配置日志管理和外部系统日志服务器
StorageGRID software

NetApp
October 07, 2025

目录

配置日志管理和外部系统日志服务器

使用外部系统日志服务器的注意事项

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、您可以减少管理节点上的网络流量、并更高效地管理信息。对于StorageGRID、出站系统日志消息数据包格式符合RFC 3164。

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

何时使用外部系统日志服务器

如果您的网格较大、使用多种类型的S3应用程序或希望保留所有审核数据、则外部系统日志服务器尤其有用。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8、192字节的单个日志会在消息末尾被截断、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限度地恢复数据，(`localaudit.log`每个节点上最多保留20 GB的本地审核记录日志。

如何配置外部系统日志服务器

要了解如何配置外部 syslog 服务器，请参阅"配置日志管理和外部系统日志服务器"。

如果您计划配置使用TLS或RELP/TLS协议、则必须具有以下证书：

- 服务器**CA**证书：一个或多个可信CA证书，用于验证采用PEM编码的外部系统日志服务器。如果省略此参数，则会使用默认网格 CA 证书。
- 客户端证书：以PEM编码向外部系统日志服务器进行身份验证的客户端证书。
- 客户端专用密钥：PEM编码的客户端证书专用密钥。

> 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）。

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、最重要的其他变量是S3操作的放置(与获取)百分比、以及以下S3字段的平均大小(表中使用的4个字符缩写为审核日志字段名称)(以字节为单位)：

代码	字段	说明
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。

代码	字段	说明
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 ）。

让我们使用K来表示S3帐户名称、S3存储分段和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
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、最重要的其他变量是数据保护策略(复制与纠删编码)、S3操作的放置百分比(与Gets/Other)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	说明
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：

