如何在您的环境中启用StorageGRID

How to enable StorageGRID in your environment

NetApp
March 07, 2024

目录

如何在您的环境中启用StorageGRID

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 11.8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
- 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 11.7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
- 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 11.6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

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使用Amazon OpenSearch服务或内部Elasticsearch配置NetApp StorageGRID 11.6搜索集成服务。

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"。

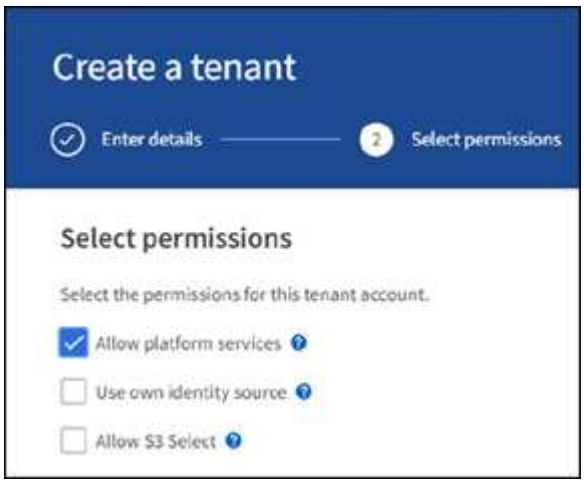
本文档是对的补充 "《StorageGRID 11.6租户指南》" 和为搜索集成服务的端点和存储分段配置提供了分步说明和示例。此处提供的Amazon Web Services (AWS)或内部Elasticsearch设置说明仅用于基本测试或演示。

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

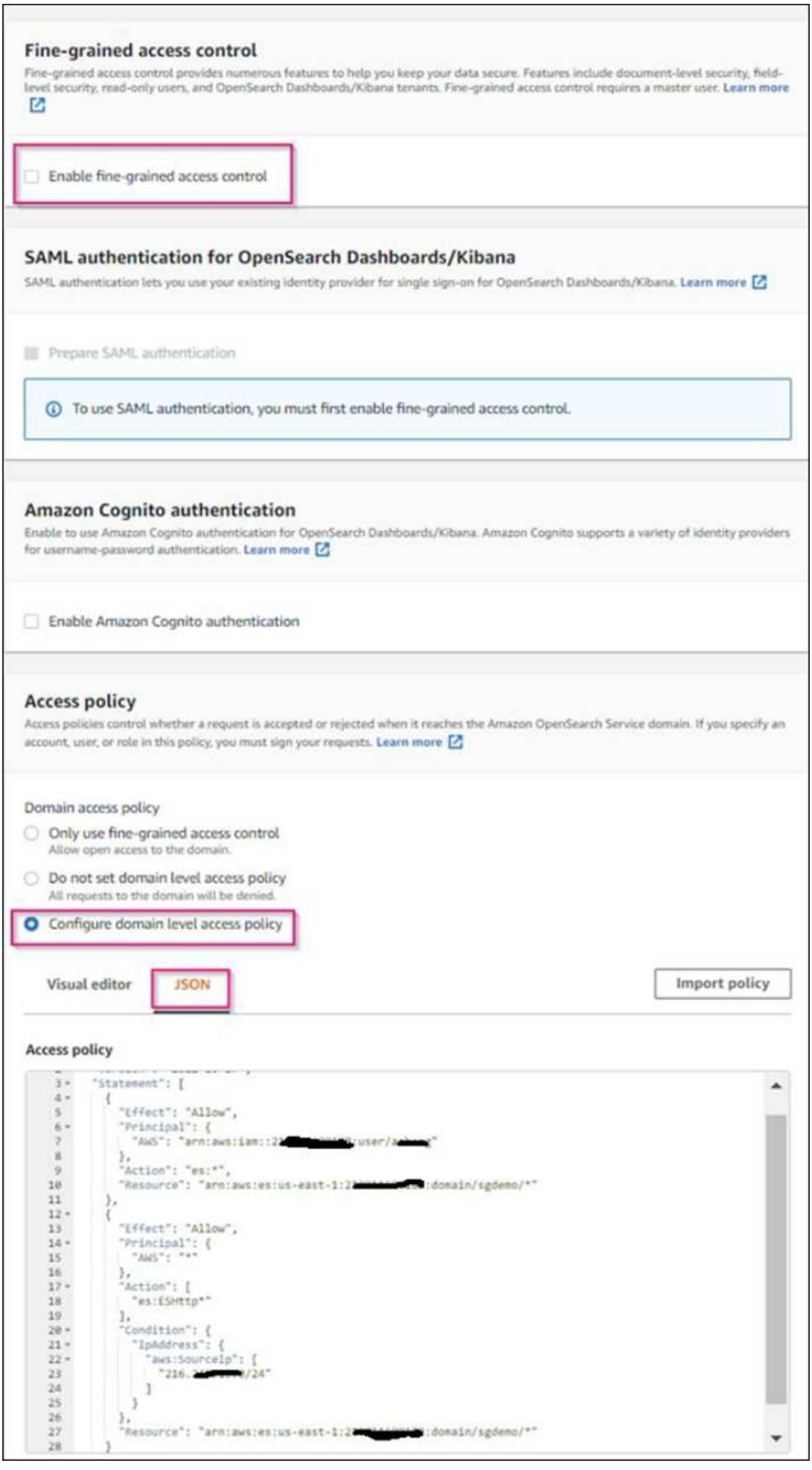
Amazon OpenSearch (以前称为Elasticsearch)服务设置

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。

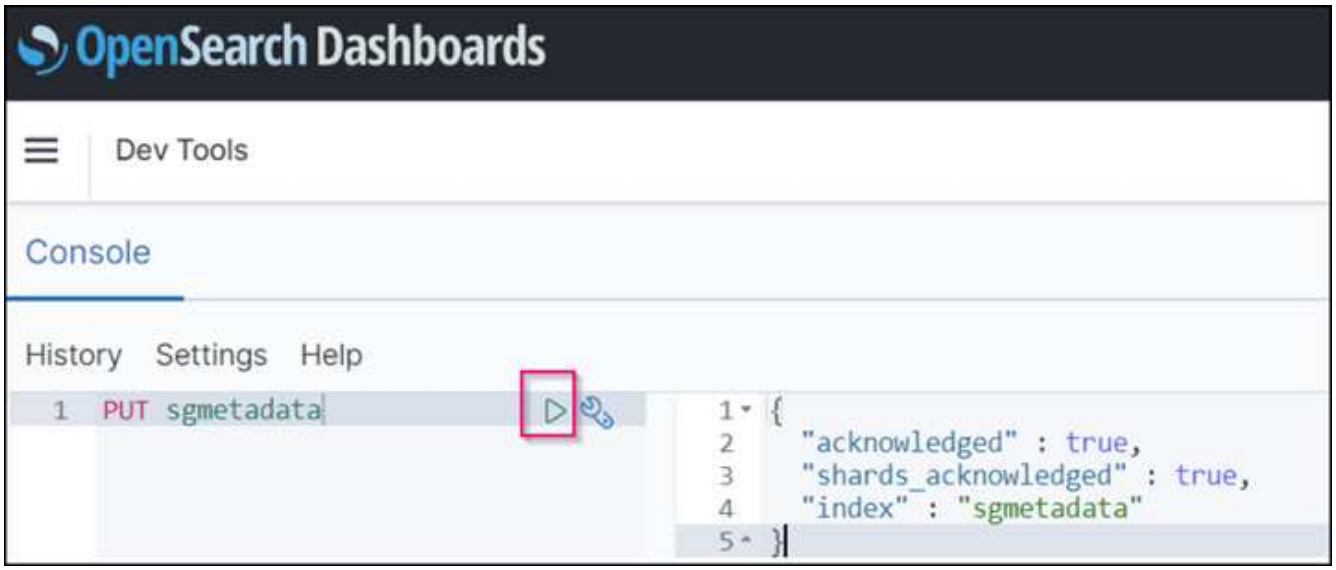
1. 按照中的说明创建新域 "AWS OpenSearch服务入门"、但以下情况除外：
   - 第 4 步域名：sgdemo
   - 第10步：细化访问控制：取消选择启用细化访问控制选项。
   - 第12步：访问策略：选择配置级别访问策略、然后选择JSON选项卡以使用以下示例修改访问策略：
     - 将突出显示的文本替换为您自己的AWS身份和访问管理(IAM) ID和用户名。
     - 将突出显示的文本(IP地址)替换为用于访问AWS控制台的本地计算机的公有 IP地址。
     - 打开浏览器选项卡以 "https://checkip.amazonaws.com" 以查找公有 IP。

```
{

    "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/*"
        }
    ]
}
```

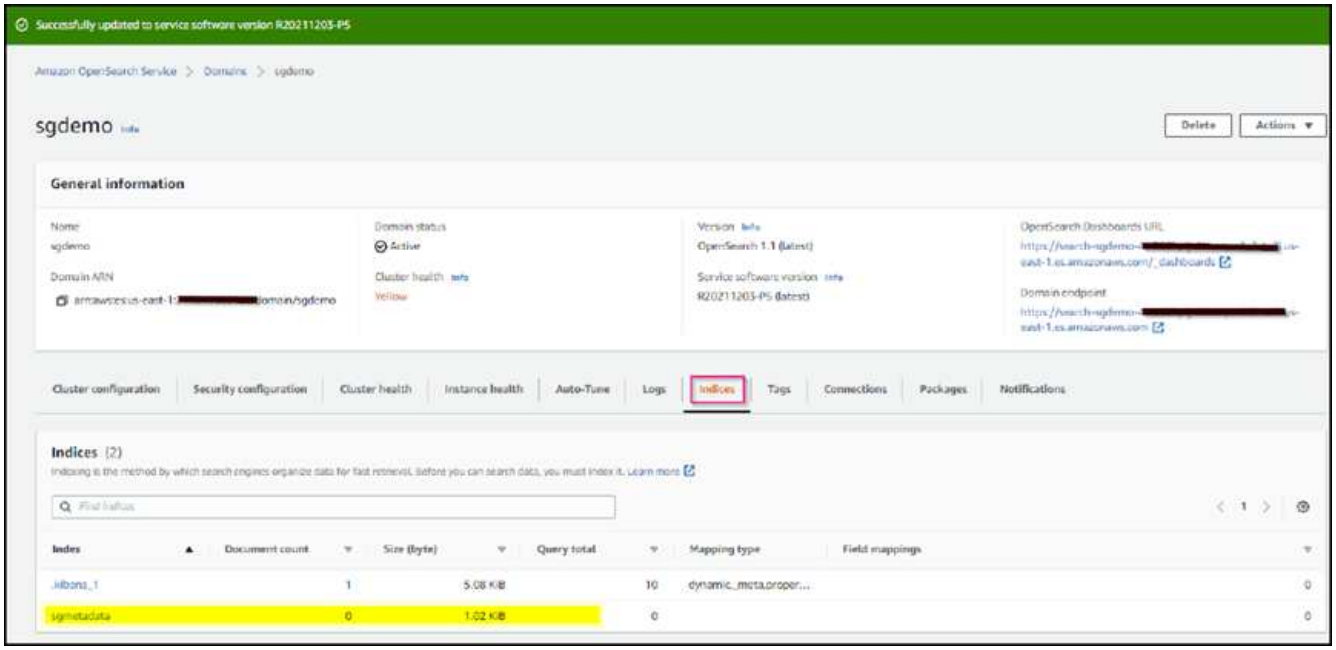

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more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

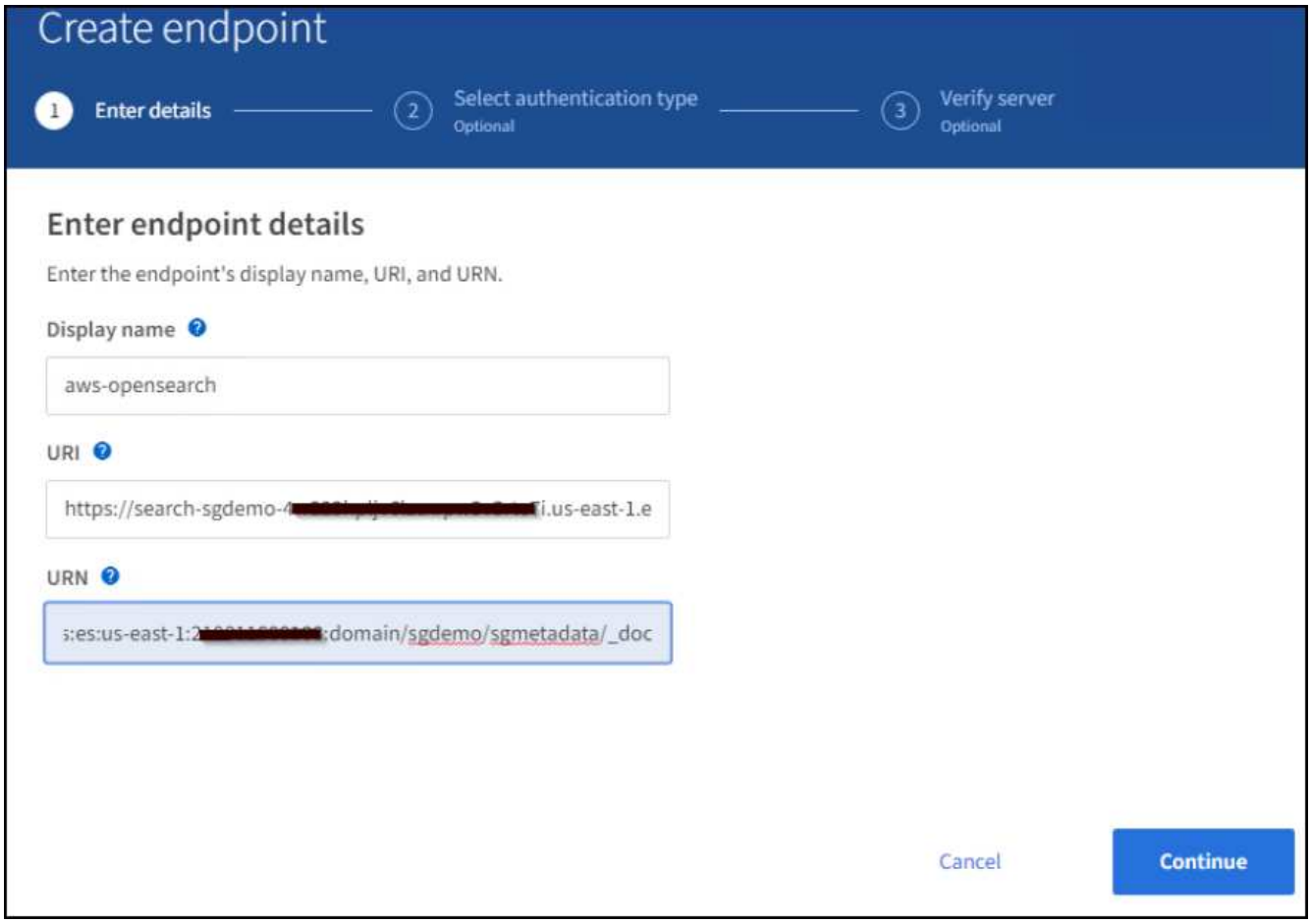


平台服务端点配置

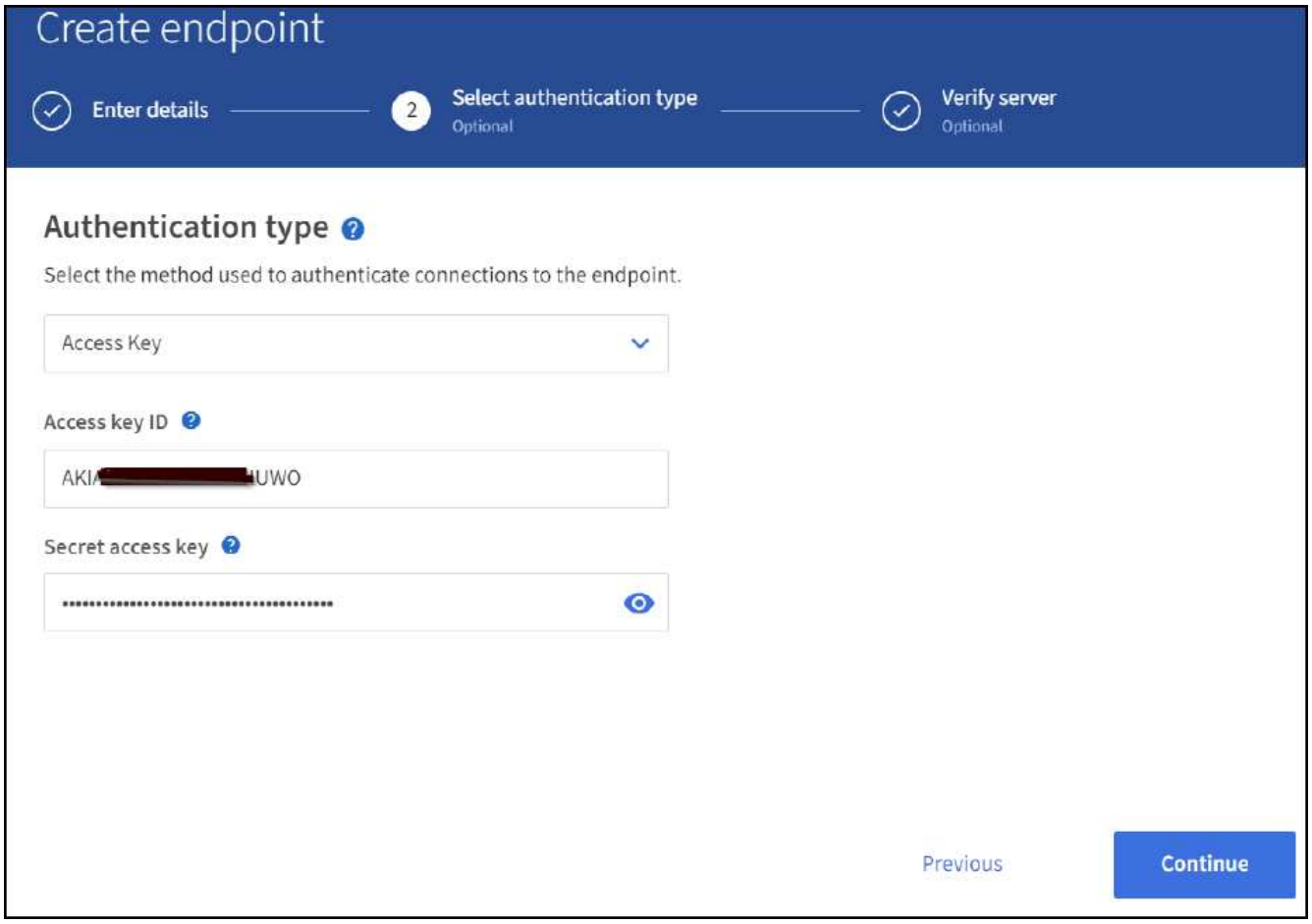
要配置平台服务端点、请执行以下步骤：

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。

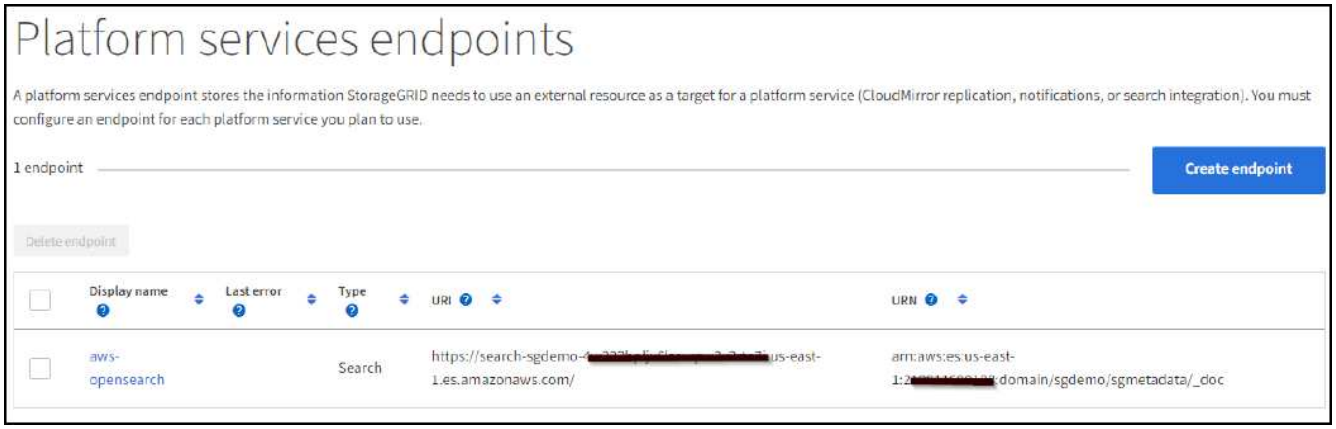
     在此示例中、URN变为`arn：AWS：es：us-east-1：211234567890：domain/sgdemo /sgmedata/_doc`。



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.

