配置日志管理和外部 syslog 服务器

StorageGRID software

NetApp
July 23, 2026

目录

配置日志管理和外部 syslog 服务器

StorageGRID 中的外部系统日志服务器

外部 syslog 服务器是 StorageGRID 外部的服务器，可用于在单个位置收集系统审核信息。使用外部 syslog 服务器可以减少管理节点上的网络流量并更有效地管理信息。对于 StorageGRID，出站 syslog 消息数据包格式符合 RFC 3164。

可以发送到外部syslog服务器的审核信息类型包括：

- 包含正常系统运行期间生成的审核消息的审核日志
- 与安全相关的事件，例如登录和升级到 root
- 如果需要开立支持案例以排查您所遇到的问题，可能会被要求提供的应用程序日志

何时使用外部 syslog 服务器

如果您有大型网格、使用多种类型的 S3 应用程序或希望保留所有审核数据，则外部 syslog 服务器特别有用。向外部 syslog 服务器发送审核信息，您可以：

- 更有效地收集和管理审计消息、应用程序日志和安全事件等审计信息。
- 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 syslog 服务器，而无需通过管理节点。

> 当日志发送到外部 syslog 服务器时，大于 8,192 字节的单个日志将在消息末尾被截断，以符合外部 syslog 服务器实现中的常见限制。

> 为了在外部系统日志服务器发生故障时最大化完整数据恢复的选项，每个节点上最多维护 20 GB 的审核记录本地日志(`localaudit.log`）。

如何配置外部 syslog 服务器

要了解如何配置外部 syslog 服务器，请参见 "配置日志管理和外部 syslog 服务器"。

如果您计划配置使用 TLS 或 RELP/TLS 协议，则必须具有以下证书：

- **Server CA certificates**：用于验证 PEM 编码的外部 syslog 服务器的一个或多个受信任的 CA 证书。如果省略，将使用默认网格 CA 证书。
- 客户端证书：用于以 PEM 编码向外部 syslog 服务器进行身份验证的客户端证书。
- 客户端私钥：PEM 编码的客户端证书私钥。

> 如果使用客户端证书，则还必须使用客户端私钥。如果提供加密的私钥，则还必须提供密码。使用加密私钥没有显著的安全性优势，因为必须存储密钥和密码；为简便起见，建议使用未加密的私钥（如果有）。

如何估计外部 **syslog** 服务器的大小

通常，您的网格大小应能达到所需的吞吐量，以每秒 S3 操作数或每秒字节数来定义。例如，您可能需要网格每秒处理 1,000 次 S3 操作，或每秒 2,000 MB 的对象提取和检索。您应根据网格的数据要求来调整外部 syslog 服务器的大小。

本节提供了一些启发式公式，可帮助您估计外部 syslog 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，以网格的已知或所需性能特征（每秒 S3 操作数）表示。

在估算公式中使用每秒 **S3** 操作数

如果您的网格大小是以每秒字节数表示的吞吐量，则必须将此大小转换为每秒 S3 操作才能使用估算公式。要转换网格吞吐量，您必须首先确定平均对象大小，可以使用现有审计日志和指标（如果有）中的信息，或利用您对将使用 StorageGRID 的应用程序的了解来确定。例如，如果网格的大小可达到 2,000 MB/秒的吞吐量，且平均对象大小为 2 MB，则网格的大小可处理每秒 1,000 次 S3 操作（2,000 MB / 2 MB）。

> 以下各节中的外部 syslog 服务器规模调整公式提供了常见情况估计（而不是最坏情况估计）。根据您的配置和工作负载，您可能会看到比公式预测的更高或更低的 syslog 消息速率或 syslog 数据量。这些公式仅用作指南。

审核日志的估算公式

如果除了网格每秒应支持的 S3 操作数之外，没有关于 S3 工作负载的信息，则可以使用以下公式估算外部 syslog 服务器需要处理的审核日志量，前提是将"审核级别"设置为默认值（所有类别都设置为"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，如果您的网格大小为每秒 1,000 个 S3 操作，则外部 syslog 服务器的大小应支持每秒 2,000 个 syslog 消息，并且应能够以每秒 1.6 MB 的速率接收（通常存储）审核日志数据。

如果您对工作负载有更多了解，则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 PUT（相对于 GET）操作占 S3 操作的百分比，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	问题描述
SACC	S3 租户帐户名称（请求发送方）	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（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
S3BK	S3 存储分段	S3 存储桶名称。
S3KY	S3密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。