- 复制
- 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存储分段和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存储分段和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
```

例如、如果您的网格的规模为每秒1、000次S3操作、则您的工作负载为50%的"放置"、而您的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为每秒支持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(并通常存储)应用程序数据。

配置日志管理

根据需要配置审计级别、协议标头以及审计消息和日志的位置。

所有StorageGRID节点都会生成审计消息和日志来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"配置外部系统日志服务器"远程保存审计信息。使用外部服务器可以最大限度地减少审计消息记录对性能的影响，而不会降低审计数据的完整性。如果您拥有大型网格、使用多种类型的 S3 应用程序或想要保留所有审计数据，则外部 syslog 服务器特别有用。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 如果您计划配置外部系统日志服务器，则您已阅读并遵循"使用外部系统日志服务器的注意事项"。
- 如果您计划使用TLS或RELP/TLS协议配置外部系统日志服务器、则您具有所需的服务器CA和客户端证书以及客户端专用密钥。

更改审核消息级别

您可以为审核日志中的以下每种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"

审核类别	默认设置	更多信息
管理	正常	"管理审核消息"
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审核消息"
跨网格复制	错误	"CGRR：跨网格复制请求"

升级期间，审计级别配置不会立即生效。

步骤

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

审核级别	说明
关闭	不会记录此类别中的任何审核消息。
错误	仅记录错误消息——结果代码不“成功”（SUCS）的审计消息。
正常	系统会记录标准事务处理消息，即这些说明中针对此类别列出的消息。
调试	已弃用。此级别的行为与正常审核级别相同。

对于任何特定级别，包含的消息都包括那些将在较高级别记录的消息。例如，正常级别包括所有错误消息。

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

3. 选择 * 保存 * 。

定义HTTP请求标头

您可以选择定义要包含在客户端读写审计消息中的任何 HTTP 请求标头。

步骤

1. 在*Audit protocol headers*部分中，定义要包含在客户端读写审核消息中的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 * 添加另一个标题 * 以创建其他标题。

在请求中找到 HTTP 标头后，它们将包含在审核消息中的字段 HTRH 下。

仅当“客户端读取”或“客户端写入”的审计级别不是“关闭*”时，才会记录审计协议请求标头。

3. 选择 * 保存 *

配置日志位置

默认情况下，审计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被删除，以防止它们占用过多的磁盘空间。如果要在外部保存审计消息和日志子集，使用外部系统日志服务器 。

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桶并启用日志存档。

使用外部系统日志服务器

您可以选择配置外部系统日志服务器、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某个位置。

如果您不想使用外部系统日志服务器，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，则可以使用端点应用其他配置选项 `audit-destinations`，这些端点位于的私有API部分"网格管理 API"。例如、如果要对不同的节点组使用不同的系统日志服务器、则可以使用API。

输入系统日志信息

访问配置外部系统日志服务器向导、并提供StorageGRID访问外部系统日志服务器所需的信息。

步骤

1. 从本地节点和外部服务器选项卡中，选择*配置外部系统日志服务器*。或者，如果您之前配置了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。

2. 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。
3. 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。
4. 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。

5. 选择 * 继续 * 。
6. [[attache-certificate]如果选择了*tls*或*RELP/tls*，请上传服务器CA证书、客户端证书和客户端专用密钥。

a. 为要使用的证书或密钥选择 * 浏览 * 。
b. 选择证书或密钥文件。
c. 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。

7. 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"StorageGRID软件日志文件"对故障排除很有用的信息，包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`(仅限管理节点)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - 发送访问日志：将外部请求的HTTP访问日志发送到网格管理器、租户管理器、已配置的负载平衡器端点以及来自远程系统的网格联合请求。
2. 使用下拉菜单为您要发送的每类审核信息选择严重性和设施(消息类型)。

   设置严重性和设施值可帮助您以可自定义的方式聚合日志、以便于分析。

   a. 对于*严重性*，请选择*直通*，或选择介于0到7之间的严重性值。

      如果您选择一个值、则所选值将应用于此类型的所有消息。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	说明
直通	发送到外部系统日志的每条消息的严重性值与在本地记录到节点时的严重性值相同： • 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分发版生成。 • 对于应用程序日志、"info"和"noty"之间的严重级别因问题描述的定义而异。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"note"。 • 对于访问日志、严重性为"info"。
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

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

如果您选择一个值，它将应用于此类型的所有消息。如果您使用固定值覆盖医院、则有关不同医院的信息将丢失。

设施	说明
直通	发送到外部系统日志的每条消息都具有与在本地记录到节点上时相同的工具值： • 对于审核日志、发送到外部系统日志服务器的工具为"local7"。 • 对于安全事件、工具值由节点上的Linux分发版生成。 • 对于应用程序日志、发送到外部系统日志服务器的应用程序日志具有以下工具值： ◦ `bycast.log`：用户或守护进程 ◦ `bycast-err.log`：用户、守护进程、local3或local4 ◦ `jaeger.log`：local2 ◦ `nms.log`: local3. ◦ `prometheus.log`：本地4 ◦ `raft.log`：local5. ◦ `hagroups.log`：local6 • 对于访问日志、发送到外部系统日志服务器的工具为"local0"。
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
9	cron （时钟守护进程）
10	安全性（安全性 / 授权消息）
11	FTP

设施	说明
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	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

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*。

   绿色横幅表示配置已保存。

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. 如果您在 syslog 服务器配置期间或运行时收到任何错误，请更正它们并再次选择*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。

> 如果您使用 UDP，请检查整个日志收集基础设施。 UDP 协议不像其他协议那样允许严格的错误检测。

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。绿色横幅表示系统日志服务器配置已保存。

> 直到您选择包含外部系统日志服务器的目标时， StorageGRID审计信息才会发送到外部系统日志服务器。

选择日志位置

您可以指定审计日志、安全事件日志、"StorageGRID应用程序日志" ，并发送访问日志。

> StorageGRID默认使用本地节点审核目标，并将审核信息存储在中 `/var/local/log/localaudit.log`。
>
> 使用时 `/var/local/log/localaudit.log`，Grid Manager和租户管理器审核日志条目可能会发送到存储节点。您可以使用命令查找哪个节点具有最新的条目 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`。
>
> 只有在配置了外部系统日志服务器后、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。

> *仅限本地节点*和*外部系统日志服务器*通常可提供更好的性能。

选项	说明
仅本地节点(默认)	审计消息、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。每个本地节点生成的审计信息存储在 `/var/local/log/localaudit.log`。 注意： StorageGRID会定期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新的日志文件。日志的轮换限制为 21 个文件。当创建第 22 个版本的日志文件时，最旧的日志文件将被删除。每个节点平均存储约 20 GB 的日志数据。为了长期保存日志，使用租户和存储桶进行日志存储 。

选项	说明
管理节点/本地节点	审核消息会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会存储在生成这些消息的节点上。审核信息存储在以下文件中： • 管理节点（主要和非主要）：`/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、例如某些消息的附加副本。
外部系统日志服务器	审计信息被发送到外部系统日志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系统日志服务器。此选项仅在您配置外部系统日志服务器。
管理节点和外部系统日志服务器	审计消息被发送到审计日志（`/var/local/audit/export/audit.log`），并将审计信息发送到外部系统日志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系统日志服务器。此选项仅在您配置外部系统日志服务器。

3. 选择 * 保存 * 。

   此时将显示一条警告消息。

4. 选择*OK*确认要更改审核信息的目标。

   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。

使用存储桶

日志会定期轮换。使用同一网格中的 S3 存储桶来长期存储日志。

1. 选择*日志位置* > 使用存储桶。
2. 选中“启用存档日志”复选框。
3. 如果列出的租户和存储桶不是您想要使用的，请选择*更改租户和存储桶*，然后选择*创建租户和存储桶*或*选择租户和存储桶*。

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*。

选择租户和存储分段

a. 从下拉菜单中选择租户名称。
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 * 保存 * 。

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
```