产品功能指南

How to enable StorageGRID in your environment

NetApp
March 07, 2024

目录

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"。

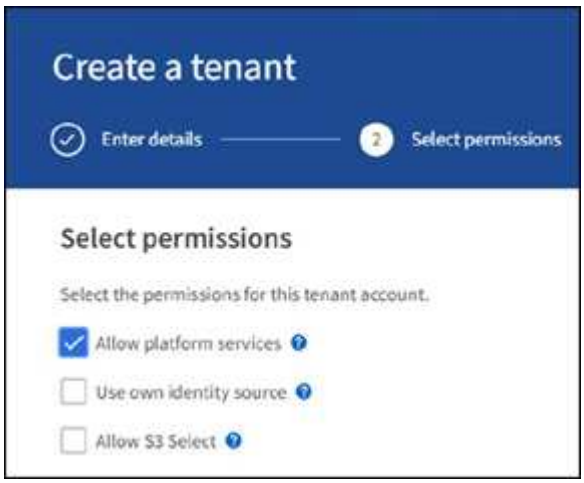
本文档是对的补充 "《StorageGRID 11.6租户指南》" 和为搜索集成服务的端点和存储分段配置提供了分步说明和示例。此处提供的Amazon Web Services (AWS)或内部Elasticsearch设置说明仅用于基本测试或演示。

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

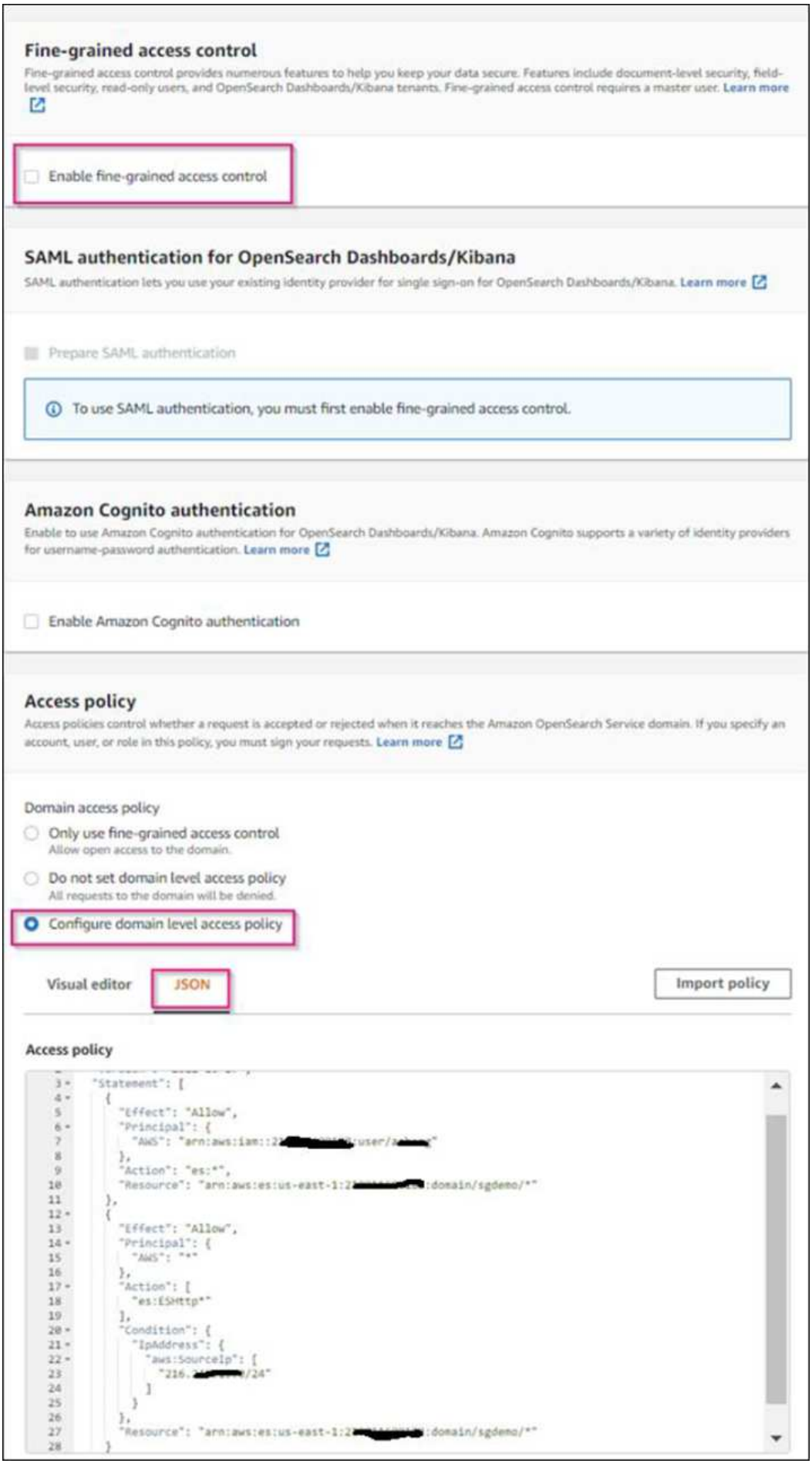
Amazon OpenSearch (以前称为Elasticsearch)服务设置

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。

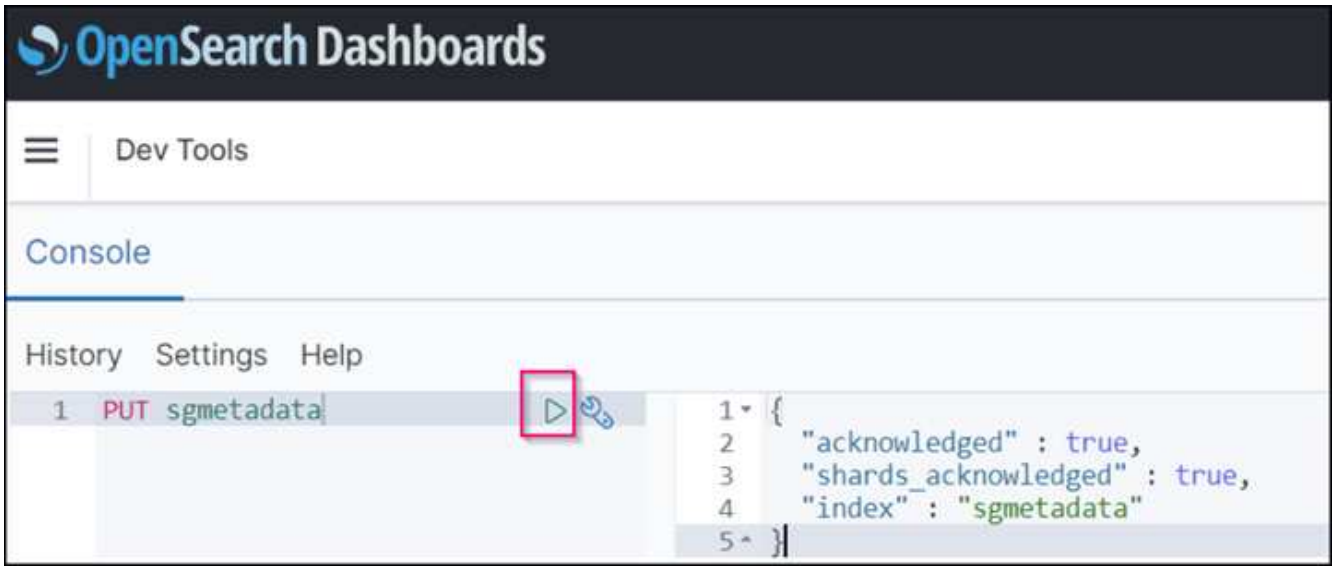
1. 按照中的说明创建新域 "AWS OpenSearch服务入门"、但以下情况除外：
   - 第 4 步域名：sgdemo
   - 第10步：细化访问控制：取消选择启用细化访问控制选项。
   - 第12步：访问策略：选择配置级别访问策略、然后选择JSON选项卡以使用以下示例修改访问策略：
     - 将突出显示的文本替换为您自己的AWS身份和访问管理(IAM) ID和用户名。
     - 将突出显示的文本(IP地址)替换为用于访问AWS控制台的本地计算机的公有 IP地址。
     - 打开浏览器选项卡以 "https://checkip.amazonaws.com" 以查找公有 IP。

```
{

    "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/*"
        }
    ]
}
```

