使用外部系统日志服务器

StorageGRID 11.7

NetApp
April 12, 2024

目录

使用外部系统日志服务器

外部系统日志服务器的注意事项

请按照以下准则估算所需外部系统日志服务器的大小。

什么是外部系统日志服务器?

外部系统日志服务器是 StorageGRID 外部的服务器，您可以使用它在一个位置收集系统审核信息。通过使用外部系统日志服务器，您可以配置审核信息的目标，以便减少管理节点上的网络流量并更高效地管理信息。可以发送到外部系统日志服务器的审核信息类型包括：

- 包含在正常系统操作期间生成的审核消息的审核日志
- 与安全相关的事件，例如登录和上报给 root
- 如果需要创建支持案例以对遇到的问题描述 进行故障排除，则可能需要请求的应用程序日志

如何估算外部系统日志服务器的大小

通常，您的网格会进行规模估算，以达到所需的吞吐量，该吞吐量是按每秒 S3 操作数或每秒字节数定义的。例如，您可能要求网格每秒处理 1 ， 000 次 S3 操作，或者每秒处理 2 ， 000 MB 的对象载入和检索。您应根据网格的数据要求调整外部系统日志服务器的大小。

本节提供了一些启发式公式，可帮助您估算外部系统日志服务器需要能够处理的各种类型的日志消息的速率和平均大小，这些消息以网格的已知或所需性能特征（每秒 S3 操作数）表示。

在估计公式中使用每秒 **S3** 操作数

如果网格的大小以每秒字节为单位表示，则必须将此规模估算转换为每秒 S3 操作，才能使用估算公式。要转换网格吞吐量，您必须先确定平均对象大小，您可以使用现有审核日志和指标（如果有）中的信息或根据您对将使用 StorageGRID 的应用程序的了解来确定平均对象大小。例如，如果您的网格大小调整为可实现 2 ， 000 MB/ 秒的吞吐量，而您的平均对象大小为 2 MB ，则您的网格大小将调整为能够每秒处理 1 ， 000 次 S3 操作（ 2 ， 000 MB/ 2 MB ）。

> 以下各节中用于估算外部系统日志服务器规模的公式提供了常见案例估算（而不是最坏案例估算）。根据您的配置和工作负载，您可能会发现系统日志消息或系统日志数据卷的速率高于或低于公式的预测。这些公式仅供参考。

审核日志的估计公式

如果除了网格应支持的每秒 S3 操作数之外，您没有其他有关 S3 工作负载的信息，则可以使用以下公式估算外部系统日志服务器需要处理的审核日志卷， 假设您将审核级别设置为默认值（所有类别均设置为正常，但存储设置为错误除外）：

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，则外部系统日志服务器的大小应为每秒支持 2 ， 000 条系

统日志消息，并且应能够以每秒 1.6 MB 的速率接收（并且通常存储）审核日志数据。

如果您对工作负载有更多了解，可以进行更准确的估计。对于审核日志，最重要的附加变量是放置的 S3 操作的百分比（与获取）以及以下 S3 字段的平均大小（以字节为单位）（表中使用的 4 个字符缩写为审核日志字段名称）：

代码	字段	**Description**
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。

让我们使用 P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

我们使用 K 表示 S3 帐户名称， S3 Bucket 和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。然后， K 值为 90 （ 13+13+28+36 ）。

如果您可以确定 P 和 K 的值，则可以使用以下公式估算外部系统日志服务器需要处理的审核日志卷，前提是您将审核级别设置为默认值（除存储外的所有类别均设置为正常）。 设置为 Error ）：

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

例如，如果您的网格大小为每秒 1 ， 000 次 S3 操作，则工作负载将占 50% ， S3 帐户名称，存储分段名称，对象名称平均为 90 字节，您的外部系统日志服务器应调整大小以支持每秒 1 ， 500 条系统日志消息，并且应能够以大约每秒 1 MB 的速率接收（并且通常存储）审核日志数据。

非默认审核级别的估计公式

为审核日志提供的公式假定使用默认审核级别设置（所有类别均设置为 " 正常 " ，但存储设置为 " 错误 " 除外）。未提供用于估计非默认审核级别设置的审核消息速率和平均大小的详细公式。不过，下表可用于粗略估计费率； 您可以使用为审核日志提供的平均大小公式、但请注意、它可能会导致高估、因为"额外"审核消息平均小于默认审核消息。

条件	公式
Replication： Audit Levels all set to Debug or Normal	审核日志速率 = 8 x S3 操作速率

条件	公式
纠删编码：审核级别均设置为 " 调试 " 或 " 正常 "	使用与默认设置相同的公式

安全事件的估计公式

安全事件与S3操作无关、通常会生成极少的日志和数据。出于这些原因，不提供任何估计公式。

应用程序日志的估计公式

如果除了网格预期支持的每秒 S3 操作数之外，您没有其他有关 S3 工作负载的信息，则可以使用以下公式估算外部系统日志服务器需要处理的应用程序日志卷：

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

因此，例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，则外部系统日志服务器的大小应为每秒支持 3 ， 300 个应用程序日志，并且能够以大约每秒 1.2 MB 的速率接收（和存储）应用程序日志数据。

