审核消息概述
StorageGRID 11.5

NetApp
April 11, 2024

目录

审核消息概述

这些说明包含有关 StorageGRID 审核消息和审核日志的结构和内容的信息。您可以使用此信息读取和分析系统活动的审核跟踪。

这些说明适用于负责生成系统活动和使用情况报告的管理员，这些报告需要分析 StorageGRID 系统的审核消息。

我们假定您已对StorageGRID 系统中已审核活动的性质有了充分的了解。要使用文本日志文件，您必须有权访问管理节点上配置的审核共享。

相关信息

"管理 StorageGRID"

审核消息流和保留

所有 StorageGRID 服务都会在系统正常运行期间生成审核消息。您应了解这些审核消息如何在StorageGRID 系统中移动到 `audit.log` 文件

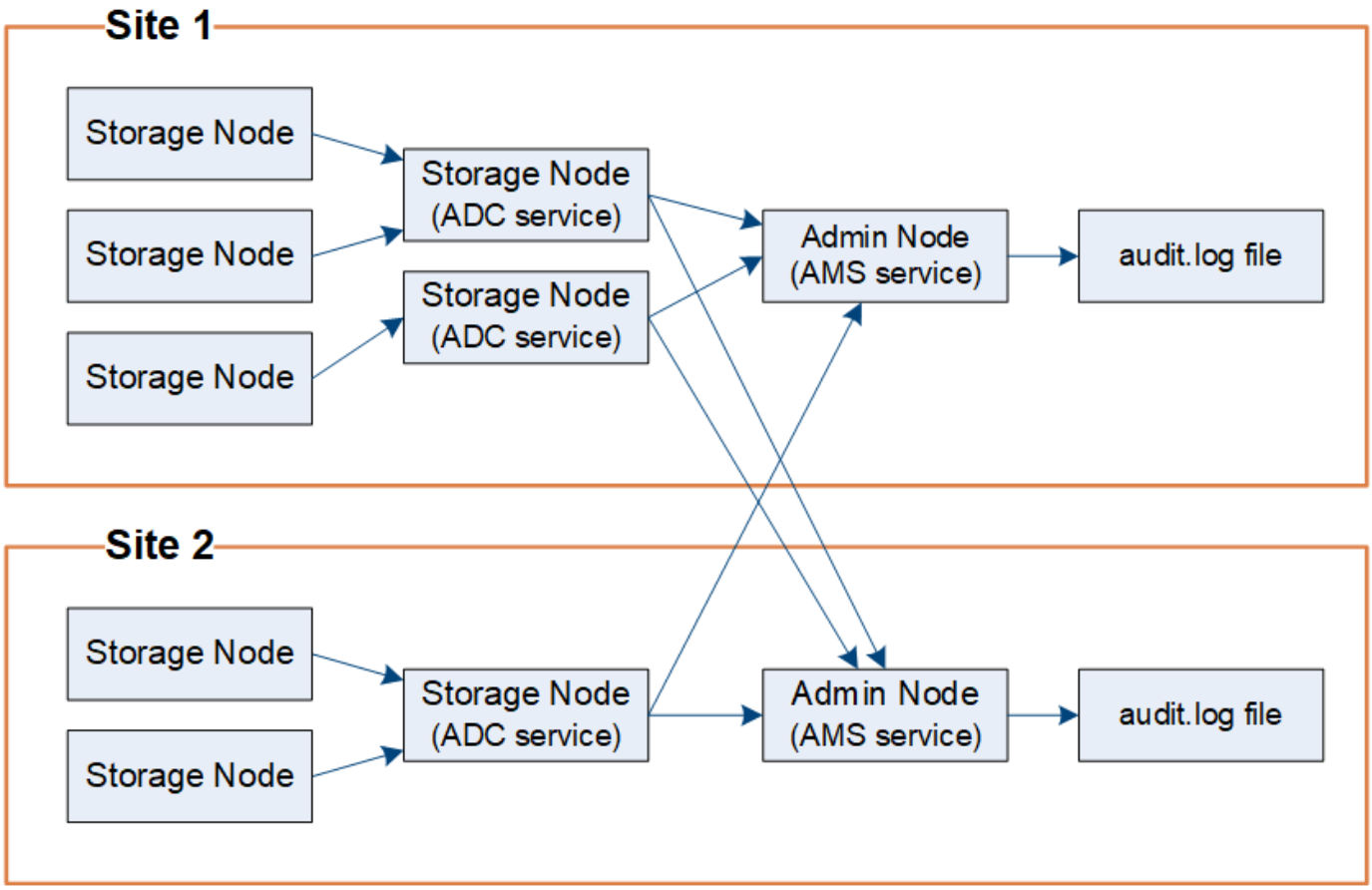
审核消息流

审核消息由管理节点以及具有管理域控制器（ ADO ）服务的存储节点处理。

如审核消息流程图所示，每个 StorageGRID 节点都会将其审核消息发送到数据中心站点的一个模板服务。每个站点上安装的前三个存储节点会自动启用此 ADC-Service 。

反过来，每个 ADC 服务都充当中继，并将其审核消息集合发送到 StorageGRID 系统中的每个管理节点，从而为每个管理节点提供完整的系统活动记录。

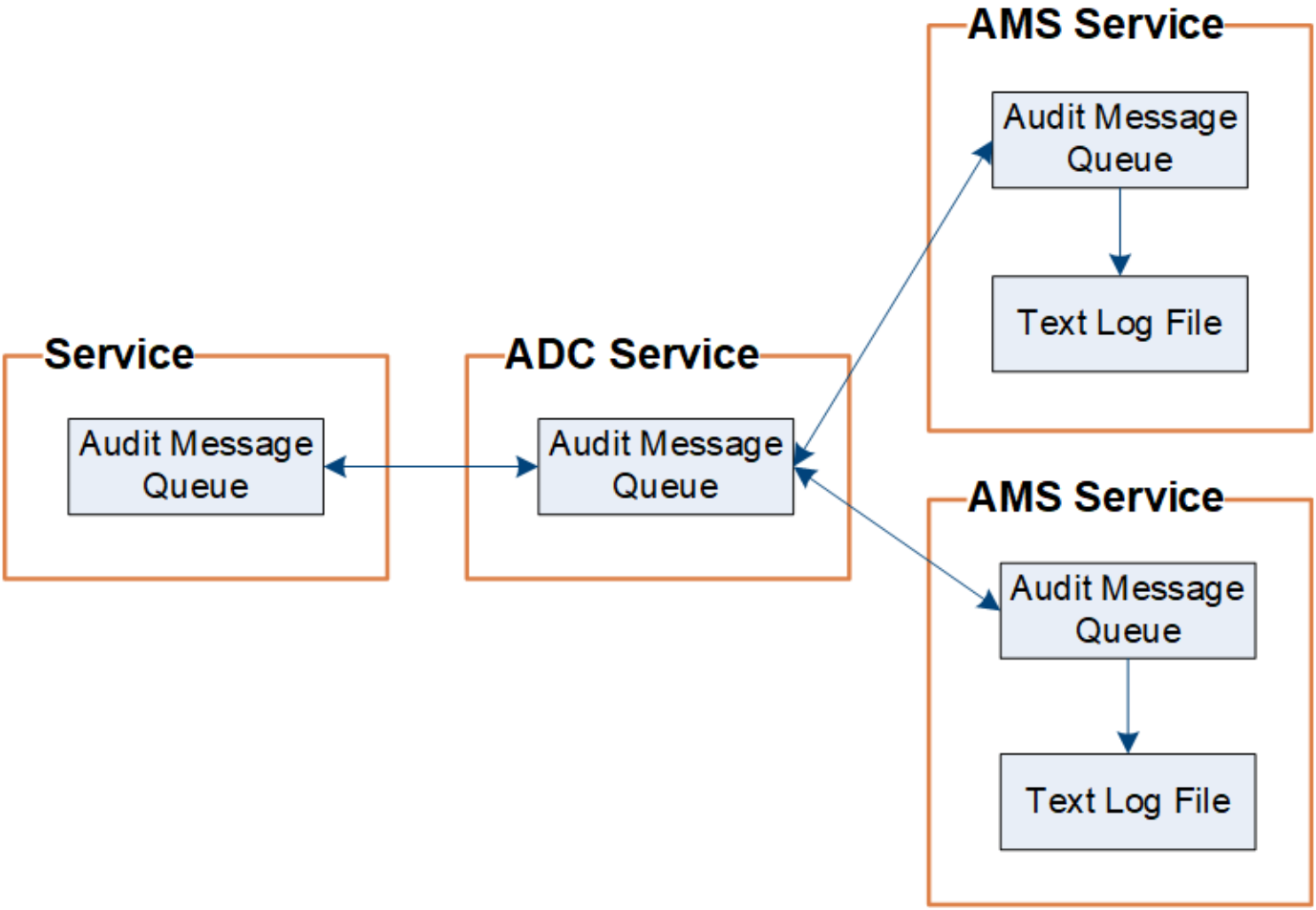
每个管理节点都会将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log`。