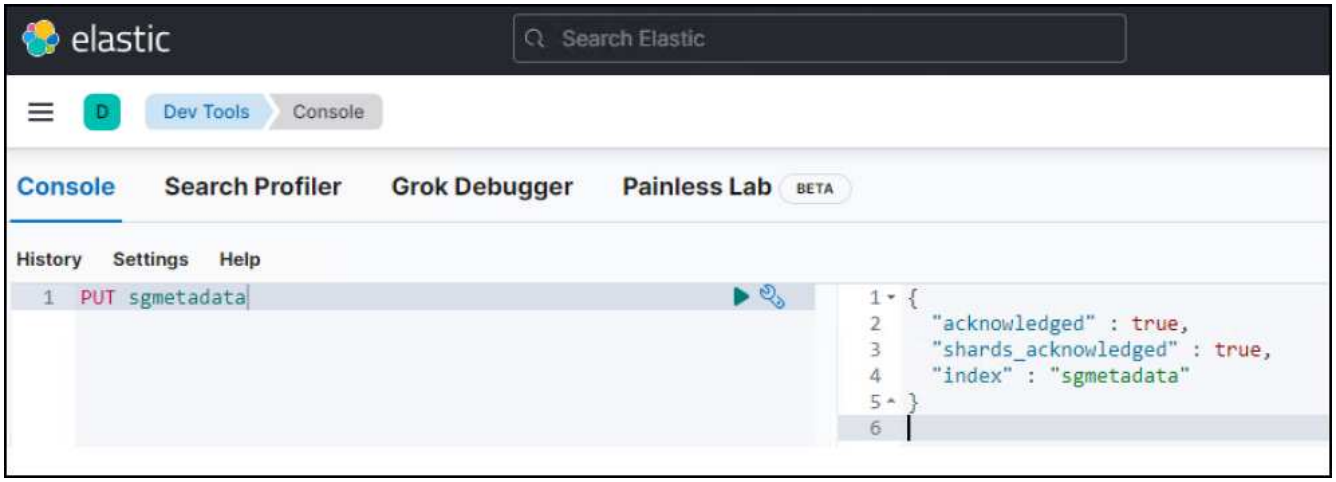
1. In a new terminal session, run:

```
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.

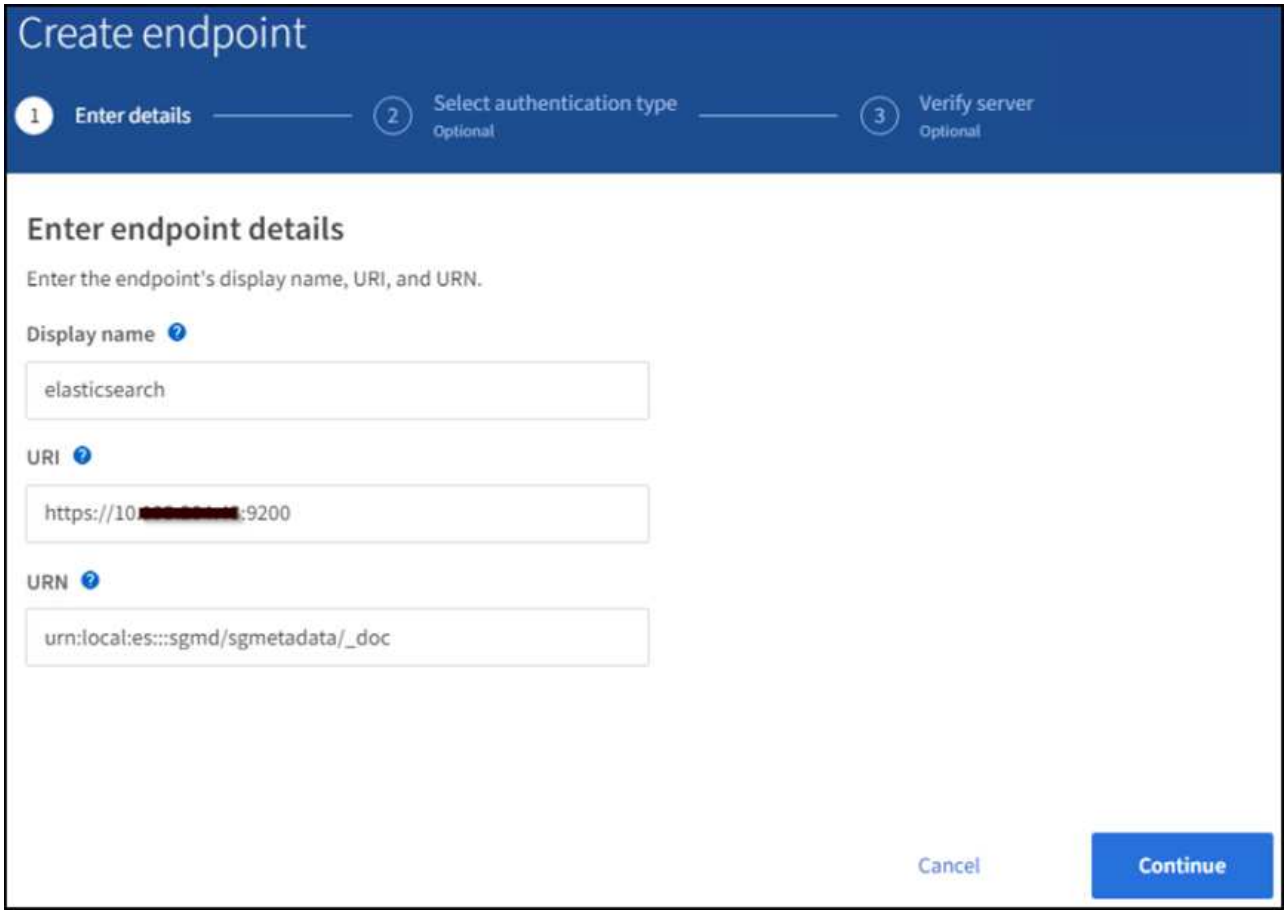
3. 启动Kibana Docker容器后、控制台中将显示URL链接`\https://0.0.0.0:5601`。将0.0.0.0替换为URL中的服务器IP地址。
4. 使用用户名`弹性`和Elastic在上一步中生成的密码登录到Kibana UI。
5. 首次登录时、请在信息板欢迎页面上选择"Explore on your own"。从菜单中、选择"Management">"Dev Tools"。
6. 在开发工具控制台屏幕上、输入`PUT <index>`、在此可以使用此索引存储StorageGRID 对象元数据。我们在此示例中使用索引名称`sgmetadata`。单击小三角形符号以执行PUT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



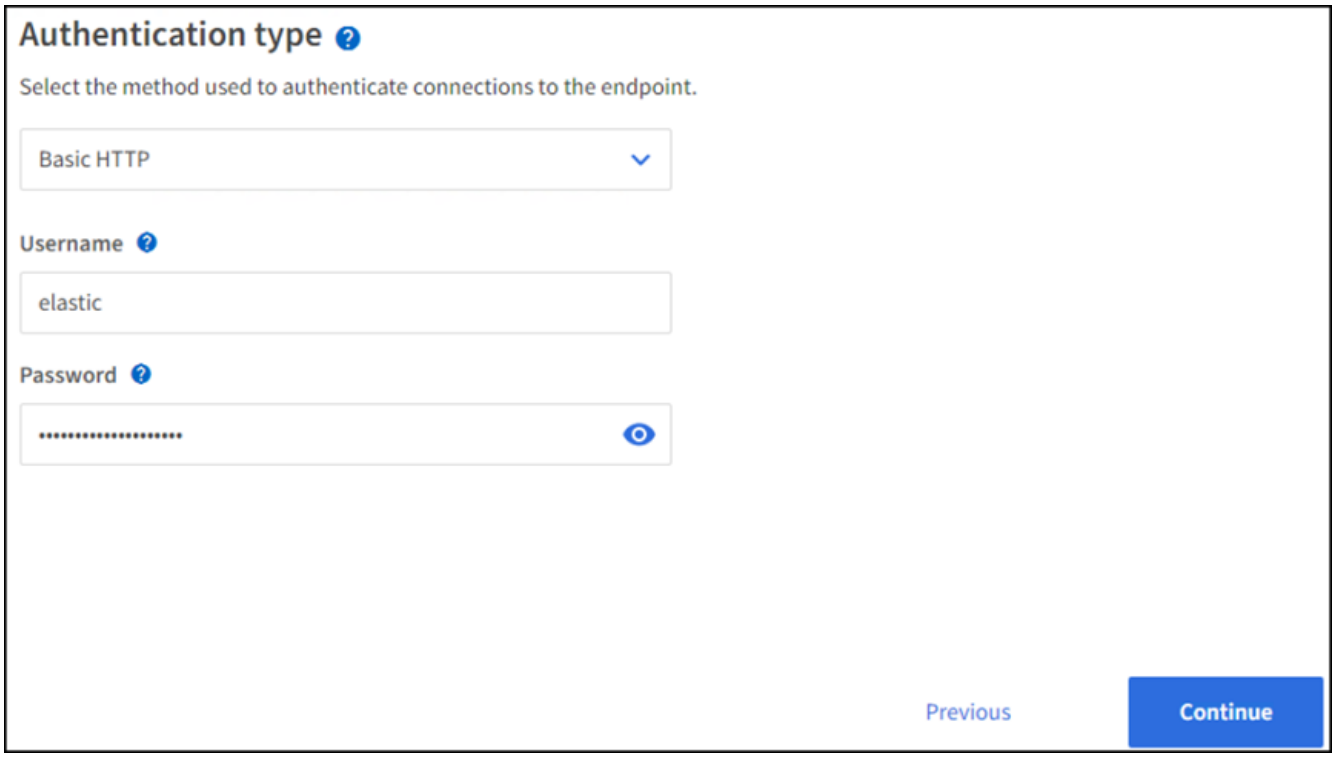
平台服务端点配置

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`

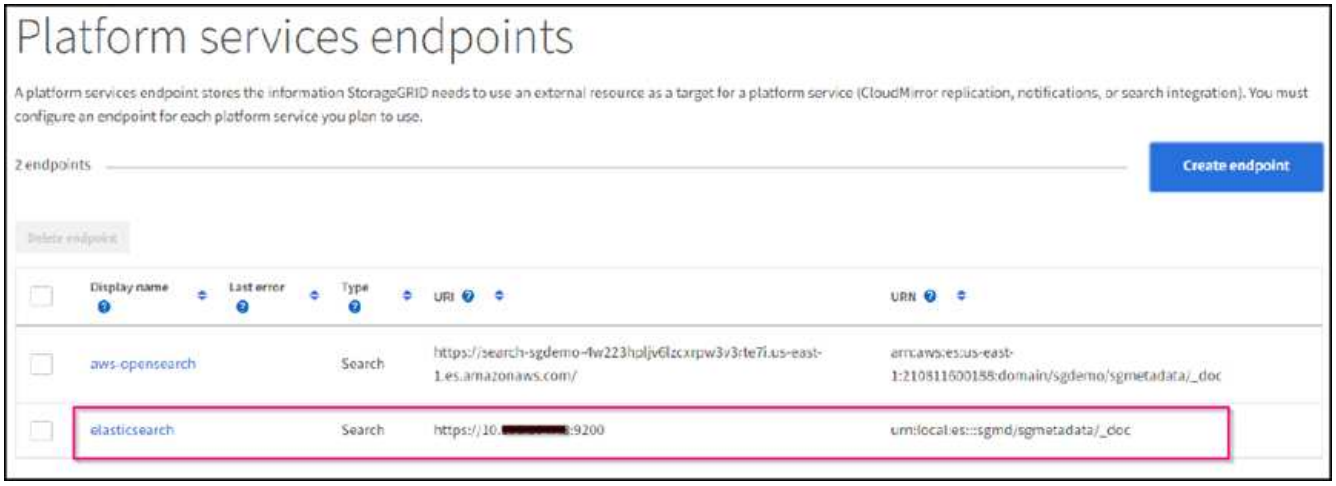


3. 选择基本HTTP作为身份验证类型、输入用户名`弹性`以及Elasticsearch安装过程生成的密码。要转到下一页、请单击继续。



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：

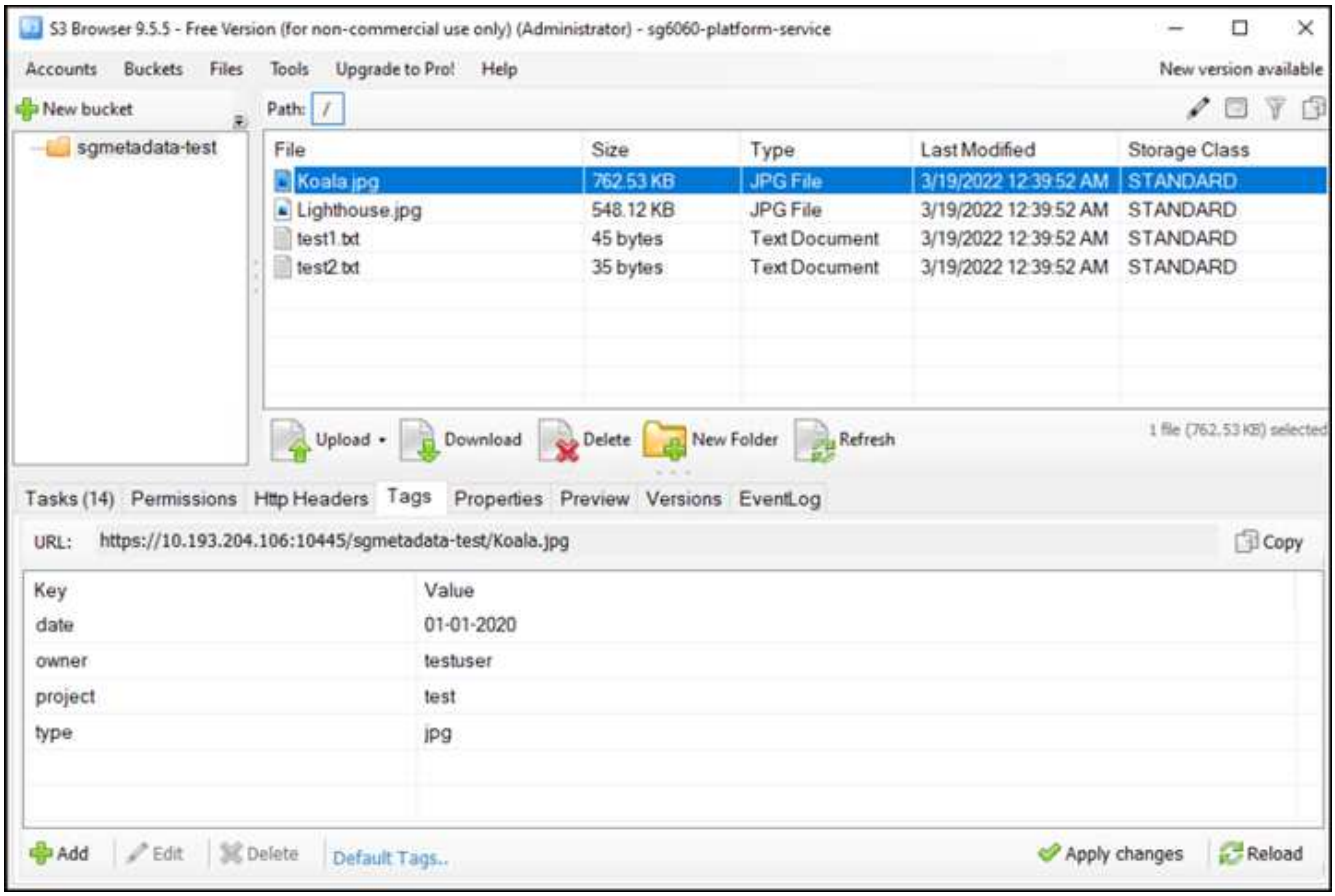
1. 在租户管理器中、转至存储(S3)>分段
2. 单击Create Bucket、输入存储分段名称(例如、`sgmetada-test`)并接受默认值`us-east-1` Region。
3. 单击"继续">"创建存储分段"。
4. 要打开存储分段概述页面、请单击存储分段名称、然后选择平台服务。
5. 选择启用搜索集成对话框。在提供的XML框中、使用以下语法输入配置XML。

   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。



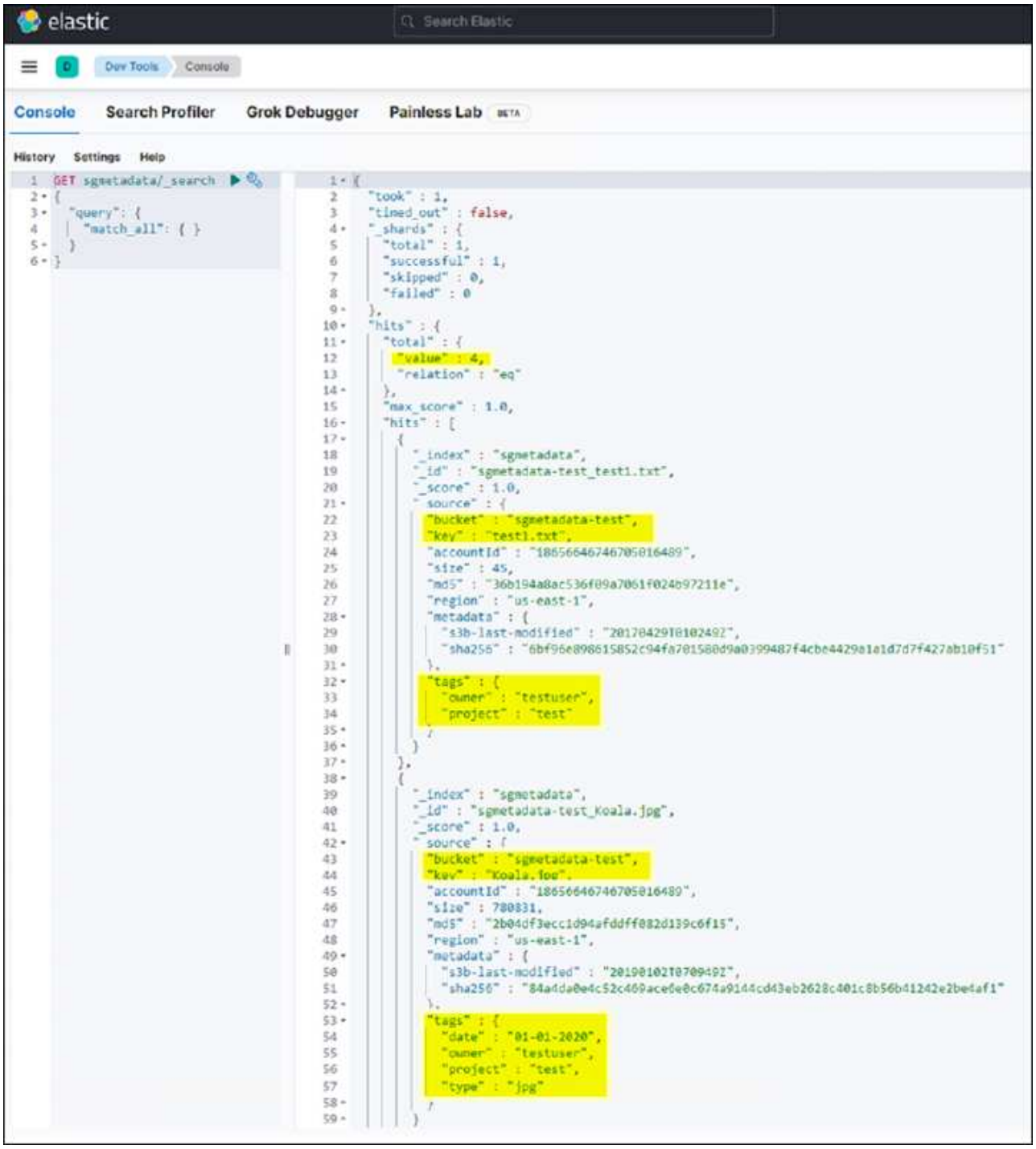
7. 使用Kibana UI验证对象元数据是否已加载到sgmetadata的索引中。

   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。

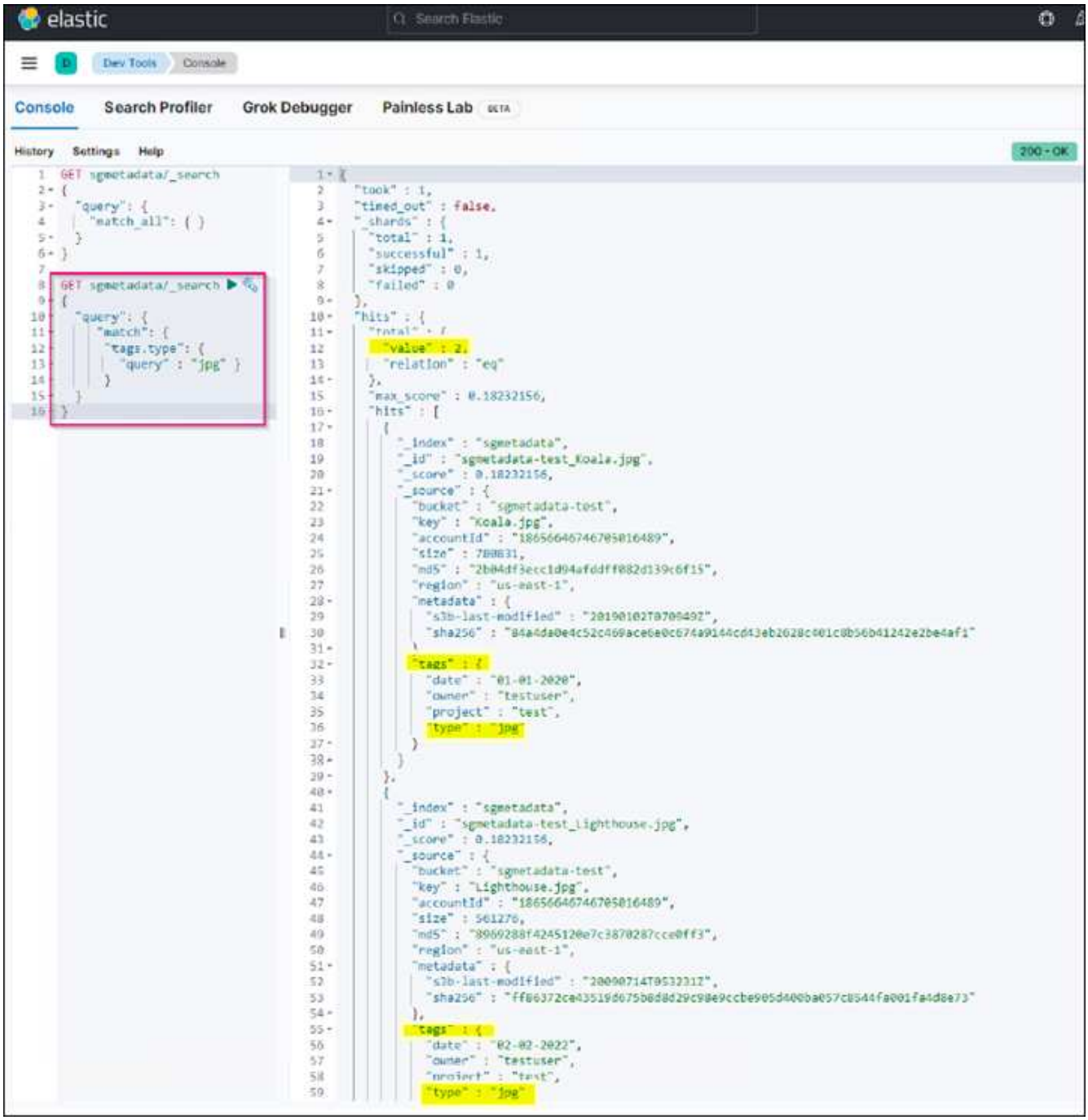
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



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。
- 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。
- 对于带有扩展架的SG6060、您需要将正确磁盘架驱动器大小的时间与基本设备时间相加、以获得完整的克隆持续时间。

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 →任何

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
10 Gb	1 天	2天	2.5天	3天	4天	4.5天
25 GB	1 天	2天	2.5天	3天	4天	4.5天

SG5712 →任何

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
10 Gb	1 天	2天	2.5天	3天	4天	4.5天
25 GB	1 天	2天	2.5天	3天	4天	4.5天

SG5660 → SG5760

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
10 Gb	3天	6天	7 天	8.5天	11.5天	• 13天*
25 GB	3天	6天	7 天	8.5天	11.5天	• 13天*

SG5660 → SG6060

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
10 Gb	2.5天	4.5天	5.5天	6.5天	9天	10天
25 GB	2天	4天	5天	6天	8天	9天

SG5760 → SG5760

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
10 Gb	3天	6天	7 天	8.5天	11.5天	• 13天*
25 GB	3天	6天	7 天	8.5天	11.5天	• 13天*

SG5760 → SG6060

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
10 Gb	2.5天	4.5天	5.5天	6.5天	9天	10天
25 GB	1.5天	3天	3.5天	4.5天	6天	6.5天

SG6060 → SG6060

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
10 Gb	2.5天	4.5天	5.5天	6.5天	8.5天	9.5天
25 GB	1.5天	3天	3.5天	4天	5.5天	6天

DDP16

SG5760 → SG5760

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
10 Gb	3.5天	6.5天	8天	9.5天	12：5天	• 14天*
25 GB	3.5天	6.5天	8天	9.5天	12：5天	• 14天*

SG5760 → SG6060

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
10 Gb	2.5天	5天	6天	7.5天	10天	11天
25 GB	2天	3.5天	4天	5天	6.5天	7 天

SG6060 → SG6060

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
10 Gb	3.5天	5天	6天	7 天	9.5天	10.5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
25 GB	2天	3天	4天	4.5天	6天	7 天

扩展架(在源设备上的每个磁盘架上添加到**SG6060**以上)

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
10 Gb	3.5天	5天	6天	7 天	9.5天	10.5天
25 GB	2天	3天	4天	4.5天	6天	7 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

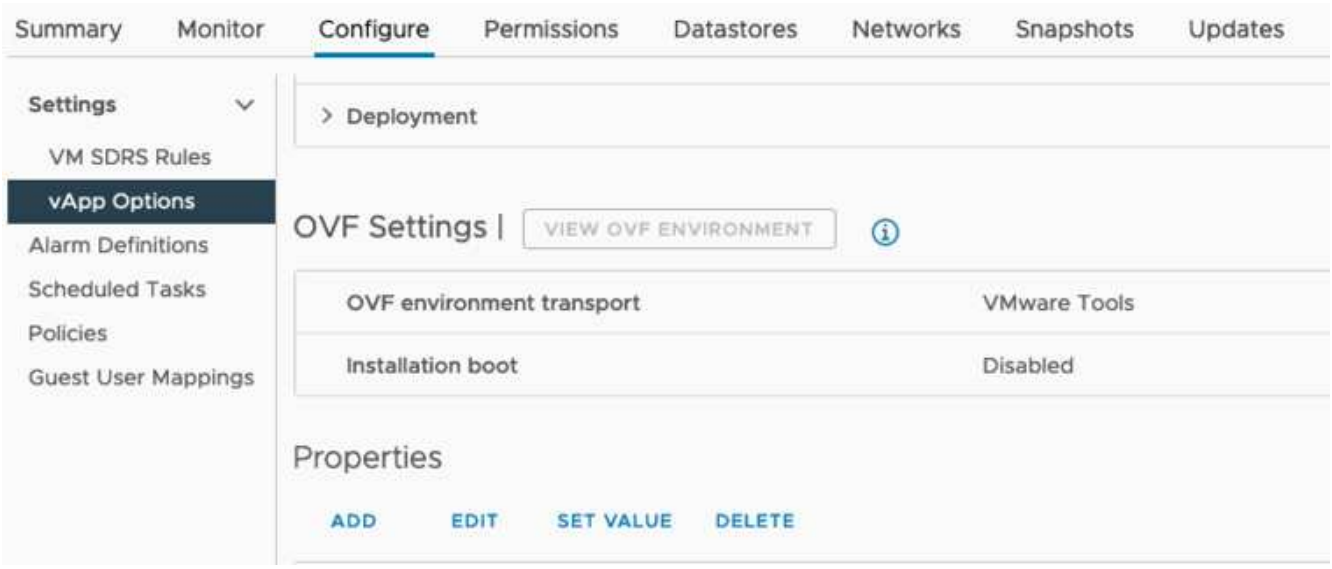
要销毁第一个网关节点、请执行以下步骤：

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。

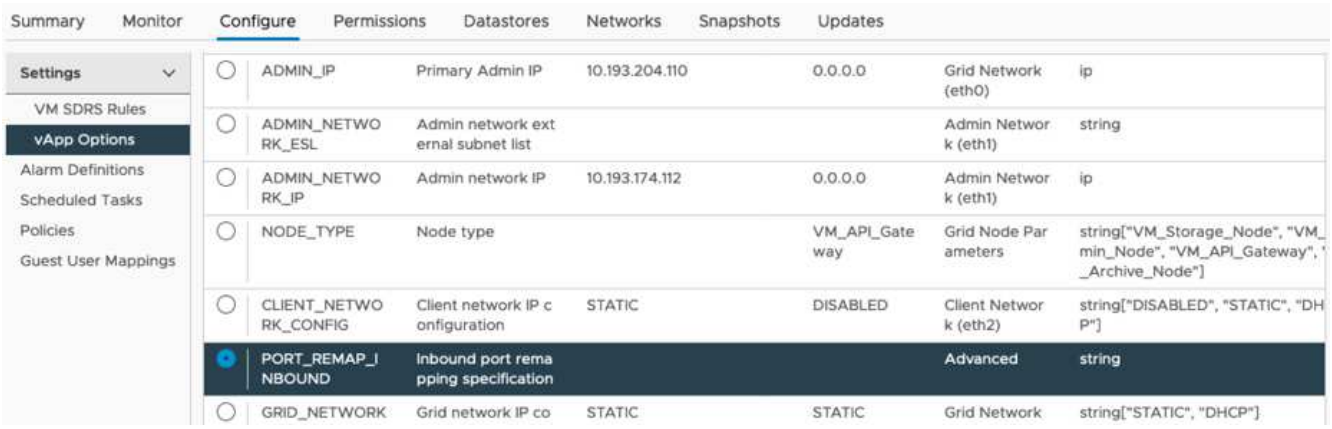
部署替代网关节点

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

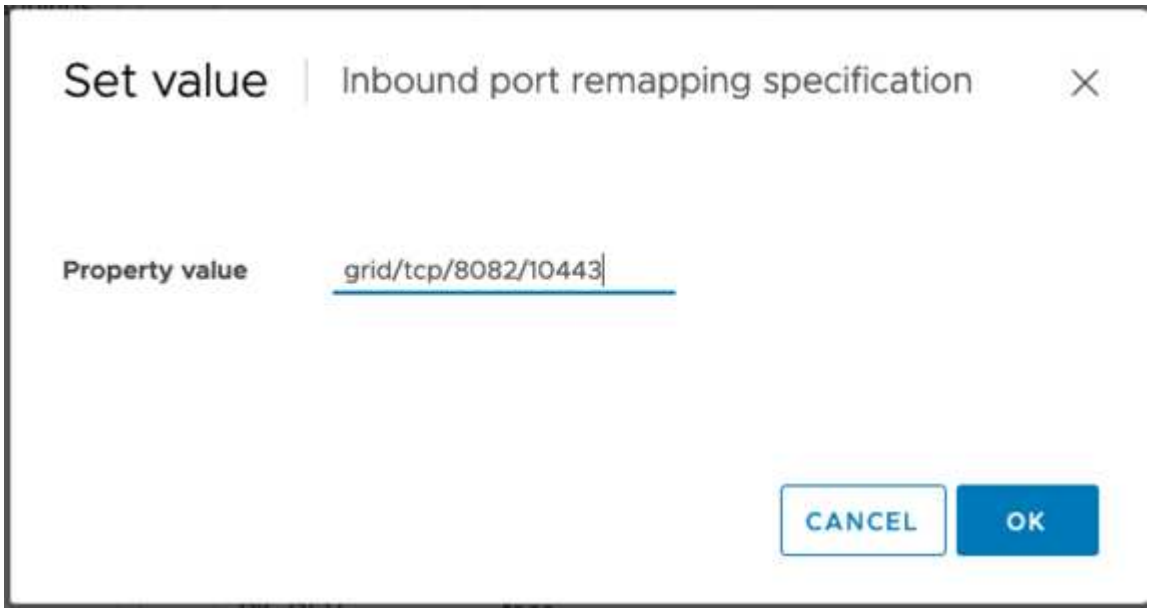


4. 滚动到属性列表顶部、然后单击编辑

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。

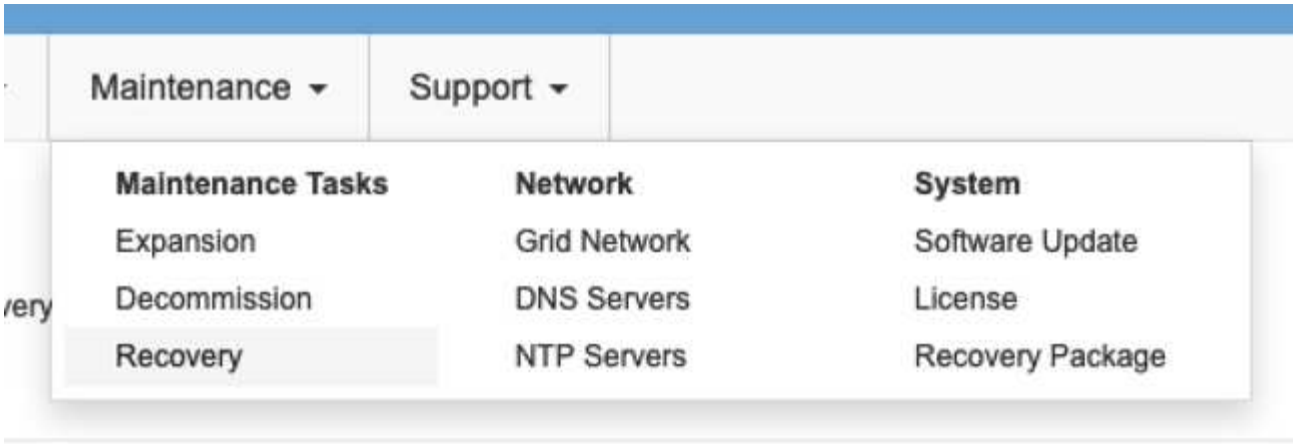


8. 如果使用多个网络、请使用逗号(、)分隔网络字符串、例如GRIDE/TCP/8082/10443、admin/TCP/8082/10443、client/TCP/8082/10443

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`

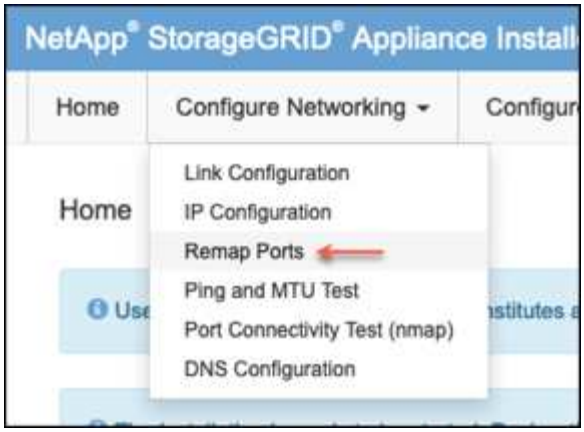
重建管理节点

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`

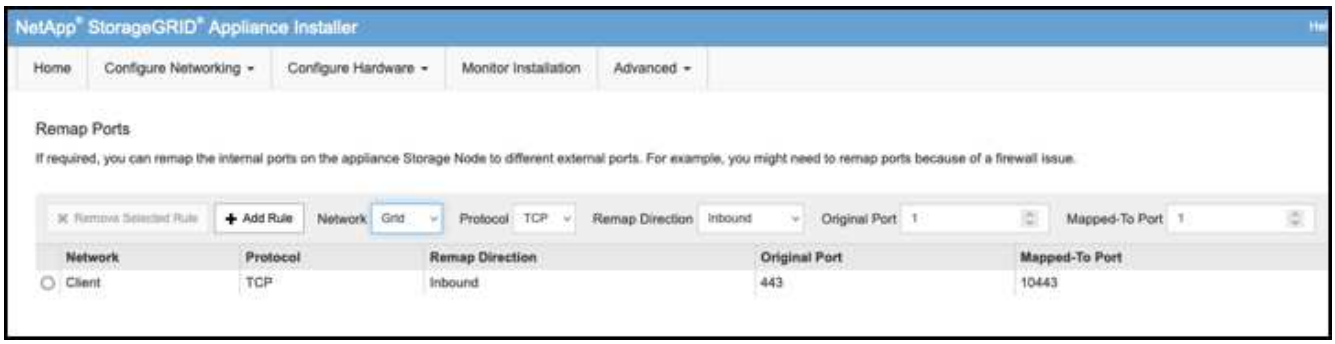
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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*

工具和应用程序指南

将Cloudera Hadoop S3A连接器与StorageGRID 结合使用

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
```