如果您对工作负载有更多了解，可以进行更准确的估计。对于应用程序日志，最重要的附加变量是数据保护策略（复制与纠删编码），所执行 S3 操作的百分比（与GES/OTHER其他 ）以及以下 S3 字段的平均大小（以字节为单位）（表中使用的 4 个字符缩写是审核日志字段名称）：

代码	字段	**Description**
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。

规模估算示例

本节介绍了如何使用网格估算公式和以下数据保护方法的示例案例：

- Replication
- 纠删编码

如果使用复制来保护数据

Let P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100%

GET 工作负载， P = 0 ）。

让 K 表示 S3 帐户名称， S3 Bucket 和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。K 的值为 90 （ 13+13+28+36 ）。

如果您可以确定 P 和 K 的值，则可以使用以下公式估算外部系统日志服务器必须能够处理的应用程序日志卷。

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

因此，例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，工作负载占用率为 50% ， S3 帐户名称，存储分段名称和对象名称平均为 90 字节，则外部系统日志服务器的大小应为每秒支持 1800 个应用程序日志。 并且将以每秒 0.5 MB 的速率接收（并通常存储）应用程序数据。

如果您使用纠删编码进行数据保护

Let P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

让 K 表示 S3 帐户名称， S3 Bucket 和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。K 的值为 90 （ 13+13+28+36 ）。

如果您可以确定 P 和 K 的值，则可以使用以下公式估算外部系统日志服务器必须能够处理的应用程序日志卷。

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

因此，例如，如果您的网格大小为每秒 1 ， 000 次 S3 操作，则您的工作负载为 50% ， S3 帐户名称，存储分段名称， 对象名称平均为 90 字节，您的外部系统日志服务器应调整大小以支持每秒 2 ， 250 个应用程序日志，并且应能够以每秒 0.6 MB 的速率接收并将其存储。

有关配置审核消息级别和外部系统日志服务器的详细信息、请参见以下内容：

- "配置外部系统日志服务器"
- "配置审核消息和日志目标"

配置外部系统日志服务器

如果要将审核日志，应用程序日志和安全事件日志保存到网格外部的位置，请使用此操作步骤 配置外部系统日志服务器。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

- 您具有维护或 root 访问权限。
- 您有一个能够接收和存储日志文件的系统日志服务器。有关详细信息，请参见 "外部系统日志服务器的注意事项"。
- 如果您计划使用 TLS 或 ROLP/TLS ，则您拥有正确的服务器和客户端认证。

关于此任务

如果要将审核信息发送到外部系统日志服务器，则必须先配置外部服务器。

通过将审核信息发送到外部系统日志服务器，您可以：

- 更高效地收集和管理审核信息，例如审核消息，应用程序日志和安全事件
- 减少管理节点上的网络流量，因为审核信息直接从各种存储节点传输到外部系统日志服务器，而无需通过管理节点

> 将日志发送到外部系统日志服务器时，超过 8192 字节的单个日志会在消息末尾截断，以符合外部系统日志服务器实施中的常见限制。

> 为了在外部系统日志服务器发生故障时最大程度地提高完整数据恢复的选项，每个节点上最多会保留 20 GB 的本地审核记录日志（ localaudit.log ）。

> 如果此操作步骤 中提供的配置选项不够灵活、无法满足您的要求、则可以使用专用API应用其他配置选项 `audit-destinations` 端点。例如，可以对不同的节点组使用不同的系统日志服务器。

配置外部服务器

访问向导

要启动、请访问配置外部系统日志服务器向导。

步骤

1. 选择 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。
2. 从 Audit and syslog server 页面中，选择 * 配置外部系统日志服务器 * 。如果先前已配置外部系统日志服务器，请选择 * 编辑外部系统日志服务器 * 。

   此时将显示配置外部系统日志服务器向导。

输入系统日志信息

您必须提供StorageGRID 访问外部系统日志服务器所需的信息。

步骤

1. 对于向导的*Enter syslog info*步骤，在*Host*字段中输入外部系统日志服务器的有效完全限定域名或IPv4或IPv6地址。
2. 输入外部系统日志服务器上的目标端口（必须是介于 1 到 65535 之间的整数）。默认端口为 514 。

3. 选择用于向外部系统日志服务器发送审核信息的协议。

   建议使用*TLS*或*RELP/TLS*。您必须上传服务器证书才能使用其中任一选项。使用证书有助于确保网格与外部系统日志服务器之间的连接安全。有关详细信息，请参见 "管理安全证书"。