审核消息保留

StorageGRID 使用复制和删除过程来确保在将审核消息写入审核日志之前不会丢失任何审核消息。

当节点生成或转发审核消息时，此消息会存储在网格节点的系统磁盘上的审核消息队列中。消息的副本始终保留在审核消息队列中、直到消息写入管理节点的审核日志文件为止 `/var/local/audit/export` 目录。这有助于防止传输期间丢失审核消息。



由于网络连接问题或审核容量不足，审核消息队列可能会暂时增加。随着队列的增加、它们会占用每个节点中更多的可用空间 `/var/local/` 目录。如果问题描述 仍然存在，并且节点的审核消息目录过满，则各个节点将优先处理其积压工作，并暂时不可用于处理新消息。

具体来说，您可能会看到以下行为：

- 如果 `/var/local/audit/export` 管理节点使用的目录已满、管理节点将标记为不可用于新审核消息、直到目录不再全满为止。S3 和 Swift 客户端请求不受影响。如果无法访问审核存储库，则会触发 XAMS （无法访问审核存储库）警报。
- 如果 `/var/local/` 具有此ADA服务的存储节点使用的目录已满92%、此节点将被标记为不可用于审核消息、直到目录已满87%为止。对其他节点的 S3 和 Swift 客户端请求不受影响。如果无法访问审核中继，则会触发 NRLY （可用审核中继）警报。

  如果没有可用于此ADA服务的存储节点、则存储节点会将审核消息存储在本地。

- 如果 `/var/local/` 存储节点使用的目录已满85%、此节点将开始拒绝S3和Swift客户端请求 `503 Service Unavailable`。

以下类型的问题可能会使发生原因 审核消息队列变得非常庞大：

- 管理节点或存储节点使用 ADC-Service 中断的情况。如果系统的一个节点已关闭，则其余节点可能会回记录。
- 超过系统审核容量的持续活动率。

- 。 `/var/local/` 由于与审核消息无关的原因、一个模块存储节点上的空间已满。发生这种情况时，节点将停止接受新的审核消息，并优先处理当前的积压工作，而这可能会使发生原因 回退到其他节点上。

