配置信息。请按照以下步骤操作：

步骤

1. 查看摘要页面。



2. 验证所有网格配置信息是否正确。使用摘要页面上的修改链接返回并更正任何错误。
3. 单击安装。

> 如果将某个节点配置为使用客户端网络、则当您单击安装时、该节点的默认网关将从网格网络切换到客户端网络。如果连接断开、请确保您通过可访问的子网访问主管理节点。有关详细信息，请参阅"网络安装和配置"。

4. 单击Download Recovery Package。

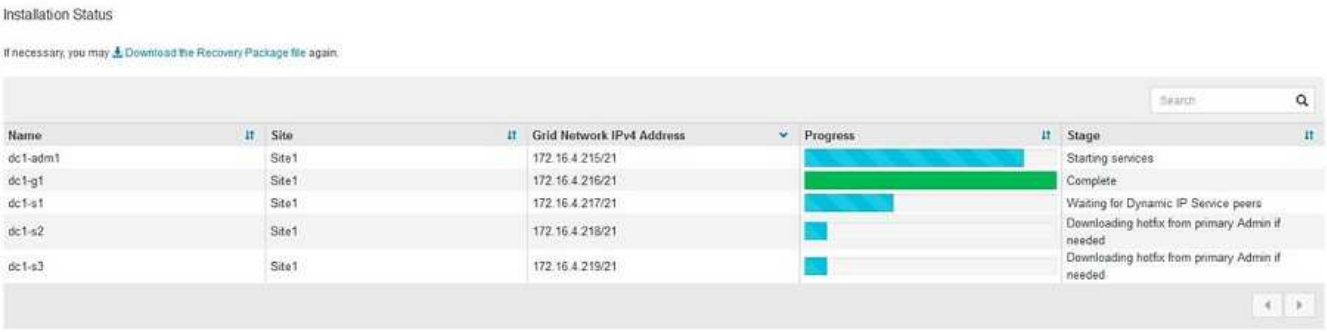
   在安装过程中，如果网格拓扑已定义，系统将提示您下载恢复软件包文件 (`.zip`()并确认您可以访问此文件的内容。您必须下载恢复软件包文件、以便在一个或多个网格节点发生故障时恢复StorageGRID系统。

   确认您可以提取文件的内容 `.zip` 、然后将其保存在两个安全、独立的位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

5. 选择I have successfully downloaded and Verified the Recovery Package File (我已成功下载并验证恢复软件包文件)选项、然后单击Next (下一步)。

如果安装仍在进行中、则会打开安装状态页面。此页面指示每个网格节点的安装进度。



当所有网格节点都达到完成阶段时、将打开网格管理器的登录页面。

6. 以root用户身份使用您在安装期间指定的密码登录到网格管理器。

在StorageGRID中升级裸机节点

了解StorageGRID中裸机节点的升级过程。

裸机节点的升级过程与设备或VMware节点的升级过程不同。在执行裸机节点升级之前、您必须先升级所有主机上的RPM文件、然后再通过GUI运行升级。

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

现在、您可以通过GUI继续进行软件升级。

TR-4904：《使用Veritas Enterprise Vault配置StorageGRID》

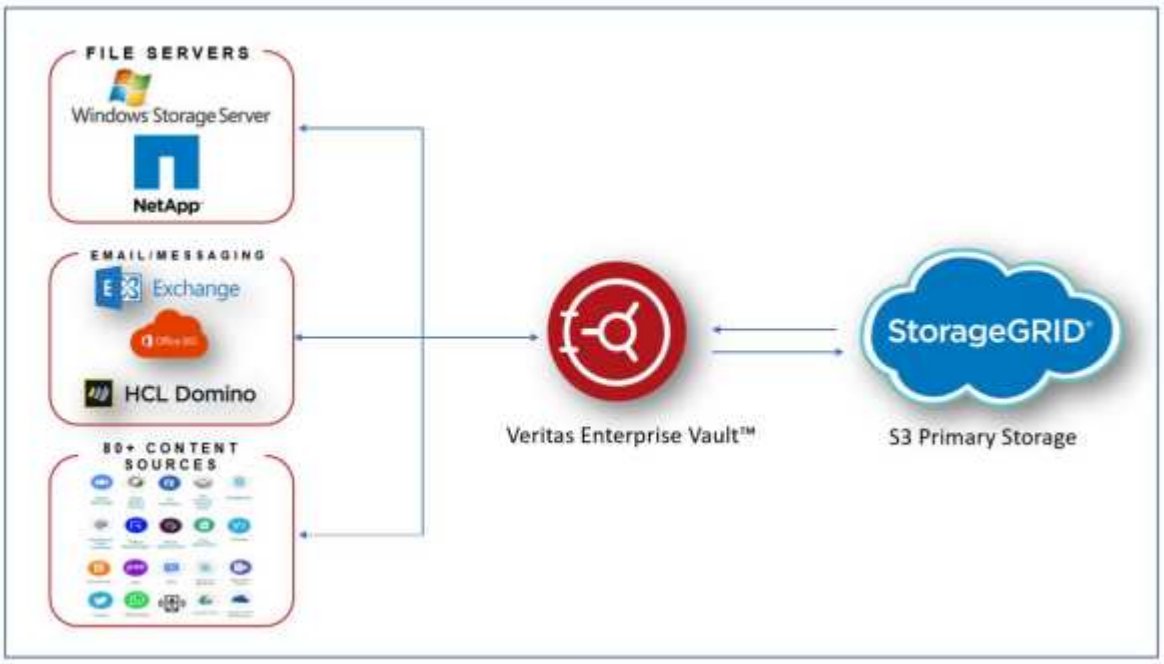
为站点故障转移配置StorageGRID简介

了解Veritas Enterprise Vault如何使用StorageGRID作为灾难恢复的主要存储目标。

本配置指南介绍了将NetApp®StorageGRID®配置为Veritas Enterprise Vault主存储目标的步骤。此外、还介绍了如何在灾难恢复(DR)情形下配置StorageGRID以实现站点故障转移。

参考架构

StorageGRID为Veritas Enterprise Vault提供了一个与S3兼容的内部云备份目标。下图展示了Veritas Enterprise Vault和StorageGRID架构。



从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- NetApp StorageGRID文档中心 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID支持 https://docs.netapp.com/us-en/storagegrid-enable/
- NetApp产品文档 https://www.netapp.com/support-and-training/documentation/

配置StorageGRID和Veritas Enterprise Vault

了解如何实施StorageGRID 11.5或更高版本以及Veritas Enterprise Vault 14.1或更高版本的基本配置。

本配置指南基于StorageGRID 11.5和Enterprise Vault 14.1。对于一次写入、使用S3对象锁定、StorageGRID 11.5和Enterprise Vault 14.2.2进行多次读取(WORM)模式存储。有关这些准则的更多详细信息、请参见 "StorageGRID 文档" 页面或联系StorageGRID专家。