让我们使用 P 来表示 S3 操作中 PUT 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）。

让我们使用 K 来表示 S3 帐户名、S3 存储桶和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account（13 个字节），存储桶具有固定长度的名称，如 /my/application/bucket-12345（28 个字节），并且对象具有固定长度的密钥，如 5733a5d7-f069-41ef-8fbd-13247494c69c（36 个字节）。则 K 的值为 90 (13+13+28+36)。

如果可以确定 P 和 K 的值，则可以使用以下公式估算外部 syslog 服务器需要处理的审核日志量，前提是将"审核级别"设置为默认值（所有类别都设置为"正常"，存储设置为"错误"除外）：

```
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 个 S3 操作，您的工作负载为 50% PUT，并且您的 S3 帐户名称、存储桶名称和对象名称平均为 90 个字节，则外部 syslog 服务器的大小应支持每秒 1,500 个 syslog 消息，并且应能够以约 1 MB/秒的速率接收（通常存储）审核日志数据。

非默认审核级别的估算公式

为审核日志提供的公式假设使用默认审核级别设置（所有类别均设置为"正常"，但"存储"除外，后者设置为"错误"）。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可用。但是，下表可用于粗略估计速率；您可以使用为审核日志提供的平均大小公式，但请注意，这可能会导致高估，因为"额外"审核消息平均小于默认审核消息。

条件	公式
复制：审核级别均设置为"调试"或"正常"	审核日志速率 = 8 x S3 操作速率
擦除编码：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，通常产生的日志和数据量可以忽略不计。出于这些原因，没有提供估算公式。

应用程序日志的估算公式

如果除了网格每秒预计支持的 S3 操作数量之外，您没有关于 S3 工作负载的信息，则可以使用以下公式估算外部 syslog 服务器需要处理的应用程序日志量：

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

因此，例如，如果您的网格大小为每秒 1,000 个 S3 操作，则外部 syslog 服务器的大小应支持每秒 3,300 个应用程序日志，并能够以每秒约 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，则可以进行更准确的估算。对于应用程序日志，最重要的附加变量是数据保护策略（复制与擦除编码）、属于 PUT 的 S3 操作的百分比（与 GET/其他相比）以及以下 S3 字段的平均大小（以字节为单位）（表中使用的 4 字符缩写是审计日志字段名称）：

代码	字段	问题描述
SACC	S3 租户帐户名称（请求发送方）	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（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
S3BK	S3 存储分段	S3 存储桶名称。
S3KY	S3密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。

示例规模估算

本节通过以下数据保护方法，说明如何使用网格估计公式的示例案例：

- 复制
- 纠删编码

如果使用复制进行数据保护

设 P 表示作为 PUT 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、S3 存储桶和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account（13 个字节），存储桶具有固定长度的名称，如 /my/application/bucket-12345（28 个字节），并且对象具有固定长度的密钥，如 5733a5d7-f069-41ef-8fbd-13247494c69c（36 个字节）。则 K 的值为 90（13+13+28+36）。

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

```
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，如果您的网格大小为每秒 1,000 次 S3 操作，您的工作负载为 50% 的 PUT，并且您的 S3 帐户名称、存储桶名称和对象名称平均为 90 个字节，则外部 syslog 服务器的大小应支持每秒 1800 个应用程序日志，并将以每秒 0.5 MB 的速率接收（通常存储）应用程序数据。

如果使用擦除编码进行数据保护

设 P 表示作为 PUT 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、S3 存储桶和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account（13 个字节），存储桶具有固定长度的名称，如 /my/application/bucket-12345（28 个字节），并且对象具有固定长度的密钥，如 5733a5d7-f069-41ef-8fbd-13247494c69c（36 个字节）。则 K 的值为 90（13+13+28+36）。