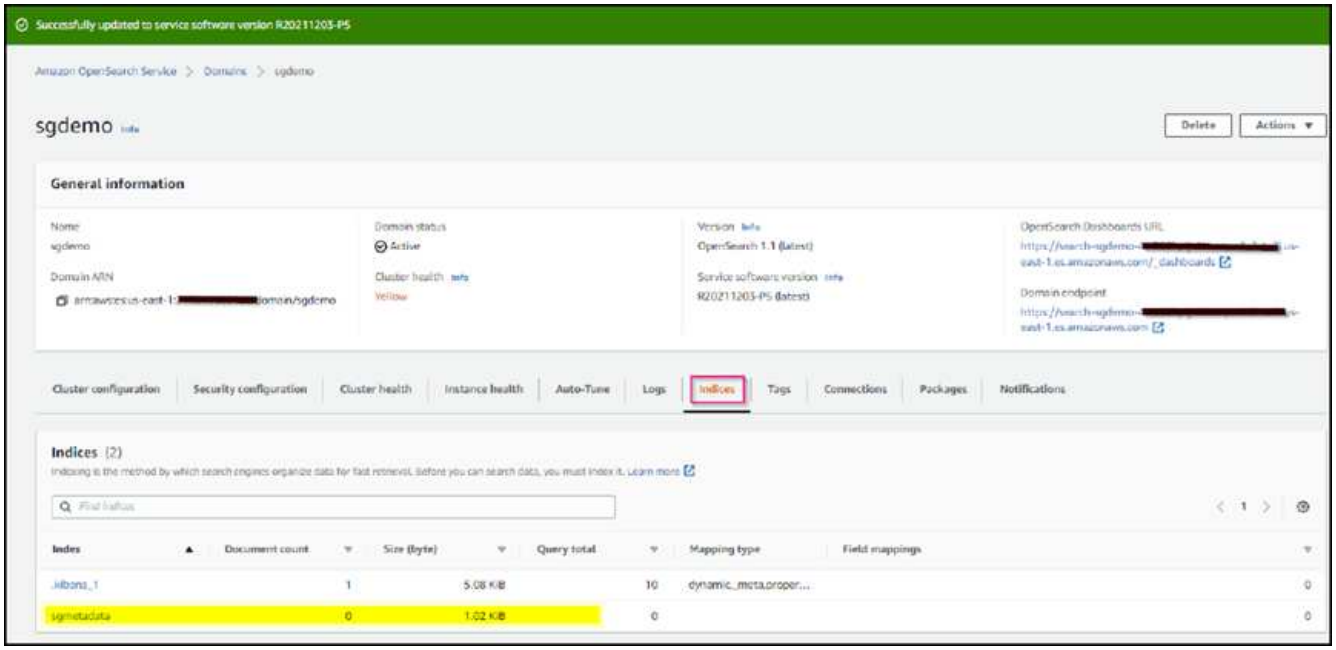

Fine-grained access control
Fine-grained access control provides numerous features to help you keep your data secure. Features include document-level security, field-level security, read-only users, and OpenSearch Dashboards/Kibana tenants. Fine-grained access control requires a master user. Learn more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