配置StorageGRID和Veritas Enterprise Vault的前提条件

- 在使用Veritas Enterprise Vault配置StorageGRID之前、请验证以下前提条件：

> 对于WORM存储(对象锁定)、需要使用StorageGRID 11.5或更高版本。

- 已安装Veritas Enterprise Vault 14.1或更高版本。

> 对于WORM存储(对象锁定)、需要Enterprise Vault 14.2.2或更高版本。

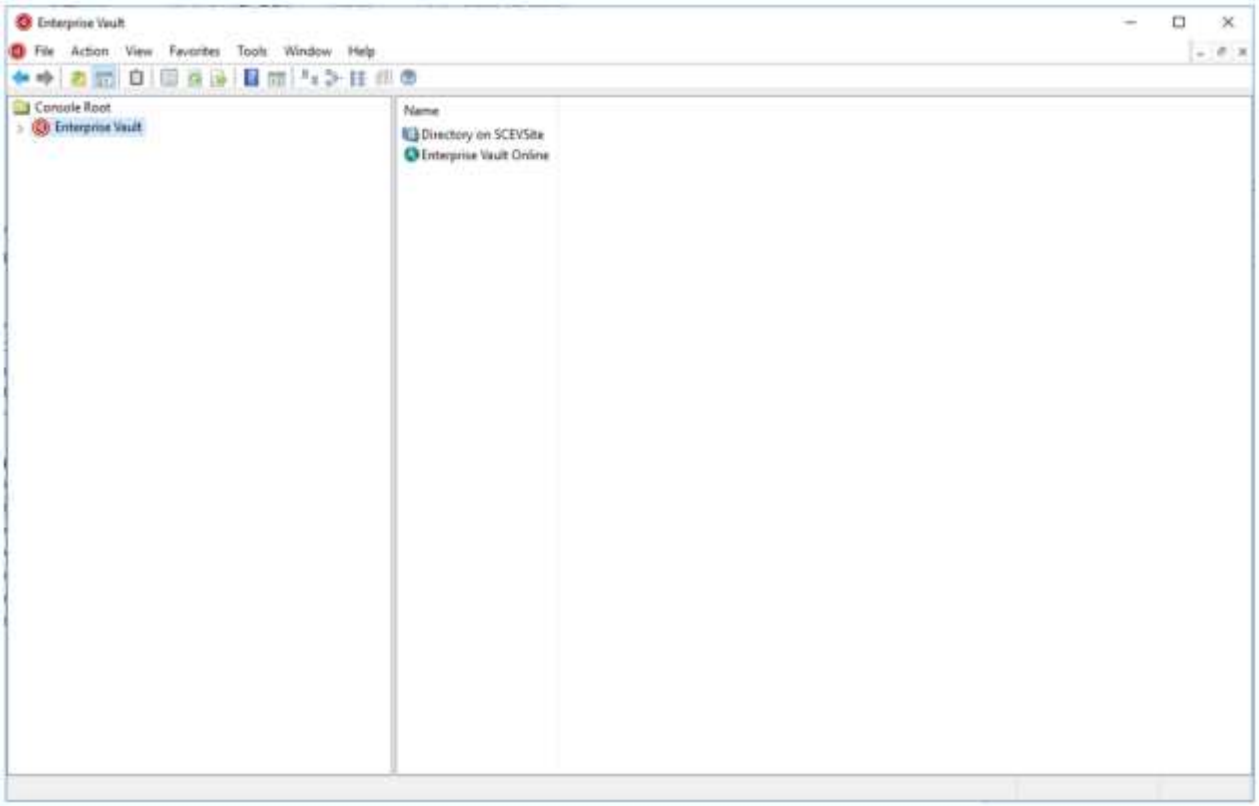
- 已创建存储组和存储存储。有关详细信息、请参见《Veritas Enterprise Vault管理指南》。
- 已创建StorageGRID租户、访问密钥、机密密钥和存储分段。
- 已创建StorageGRID负载平衡器端点(HTTP或HTTPS)。
- 如果使用自签名证书、请将StorageGRID自签名CA证书添加到企业存储服务器。有关详细信息，请参见此 "Veritas知识库文章"。
- 更新并应用最新的企业存储配置文件以启用受支持的存储解决方案、例如NetApp StorageGRID。有关详细信息，请参见此 "Veritas知识库文章"。

使用Veritas Enterprise Vault配置StorageGRID

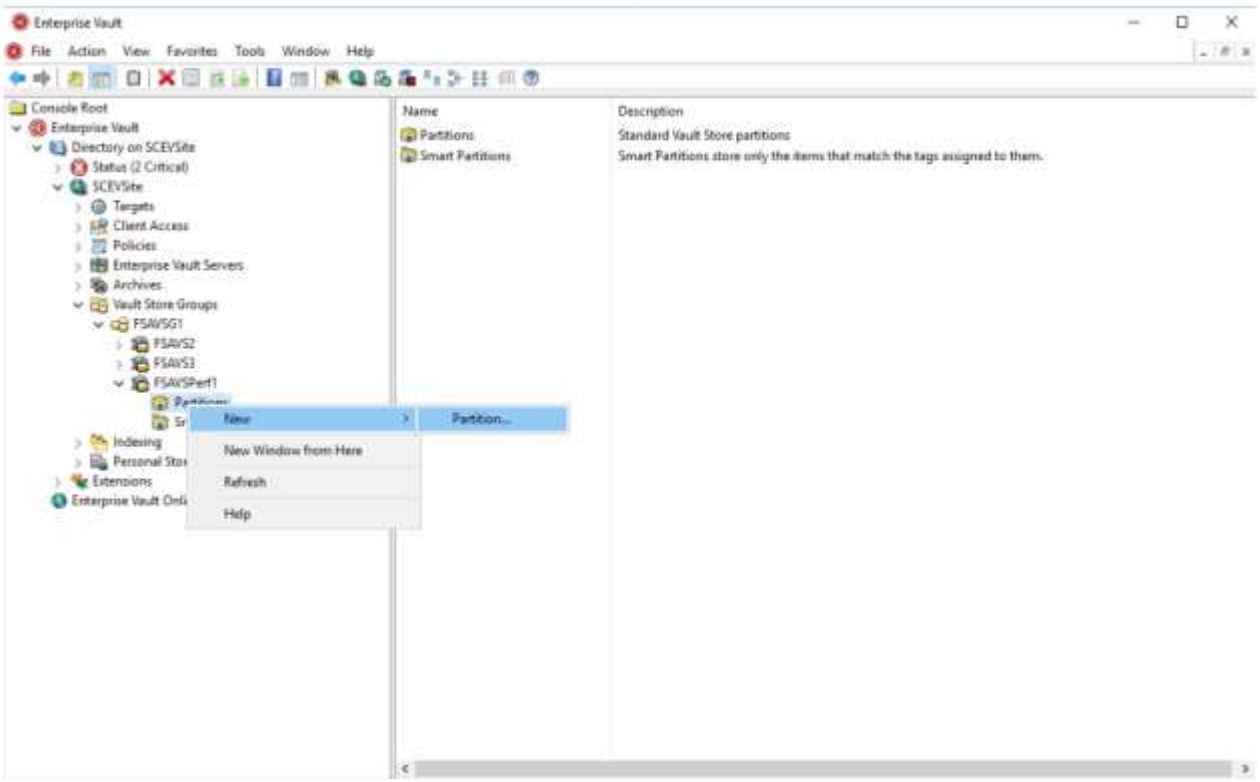
要使用Veritas Enterprise Vault配置StorageGRID、请完成以下步骤：