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

```
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，您的工作负载为 50% PUTs，并且您的 S3 帐户名、存储桶名和对象名平均为 90 个字节，则您的外部 syslog 服务器的大小应支持每秒 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（通常为存储）应用程序数据。

在 StorageGRID 中配置日志管理

根据需要，配置审核级别、协议标头以及审核消息和日志的位置。

所有 StorageGRID 节点都会生成审计消息和日志，以跟踪系统活动和事件。审计消息和日志是监控和故障排除的重要工具。

或者，您可以"配置外部 syslog 服务器"远程保存审核信息。使用外部服务器可最大限度地减少审核消息日志记录的性能影响，而不会降低审核数据的完整性。如果您拥有大型网格、使用多种类型的 S3 应用程序或希望保留所有审核数据，则外部 syslog 服务器特别有用。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。
- 如果您计划配置外部 syslog 服务器，则已查看并遵循 "使用外部 syslog 服务器的注意事项"。
- 如果您计划使用 TLS 或 RELP/TLS 协议配置外部 syslog 服务器，则拥有所需的服务器 CA 和客户端证书以及客户端私钥。

更改审核消息级别

可为审核日志中的以下每类消息设置不同的审核级别：

审核类别	默认设置	更多信息
系统	正常	"系统审核消息"
存储	错误	"对象存储审核消息"
管理	正常	"管理审计消息"
客户端读取	正常	"客户端读取审核消息"
客户端写入	正常	"客户端写入审核消息"
ILM	正常	"ILM审计消息"

审核类别	默认设置	更多信息
跨网格复制	错误	"CGRR：跨网格复制请求"

在升级期间，审核级别配置不会立即生效。

步骤

1. 选择*配置* > 监控 > 日志管理。
2. 对于每个审计消息类别，从下拉列表中选择一个审计级别：

审核级别	问题描述
关闭	该类别中没有任何审核消息被记录。
错误	仅记录错误消息——结果代码未"成功"(SUCS)的审核消息。
正常	将记录标准事务性消息——这些说明中列出的该类别的消息。
调试	已弃用。此级别与正常审核级别相同。

任何特定级别所包含的消息，也包括将在更高级别记录的消息。例如，Normal 级别包含所有 Error 消息。

如果您不需要 S3 应用程序的客户端读取操作的详细记录，可以选择将*客户端读取*设置更改为*错误*，以减少审核日志中记录的审核消息数量。

3. 选择 **Save**。

定义 HTTP 请求标头

可以选择定义要包含在客户端读取和写入审核消息中的任何 HTTP 请求标头。

步骤

1. 在*审核协议标头*部分中，定义要包含在客户端读取和写入审核消息中的 HTTP 请求标头。

   使用星号 (*) 作为通配符，以匹配零个或多个字符。使用转义序列 (*) 匹配文字星号。

2. 如果需要，选择 **Add another header** 以创建其他标题。

   当在请求中找到 HTTP 标头时，它们将包含在 HTRH 字段下的审核消息中。

   仅当*客户端读取*或*客户端写入*的审核级别不为*关闭*时，才会记录审核协议请求标头。

3. 选择 **Save**

配置日志位置

默认情况下，审核消息和日志保存在生成它们的节点上。它们会定期轮换并最终删除，以防止占用过多的磁盘空间。如果要在外部保存审核消息和日志子集，请 使用外部 syslog 服务器。

如果要在内部保存日志文件，请选择用于日志存储的租户和存储区并启用日志存档。

使用外部 **syslog** 服务器

您可以选择配置外部 syslog 服务器，以将审核日志、应用程序日志和安全事件日志保存到网格外部的位置。

如果不想使用外部 syslog 服务器，请跳过此步骤并转到 选择日志位置。

如果此过程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 `audit-destinations`端点应用其他配置选项，这些端点位于"网格管理 API"的私有 API 部分。例如，如果要为不同的节点组使用不同的 syslog 服务器，则可以使用 API。

输入 **syslog** 信息

访问配置外部 syslog 服务器向导，并提供 StorageGRID 访问外部 syslog 服务器所需的信息。

步骤

1. 从本地节点和外部服务器选项卡中，选择*配置外部 syslog 服务器*。或者，如果您之前已配置过外部 syslog 服务器，请选择*编辑外部 syslog 服务器*。

   此时将显示Configure external syslog server向导。

2. 对于向导的 **Enter syslog info** 步骤，请在 **Host** 字段中为外部 syslog 服务器输入有效的完全限定域名或 IPv4 或 IPv6 地址。
3. 输入外部 syslog 服务器上的目标端口（必须是 1 到 65535 之间的整数）。默认端口为 514。
4. 选择用于将审核信息发送到外部 syslog 服务器的协议。