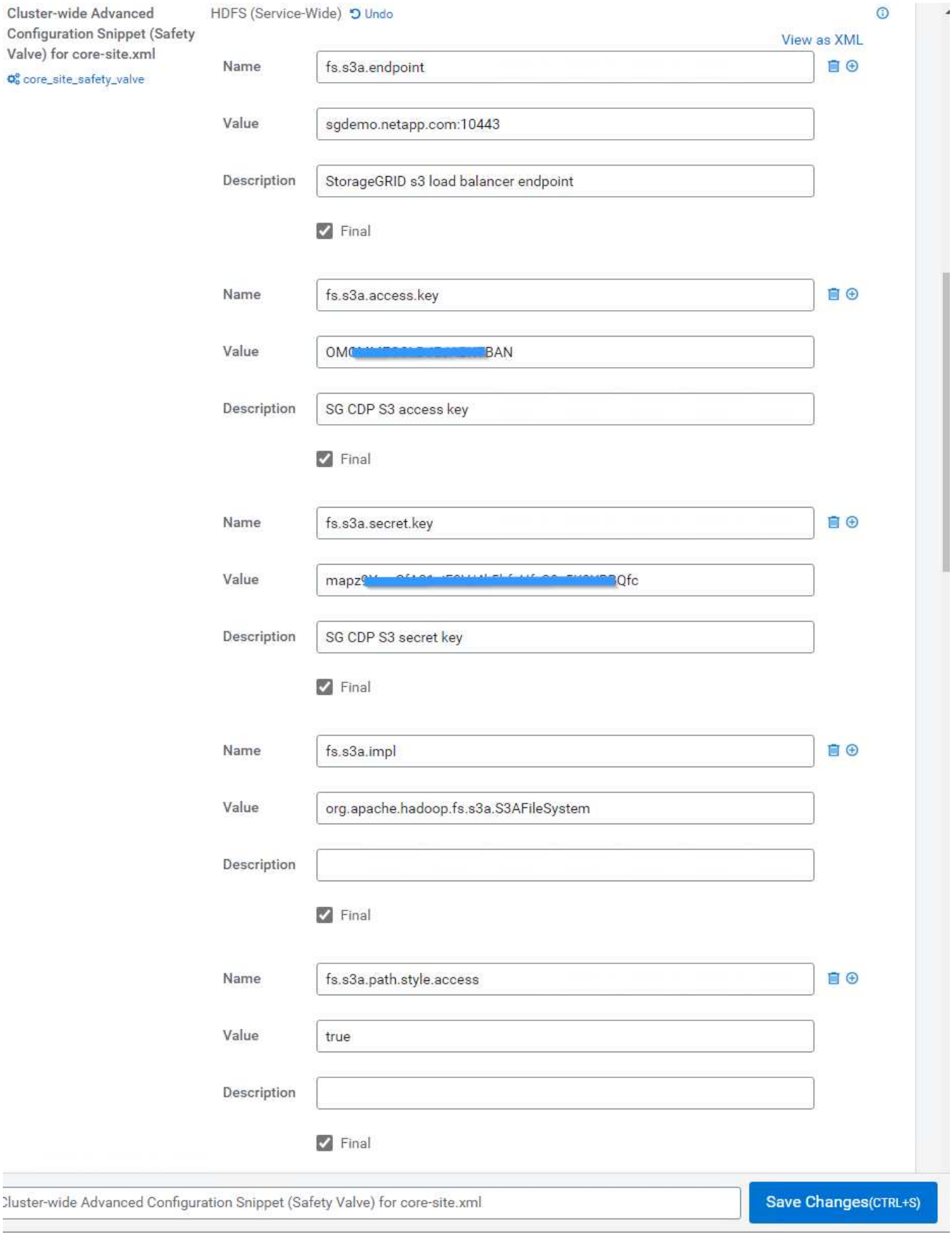
Cloudera HDFS S3A配置

- 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。

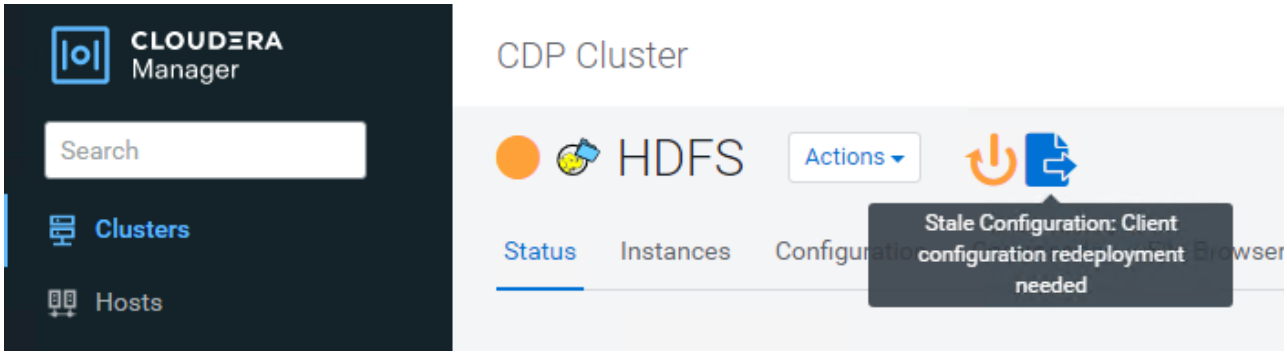
Name	价值
fs.s3a.access.key	< *StorageGRID* 中的租户*S3*访问密钥>
fs.s3a.secret.key	< *StorageGRID* 中的租户*S3*密钥>
fs.s3a.connection.ssl.enabled	true或false (如果缺少此条目、则默认为https)
fs.s3a.endpoint	StorageGRID S3端点：端口>_
fs.s3a.impl	org.apache.hadoop.fs.s3a.s3AFileSystem
fs.s3a.path.style.access	true或false (如果缺少此条目、则默认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

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>
```

故障排除提示

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

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
  ```