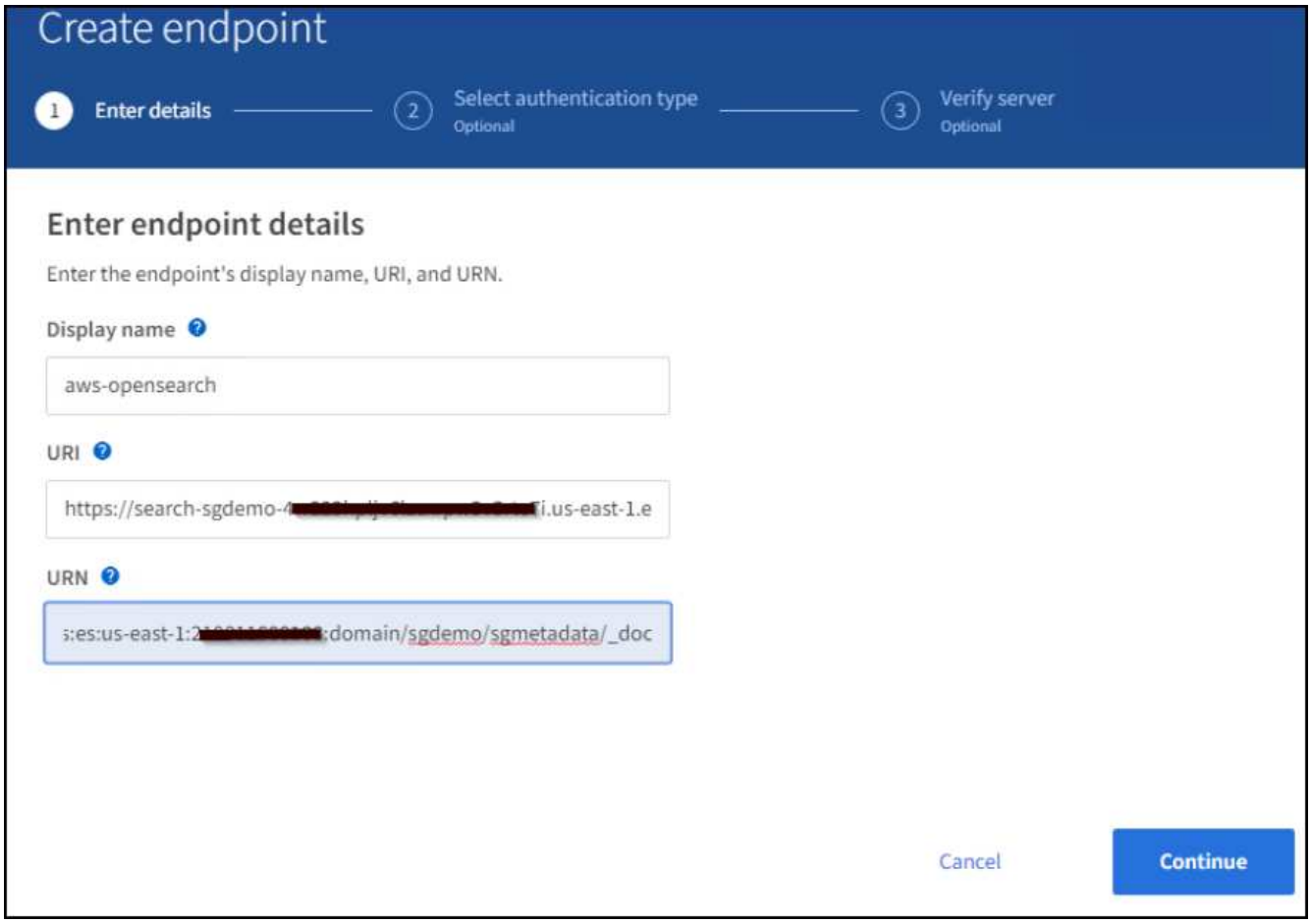


平台服务端点配置

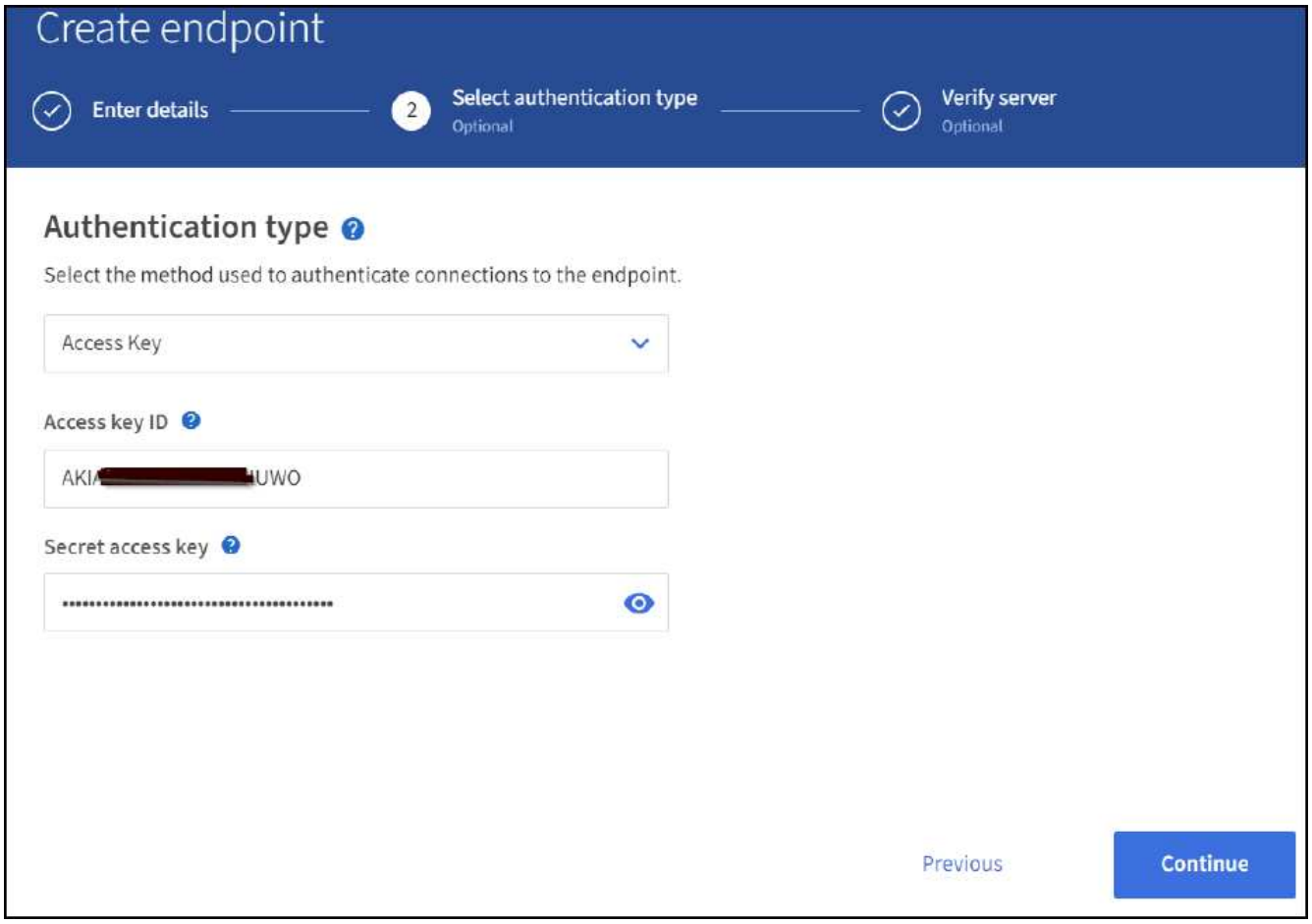
要配置平台服务端点、请执行以下步骤：

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。

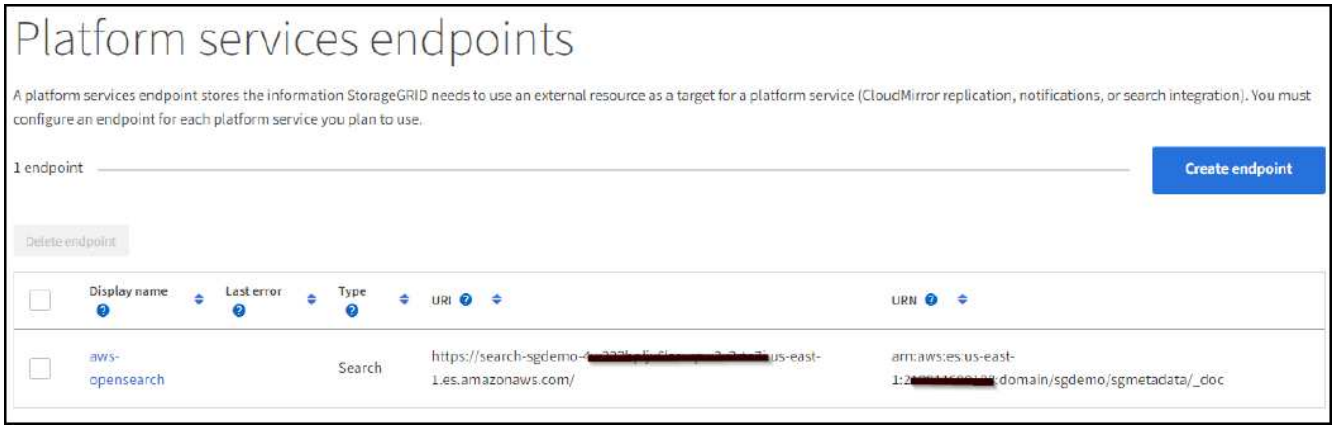
     在此示例中、URN变为`arn：AWS：es：us-east-1：211234567890：domain/sgdemo /sgmedata/_doc`。



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.