   建议使用 **TLS** 或 **RELP/TLS**。您必须上传服务器证书才能使用这些选项之一。使用证书有助于保护网格与外部 syslog 服务器之间的连接。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 syslog 服务器的支持和配置。您必须选择一个与外部 syslog 服务器兼容的选项。

   可靠事件日志记录协议 (RELP) 扩展了 syslog 协议的功能，以提供事件消息的可靠传递。使用 RELP 有助于防止在外部 syslog 服务器重新启动时丢失审计信息。

5. 选择 **Continue**。
6. 如果您选择了 **TLS** 或 **RELP/TLS**，请上传服务器 CA 证书、客户端证书和客户端私钥。
   a. 选择要使用的证书或密钥的*浏览*。
   b. 选择证书或密钥文件。
   c. 选择*打开*以上传文件。

      证书或密钥文件名旁边将显示一个绿色复选标记，通知您已成功上传。

7. 选择 **Continue**。

管理系统日志内容

您可以选择要发送至外部 syslog 服务器的信息。

步骤

1. 对于向导的*管理 syslog 内容*步骤，选择要发送到外部 syslog 服务器的每种类型的审核信息。
   - 发送审核日志：发送 StorageGRID 事件和系统活动
   - **Send security events**：发送安全事件，例如当未经授权的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"StorageGRID 软件日志文件"用于故障排除，包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` （仅管理节点）
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - 发送访问日志：将外部请求的 HTTP 访问日志发送到 Grid Manager、Tenant Manager、配置的负载均衡器端点以及来自远程系统的网格联合请求。
2. 使用下拉菜单为要发送的每个审核信息类别选择严重性和设施（消息类型）。

   设置严重程度和设施值可以帮助您以可自定义的方式聚合日志，以便更轻松地进行分析。

   a. 对于*严重程度*，选择*Passthrough*，或选择一个介于 0 到 7 之间的严重程度值。

      如果选择一个值，则所选值将应用于所有此类型的消息。如果使用固定值覆盖严重性，则有关不同严重性的信息将丢失。

严重性	问题描述
Passthrough	发送到外部 syslog 的每条消息都具有与本地记录到节点上时相同的严重性值： • 对于审核日志，严重性为"info"。 • 对于安全事件，严重性值由节点上的 Linux 发行版生成。 • 对于应用程序日志，严重程度在"info"和"notice"之间有所不同，具体取决于问题是什么。例如，添加 NTP 服务器和配置 HA 组会给出"info"的值，而故意停止 SSM 或 RSM 服务会给出"notice"的值。 • 对于访问日志，严重性为"info"。
0	紧急情况：系统无法使用

严重性	问题描述
1	警告：必须立即采取行动
2	严重：严重情况
3	错误:错误条件
4	警告：警告条件
5	注意：正常但重要的状况
6	Informational：信息性消息
7	调试：调试级消息

b. 对于 **Facilty**，选择 **Passthrough**，或选择一个介于 0 到 23 之间的设施值。

如果选择一个值，则它将应用于所有此类型的消息。如果使用固定值覆盖设施，则有关不同设施的信息将丢失。

工具	问题描述
Passthrough	发送到外部 syslog 的每条消息都具有与本地登录到节点时相同的设施值： • 对于审核日志，发送到外部 syslog 服务器的设施为"local7"。 • 对于安全事件，设施值由节点上的 linux 发行版生成。 • 对于应用程序日志，发送到外部 syslog 服务器的应用程序日志具有以下设施值： ◦ `bycast.log`：user 或 daemon ◦ `bycast-err.log`：user、daemon、local3 或 local4 ◦ `jaeger.log`：local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`：local6 • 对于访问日志，发送到外部 syslog 服务器的设施为"local0"。
0	kern（内核消息）
1	用户（用户级消息）

工具	问题描述
2	邮件
3	守护程序（系统守护程序）
4	auth（安全/授权消息）
5	syslog（由 syslogd 内部生成的消息）
6	lpr（行打印机子系统）
7	news（网络新闻子系统）
8	UUCP
9	cron（时钟守护进程）
10	安全（安全/授权消息）
11	FTP
12	NTP
13	logaudit（日志审核）
14	logalert（日志警报）
15	clock（时钟守护进程）
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6

工具	问题描述
23	local7

3. 选择 **Continue**。

发送测试消息

在开始使用外部 syslog 服务器之前，应请求网格中的所有节点将测试消息发送到外部 syslog 服务器。在确认将数据发送到外部 syslog 服务器之前，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。

> 请勿使用外部 syslog 服务器配置，直到您确认外部 syslog 服务器收到来自网格中每个节点的测试消息，并且该消息已按预期处理。