作者：*Aron Klein*

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

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。

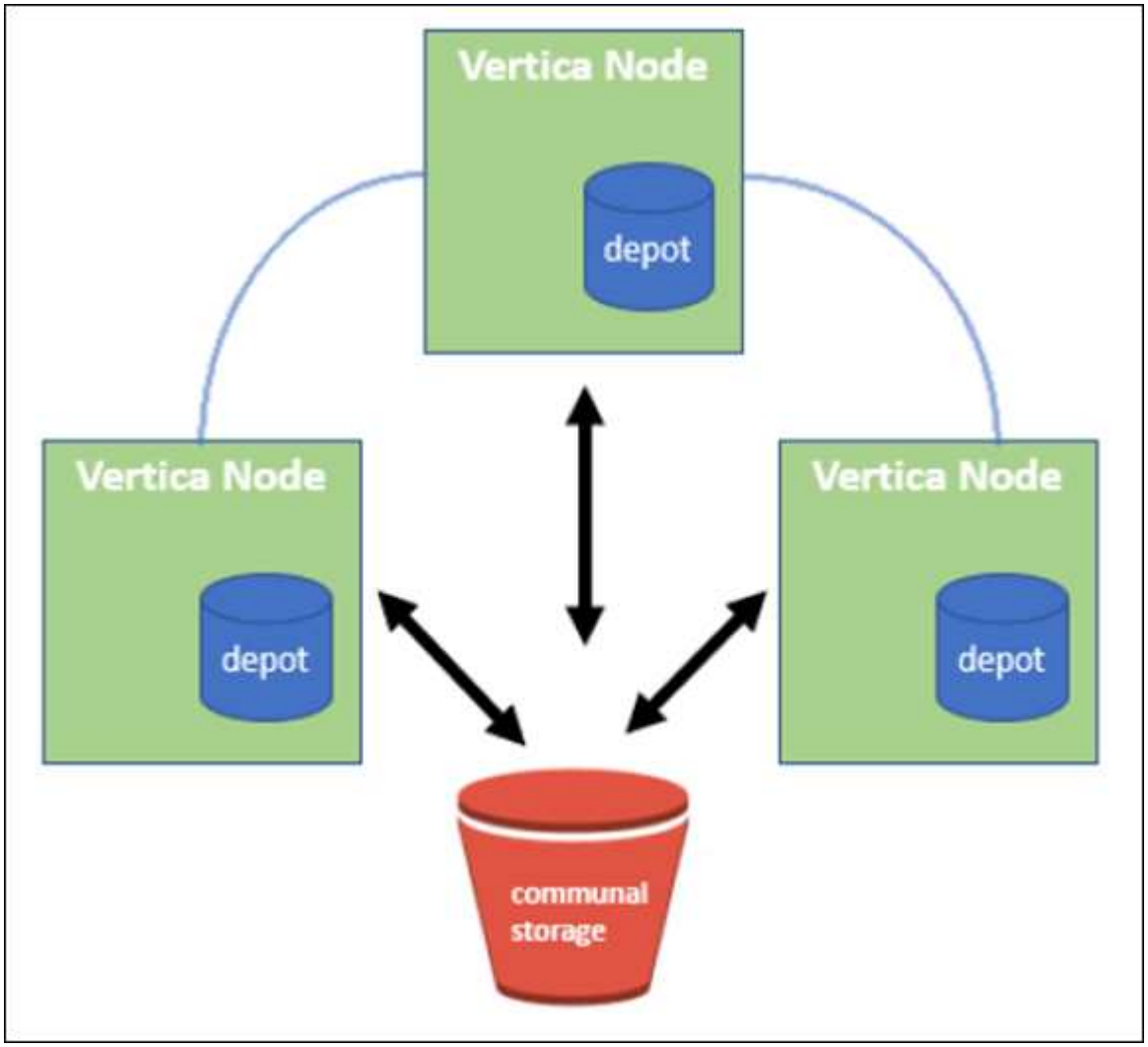
Eon和企业模式在数据存储位置方面主要不同：

- 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/026d63ae9d4a33237bf0e2c2cf2a794a00a0000000021870/026d63ae9d4a33237bf0e2c2cf2a794a00a00002187a.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_vmart node0017/Catalog/859703b06a3456d95d0be2 8575a673/checkpoint/C14_7/chkpt_1.cat.g z
232	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0017/Catalog/859703b06a3456d95d0be2 8575a673/checkpoint/C14_7/completed
822930	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0017/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_14_g7.cat.gz
755033	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0017/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_15_g8.cat
0	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0017/Catalog/859703b06a3456d95d0be2 8575a673/tiered_catalog.cat
822922	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0018/Catalog/859703b06a3456d95d0be2 8575a673/checkpoint/C14_7/chkpt_1.cat.g z
232	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0018/Catalog/859703b06a3456d95d0be2 8575a673/checkpoint/C14_7/completed
822930	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0018/Catalog/859703b06a3456d95d0be2 8575a673/Txnlogs/txn_14_g7.cat.gz
755033	s 3 : //Vertica/metadata/VMart/nodes/v_vmart node0018/Catalog/859703b06a3456d95d0be2 8575a673/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

通过StorageGRID 11.6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。请观看 "使用ELK视频进行StorageGRID 日志分析" 查看ELK配置示例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。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

假设

读者熟悉StorageGRID 和ELK的术语和操作。

说明

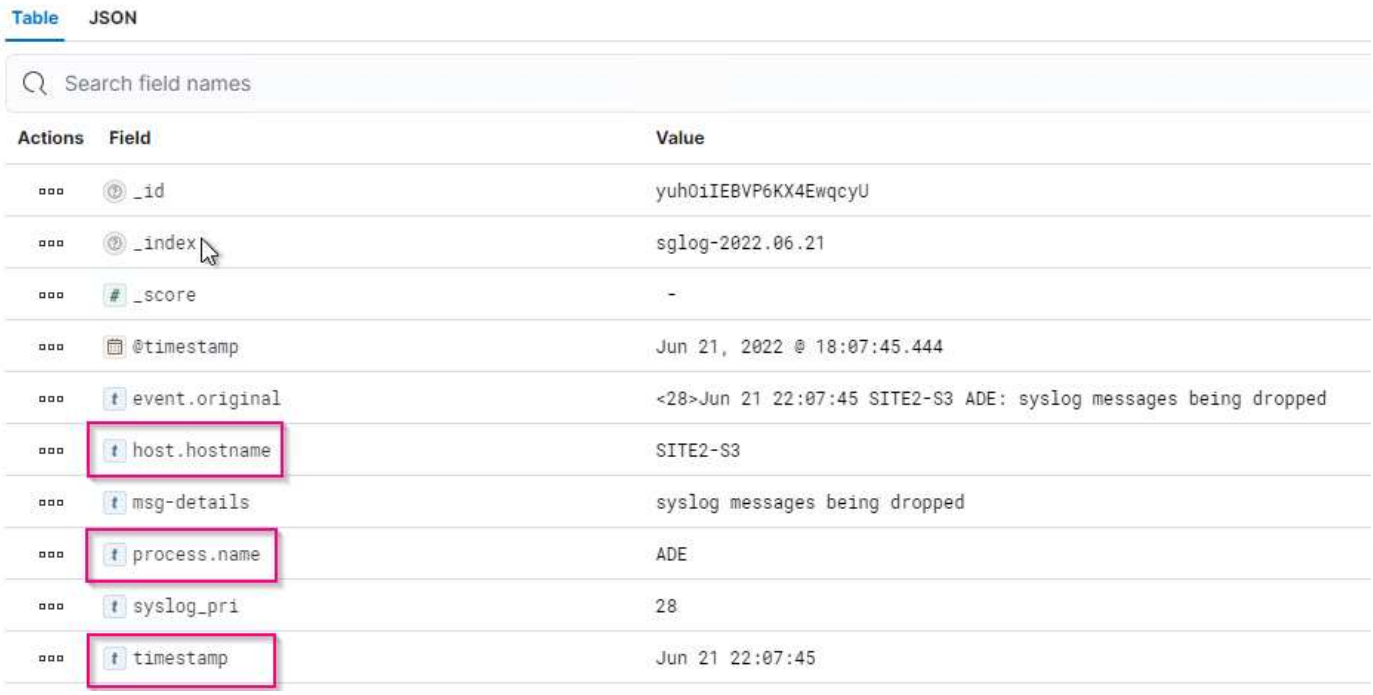
由于Grok模式定义的名称不同、因此提供了两个示例版本。+例如、Logstash配置文件中的SYSLOGBASE格式根据安装的Logstash版本定义不同的字段名称。

```
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
```

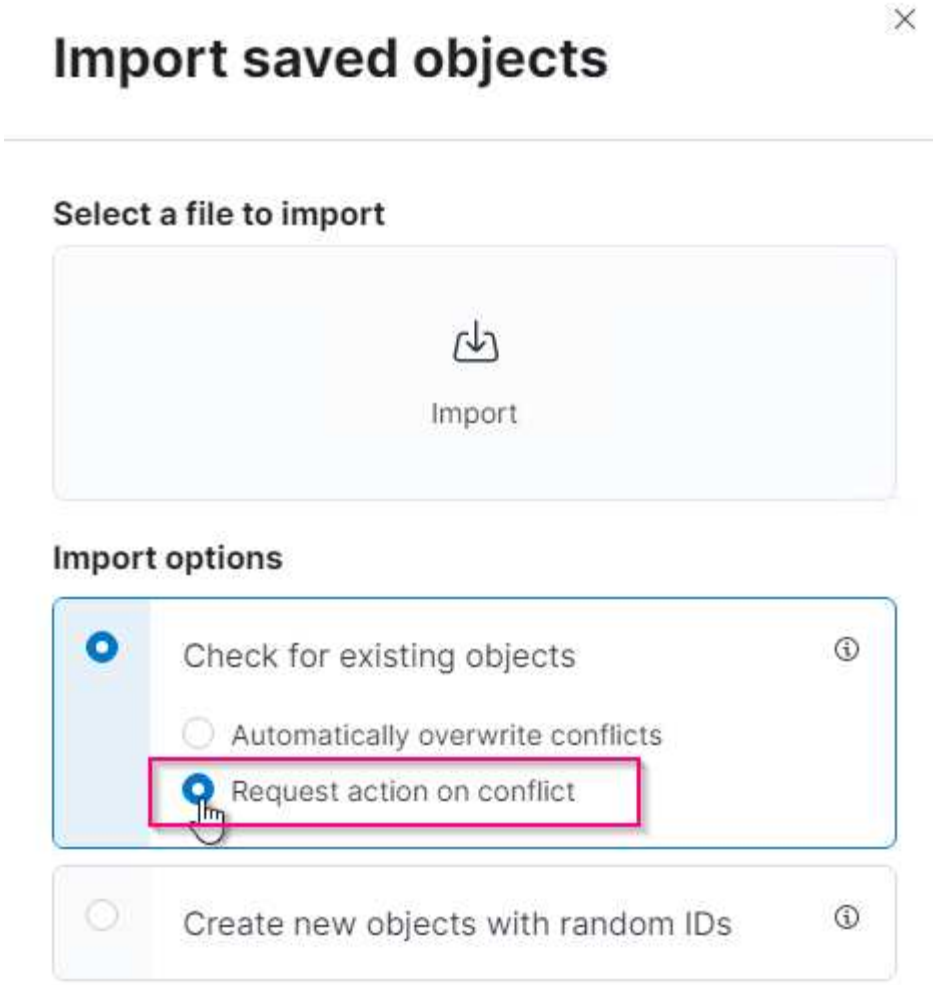
4. 检查/var/log/logstash/logstash-plain.log并确认在使用新配置文件启动Logstash时没有错误。
5. 确认TCP端口已启动并正在侦听。+在此示例中、使用TCP端口5000。

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

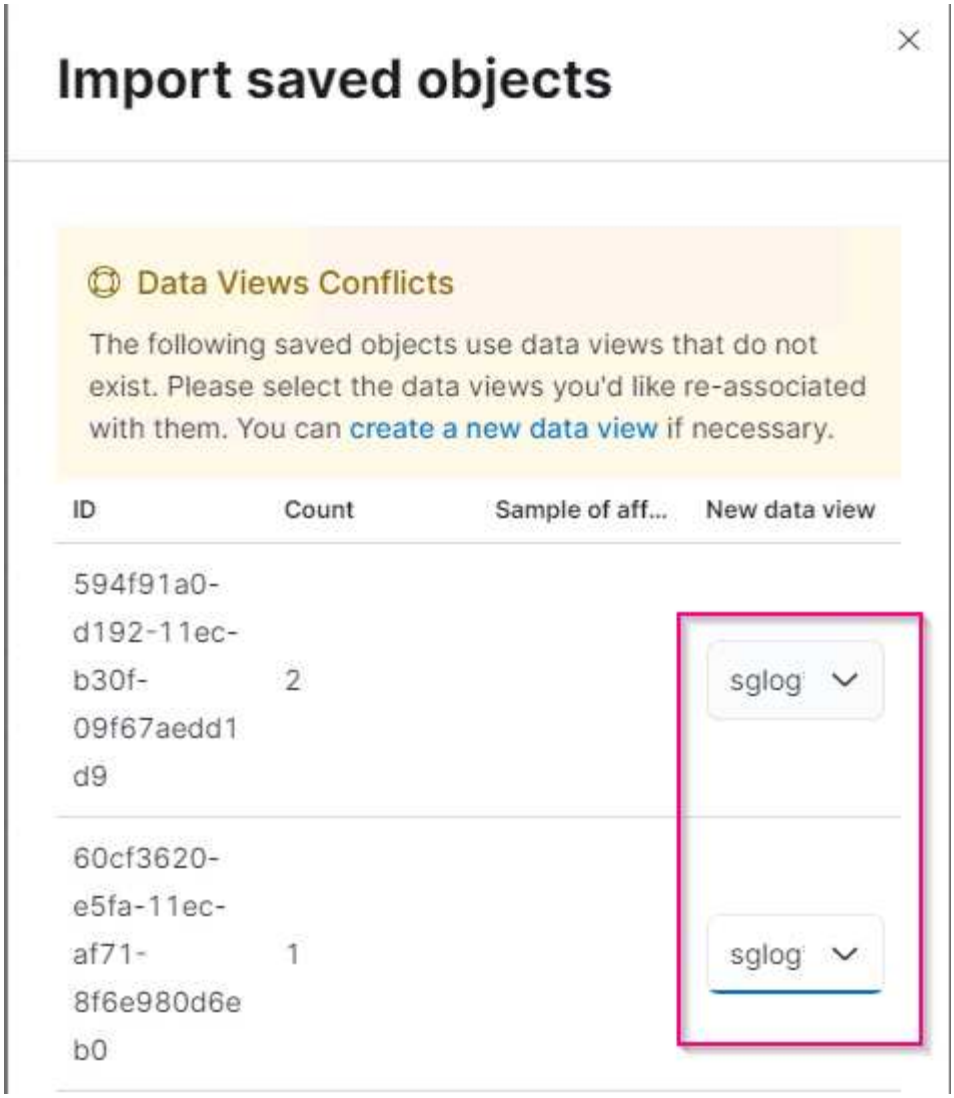
6. 在StorageGRID 管理器图形用户界面中、配置外部系统日志服务器以向Logstash发送日志消息。请参见"演示视频" 了解详细信息。
7. 您需要在Logstash服务器上配置或禁用防火墙、以允许StorageGRID 节点连接到定义的TCP端口。
8. 在Kibana GUI中、选择Management → Dev Tools。在控制台页面上、运行此get命令以确认已在Elasticsearch上创建新索引。

```
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。



导入以下Kibana对象： *查询** audit-msg-s3rq-orlm * byncast log S3相关消息日志级别警告或更高**+***失败的安全事件**+***图表* S3请求计数基于bycast.log +* HTTP状态代码审核消息类型细分**+***平均**S3**响应 时间**+***信息板+* S3请求信息板使用上述图表。

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"

作者：郑安杰

使用Prometheus和Grafana延长指标保留期限

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

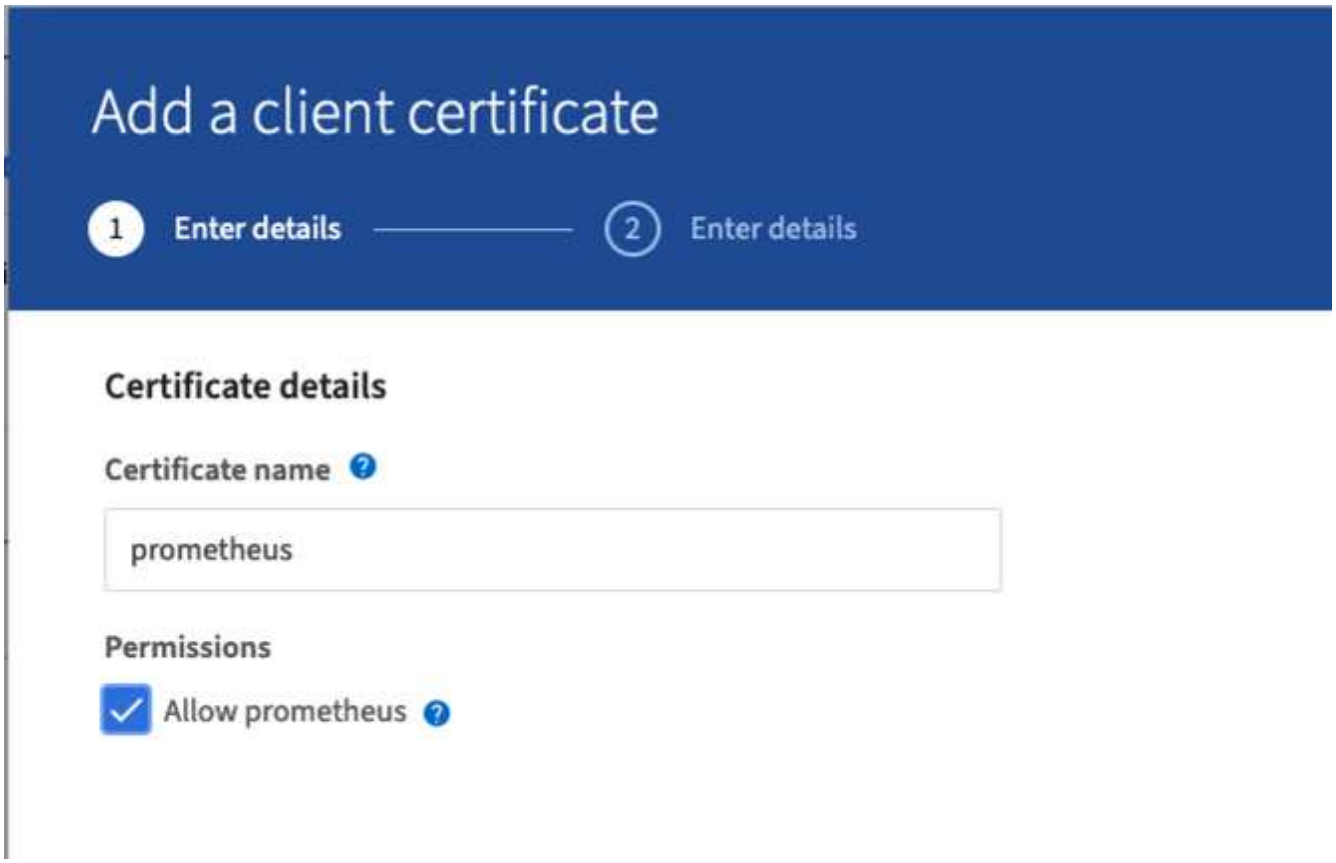
实验室详细信息

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/ 。

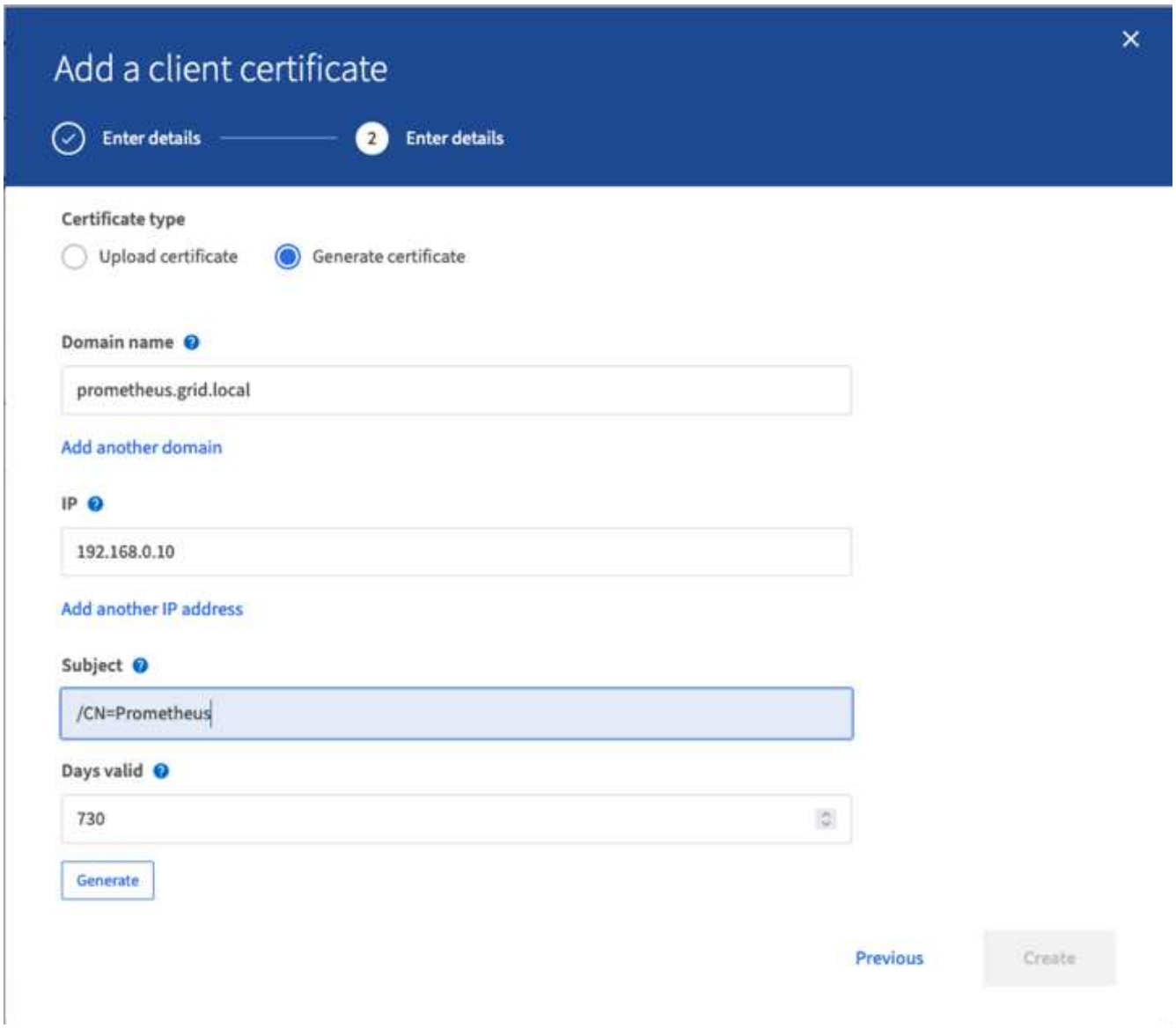
为Prometheus客户端访问配置StorageGRID

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。

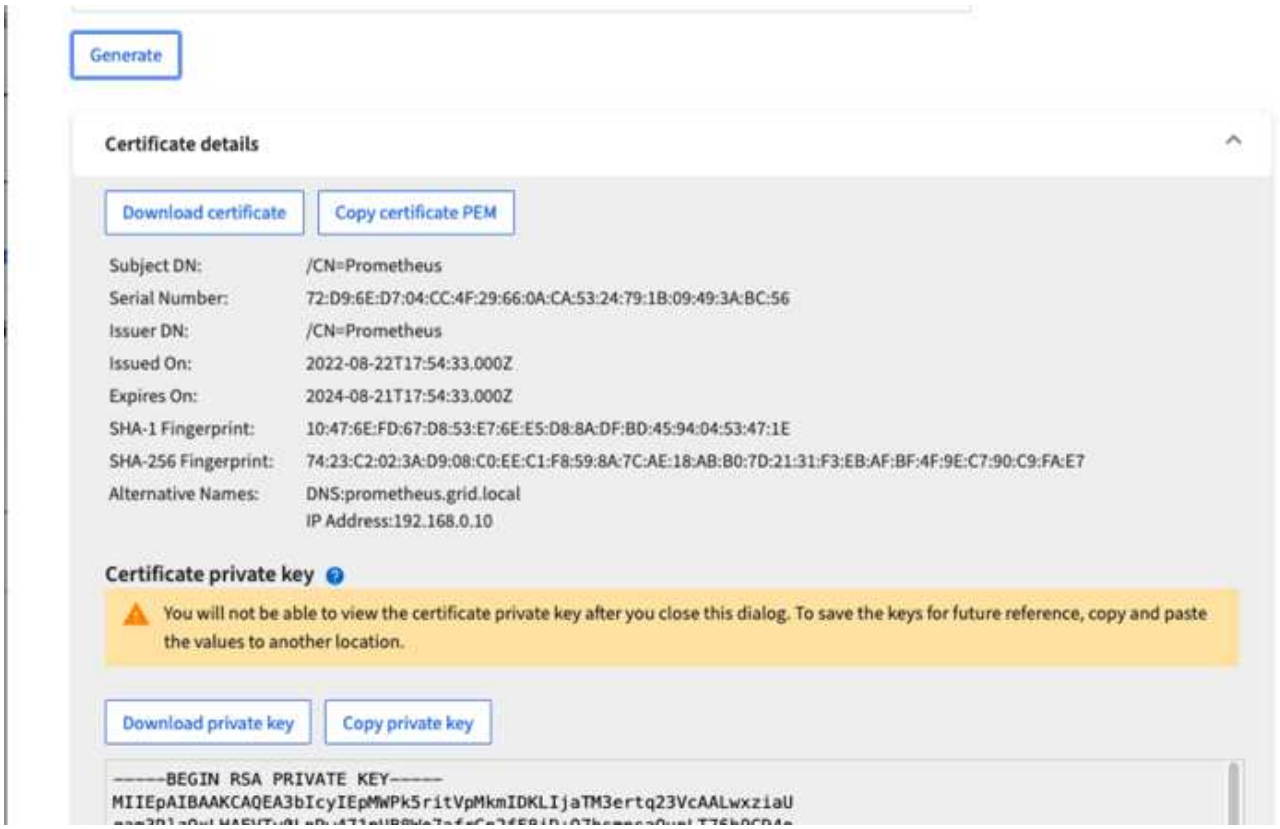


4. 如果您拥有CA签名的证书、则可以选择"上传证书"单选按钮、但在我们的情况下、我们将通过选择"生成证书"单选按钮让StorageGRID 生成客户端证书。此时将显示要填写的必填字段。输入客户端服务器的FQDN、服务器的IP、主题和有效天数。然后单击"生成"按钮。



> 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。

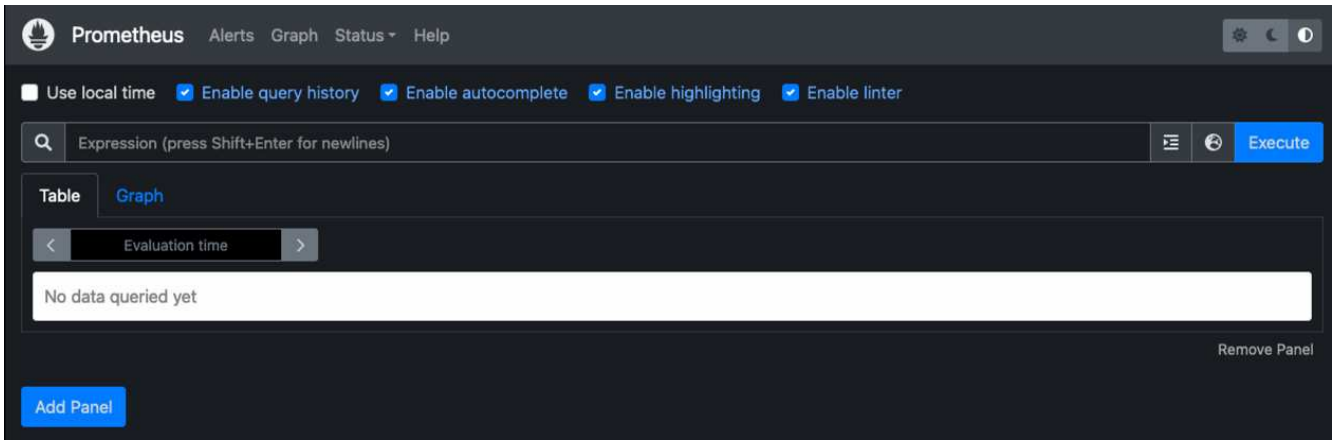
```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