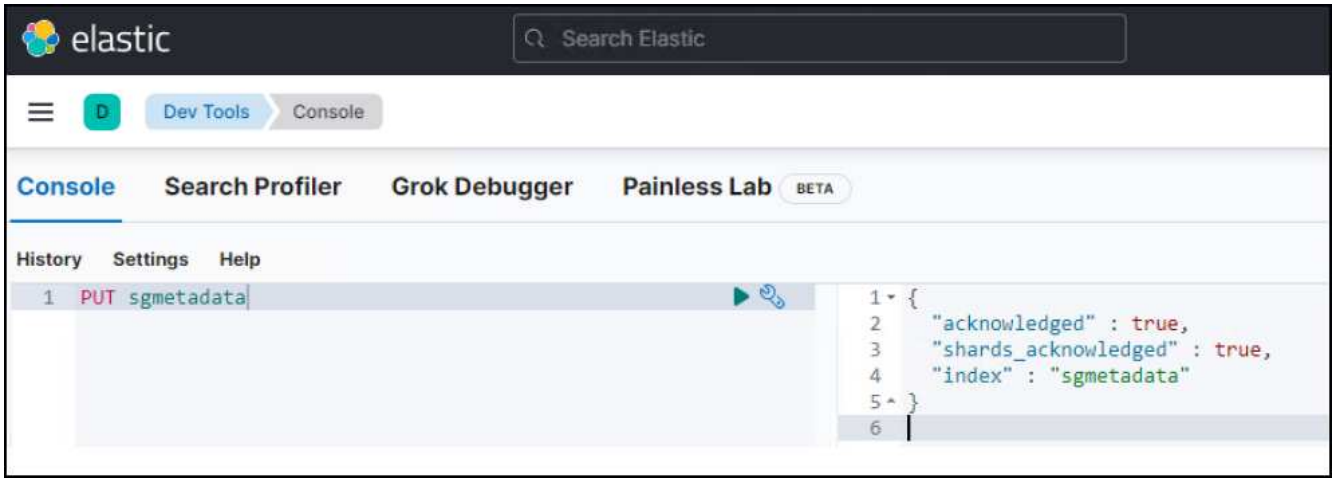
1. In a new terminal session, run:

```
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.

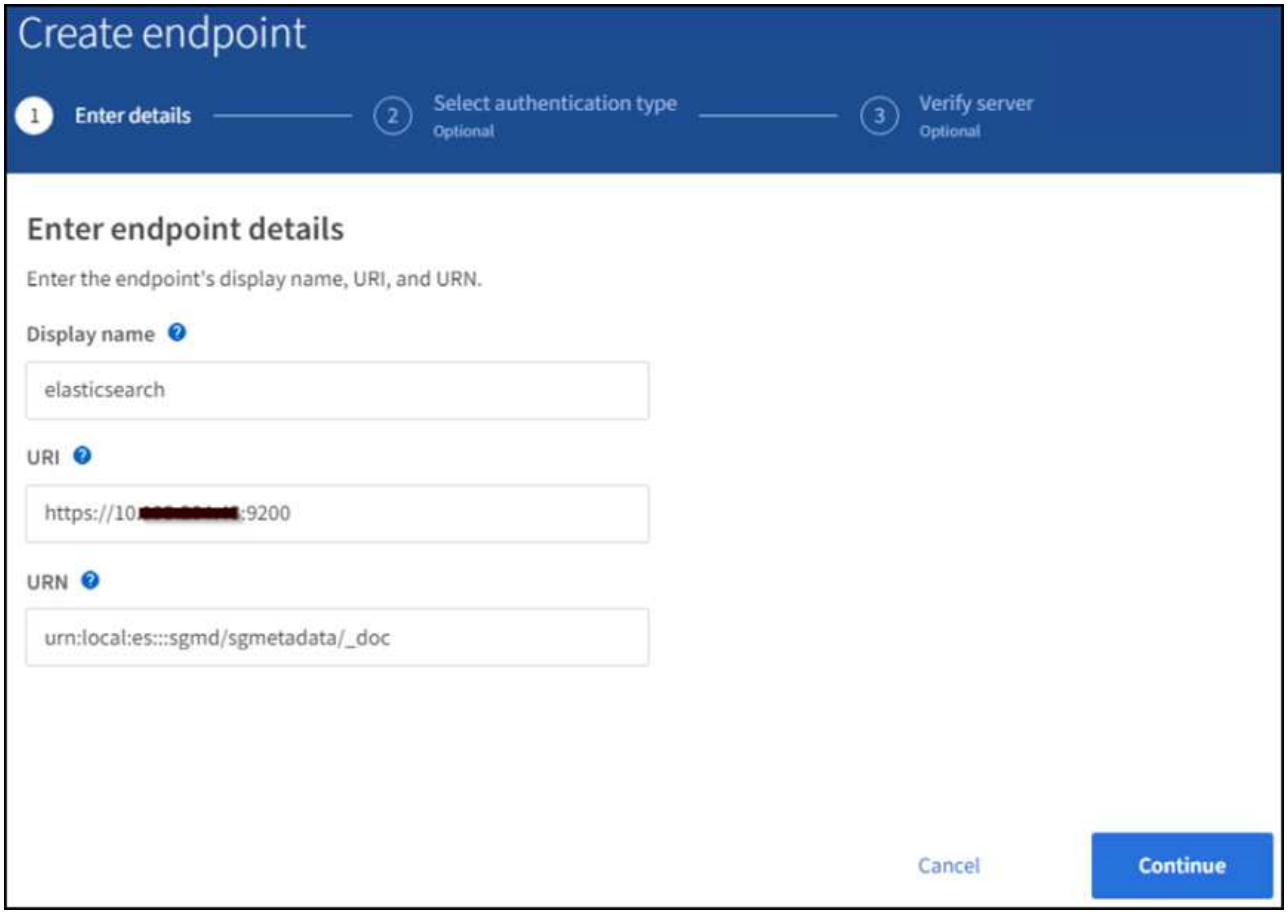
3. 启动Kibana Docker容器后、控制台中将显示URL链接`\https://0.0.0.0:5601`。将0.0.0.0替换为URL中的服务器IP地址。
4. 使用用户名`弹性`和Elastic在上一步中生成的密码登录到Kibana UI。
5. 首次登录时、请在信息板欢迎页面上选择"Explore on your own"。从菜单中、选择"Management">"Dev Tools"。
6. 在开发工具控制台屏幕上、输入`PUT <index>`、在此可以使用此索引存储StorageGRID 对象元数据。我们在此示例中使用索引名称`sgmetadata`。单击小三角形符号以执行PUT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