   所有协议选项都需要外部系统日志服务器的支持和配置。您必须选择与外部系统日志服务器兼容的选项。

   > 可靠事件日志记录协议（ Relp ）扩展了系统日志协议的功能，可提供可靠的事件消息传送。如果外部系统日志服务器必须重新启动，则使用 RELP 有助于防止审核信息丢失。

4. 选择 * 继续 * 。
5. 【附加证书】如果您选择了 * TLS * 或 * ROLP/TLS* ，请上传以下证书：
   - * 服务器 CA 证书 * ： 一个或多个用于验证外部系统日志服务器的可信 CA 证书（采用 PEM 编码）。如果省略此参数，则会使用默认网格 CA 证书。您在此上传的文件可能是 CA 捆绑包。
   - * 客户端证书 * ： 用于向外部系统日志服务器进行身份验证的客户端证书（采用 PEM 编码）。
   - * 客户端专用密钥 * ： 客户端证书的专用密钥（采用 PEM 编码）。

     > 如果使用客户端证书，则还必须使用客户端专用密钥。如果您提供加密的私钥，则还必须提供密码短语。使用加密的私钥不会带来显著的安全优势，因为必须存储密钥和密码短语；为了简化操作，建议使用未加密的私钥（如果可用）。

     i. 为要使用的证书或密钥选择 * 浏览 * 。
     ii. 选择证书文件或密钥文件。
     iii. 选择 * 打开 * 上传文件。

     证书或密钥文件名称旁边会显示一个绿色复选框，通知您已成功上传此证书或密钥文件。

6. 选择 * 继续 * 。

管理系统日志内容

您可以选择要发送到外部系统日志服务器的信息。

步骤

1. 对于向导的*管理系统日志内容*步骤，选择要发送到外部系统日志服务器的每种审核信息类型。
   - 发送审核日志：发送StorageGRID 事件和系统活动
   - 发送安全事件：发送安全事件，例如未授权用户尝试登录或用户以root身份登录时
   - 发送应用程序日志：发送对故障排除有用的日志文件，包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (仅限管理节点)
     - `prometheus.log`

- raft.log
- hagroups.log

2. 使用下拉菜单为要发送的审核信息类别选择严重性和工具（消息类型）。

   如果为严重性和设备选择 * 直通 * ，则发送到远程系统日志服务器的信息将获得与本地登录到节点时相同的严重性和设备。设置工具和严重性可以帮助您以可自定义的方式聚合日志，以便于分析。

   > 有关StorageGRID 软件日志的详细信息、请参见 "StorageGRID 软件日志"。

   a. 对于 * 严重性 * ，如果希望发送到外部系统日志的每个消息的严重性值与本地系统日志中的严重性值相同，请选择 * 直通 * 。

      对于审核日志，如果选择*PassThrough *，则严重性为"info"。

      对于安全事件，如果选择*PassThrough *，则严重性值由节点上的Linux分发版生成。

      对于应用程序日志，如果选择 * 直通 * ，则 " 信息 " 和 " 通知 " 之间的严重性会有所不同，具体取决于问题描述 的含义。例如、添加NTP服务器并配置HA组时、值为"info"、而故意停止SSM或RSM服务时、值为"notee"。

   b. 如果不想使用直通值、请选择介于0到7之间的严重性值。

      选定值将应用于此类型的所有消息。如果选择使用固定值覆盖严重性，则有关不同严重性的信息将丢失。

severity	Description
0	紧急：系统不可用
1.	alert ： 必须立即执行操作
2.	严重：严重情况
3.	错误：错误情况
4.	警告：警告条件
5.	注意：正常但重要的情况
6.	Informational ： 信息性消息
7.	debug ： 调试级别的消息

   c. 对于 * 设备 * ，如果希望发送到外部系统日志的每个消息都与本地系统日志中的设备值相同，请选择 * 直通 * 。

      对于审核日志、如果选择*直通*、则发送到外部系统日志服务器的工具为"local7"。

对于安全事件，如果选择 * 直通 * ，则设备值由节点上的 Linux 分发版生成。

对于应用程序日志，如果选择 * 直通 * ，则发送到外部系统日志服务器的应用程序日志具有以下设施值：

应用程序日志	直通值
bycast.log	用户或守护进程
bycast-err.log	用户，守护进程， local3 或 local4
jaeger.log	本地 2.
nms.log	本地 3.
prometheus.log	本地 4.
raft.log	本地 5.
hagroups.log	本地 6.