大型审核队列警报和审核消息已排队（ **Audit Messages Queued** ， **AMQS** ）警报

为了帮助您监控一段时间内审核消息队列的大小，当存储节点队列或管理节点队列中的消息数量达到特定阈值时，将触发 * 大型审核队列 * 警报和原有 AMQS 警报。

如果触发了 * 大型审核队列 * 警报或原有 AMQS 警报，请首先检查系统上的负载—如果最近发生了大量事务，则警报和警报应随着时间的推移而解决，并且可以忽略。

如果警报或警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。通过将客户端写入和客户端读取的审核级别更改为 " 错误 " 或 " 关闭 " 来降低客户端操作速率或减少记录的审核消息数量。请参见 "'更改审核消息级别"。 "

重复的消息

如果发生网络或节点故障， StorageGRID 系统会采取保守的方法。因此，审核日志中可能存在重复的消息。

更改审核消息级别

您可以调整审核级别、以增加或减少每个审核消息类别的审核日志中记录的审核消息数量。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

审核日志中记录的审核消息将根据*配置*>*监控*>*审核*页面上的设置进行筛选。

您可以为以下每种消息设置不同的审核级别：

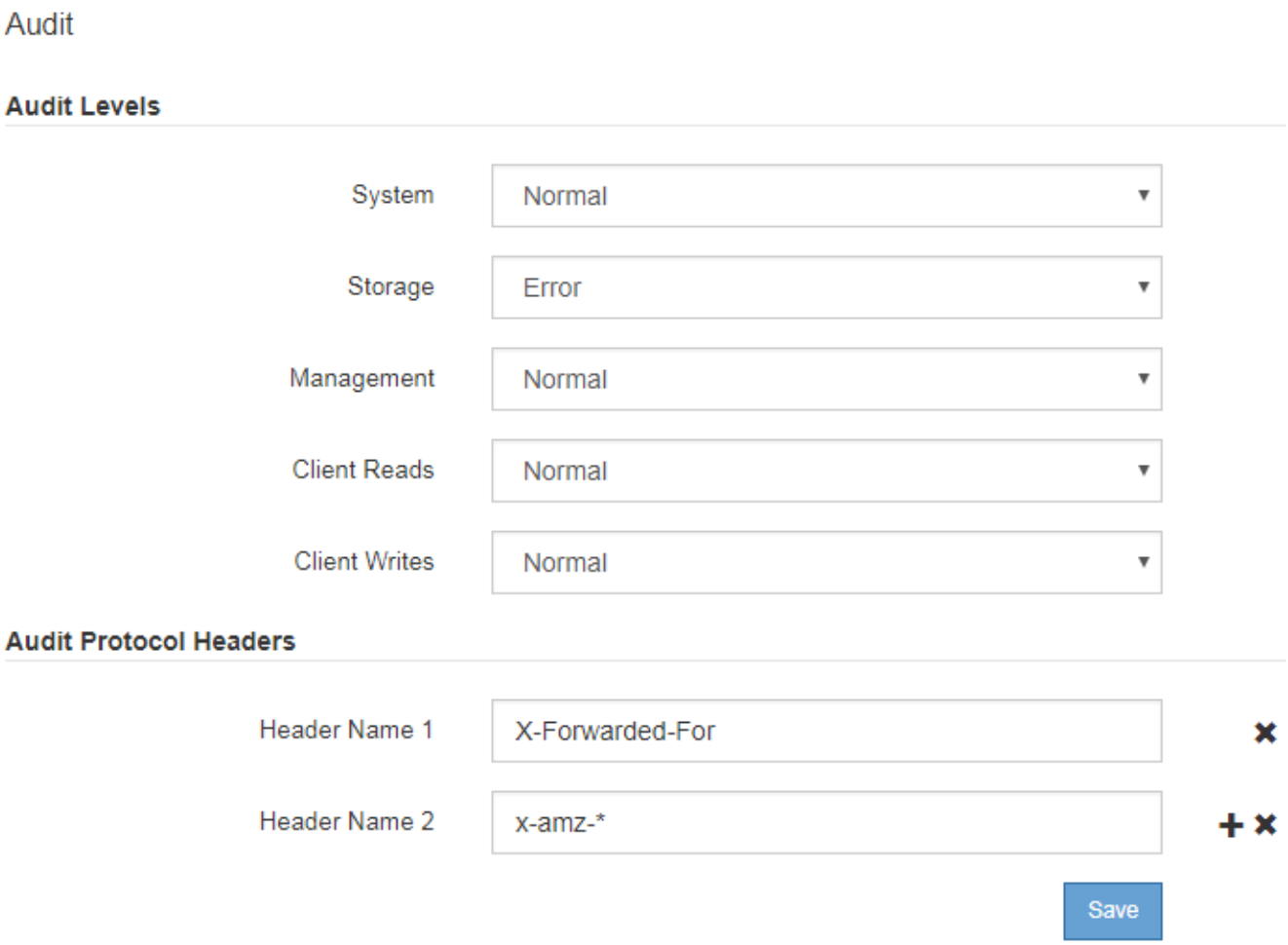
- 系统：默认情况下、此级别设置为正常。
- 存储：默认情况下、此级别设置为错误。
- 管理：默认情况下、此级别设置为正常。
- 客户端读取：默认情况下、此级别设置为正常。
- 客户端写入：默认情况下、此级别设置为正常。