5. 检查服务是否运行正常

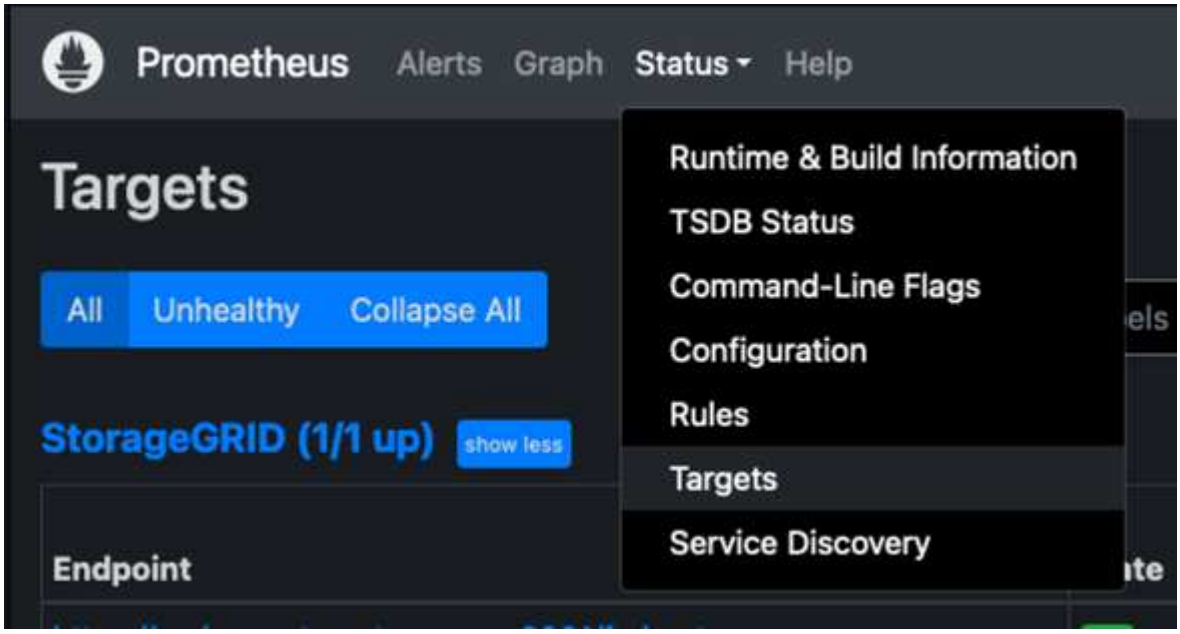
```
sudo systemctl status prometheus
```

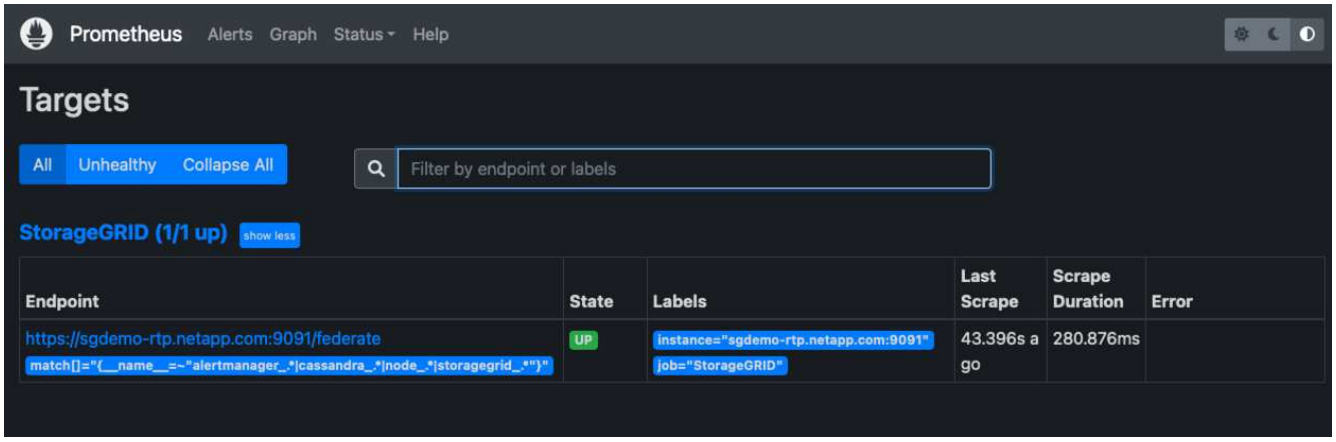
```
● prometheus.service - Prometheus Time Series Collection and Processing
Server
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled;
vendor preset: enabled)
     Active: active (running) since Mon 2022-08-22 15:14:24 EDT; 2s ago
   Main PID: 6498 (prometheus)
      Tasks: 13 (limit: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

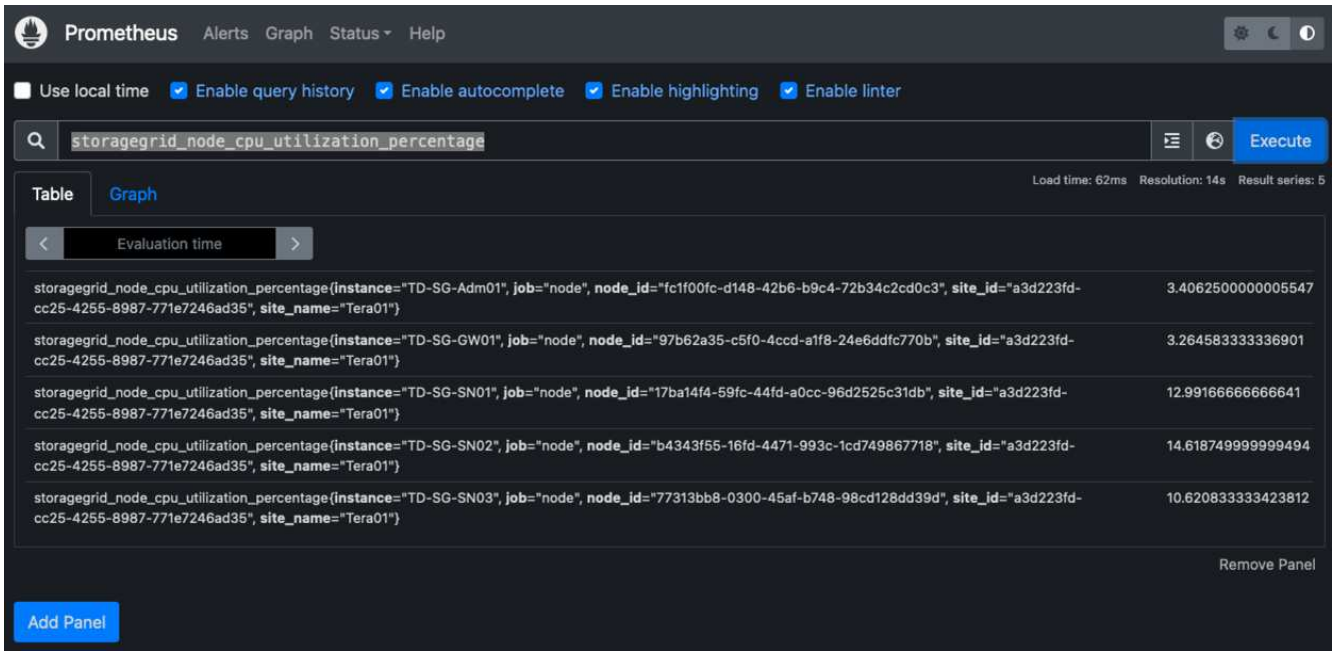


7. 在"Status" Targets下、您可以看到我们在Prometheus.yml中配置的StorageGRID 端点的状态





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。

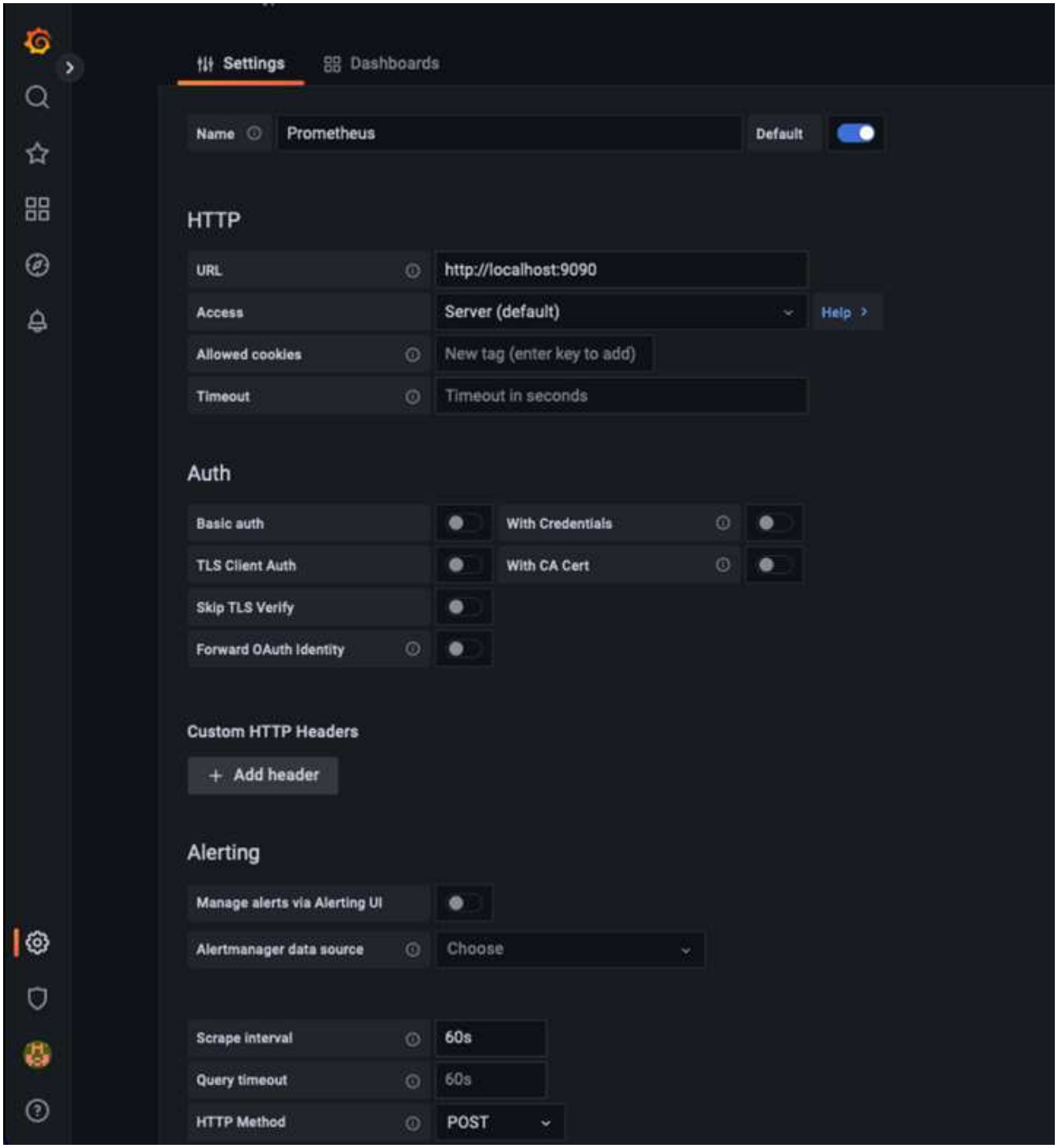
```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl enable grafana-server.service
```

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。

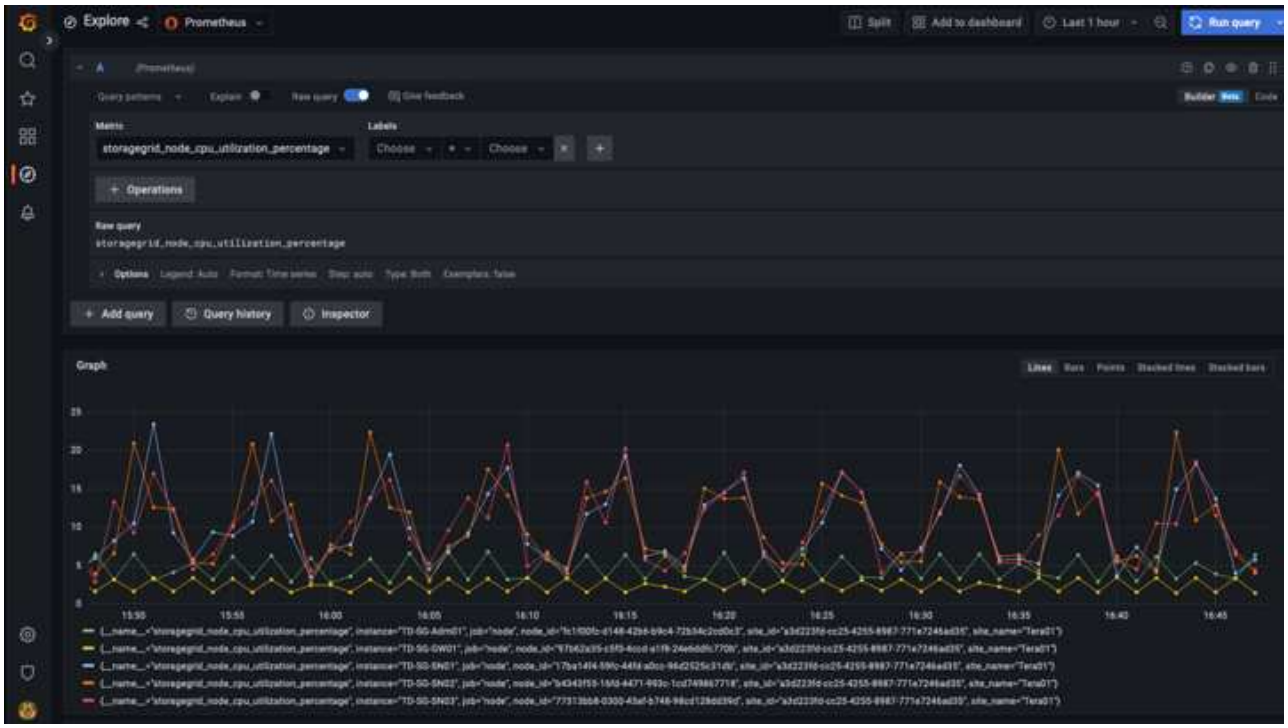
为**StorageGRID** 创建**Grafana**信息板

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

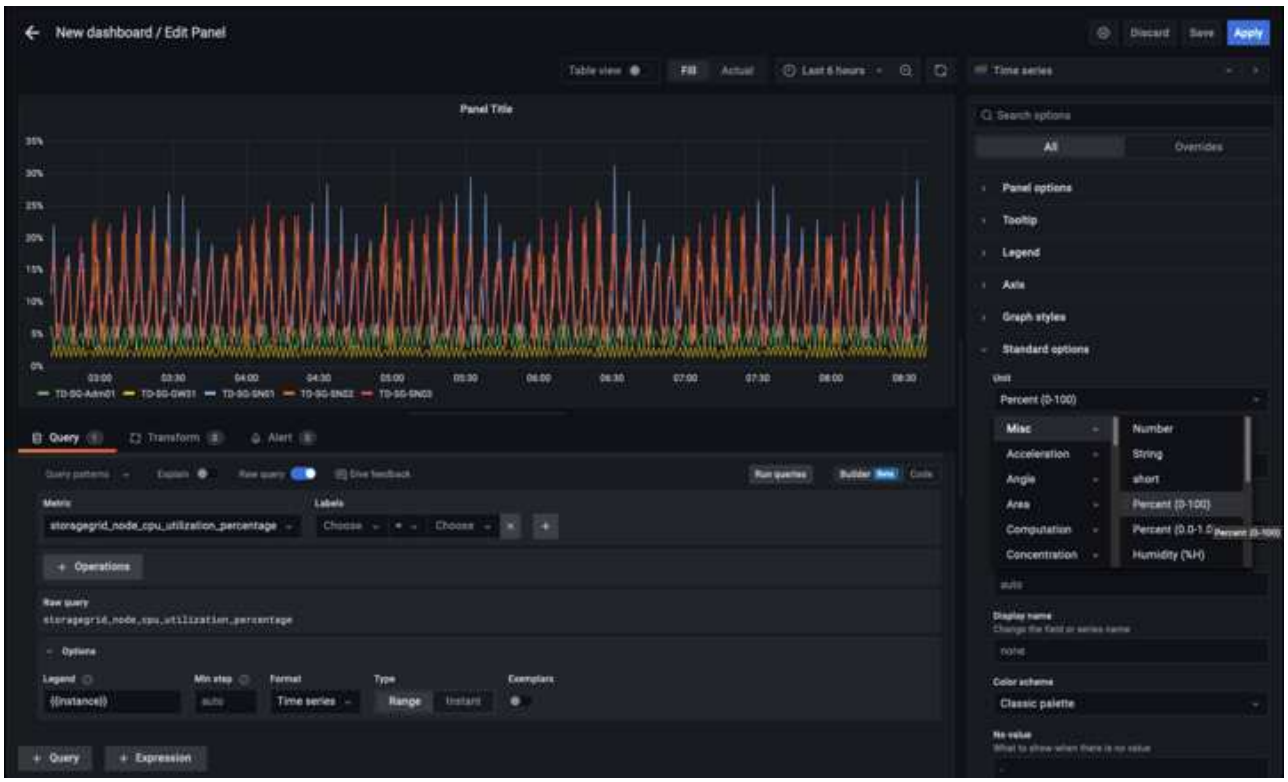


6. 现在、我们已配置数据源、可以创建一个信息板。

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

   b. 选择"添加新面板"

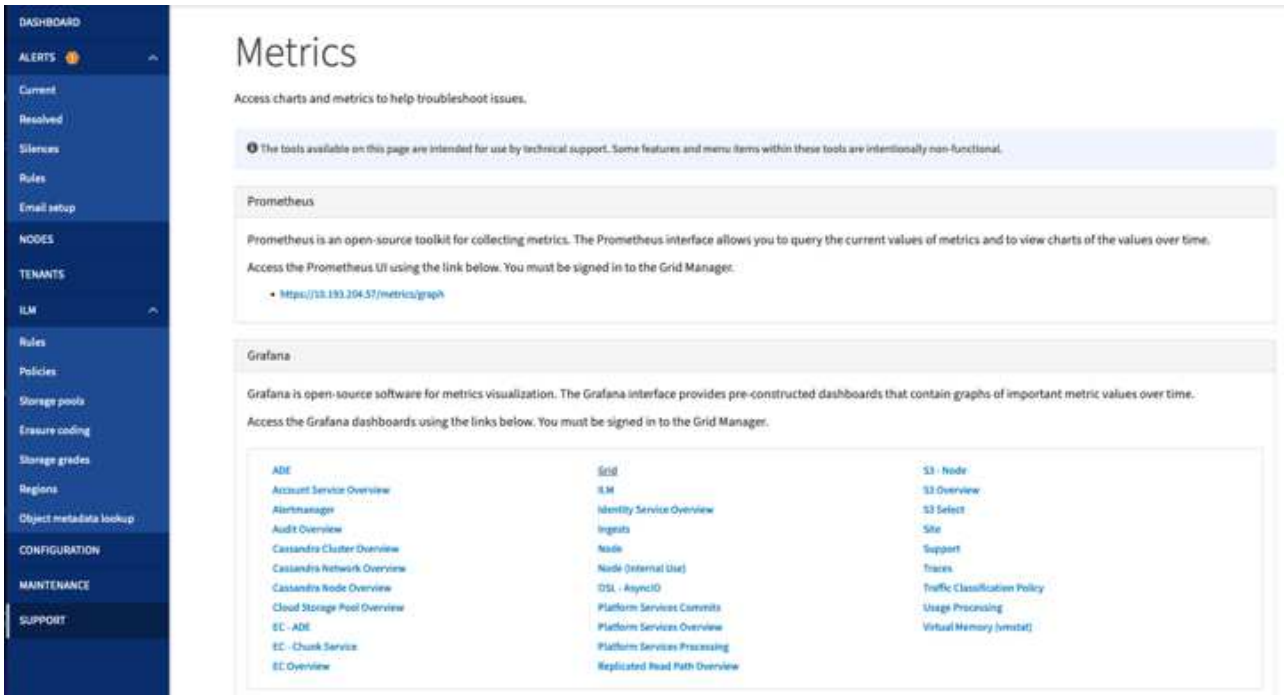
   c. 通过选择指标来配置新面板、我将再次使用"storagegrid node_cpu_utilization_percentage "、输入面板标题、展开底部的"选项"、并将图例更改为自定义、然后输入" ｛ {instance} ｝ "来定义节点名称、并在右侧窗格的"标准选项"下将"单元"设置为"Misc 100/percent (0%)"。然后单击"应用"将面板保存到信息板。



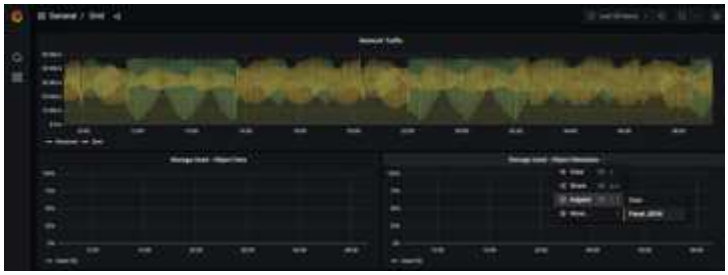
7. 我们可以继续为所需的每个指标构建这样的信息板、但幸运的是、StorageGRID 已经拥有包含面板的信息板、我们可以复制到自定义信息板中。

   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。

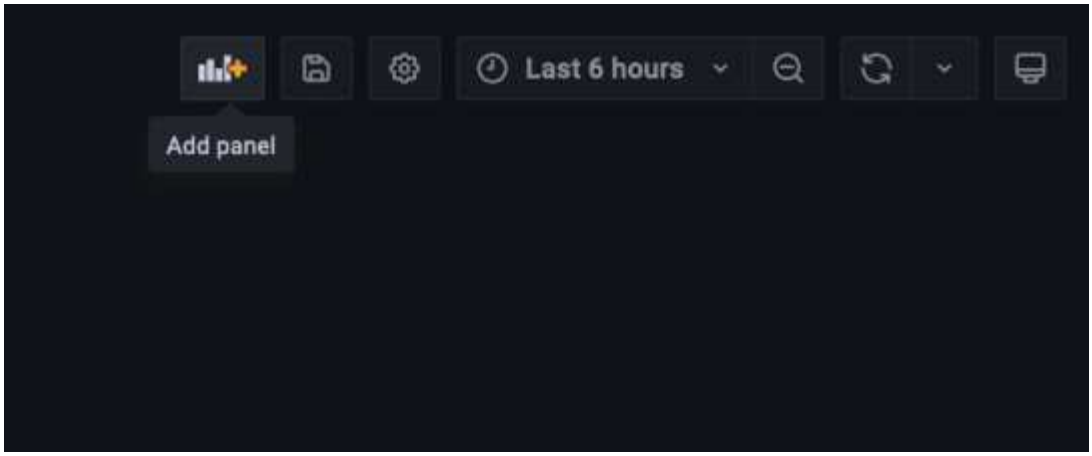


   c. 在网格信息板中、我们选择"已用存储-对象元数据"面板。单击小下箭头和面板标题的末尾以下拉菜单。从此菜单中选择"检查"和"面板JSON"。



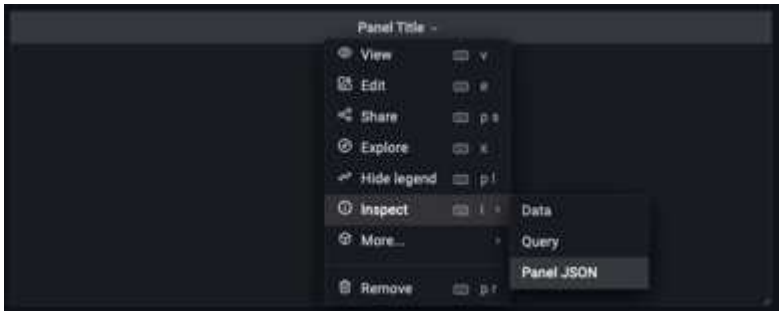
   d. 复制JSON代码并关闭窗口。

e. 在新信息板中、单击图标以添加新面板。

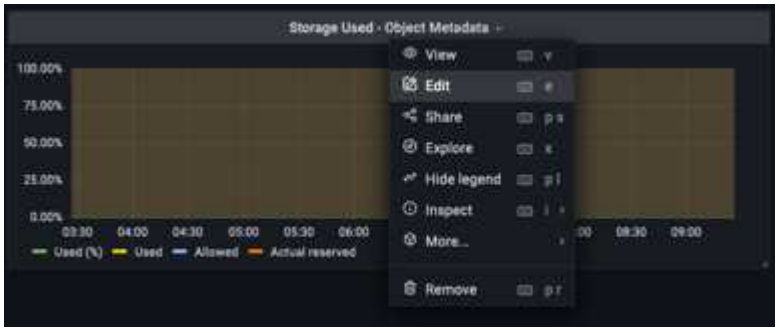


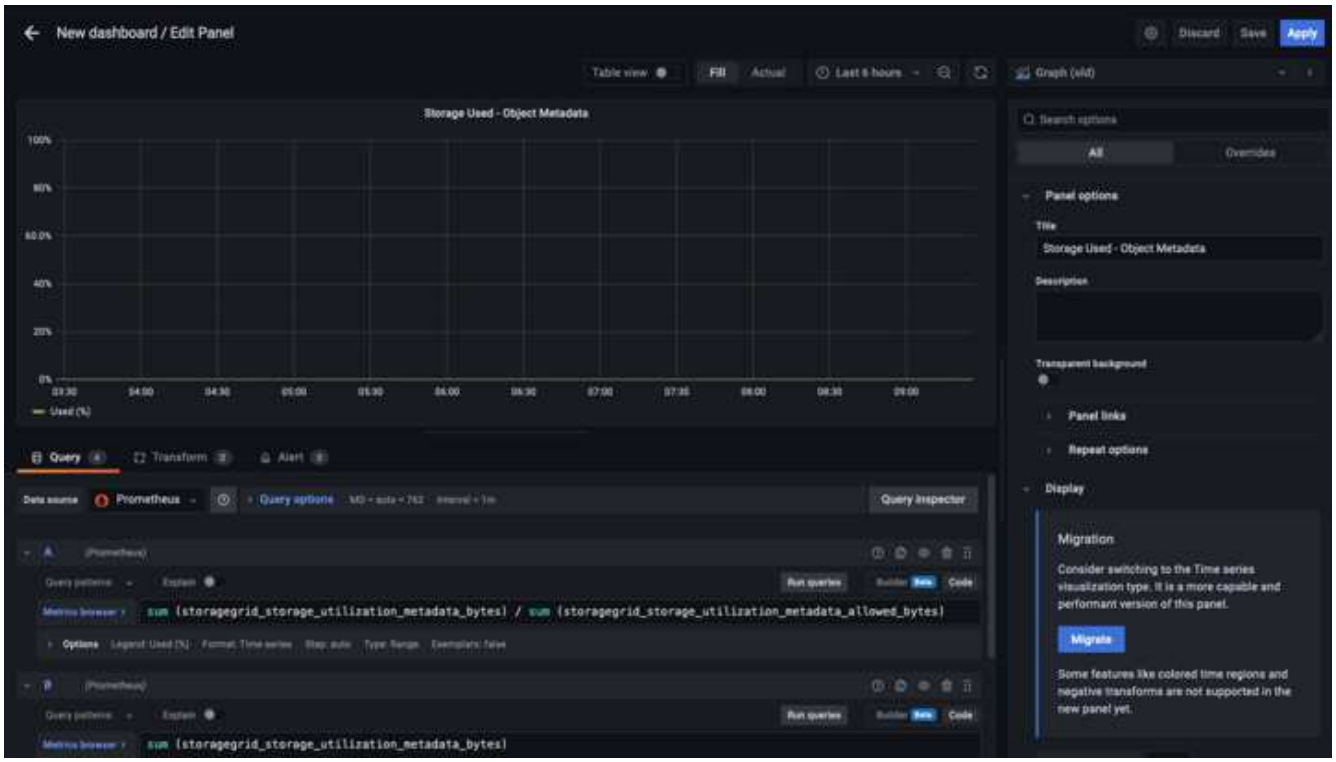
f. 应用新面板而不进行任何更改

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"。

作者：*Aron Klein*

Datadog SNMP配置

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'
```