d. 如果您不想使用直通值、请选择介于0到23之间的医院值。

选定值将应用于此类型的所有消息。如果您选择使用固定值覆盖设施，则有关不同设施的信息将丢失。

设施	**Description**
0	KERN （内核消息）
1.	用户（用户级消息）
2.	邮件
3.	守护进程（系统守护进程）
4.	auth （安全 / 授权消息）
5.	系统日志（由 syslogd 在内部生成的消息）
6.	LPR （行式打印机子系统）
7.	新闻（网络新闻子系统）
8.	uucp

设施	Description
9	cron （时钟守护进程）
10	安全性（安全性 / 授权消息）
11.	FTP
12	NTP
13	日志审核（日志审核）
14	日志警报（日志警报）
15	时钟（时钟守护进程）
16.	本地 0
17	本地 1
18	本地 2.
19	本地 3.
20	本地 4.
21	本地 5.
22.	本地 6.
23	本地 7.

3. 选择 * 继续 * 。

发送测试消息

在开始使用外部系统日志服务器之前，您应请求网格中的所有节点向外部系统日志服务器发送测试消息。在提交向外部系统日志服务器发送数据之前，您应使用这些测试消息来帮助验证整个日志收集基础架构。

> 在确认外部系统日志服务器收到来自网格中每个节点的测试消息且该消息已按预期处理之前、请勿使用外部系统日志服务器配置。

步骤

1. 如果由于您确定外部系统日志服务器配置正确并且可以从网格中的所有节点接收审核信息而不想发送测试消息，请选择*跳过并完成*。

此时将显示一个绿色横幅，指示您的配置已成功保存。

2. 否则，请选择*发送测试消息*(建议)。

   测试结果会持续显示在页面上，直到您停止测试为止。测试期间，审核消息会继续发送到先前配置的目标。

3. 如果收到任何错误，请更正这些错误，然后再次选择 * 发送测试消息 * 。

   请参见 "对外部系统日志服务器进行故障排除" 以帮助您解决任何错误。

4. 请等待，直到看到一个绿色横幅，指示所有节点均已通过测试。
5. 检查系统日志服务器以确定是否按预期接收和处理了测试消息。

   > 如果使用的是 UDP ，请检查整个日志收集基础架构。UDP 协议不允许像其他协议那样严格地检测错误。

6. 选择 * 停止并完成 * 。

   此时将返回到 * 审核和系统日志服务器 * 页面。此时将显示一个绿色横幅，通知您已成功保存系统日志服务器配置。

   > 除非选择包含外部系统日志服务器的目标，否则不会将 StorageGRID 审核信息发送到外部系统日志服务器。

选择审核信息目标

您可以指定将安全事件日志，应用程序日志和审核消息日志发送到何处。

> 有关StorageGRID 软件日志的详细信息、请参见 "StorageGRID 软件日志"。

步骤

1. 在 Audit and syslog server 页面上，从列出的选项中选择审核信息的目标：

选项	**Description**
默认（管理节点 / 本地节点）	审核消息会发送到审核日志 (`audit.log`)、安全事件日志和应用程序日志存储在生成它们的节点(也称为"本地节点")上。
外部系统日志服务器	审核信息将发送到外部系统日志服务器并保存在本地节点上。发送的信息类型取决于您配置外部系统日志服务器的方式。只有在配置了外部系统日志服务器之后，才会启用此选项。
管理节点和外部系统日志服务器	审核消息会发送到审核日志 (`audit.log`)、审核信息将发送到外部系统日志服务器并保存在本地节点上。发送的信息类型取决于您配置外部系统日志服务器的方式。只有在配置了外部系统日志服务器之后，才会启用此选项。

选项	Description
仅限本地节点	不会向管理节点或远程系统日志服务器发送任何审核信息。审核信息仅保存在生成该信息的节点上。 • 注 *： StorageGRID 会定期轮换删除这些本地日志以释放空间。当节点的日志文件达到 1 GB 时，系统将保存现有文件并启动新的日志文件。日志的轮换限制为 21 个文件。创建日志文件的第 22 版时，将删除最早的日志文件。每个节点平均存储约 20 GB 的日志数据。

> 在每个本地节点上生成的审核信息存储在中 `/var/local/log/localaudit.log`

2. 选择 * 保存 * 。然后，选择*OK*接受对日志目标的更改。
3. 如果选择 * 外部系统日志服务器 * 或 * 管理节点和外部系统日志服务器 * 作为审核信息的目标，则会显示一条附加警告。查看警告文本。

   > 您必须确认外部系统日志服务器可以接收测试 StorageGRID 消息。

4. 选择*OK*确认要更改审核信息的目标。

   此时将显示一个绿色横幅，通知您已成功保存审核配置。

   新日志将发送到选定的目标。现有日志将保留在其当前位置。

相关信息

"审核消息概述"

"配置审核消息和日志目标"

"系统审核消息"

"对象存储审核消息"

"管理审核消息"

"客户端读取审核消息"

"管理 StorageGRID"