步骤

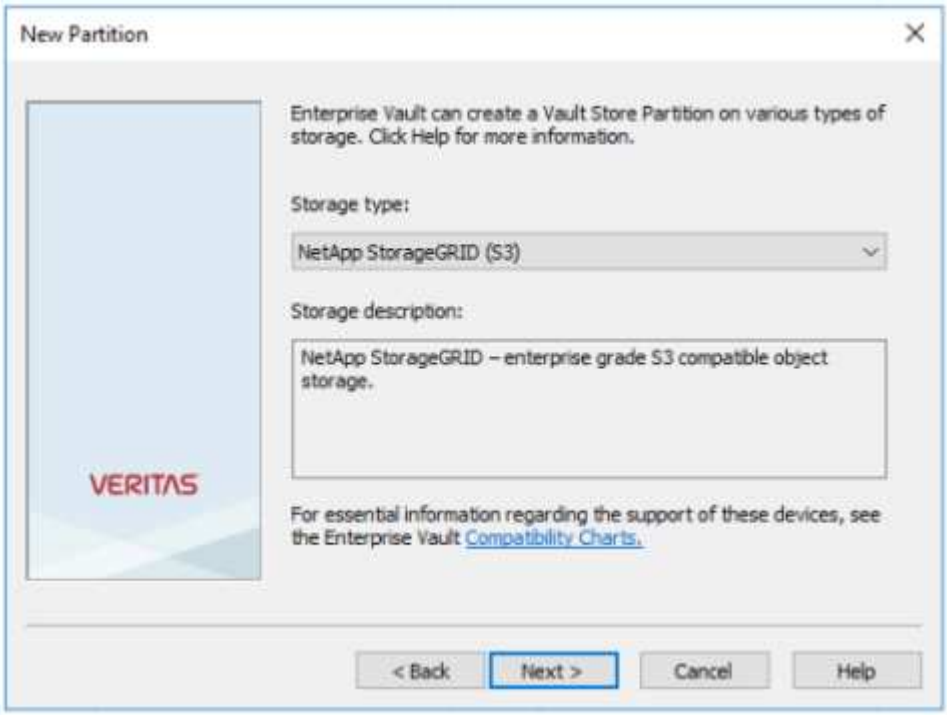
1. 启动Enterprise Vault管理控制台。



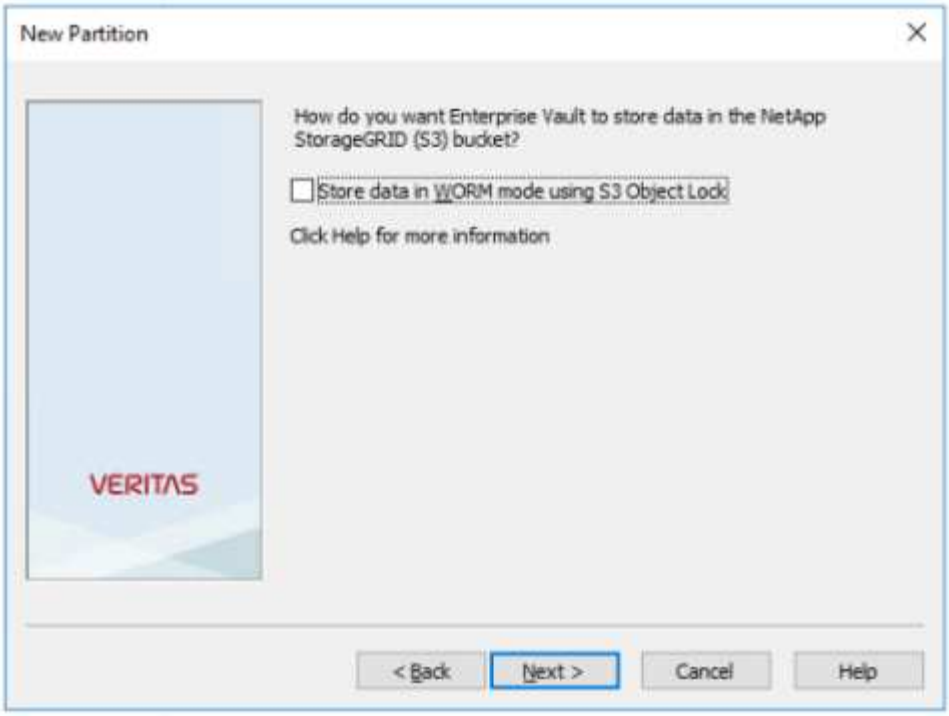
2. 在适当的存储库中创建新的存储分区。展开存储组文件夹、然后展开相应的存储。右键单击分区并选择菜单：新建[Partition (分区)]。



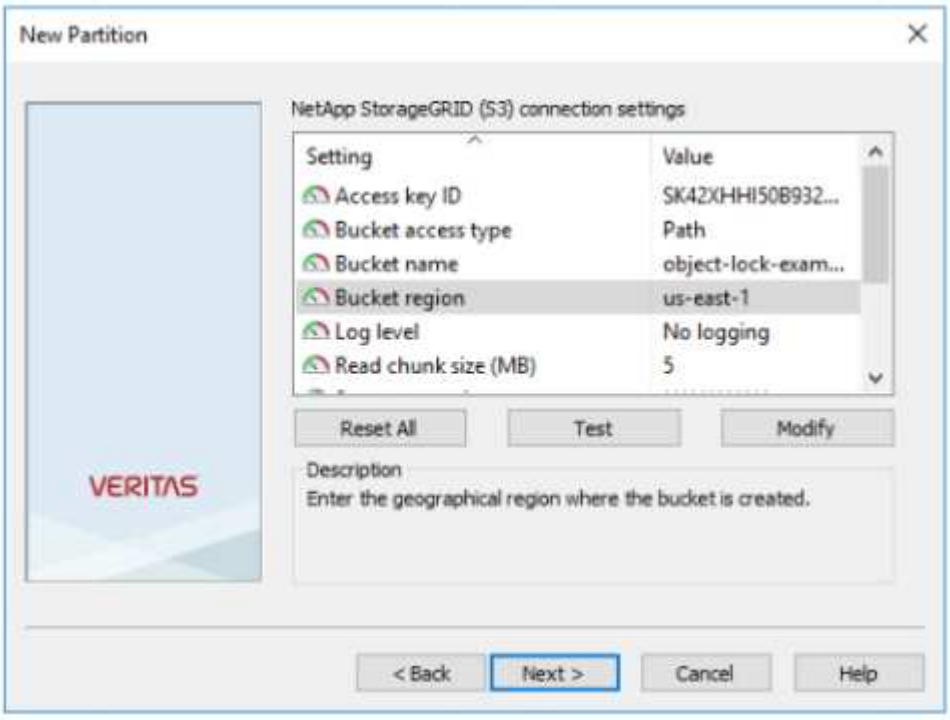
3. 按照新建分区创建向导进行操作。从存储类型下拉菜单中、选择NetApp StorageGRID (S3)。单击下一步。



4. 保持选中"Store Data in WORM Mode Using S3 Object Lock"(使用S3对象锁定在WORM模式下存储数据)选项。单击下一步。