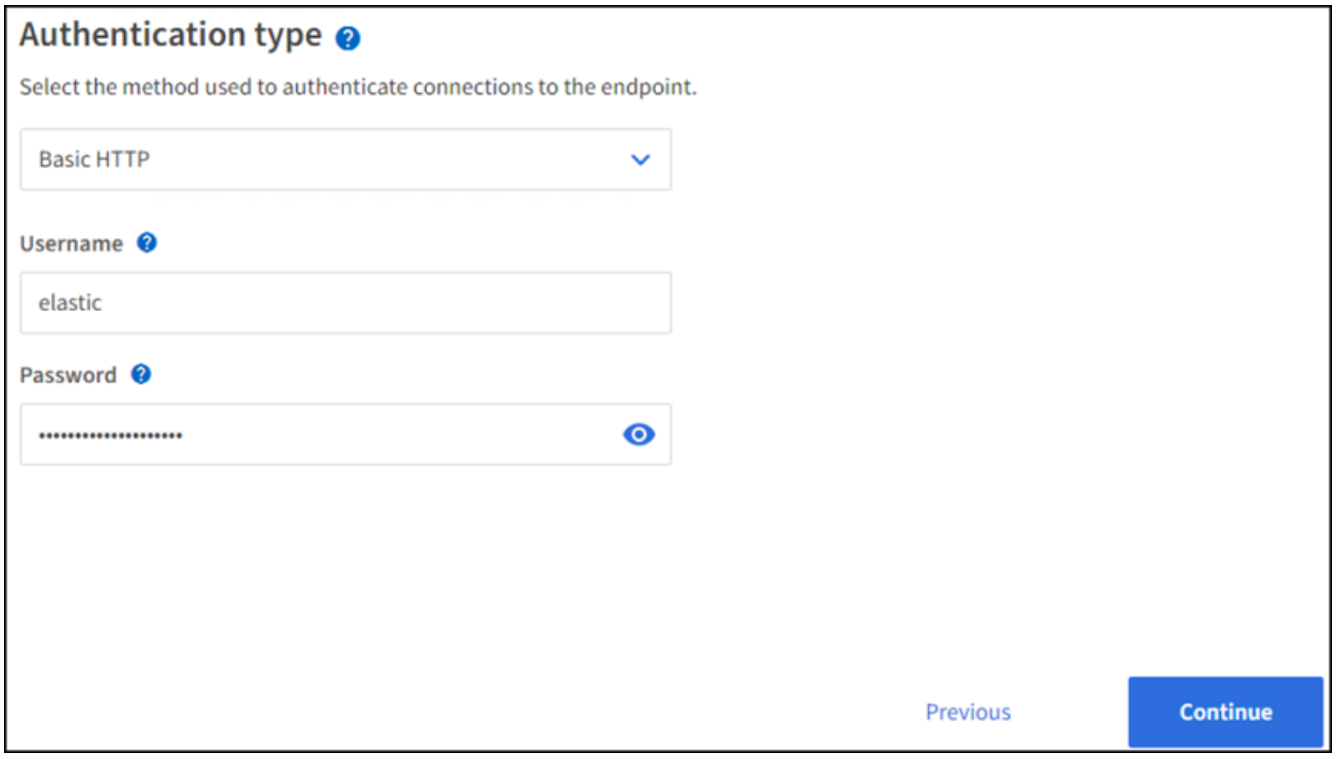
平台服务端点配置

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`

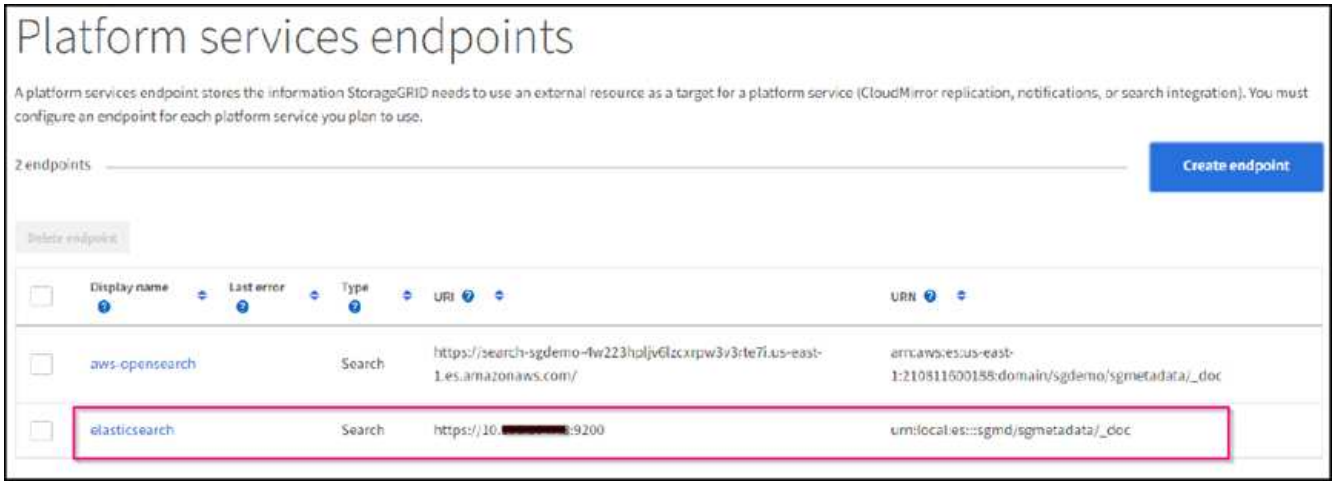


3. 选择基本HTTP作为身份验证类型、输入用户名`弹性`以及Elasticsearch安装过程生成的密码。要转到下一页、请单击继续。



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：

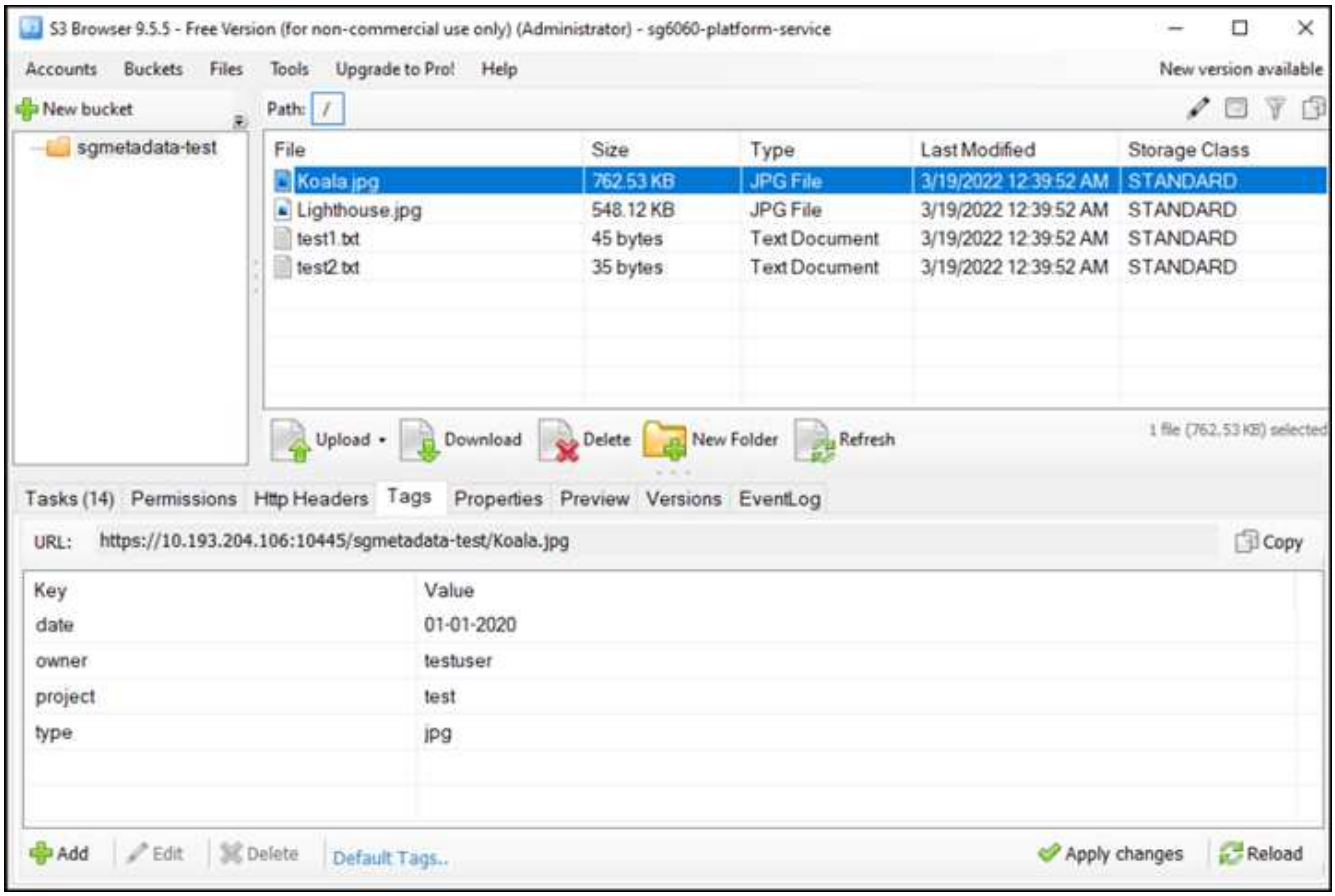
1. 在租户管理器中、转至存储(S3)>分段
2. 单击Create Bucket、输入存储分段名称(例如、`sgmetada-test`)并接受默认值`us-east-1` Region。
3. 单击"继续">"创建存储分段"。