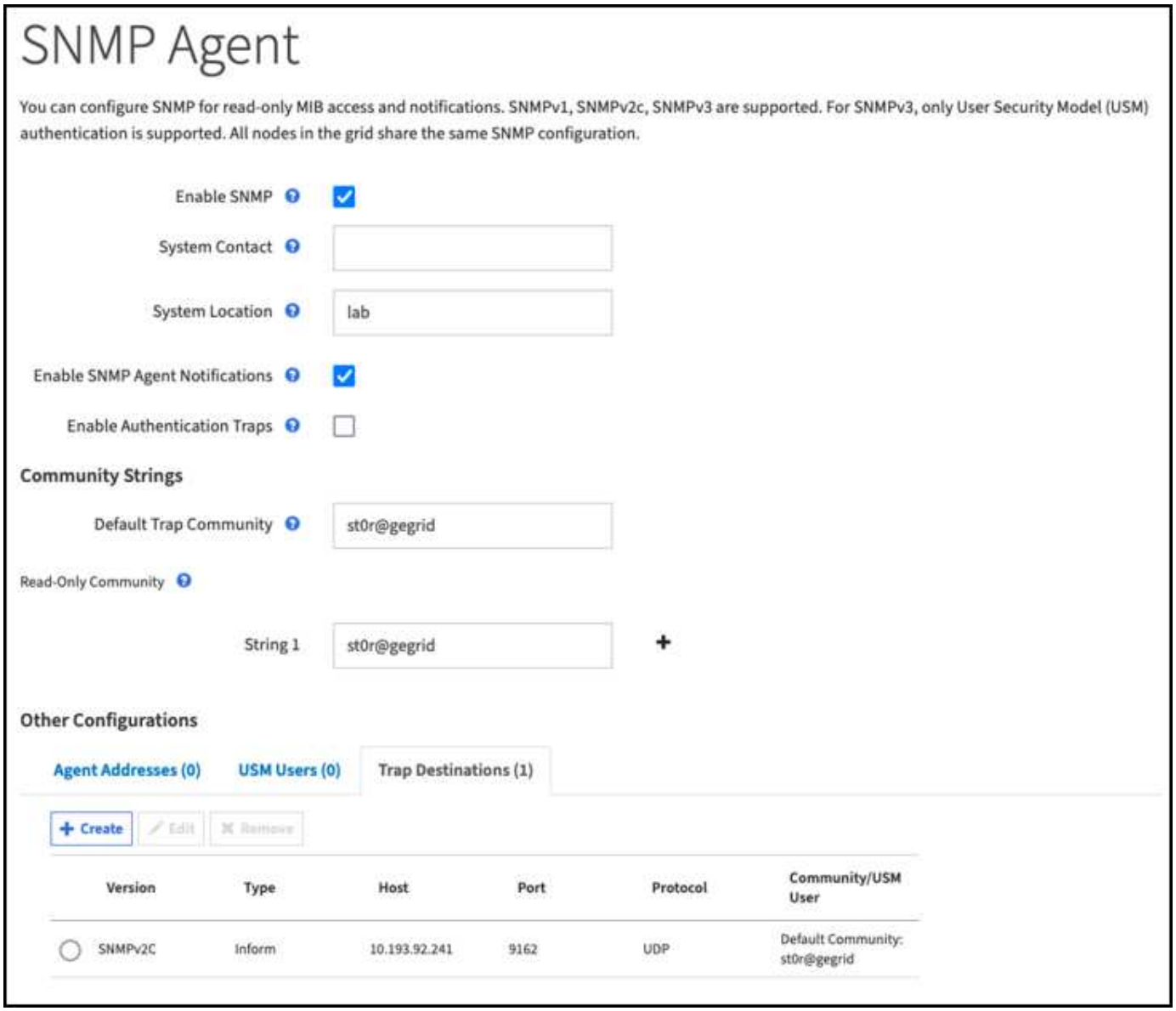
陷阱的**SNMP**配置

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。



作者：*Aron Klein*

使用rclone在StorageGRID 上迁移、放置和删除对象

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
```

作者：Siegfried Hepp和Aron Klein_

使用Veeam备份和复制进行部署的StorageGRID最佳实践

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系统应用最新的修补程序。目前、我们建议至少安装Veeam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 11.5或11.7版本。StorageGRID 11.6.0.11和11.7.0.4中引入了许多优化功能、这些功能对Veeam工作负载非常有用。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、Loadbalanacer.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。

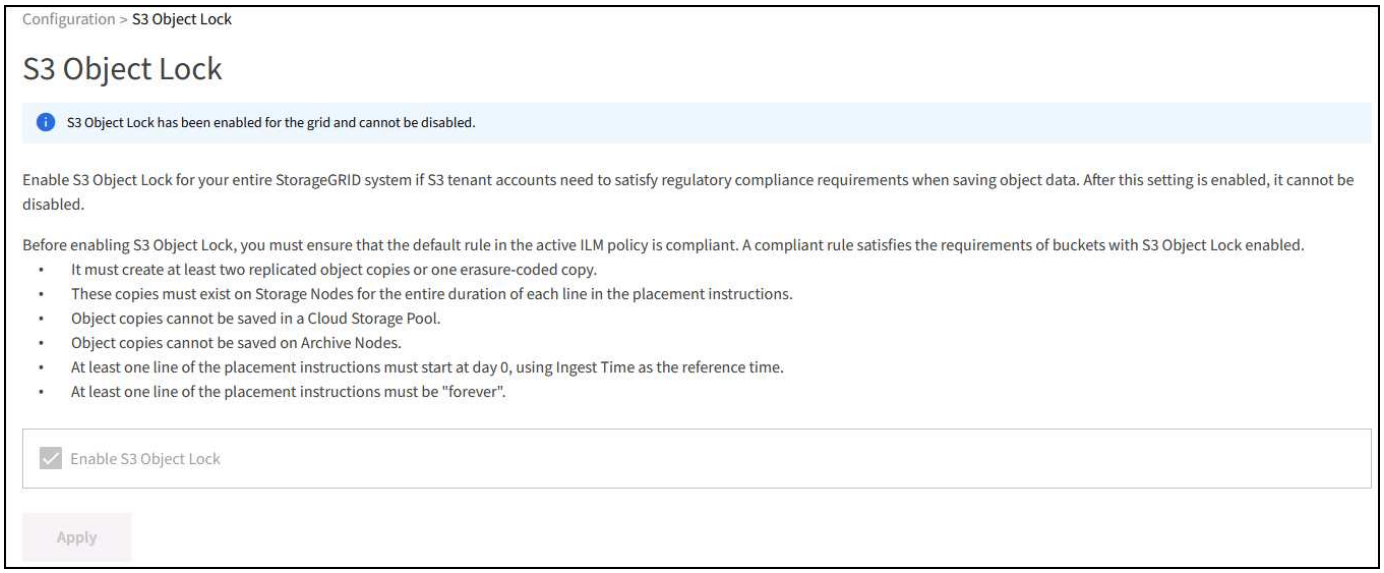
生命周期管理

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。

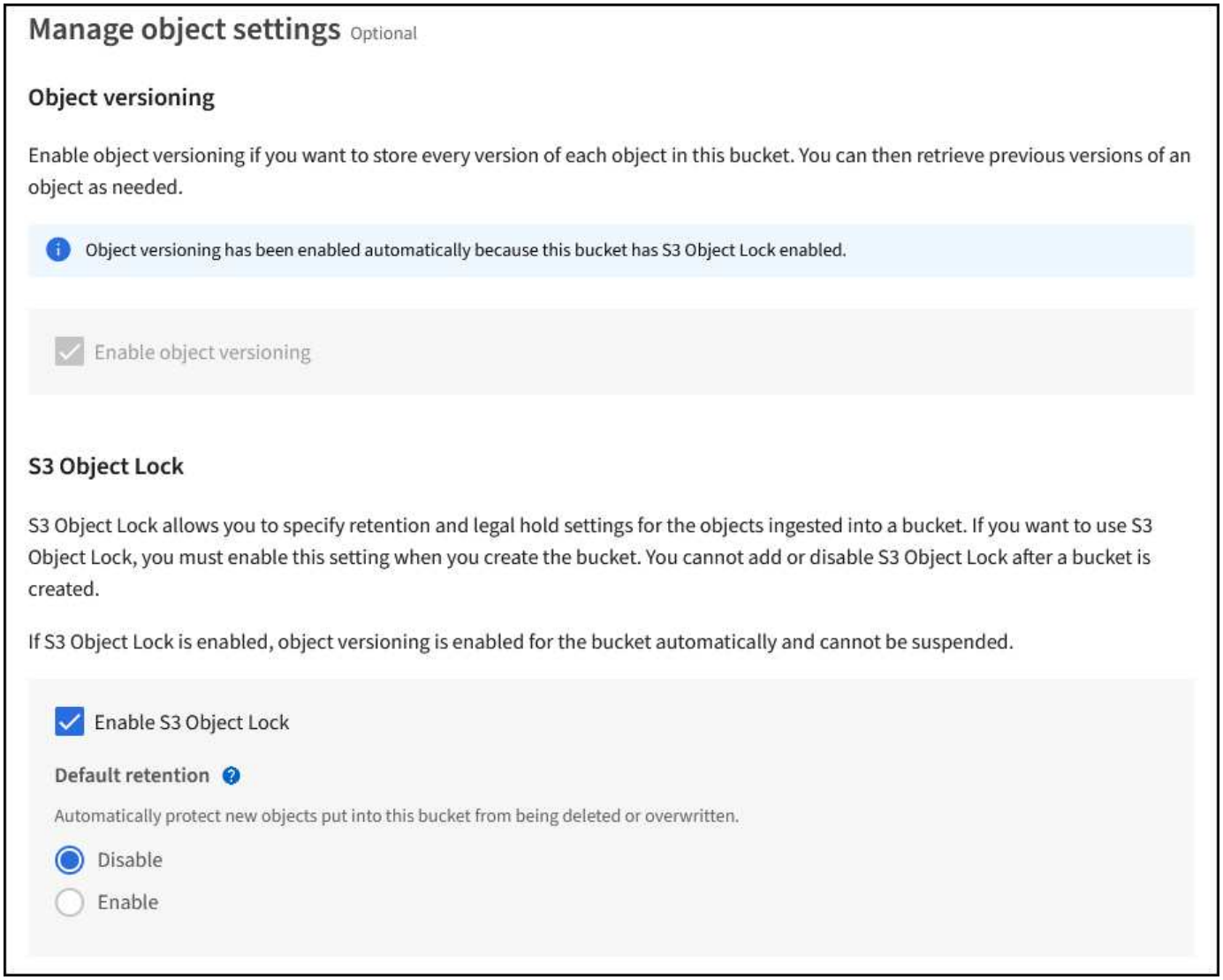
实施要点

StorageGRID

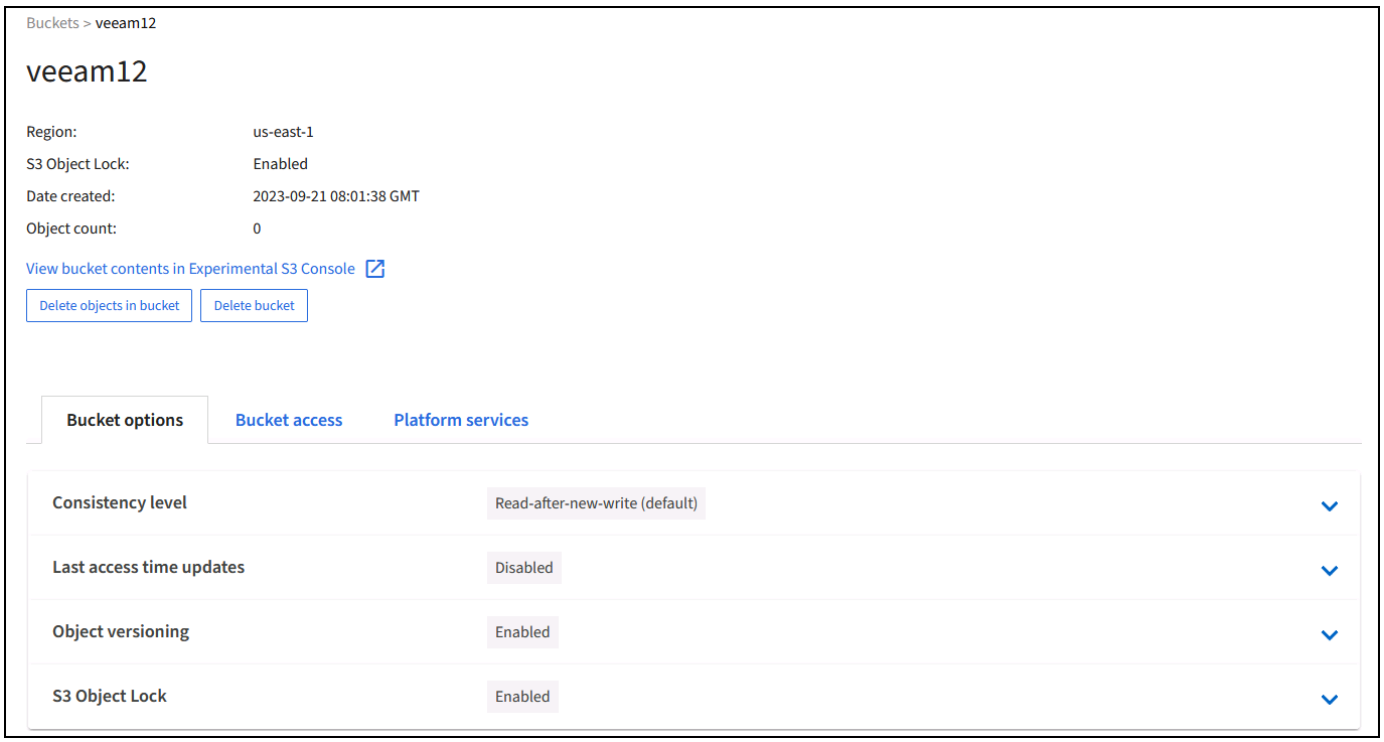
如果需要不可破坏性、请确保在StorageGRID系统上启用对象锁定。在管理UI中的"Configuration/S3 Object Lock"(配置/S3对象锁定)下找到相应选项。



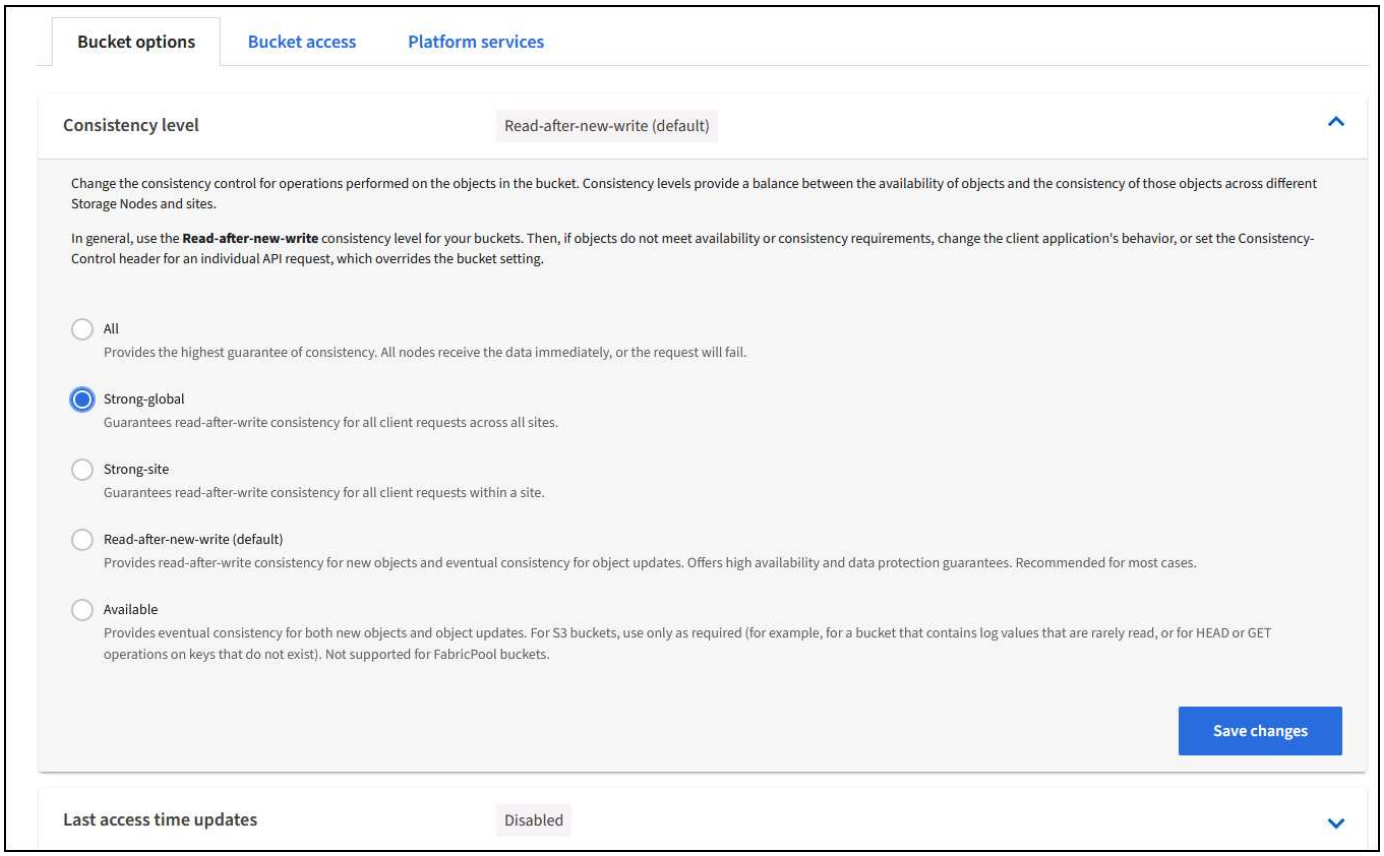
创建存储分段时、如果要将此存储分段用于不可移动备份、请选择"Enable S3 Object Lock"(启用S3对象锁定)。这将自动启用存储分段版本控制。保持禁用默认保留、因为Veeam将明确设置对象保留。如果Veeam不创建不可变备份、则不应选择版本控制和S3对象锁定。



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。

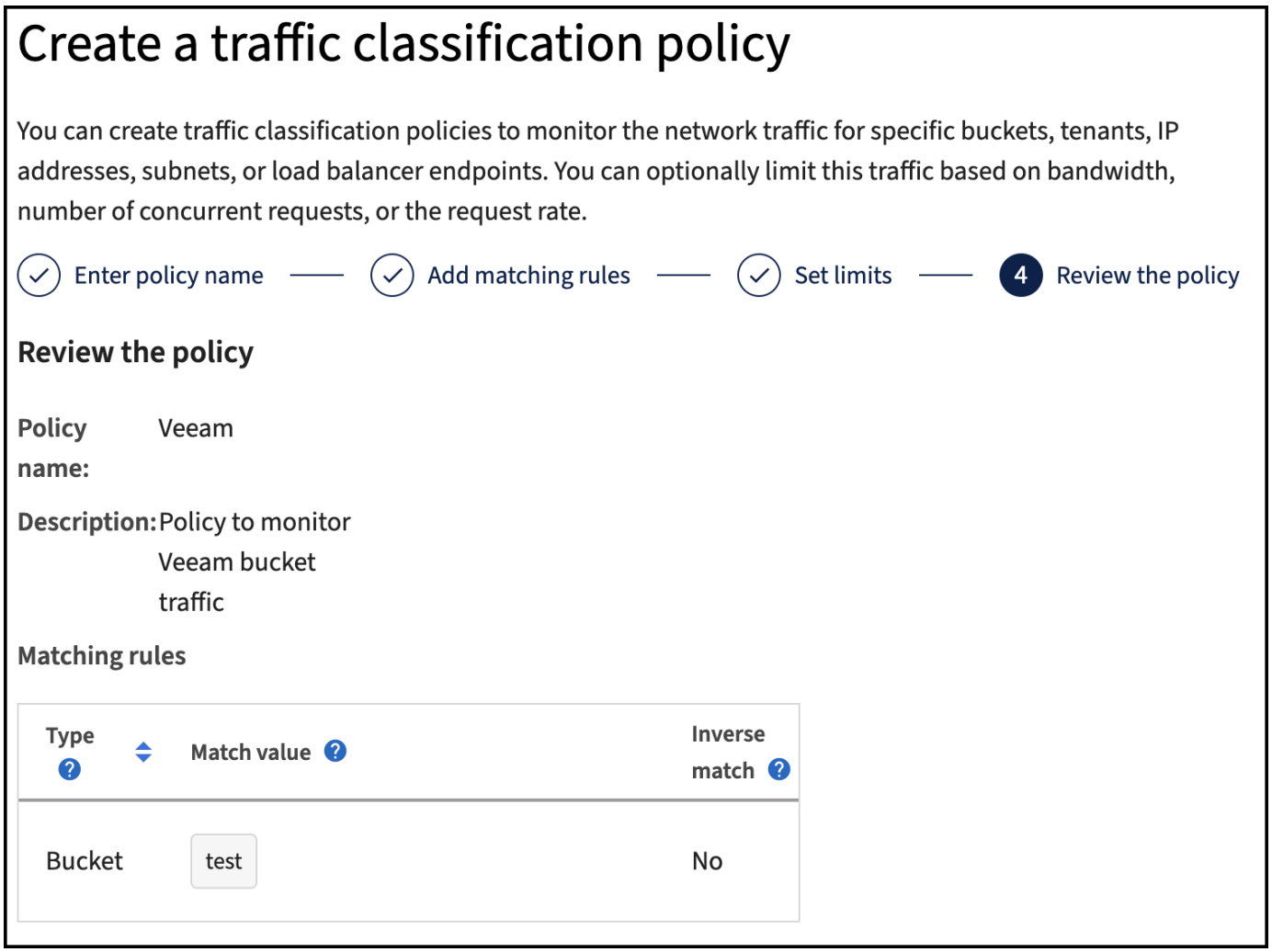


Veeam要求S3存储分段具有强大的一致性。因此、对于Veeam从多个位置访问数据的多站点部署、请选择"strong-globation"。如果Veeam备份和还原仅在单个站点上进行、则一致性级别应设置为"strong-site"。保存更改。



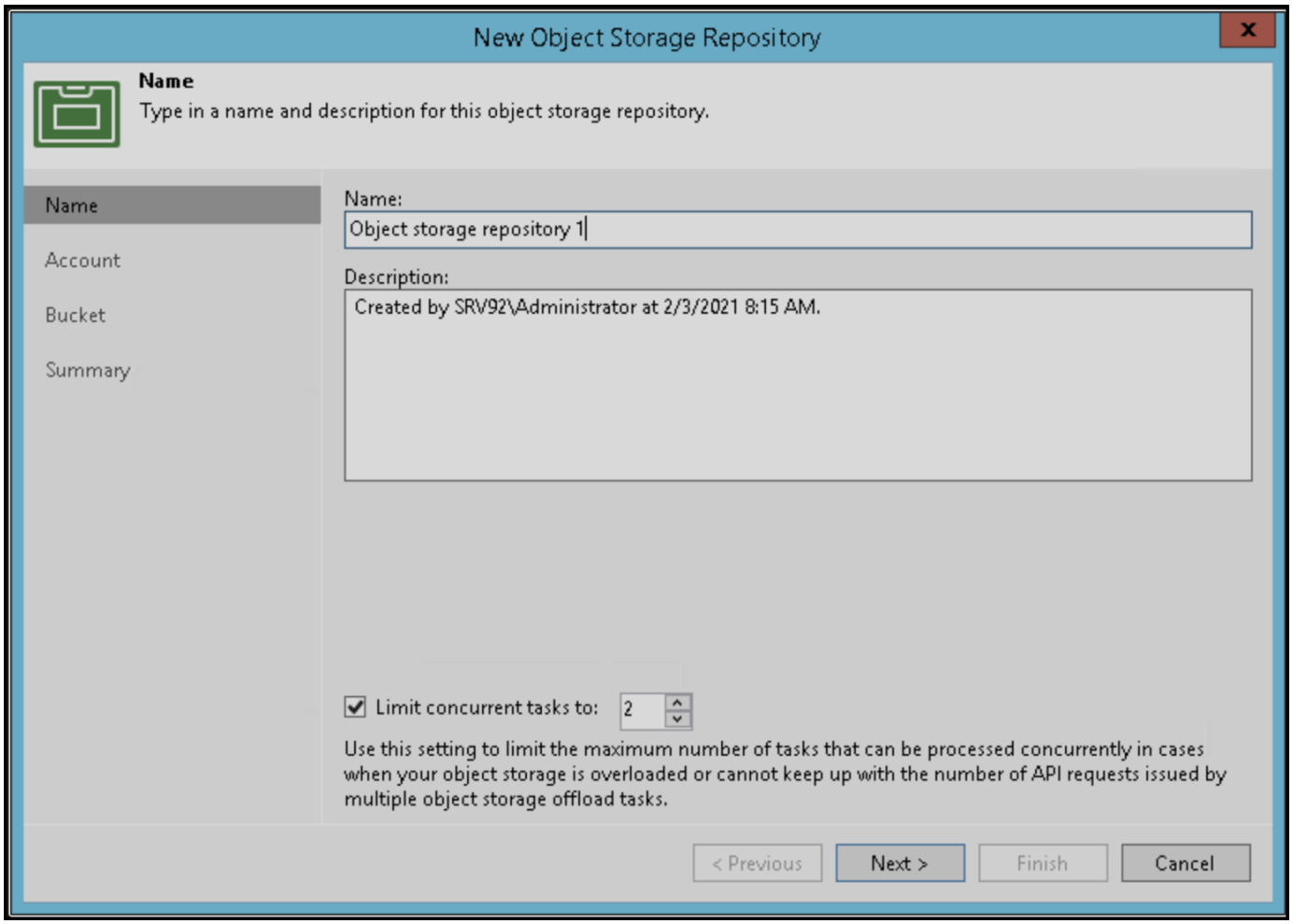
StorageGRID在每个管理节点和专用网关节点上提供集成负载平衡器服务。使用此负载平衡器的众多优势之一是能够配置流量分类策略(QoS)。虽然这些指标主要用于限制应用程序对其他客户端工作负载的影响或将工作负载划分为优先级、但它们还提供了额外的指标收集功能、以协助监控。

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。

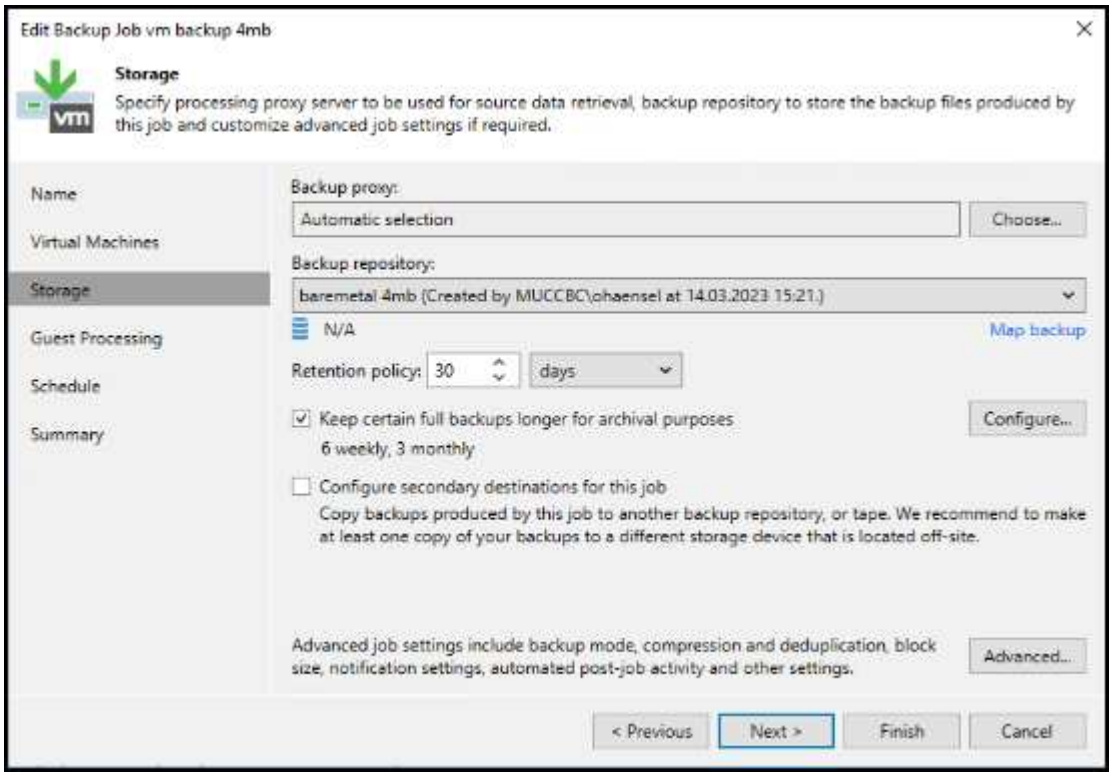


Veeam

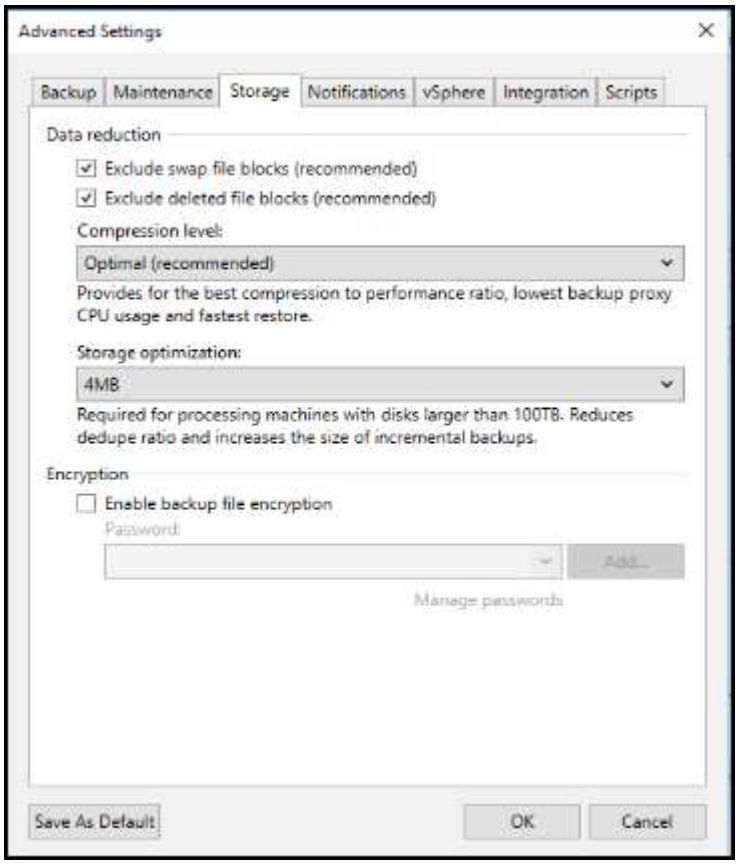
根据StorageGRID设备的型号和数量、可能需要选择并配置对存储分段上的并发操作数的限制。