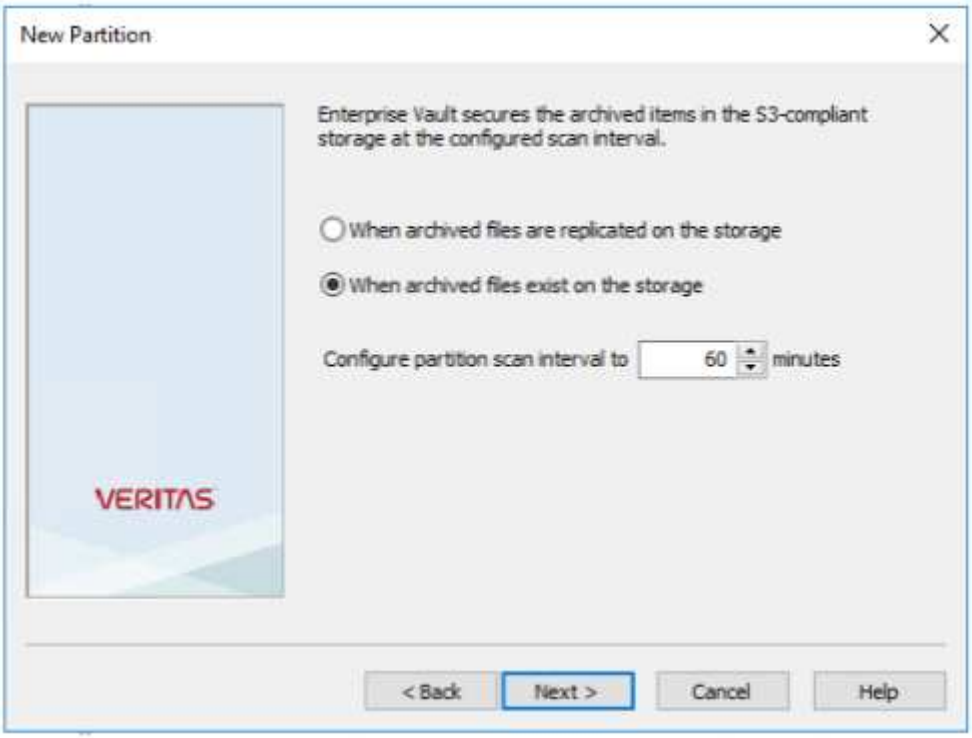


5. 在连接设置页面上、提供以下信息：
   - 访问密钥 ID
   - 机密访问密钥
   - 服务主机名称：确保包括在StorageGRID中配置的负载平衡器端点(LBE)端口(例如\https：//Data <hostname>：<LBE_port>)
   - 存储分段名称：预先创建的目标存储分段的名称。Veritas Enterprise Vault不会创建存储分段。
   - 存储分段区域： `us-east-1` 为默认值。

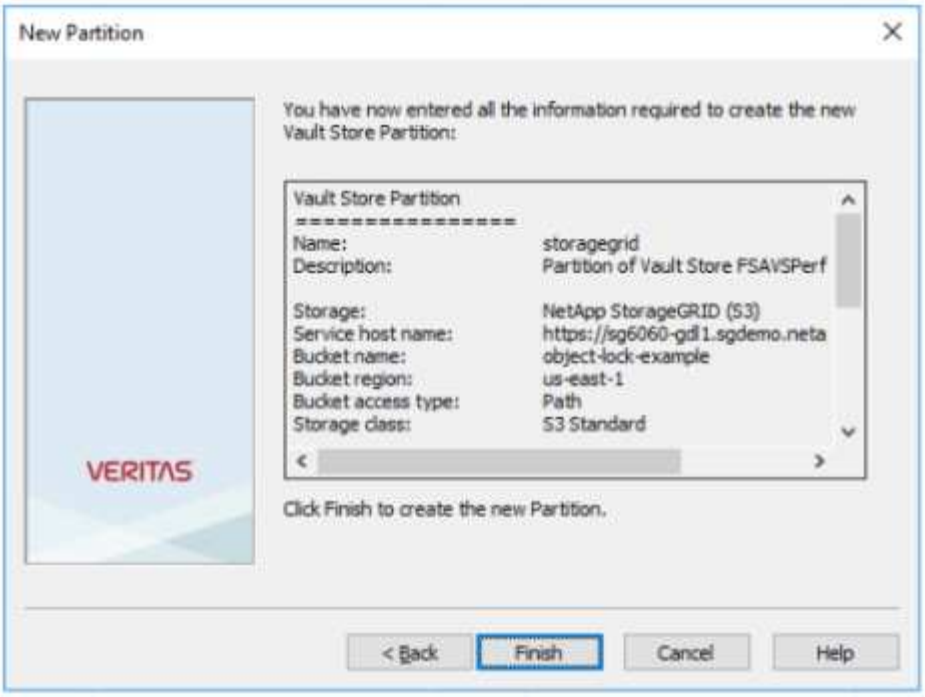


6. 要验证与StorageGRID存储分段的连接、请单击测试。验证连接测试是否成功。单击"OK"(确定)、然后单击"Next"(下一步)。

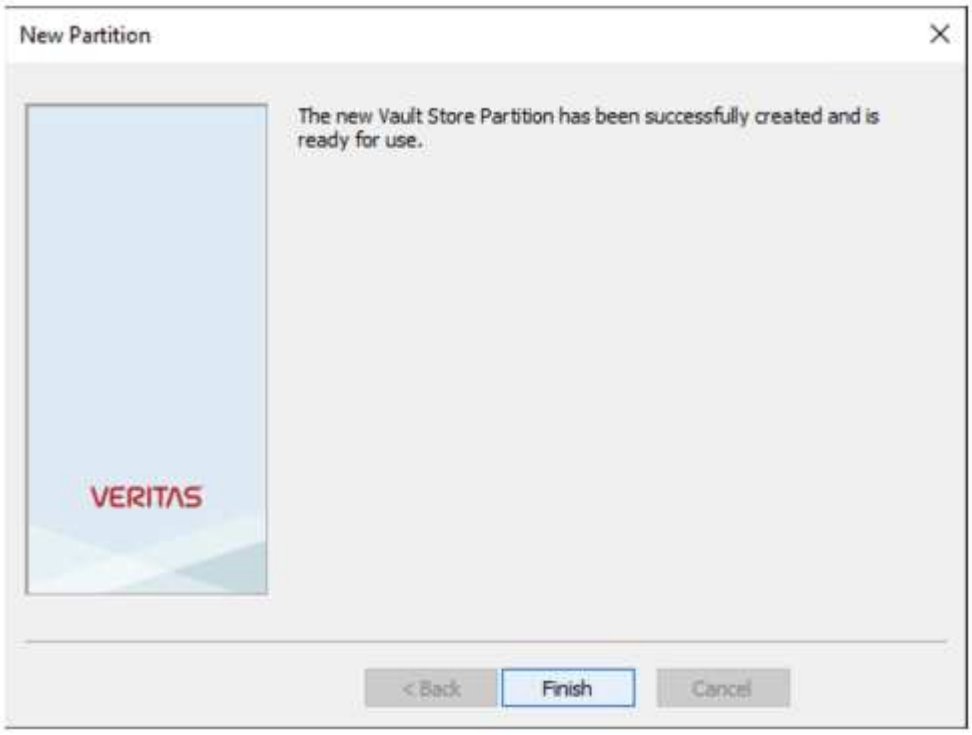
7. StorageGRID不支持S3复制参数。为了保护对象、StorageGRID使用信息生命周期管理(ILM)规则指定数据保护方案-多个副本或纠删编码。选择When Archived Files Existing on the Storage (存储上存在归档文件时)选项、然后单击Next (下一步)。