4. 要打开存储分段概述页面、请单击存储分段名称、然后选择平台服务。
5. 选择启用搜索集成对话框。在提供的XML框中、使用以下语法输入配置XML。

   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。



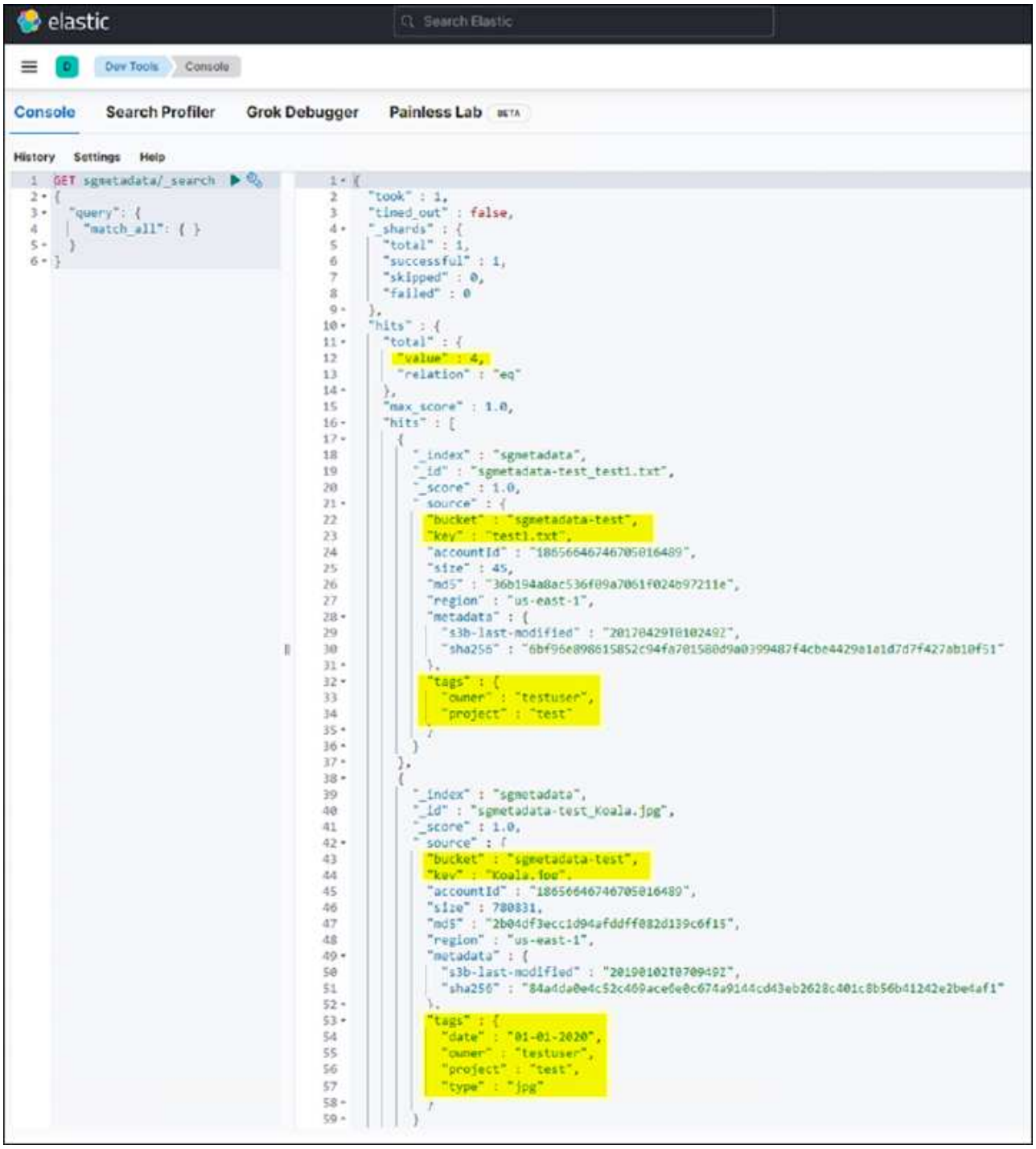
7. 使用Kibana UI验证对象元数据是否已加载到sgmetadata的索引中。

   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。

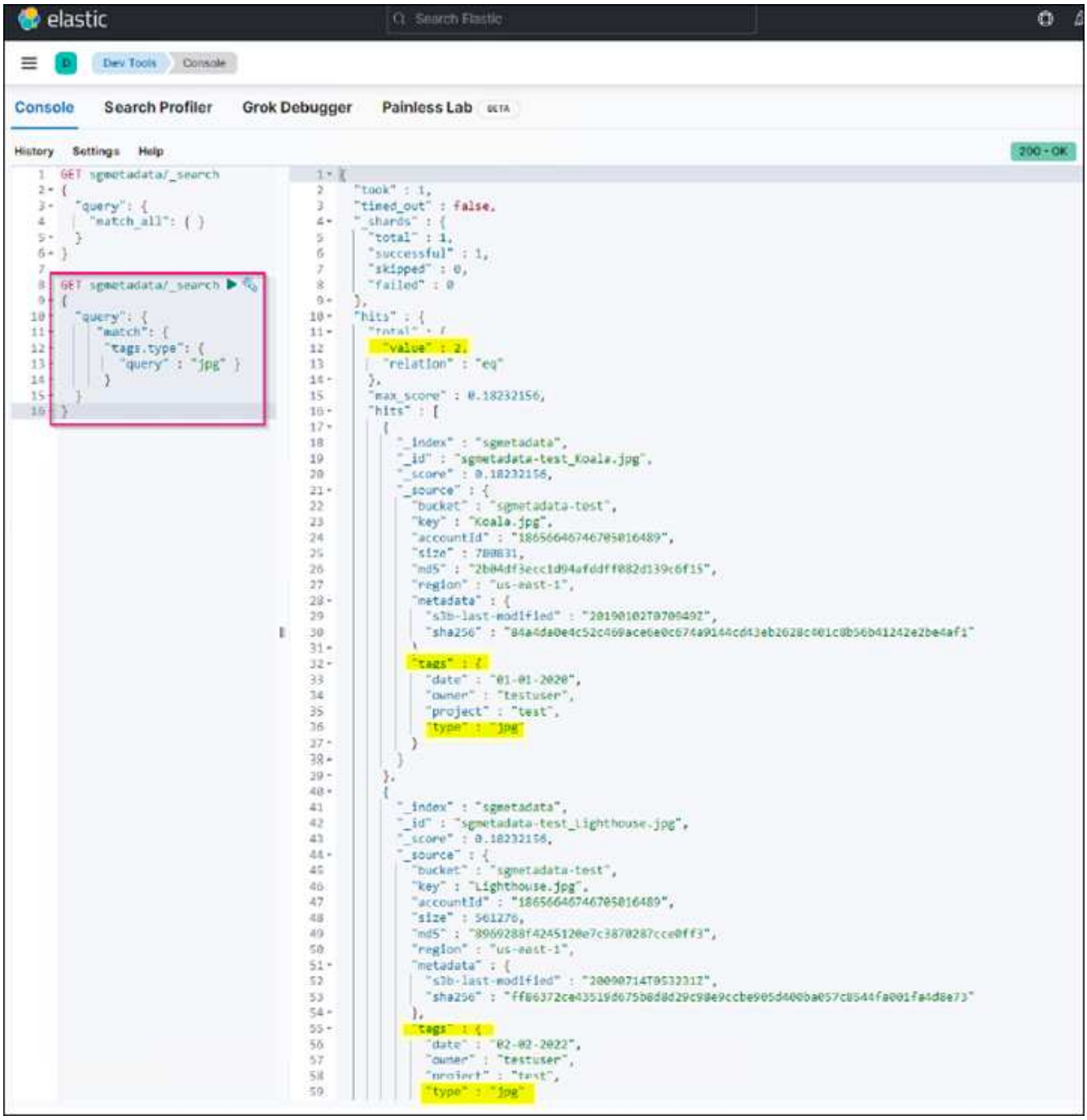
```
GET sgmetadata/_search
{
    "query": {
        "match_all": { }
}
}
```



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