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

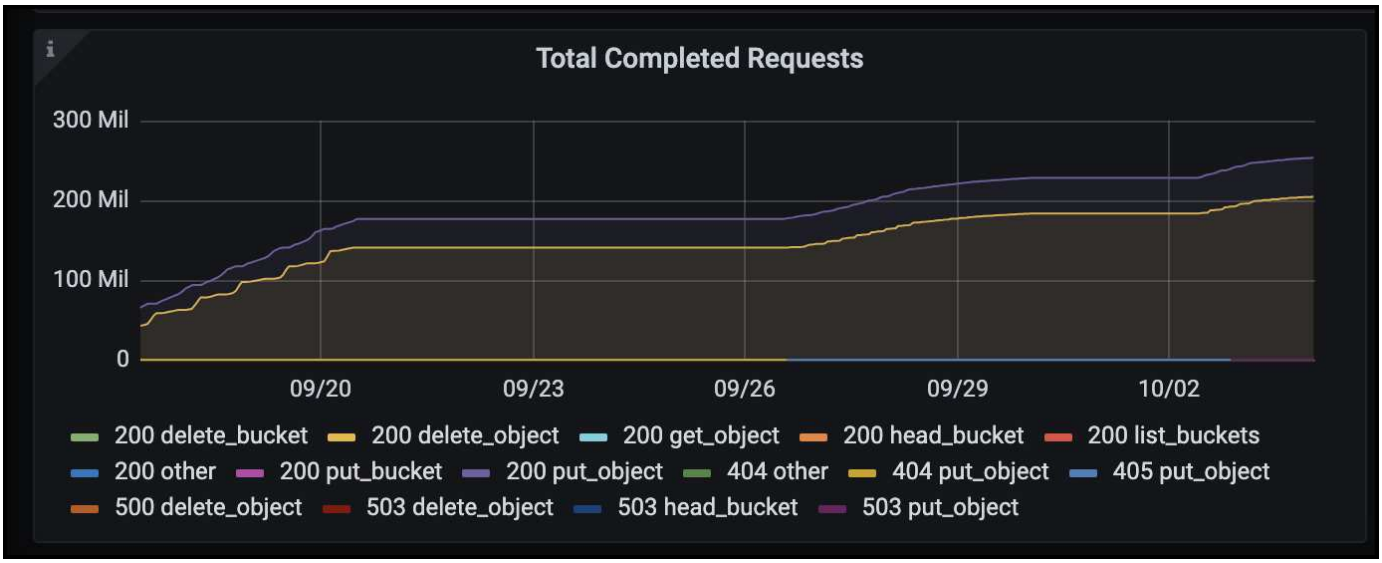
要全面了解Veeam和StorageGRID的协同运行情况、您需要等待第一个备份的保留时间到期。到目前为止、Veeam工作负载主要由Put操作组成、尚未执行任何删除操作。备份数据过期并进行清理后、您现在可以在对象存储中看到完全一致的使用情况、并根据需要调整Veeam中的设置。

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。

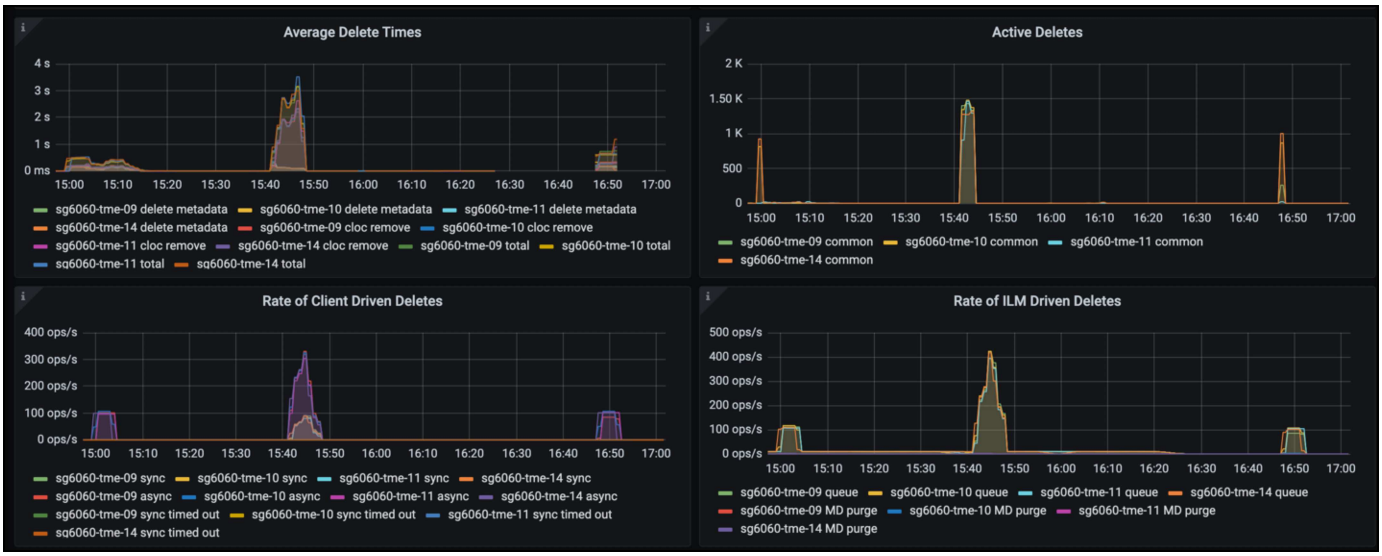
通过查看S3速率和活动请求、您可以按类型查看每个节点正在处理的负载以及请求总数。

"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 11.7产品文档"
- "Veeam备份和复制"

作者：*Oliver Haensel*和*Aron Klein*

使用StorageGRID配置d不良 数据源

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

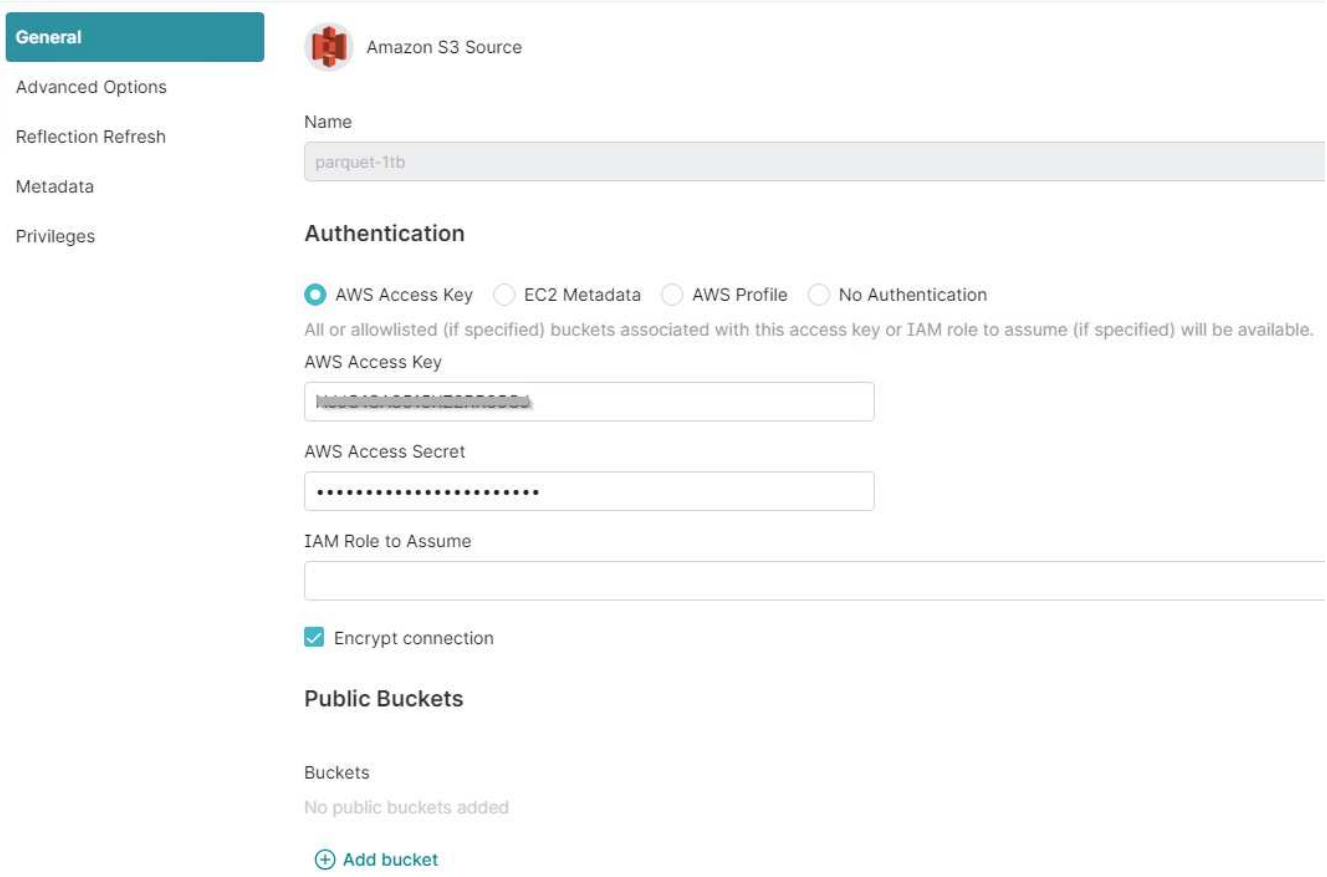
- StorageGRID S3端点URL、租户S3访问密钥ID和机密访问密钥。
- StorageGRID配置建议：禁用数据压缩(默认情况下处于禁用状态)。
  DERMIO使用字节范围GET在查询期间同时从同一对象中提取不同的字节范围。 字节范围请求的典型大小为1 MB。经过压缩的对象会降低字节范围GET性能。

d不良 指南

"连接到Amazon S3 -配置S3兼容存储"。

说明

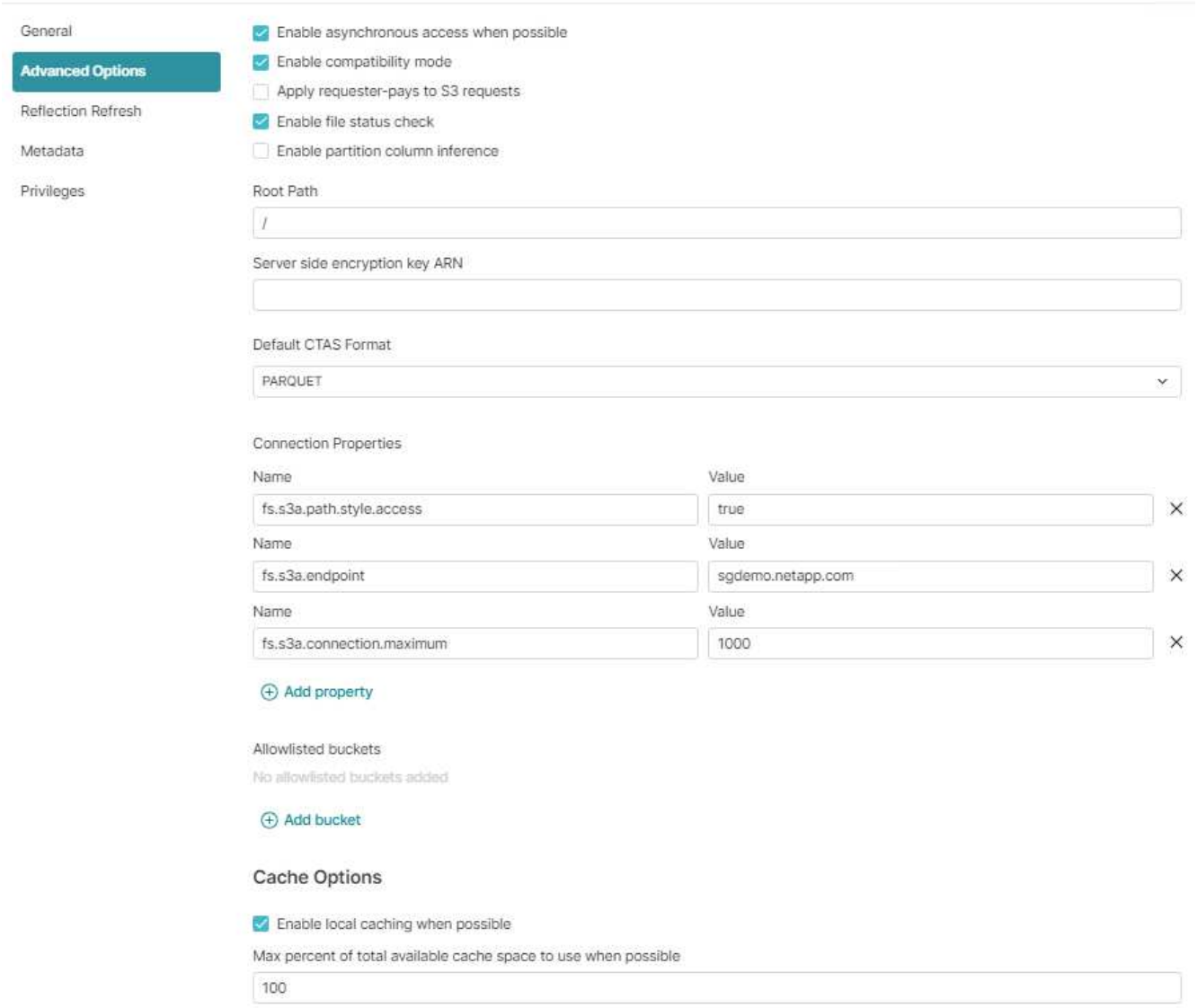
1. 在"Desmio数据集"页面上、单击+符号以添加源、然后选择"Amazon S3"。
2. 输入此新数据源的名称、StorageGRID S3租户访问密钥ID和机密访问密钥。
3. 如果使用https连接到StorageGRID S3端点、请选中"加密连接"复选框。+
   如果对此S3端点使用自签名CA证书、请按照dremio指南说明将此CA证书添加到<JAVA_HOME>服务器的dre/jre/lib/security +中
   屏幕截图示例



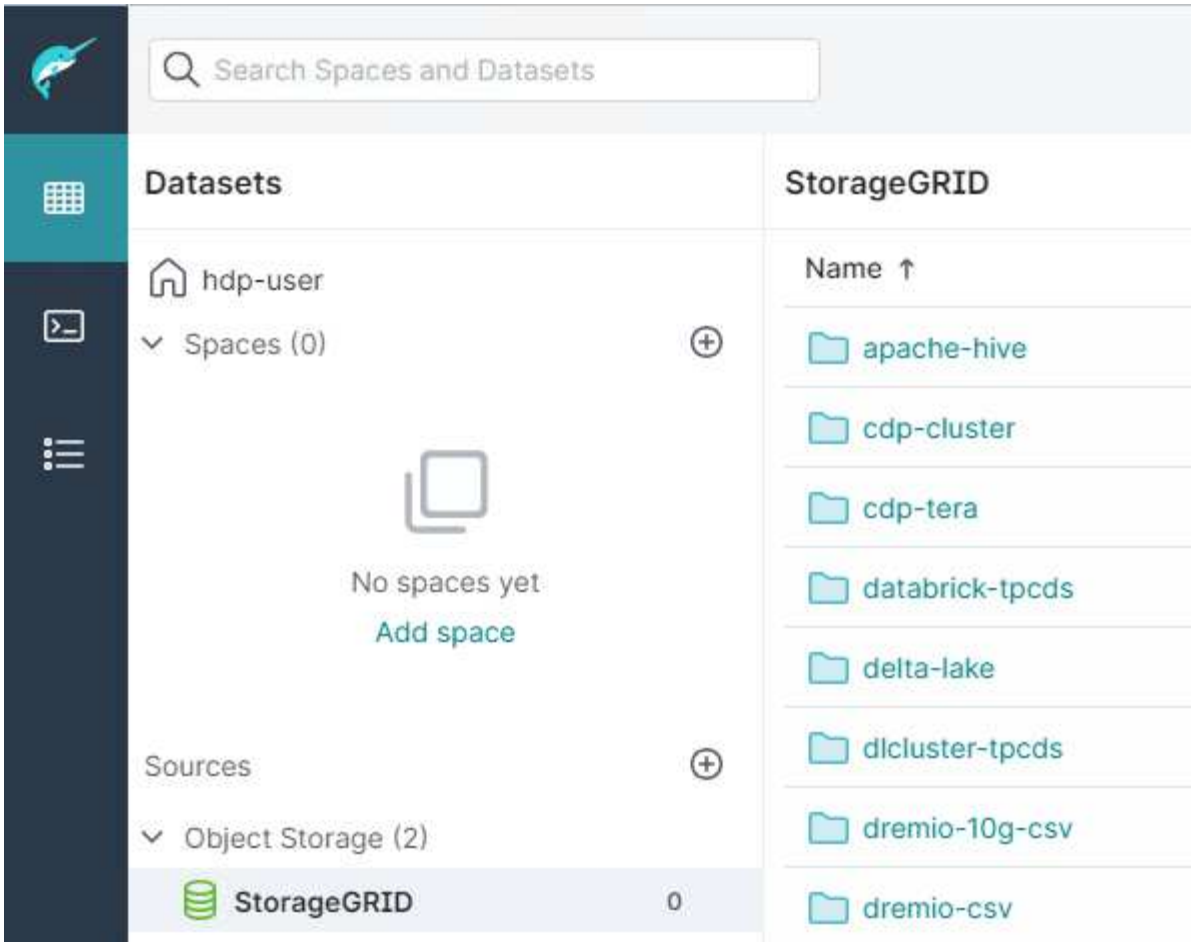
4. 单击"高级选项"、选中"启用兼容模式"
5. 在连接属性下、单击+添加属性并添加这些S3A属性。
6. fs.s3a.connection．maximum默认值为100。 如果S3数据集包含具有100个或更多列的大型镶木地板文件、则必须输入一个大于100的值。 有关此设置的信息、请参见《drefio指南》。

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


Search Spaces and Datasets
Datasets
StorageGRID
hdp-user
Spaces (0)
No spaces yet
Add space
Sources
Object Storage (2)
StorageGRID
0
Name
apache-hive
cdp-cluster
cdp-tera
databrick-tpcds
delta-lake
dlcluster-tpcds
dremio-10g-csv
dremio-csv

作者：郑安杰

过程和API示例

在StorageGRID 上测试和演示S3加密选项

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
```