8. 验证摘要页面上的信息、然后单击完成。



9. 成功创建新的存储分区后、您可以在以StorageGRID作为主存储的企业存储中存档、还原和搜索数据。



为**WORM**存储配置**StorageGRID S3**对象锁定

了解如何使用S3对象锁定为WORM存储配置StorageGRID。

为WORM存储配置StorageGRID的前提条件

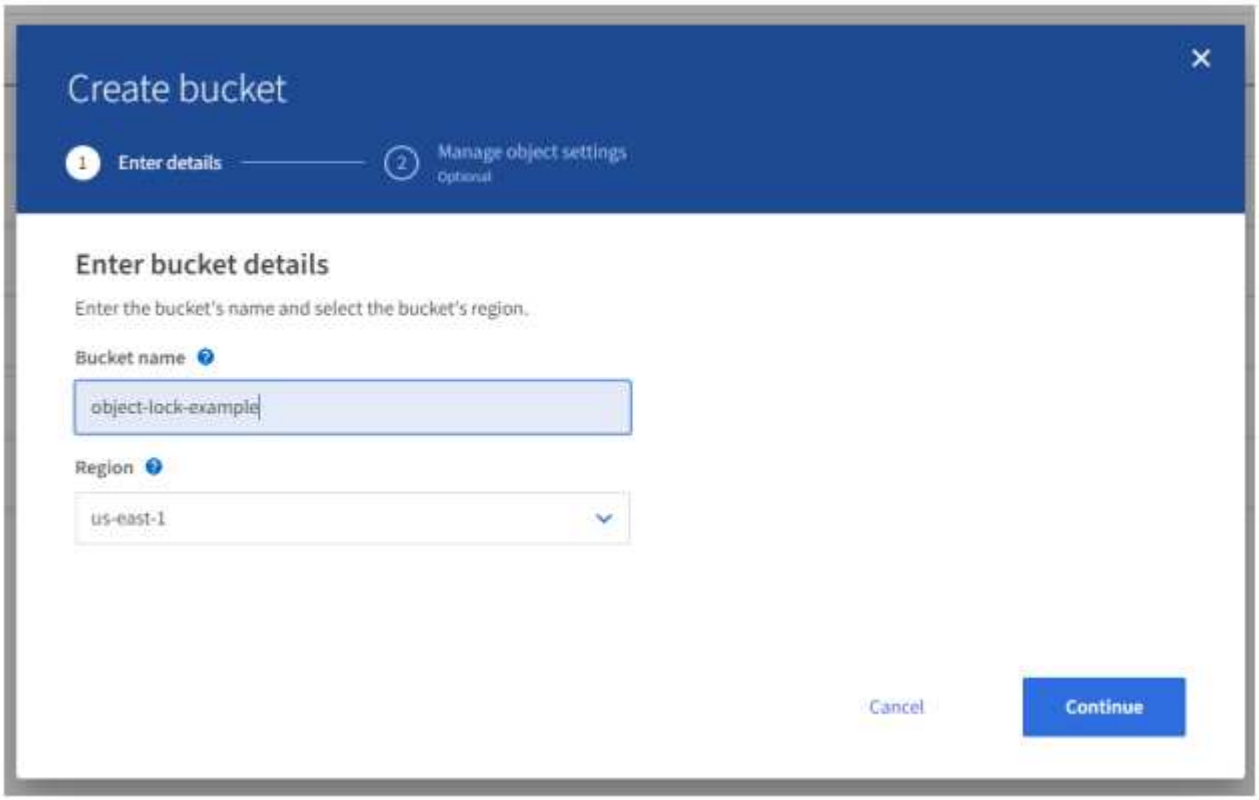
对于WORM存储、StorageGRID使用S3对象锁定来保留对象以满足合规性要求。这需要使用StorageGRID 11.5或更高版本、其中引入了S3对象锁定默认分段保留功能。Enterprise Vault还需要14.2.2或更高版本。