如果您最初使用 10.3 或更高版本安装 StorageGRID ，则这些默认设置适用。如果您已从早期版本的 StorageGRID 升级，则所有类别的默认值均设置为正常。

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*>*审核*。



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	Description
关闭	不会记录此类别中的任何审核消息。
error	仅会记录错误消息—审核结果代码不是 " 成功 " （ SUC ）的消息。
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。

3. 在*审核协议标头*下、输入要包含在客户端读取和客户端写入审核消息中的HTTP请求标头的名称。使用星号(*)作为通配符、或者使用转义序列(*)作为文字星号。单击加号可创建标题名称字段列表。

审核协议标头仅适用于 S3 和 Swift 请求。

如果在请求中发现此类HTTP标头、则这些标头将包含在审核消息的HTRH字段下。

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

4. 单击 * 保存 * 。

相关信息

"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"

访问审核日志文件

审核共享包含活动 `audit.log` 文件和任何压缩的审核日志文件。为了便于访问审核日志、您可以配置客户端对NFS和CIFS (已弃用)的审核共享的访问权限。您也可以直接从管理节点的命令行访问审核日志文件。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `Passwords.txt` 文件
- 您必须知道管理节点的 IP 地址。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
2. 转到包含审核日志文件的目录：

```
cd /var/local/audit/export
```

3. 根据需要查看当前审核日志文件或已保存的审核日志文件。

相关信息

"管理 StorageGRID"

审核日志文件轮换

审核日志文件会保存到管理节点的中 `/var/local/audit/export` 目录。活动审核日志文件名为 `audit.log`。

每天执行一次活动 `audit.log` 此时将保存文件、并显示一个新的 `audit.log` 文件已启动。已保存文件的名称以格式指示其保存的时间 *`yyyy-mm-dd.txt`*。如果在一天内创建了多个审核日志、则文件名将使用保存文件的日期、并附加一个数字、格式为 *`yyyy-mm-dd.txt.n`*。例如： `2018-04-15.txt` 和 `2018-04-15.txt.1` 是在2018年4月15日创建并保存的第一个和第二个日志文件。

一天之后、保存的文件将按格式进行压缩和重命名 *`yyyy-mm-dd.txt.gz`*、用于保留原始日期。随着时间的推移，这会导致为管理节点上的审核日志分配的存储被占用。脚本可监控审核日志空间占用情况、并根据需要删除日志文件以释放中的空间 `/var/local/audit/export` 目录。审核日志会根据创建日期进行删除，最早的日志会先删除。您可以在以下文件中监控脚本的操作： `/var/local/log/manage-audit.log`。

此示例显示了活动的 `audit.log` file、前一天的文件 (`2018-04-15.txt`)、以及前一天的压缩文件 (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```