TR-4626：负载平衡器

How to enable StorageGRID in your environment

NetApp

July 05, 2024

目录

TR-4626：负载平衡器

将第三方负载平衡器与StorageGRID结合使用

了解第三方和全局负载平衡器在StorageGRID等对象存储系统中的作用。

使用第三方负载平衡器实施NetApp®StorageGRID®的一般指导。

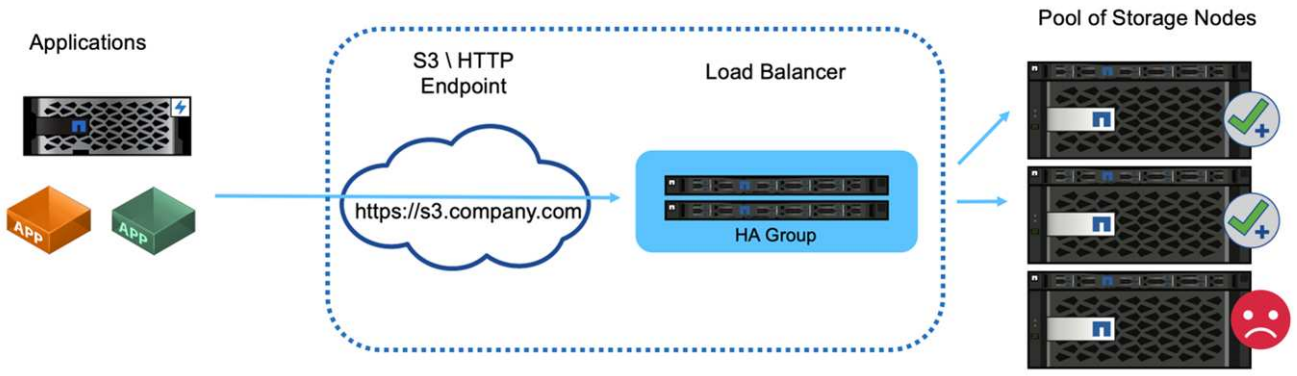
对象存储与"云存储"一词同义、正如您所期望的那样、利用云存储的应用程序会通过URL为该存储寻址。在这一简单URL的支持下、StorageGRID可以在单个站点或分布在不同地理位置的站点上扩展容量、性能和持久性。负载平衡器是实现这种精简性的组件。