配置StorageGRID S3对象锁定默认分段保留

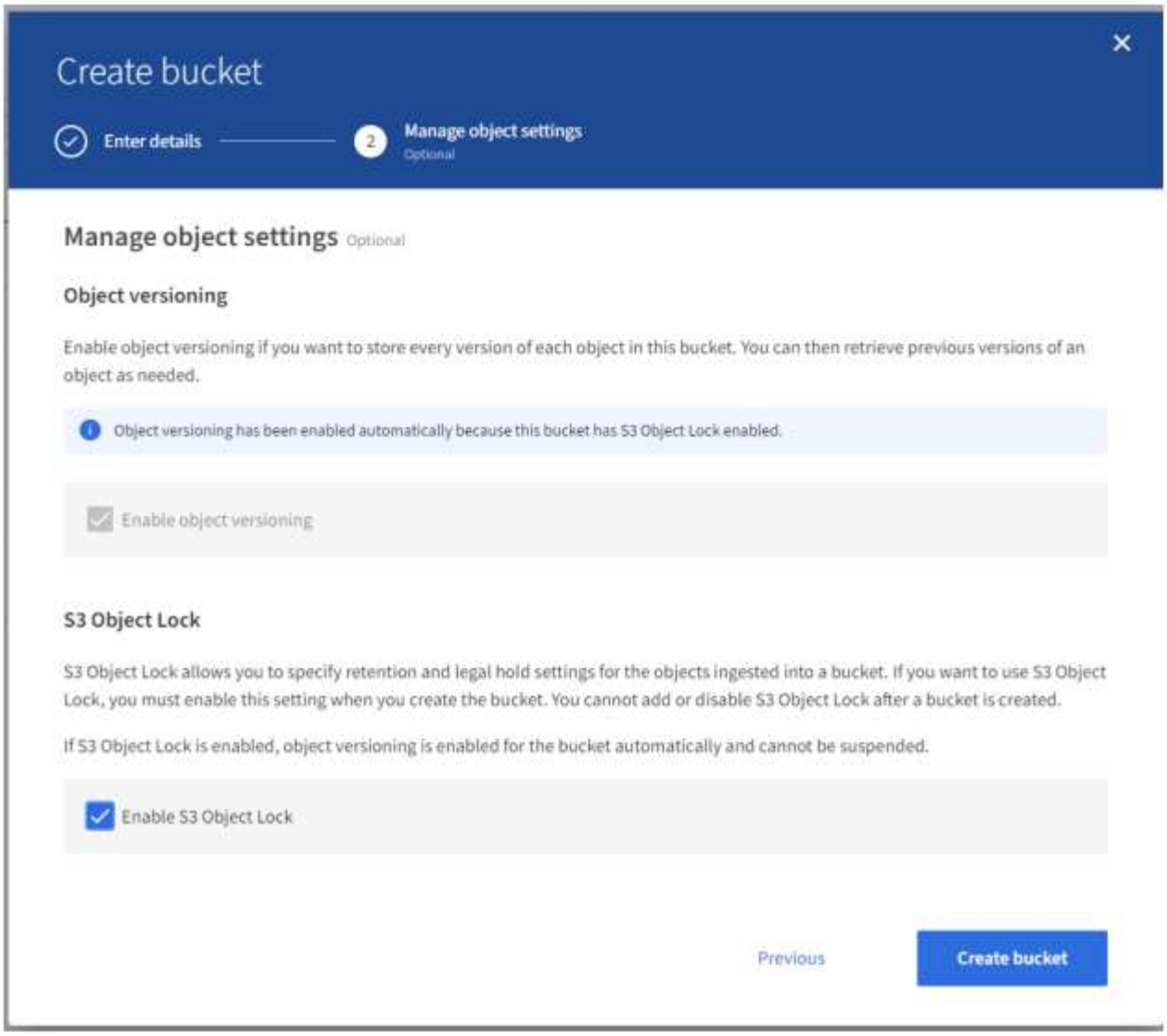
要配置StorageGRID S3对象锁定默认分段保留、请完成以下步骤：

步骤

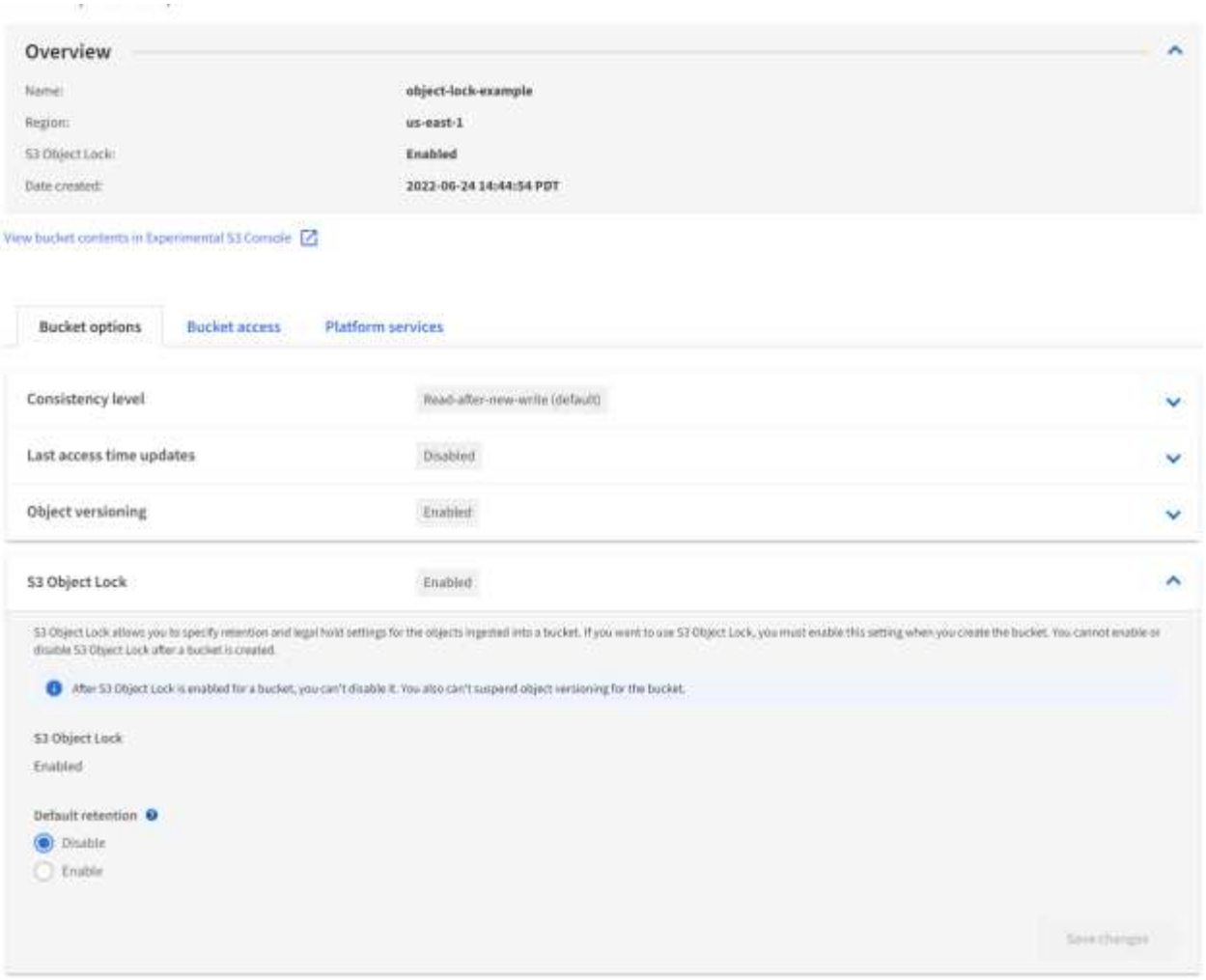
1. 在StorageGRID租户管理器中、创建存储分段、然后单击继续



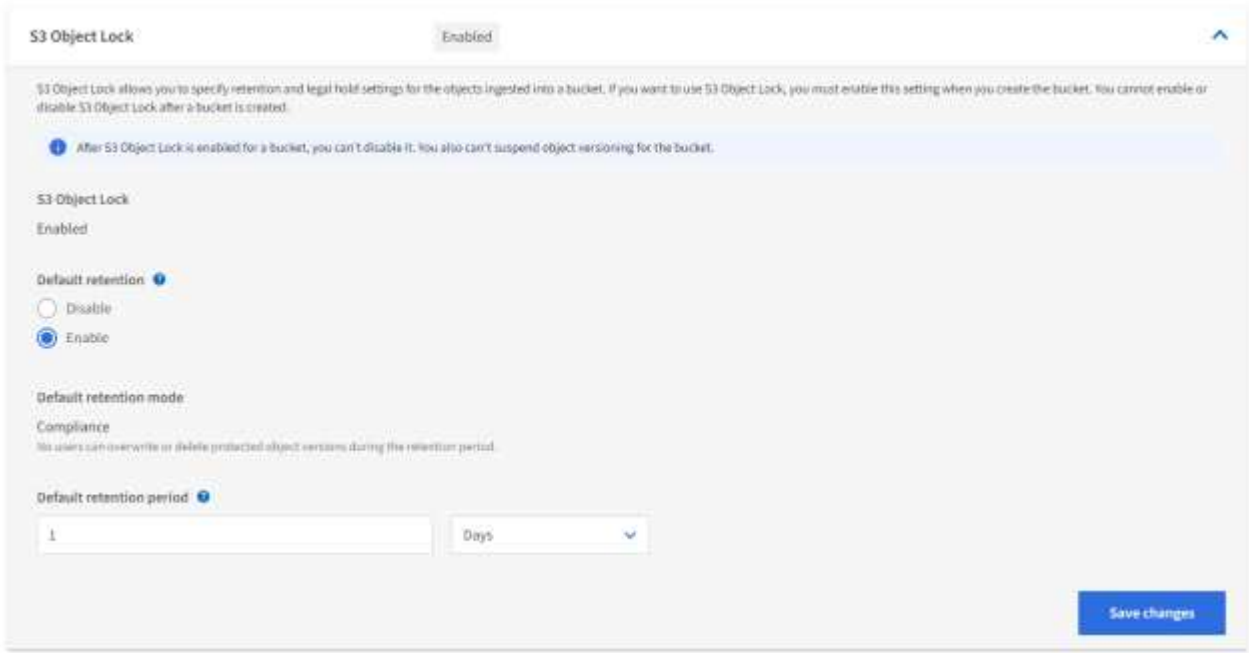
2. 选择Enable S3 Object Lock选项、然后单击Create Bucket.



3. 创建存储分段后、选择存储分段以查看存储分段选项。展开"S3 Object Lock"(S3对象锁定)下拉选项。



4. 在默认保留下、选择启用并设置默认保留期限1天。单击 Save Changes 。



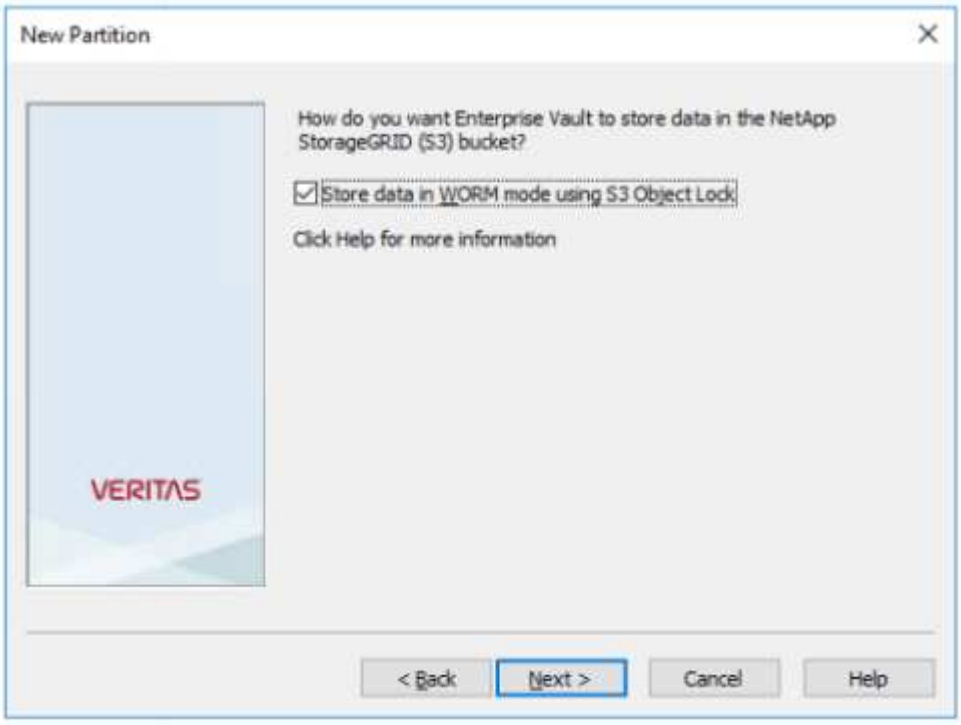
存储分段现已准备就绪、可供Enterprise Vault用来存储WORM数据。