作者：*Aron Klein*

测试并演示StorageGRID 上的S3对象锁定

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
```

作者：*Aron Klein*

分段和组(IAM)策略示例

以下是存储分段策略和组策略(IAM策略)的示例。

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:::*"
        }
    ]
}
```

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

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/*"
            ]
        }
    ]
}
```

NetApp StorageGRID 博客

您可以在此处找到一些很棒的NetApp StorageGRID 博客：

- 5月10日： "Lab on Demand是StorageGRID的最佳销售工具"
- 5月24日： "借助NetApp和Alluio打造现代化的分析工作负载"
- 5月26日： "StorageGRID：存储和管理内部备份和复制数据"
- 6月9日： "将Cloudera Hadoop S3A连接器与StorageGRID 结合使用"
- 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"
- 8月5日： "NetApp StorageGRID 获得通用标准安全认证"
- 8月16日： "将StorageGRID 与开源ELK堆栈相集成以增强客户体验"
- 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"
- 8月23日： "在StorageGRID 上构建数据湖"
- 9月1日： "请采用这些指标并绘制图表"
- 9月19日： "适用于StorageGRID 的DataLock和勒索软件保护支持"
- 9月26日： "适用于服务提供商的NetApp StorageGRID"
- 10月5日： "在StorageGRID for Snowfl您 的数据上除以数据"
- 10月5日： "NetApp Cloud Insights 增加了StorageGRID 库信息板"
- 11月7日： "StorageGRID 和ONTAP S3支持：差异、相似之处和集成"
- 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"
- 12月6日： "StorageGRID 获得KPMG合规认证"
- 1月16日： "StorageGRID 续订了NF203和ISO/IEC 25051合规性认证"
- 1月18日： "StorageGRID S3对象锁定已通过Veritas NetBackup的验证"
- 2月14日： "巧克力、滑板、表和大型机有哪些共同之处？"
- 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"
- 3月30日： "使用BlueXP通过符合3：2：1的备份策略保护Epic EHR"
- 3月30日： "适用于采用StorageGRID 的Amazon S3 alpha版本的挂载点"
- 5月16日： "StorageGRID对象存储系列中的新增功能"
- 5月16日： "介绍StorageGRID 11.7和全新全闪存对象存储设备GF6112"
- 8月30日： "Amazon S3文件系统的装载点现已正式发布"
- 9月1日： "利用Cloud Insights使用Fluent Bit监控和收集日志"
- 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"
- 11月7日： "采用StorageGRID的光谱逻辑在本机Glacier"
- 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"
- 2月2日： "隆重推出StorageGRID + Ile可 意FS解决方案简介"

- 2月16日： "StorageGRID 11.8:增强的安全性、精简性和用户体验"
- 2月16日： "隆重推出StorageGRID 11.8."

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 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