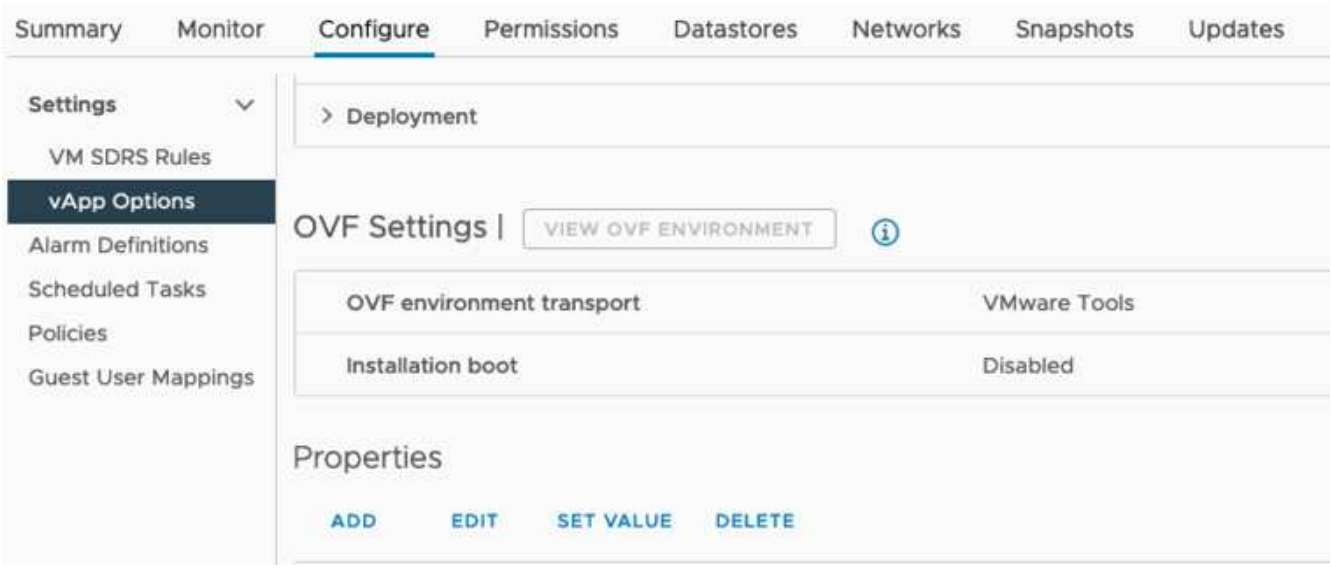
要销毁第一个网关节点、请执行以下步骤：

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。

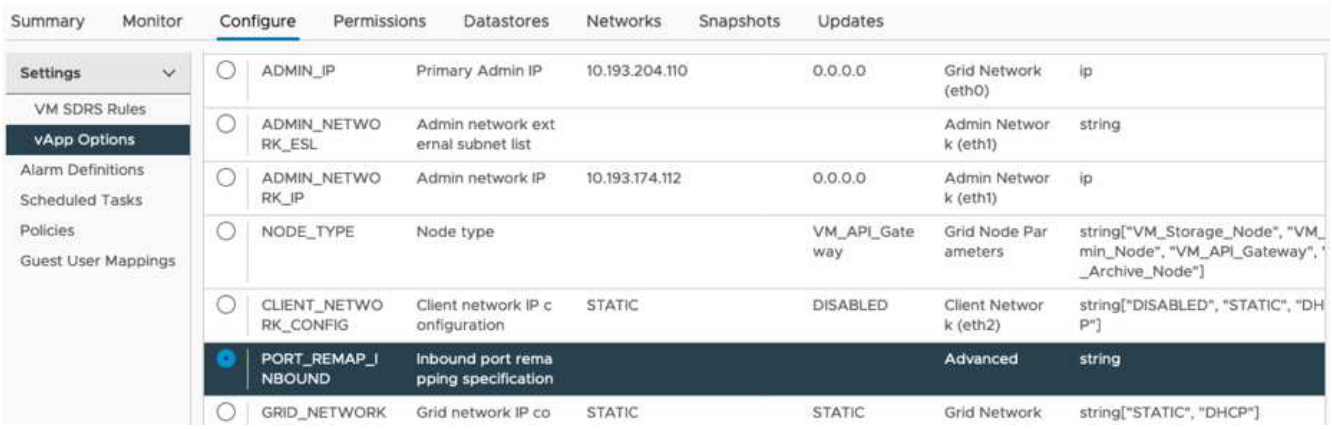
部署替代网关节点

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

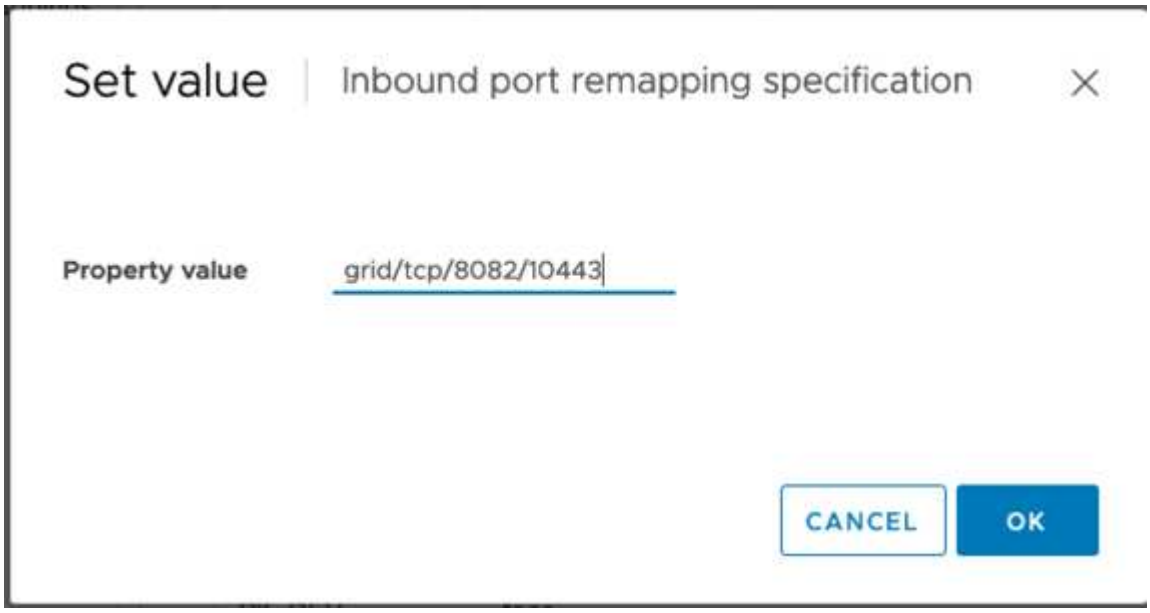


4. 滚动到属性列表顶部、然后单击编辑

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。

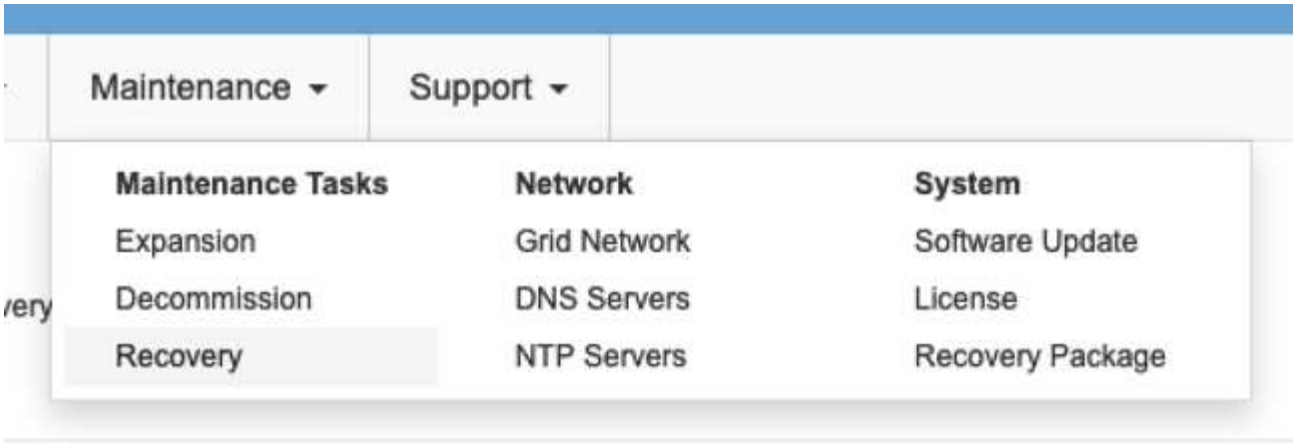


8. 如果使用多个网络、请使用逗号(、)分隔网络字符串、例如GRIDE/TCP/8082/10443、admin/TCP/8082/10443、client/TCP/8082/10443