配置Enterprise Vault

要配置Enterprise Vault、请完成以下步骤：

步骤

1. 重复部分中的步骤1-3 "基本配置" 、但这次选择使用S3对象锁定在WORM模式下存储数据选项。单击下一步。



2. 输入S3存储分段连接设置时、请确保输入的S3存储分段的名称已启用S3对象锁定默认保留。
3. 测试连接以验证设置。

配置StorageGRID站点故障转移以实现灾难恢复

了解如何在灾难恢复场景中配置StorageGRID站点故障转移。

StorageGRID架构部署通常采用多站点模式。站点可以是主动-主动站点、也可以是主动-被动站点、用于灾难恢复。在灾难恢复场景中、请确保Veritas Enterprise Vault能够保持与其主存储(StorageGRID)的连接、并在站点发生故障期间继续导入和检索数据。本节简要介绍了双站点主动-被动部署的配置指导。 有关这些准则的详细信息、请参见 "StorageGRID 文档" 页面或联系StorageGRID专家。

使用Veritas Enterprise Vault配置StorageGRID的前提条件

在配置StorageGRID站点故障转移之前、请验证以下前提条件：

- 有一个双站点StorageGRID部署；例如、Site1和Site2。
- 已在每个站点上创建一个运行负载平衡器服务的管理节点或一个网关节点来实现负载平衡。

- 已创建StorageGRID负载平衡器端点。

配置StorageGRID站点故障转移

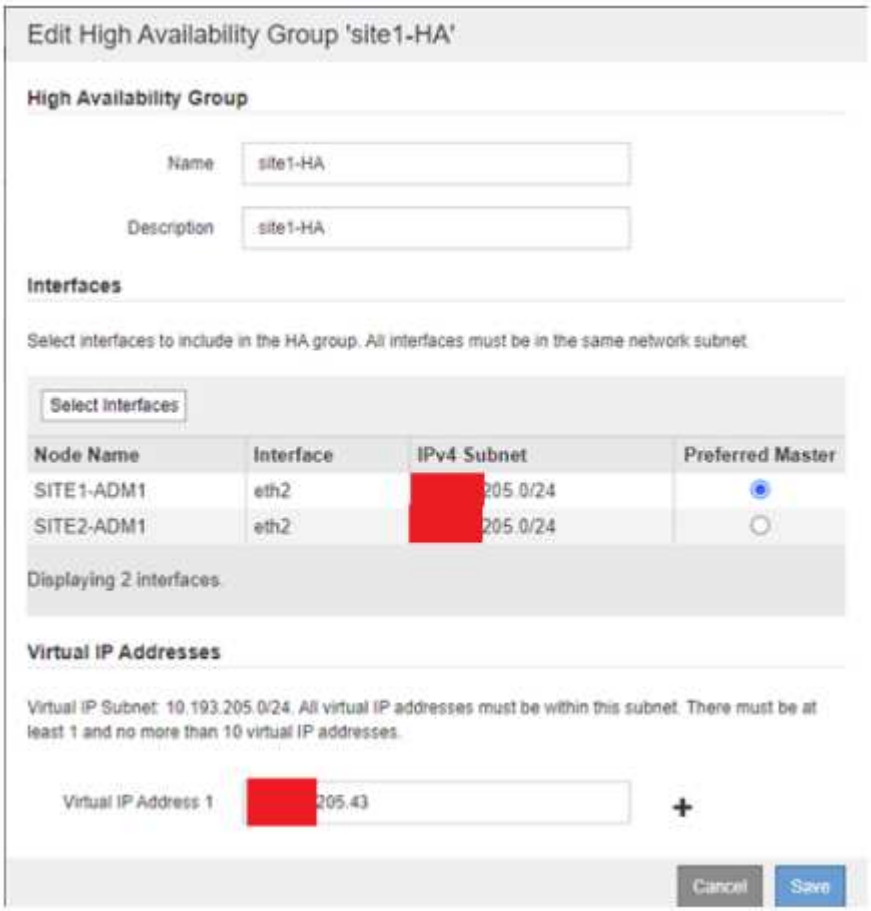
要配置StorageGRID站点故障转移、请完成以下步骤：

步骤

1. 要确保在站点出现故障期间连接到StorageGRID、请配置高可用性(HA)组。在StorageGRID网格管理器界面(GMI)中、单击配置、高可用性组和+创建。

   [veritas/veritas-cree-high-availability组]

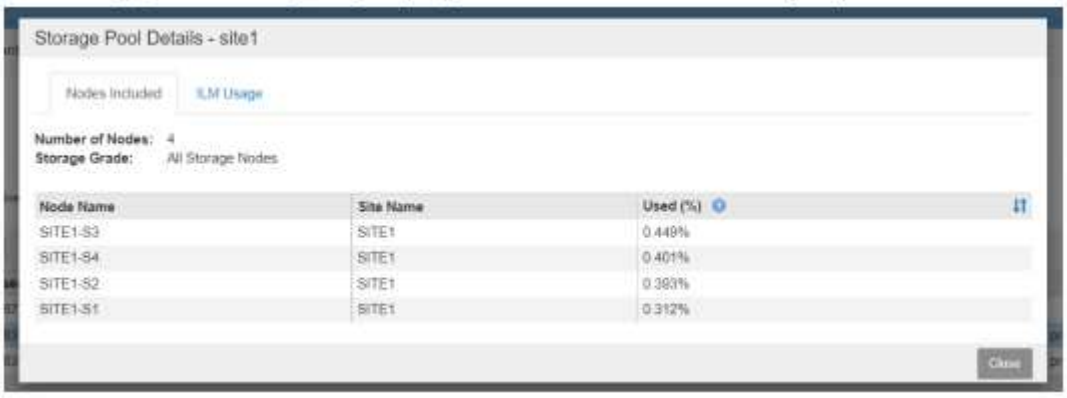
2. 输入所需信息。单击Select Interfaces"(选择接口)、并包括Site1和Site2的网络接口、其中Site1 (主站点)是首选主站点。在同一子网中分配一个虚拟IP地址。单击保存。