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

负载平衡器基础知识

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

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



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

本地和全局负载平衡器

负载平衡器有两种类型：

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

可选的、具体取决于StorageGRID站点数量和应用程序要求。

StorageGRID网关节点负载平衡器与第三方负载平衡器

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

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

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

StorageGRID负载平衡器具有以下优势：

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

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

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

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

了解如何在StorageGRID中为HTTPS实施SSL证书

了解在StorageGRID中实施SSL证书的重要性和步骤。

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

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

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

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

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

在StorageGRID中配置受信任的第三方负载平衡器

了解如何在StorageGRID中配置受信任的第三方负载平衡器。

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

了解本地流量管理器负载平衡器

浏览有关本地流量管理器负载平衡器的指导、并确定最佳配置。

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

创建存储节点的资源组

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

- S3 HTTPS：18082
- S3 HTTP：18084

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

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

运行状况检查

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

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

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

建议的轮询间隔为每秒一次、在三次检查失败后将节点标记为脱机。

S3运行状况检查示例

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

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

基于文件或内容的运行状况检查

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

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

如果需要执行基于内容的运行状况检查、请使用具有专用S3存储分段的专用租户。

会话持久性

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

虚拟托管模式寻址

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

要支持虚拟托管模式、请执行以下操作：

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

SSL终止

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

支持三种配置：

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

直通配置

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

源客户端IP可见性

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

要启用XFF标头以查看客户端应用程序的IP、请执行以下步骤：

步骤

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

负载平衡策略

大多数负载平衡解决方案都提供多种负载平衡策略。以下是常见策略：

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

随着可供选择的存储节点数量不断增加、算法的选择就不再那么重要了。

数据路径

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

验证连接分布

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

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

了解StorageGRID配置的几个用例

了解客户和NetApp IT实施的StorageGRID配置的少数用例。

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

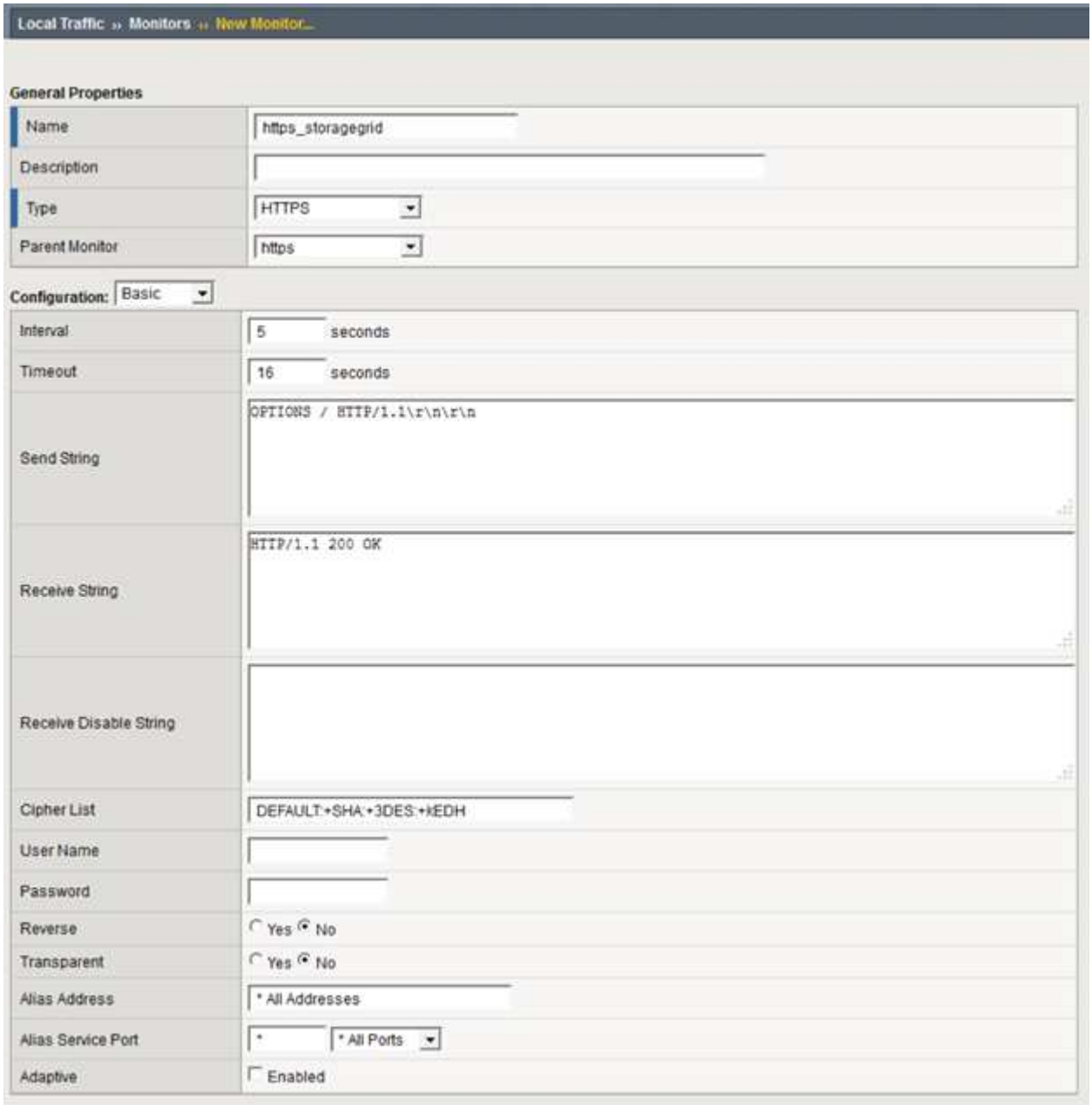
用于S3存储分段的F5 BIG-IP本地流量管理器运行状况检查监控器

要配置F5 BIG-IP本地流量管理器运行状况检查监控器、请执行以下步骤：

步骤

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

d. 在Receive String (接收字符串)字段中，输入： `HTTP/1.1 200 OK`。



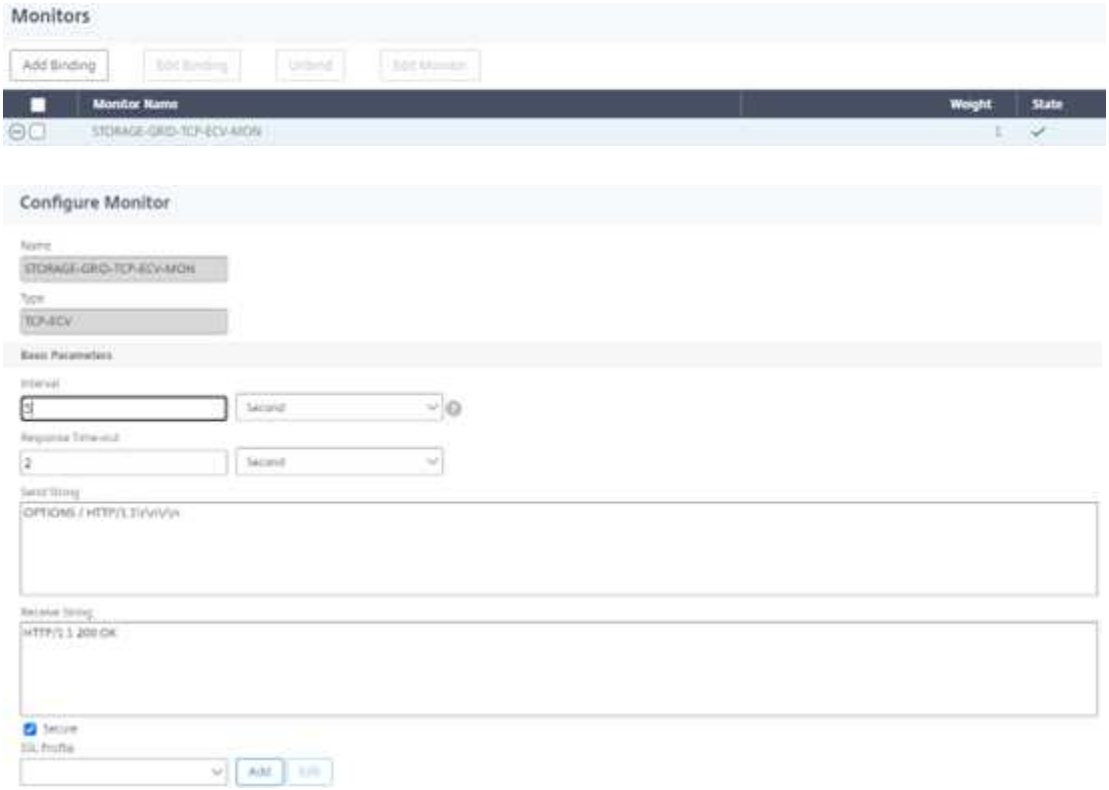
2. 在创建池中、为所需的每个端口创建一个池。
   a. 分配在上一步中创建的运行状况监控器。
   b. 选择负载平衡方法。
   c. 选择服务端口：18082 (S3)。
   d. 添加节点。

Citrix NetScaler

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

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

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



Loadbalancer.org

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

凯普

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

HA 代理

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

以下是在HAProxy上终止SSL的示例：

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

以下是SSL直通示例：

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

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

验证StorageGRID中的SSL连接

了解如何在StorageGRID中验证SSL连接。

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

了解StorageGRID的全局负载平衡要求

了解StorageGRID中全局负载平衡的设计注意事项和要求。

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

合、或者第三方的组合、或者前面讨论的许多第三方的组合可以同时提供GSLB和站点本地负载平衡。