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`

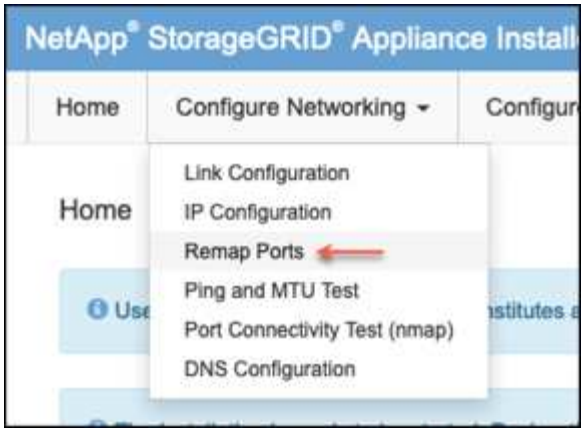
重建管理节点

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`

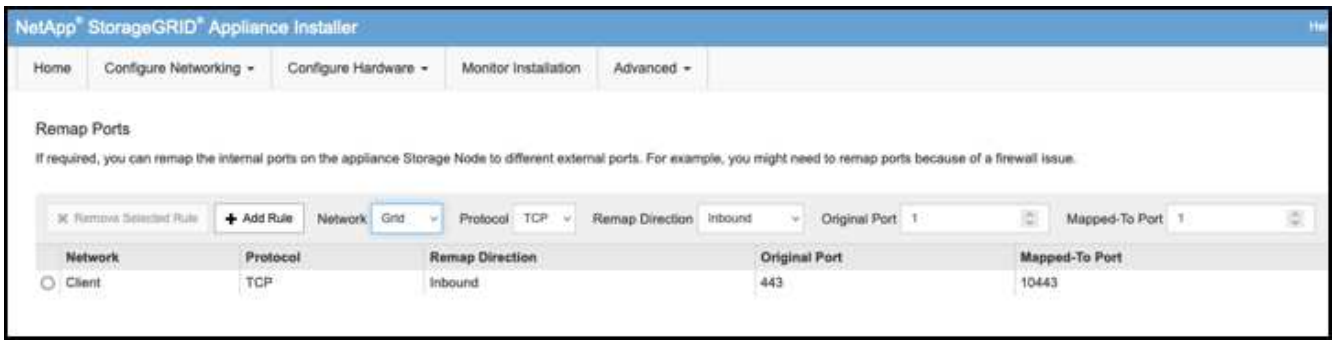
```
root@sg100-01:~ # sgareinstall
WARNING: All StorageGRID Webscale services on this node will be shut
down.
WARNING: Data stored on this node may be lost.
WARNING: You will have to reinstall StorageGRID Webscale to this
node.

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*

版权信息

商标信息