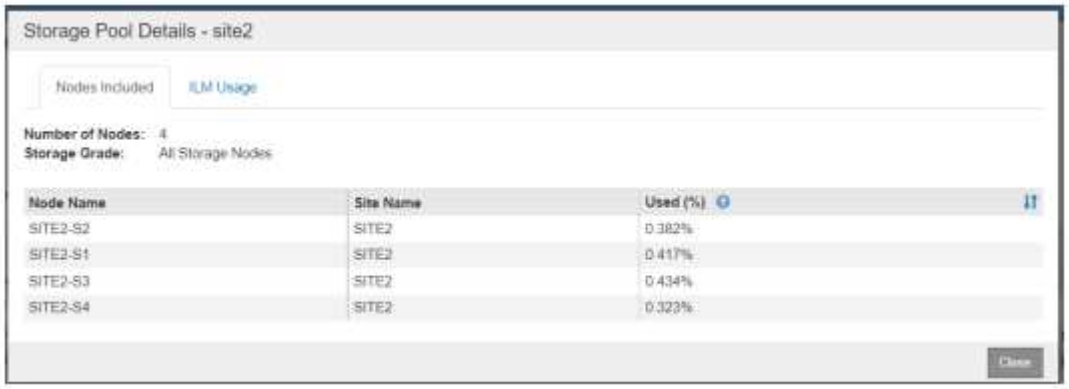


3. 此虚拟IP (VIP)地址应与Veritas Enterprise Vault分区配置期间使用的S3主机名相关联。VIP地址将流量解析为Site1、在Site1发生故障期间、VIP地址会将流量透明地重新路由到Site2。
4. 确保将数据复制到站点1和站点2。这样、如果Site1发生故障、则仍可从Site2访问对象数据。这是通过首先配置存储池来实现的。

   在StorageGRID GMI中、单击"ILM、Storage Pools"(ILM、存储池)、然后单击+"Cree"(创建)。按照向导创建两个存储池：一个用于Site1、另一个用于Site2。

   存储池是节点的逻辑分组、用于定义对象放置





5. 在StorageGRID GMI中、单击"ILM、规则"、然后单击+创建。按照向导中的说明创建ILM规则、为每个站点指定一个要存储的副本、并将其导出行为设置为平衡。

6. 将ILM规则添加到ILM策略中并激活此策略。

此配置会产生以下结果：

- 一种虚拟S3端点IP、其中Site1为主端点、Site2为二级端点。如果Site1发生故障、VIP将故障转移到Site2。
- 从Veritas Enterprise Vault发送归档数据时、StorageGRID可确保一个副本存储在Site1中、另一个DR副本存储在Site2中。如果站点1发生故障、Enterprise Vault将继续从站点2进行加网和检索。

> 这两种配置对于Veritas Enterprise Vault是透明的。S3端点、存储分段名称、访问密钥等均相同。无需在Veritas Enterprise Vault分区上重新配置S3连接设置。

访问StorageGRID评估软件的步骤

本说明面向与NetApp合作的NetApp销售人员、合作伙伴和潜在客户。

注册帐户

1. 使用您的业务电子邮件在上注册帐户 "NetApp 支持站点" 。
   a. 确保您未使用新创建的帐户登录。
   b. 如果您已有帐户、请确保您未登录、然后继续下一步。
2. 创建非技术支持案例、将访问级别提升到"潜在客户"。要执行此操作、请单击 ""报告问题"网站页脚中的""链接。
3. 选择"注册问题"作为反馈类别。
4. 在"注释"部分中、写下："我的帐户电子邮件地址是_您的电子邮件地址_。我希望获得潜在客户访问权限、以下载StorageGRID评估软件。"
   a. 提及建议潜在客户访问请求的NetApp内部人员的姓名。

下载StorageGRID

1. 在您的支持案例经过审核和批准后、NetApp支持部门将通过电子邮件通知您、您的帐户已获得潜在客户访问权限。
2. 下载 "StorageGRID评估软件"。

此Eval许可证文件位于此zip文件中。解压缩后、文件名称为StorageGRID-WebScale <version>\vSphere NLF000000.txt。

下载软件是一个涉及贸易合规措施以遵守法律要求的过程。为了确保合规性、用户必须先创建帐户并创建支持案例、然后才能获得访问权限。此流程有助于我们保持适当的控制和文档记录、同时为潜在客户提供他们所需的生产就绪软件。

我们提供StorageGRID的"生产就绪"版本、它不是开源版本或替代版本。需要注意的是，除非潜在客户升级到生产许可证，否则不提供*支持*。

如在上述步骤中遇到任何问题、请联系StorageGRID.Feedback@netapp.com。

NetApp StorageGRID 博客

您可以在此处找到一些很棒的NetApp StorageGRID 博客：

- 2024年2月16日： "StorageGRID 11.8:增强的安全性、精简性和用户体验"
- 2024年2月16日： "隆重推出StorageGRID 11.8."
- 2024年2月2日： "隆重推出StorageGRID + lle可 意FS解决方案简介"
- 2023年12月12日： "基于StorageGRID的大数据分析：德罗米奥的性能是Apache Hive的23倍"
- 2023年11月7日： "采用StorageGRID的光谱逻辑在本机Glacier"
- 2023年10月17日： "从Hadoop继续发展：借助德米奥和StorageGRID打造现代化数据分析"
- 2023年9月1日： "利用Cloud Insights使用Fluent Bit监控和收集日志"
- 2023年8月30日： "Amazon S3文件系统的装载点现已正式发布"
- 2023年5月16日： "介绍StorageGRID 11.7和全新全闪存对象存储设备GF6112"
- 2023年5月16日： "StorageGRID对象存储系列中的新增功能"
- 2023年3月30日： "适用于采用StorageGRID 的Amazon S3 alpha版本的挂载点"
- 2023年3月30日： "使用BlueXP通过符合3：2：1的备份策略保护Epic EHR"
- 2023年3月14日： "如何在符合3：2：1的架构中使用一个命令备份Epic Systems EHR数据库"
- 2023年2月14日： "巧克力、滑板、表和大型机有哪些共同之处？"
- 2023年1月18日： "StorageGRID S3对象锁定已通过Veritas NetBackup的验证"
- 2023年1月16日： "StorageGRID 续订了NF203和ISO/IEC 25051合规性认证"
- 2022年12月6日： "StorageGRID 获得KPMG合规认证"
- 2022年11月23日： "利用由NetApp和Modzy提供支持的MLOps实现可解释的人工智能"
- 2022年11月7日： "StorageGRID 和ONTAP S3支持：差异、相似之处和集成"
- 2022年10月5日： "NetApp Cloud Insights 增加了StorageGRID 库信息板"
- 2022年10月5日： "在StorageGRID for Snowfl您 的数据上除以数据"
- 2022年9月26日： "适用于服务提供商的NetApp StorageGRID"
- 2022年9月19日： "适用于StorageGRID 的DataLock和勒索软件保护支持"
- 2022年9月1日： "请采用这些指标并绘制图表"
- 2022年8月23日： "在StorageGRID 上构建数据湖"
- 2022年8月17日： "所有操作都从对象锁定…开始 为关键备份应用程序构建S3存储生态系统"
- 2022年8月16日： "将StorageGRID 与开源ELK堆栈相集成以增强客户体验"
- 2022年8月5日： "NetApp StorageGRID 获得通用标准安全认证"
- 2022年7月26日： "查看不断增长的经验证的StorageGRID合作伙伴解决方案列表"
- 2022年6月9日： "将Cloudera Hadoop S3A连接器与StorageGRID 结合使用"
- 2022年5月26日： "StorageGRID：存储和管理内部备份和复制数据"

- 2022年5月24日： "借助NetApp和Alluio打造现代化的分析工作负载"
- 2022年5月10日： "Lab on Demand是StorageGRID的最佳销售工具"

NetApp StorageGRID 文档

您可以在此处找到每个NetApp StorageGRID 版本的完整文档：

- "StorageGRID设备"
- "StorageGRID"
- "StorageGRID 11.8."
- "StorageGRID 11.7"
- "StorageGRID 11.6."
- "StorageGRID 11.5"
- "StorageGRID 11.4."
- "StorageGRID 11.3"
- "StorageGRID 11.2"

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

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

商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 NetApp 、 Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

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

专利

有关 NetApp 拥有的专利的最新列表，请访问：

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

隐私政策

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

开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

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

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