步骤

1. 如果您不想发送测试消息，因为您确定外部 syslog 服务器已正确配置并且可以从网格中的所有节点接收审核信息，请选择*跳过并完成*。

   绿色横幅指示配置已保存。

2. 否则，请选择*发送测试消息*（推荐）。

   测试结果会不断显示在页面上，直至您停止测试为止。在测试进行期间，您的审核消息将继续发送到先前配置的目的地。

3. 如果在 syslog 服务器配置或运行时收到任何错误，请更正并再次选择*发送测试消息*。

   请参阅"对外部 syslog 服务器进行故障排除"以帮助解决任何错误。

4. 等待，直到您看到一个绿色横幅，指示所有节点已通过测试。
5. 检查您的 syslog 服务器，以确定是否按预期接收和处理测试消息。

   > 如果使用的是 UDP，请检查整个日志收集基础设施。UDP 协议不支持像其他协议那样严格的错误检测。

6. 选择*停止并完成*。

   您将返回到*审核和syslog服务器*页面。绿色横幅指示已保存syslog服务器配置。

   > 在选择包含外部 syslog 服务器的目标之前，StorageGRID 审核信息不会发送到外部 syslog 服务器。

选择日志位置

您可以指定审核日志、安全事件日志、"StorageGRID 应用程序日志"和访问日志的发送位置。

StorageGRID 默认为本地节点审核目标，并将审核信息存储在 `/var/local/log/localaudit.log`中。

使用 `/var/local/log/localaudit.log`时，网格管理器和租户管理器审核日志条目可能会发送到存储节点。您可以使用 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`命令查找哪个节点具有最新条目。

仅当配置了外部 syslog 服务器时，某些目标才可用。

步骤

1. 选择*日志位置* > 本地节点和外部服务器。
2. 要更改日志类型的日志位置，请选择其他选项。

*仅本地节点*和*外部 syslog 服务器*通常提供更好的性能。

选项	问题描述
仅本地节点（默认）	审核消息、安全事件日志和应用程序日志不会发送到管理节点。相反，它们仅保存在生成它们的节点（"本地节点"）上。在每个本地节点上生成的审核信息存储在 `/var/local/log/localaudit.log`中。 注意：StorageGRID 会定期轮换删除本地日志，以释放空间。当节点的日志文件达到 1 GB 时，将保存现有文件，并启动一个新的日志文件。日志的轮换限制为 21 个文件。当创建日志文件的第 22 个版本时，将删除最旧的日志文件。每个节点上平均存储约 20 GB 的日志数据。要长时间存储日志，请 使用租户和存储桶进行日志存储。
管理节点/本地节点	审核消息发送到管理节点上的审核日志，安全事件日志和应用程序日志存储在生成它们的节点上。审核信息存储在以下文件中： • 管理节点（主节点和非主节点）：`/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log` 文件通常为空或缺失。它可能包含辅助信息，例如某些消息的其他副本。
外部 syslog 服务器	审核信息将发送到外部 syslog 服务器并保存在本地节点上（`/var/local/log/localaudit.log`）。发送的信息类型取决于您如何配置外部 syslog 服务器。只有在完成已配置外部 syslog 服务器之后，才会启用此选项。
管理节点和外部 syslog 服务器	审核消息发送到管理节点上的审核日志（`/var/local/audit/export/audit.log`），审核信息发送到外部 syslog 服务器并保存在本地节点上（`/var/local/log/localaudit.log`）。发送的信息类型取决于您如何配置外部 syslog 服务器。只有在完成已配置外部 syslog 服务器之后，才会启用此选项。

3. 选择 **Save**。

此时将显示一条警告消息。

4. 选择*OK*以确认要更改审核信息的目标。

   新日志将发送到您选择的目的地。现有日志保留在其当前位置。

使用存储桶

日志会定期轮换。使用同一网格中的 S3 存储桶将日志存储较长时间。

1. 选择*日志位置* > 使用存储桶。
2. 选中*启用归档日志*复选框。
3. 如果列出的租户和存储桶不是您要使用的，请选择 **Change tenant and bucket**，然后选择 **Create tenant and bucket** 或 **Select tenant and bucket**。

   创建租户和存储桶

   a. 输入新的租户名称。
   b. 输入并确认新租户的密码。
   c. 输入新的存储桶名称。
   d. 选择*创建并启用*。

   选择租户和存储桶

   a. 从下拉列表中选择租户名称。
   b. 从下拉菜单中选择一个存储桶。
   c. 选择*选择并启用*。

4. 选择 **Save**。

   日志将存储在您指定的租户和存储桶中。日志的对象键名称采用以下格式：

   ```
   system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
   {last_modified_time}.gz
   ```

   例如：

   ```
   system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
   ```