



日志记录

本章包含以下部分：

- [日志记录概述, on page 1](#)
- [日志类型, on page 5](#)
- [日志订用, on page 27](#)

日志记录概述

日志文件记录系统中各项活动的正常操作及异常。使用日志可以监控思科内容安全设备，解决问题并评估系统性能。

大多数日志以纯文本 (ASCII) 格式记录；但是，为了提高资源效率，跟踪日志以二进制格式记录。ASCII 文本信息在任何文本编辑器中均可读。

日志记录与报告

使用日志记录数据来调试消息流，显示基本的日常操作信息（如 FTP 连接详细信息、HTTP 日志文件，以及将其用于合规性存档）。

您可以直接在邮件安全设备上访问此日志记录数据，或将其发送到任何外部 FTP 服务器以进行归档或读取。您可以通过 FTP 连接到设备以访问日志，或将纯文本日志推送到外部服务器以便备份。

要查看报告数据，请使用设备 GUI 上的“报告” (Report) 页面。您无法以任何方式访问基础数据，而且此数据无法发送到除思科内容管理设备以外的任何设备。



Note 安全管理设备会为所有报告和跟踪提取信息，但垃圾邮件隔离区数据除外。此数据从 ESA 推送。

日志检索

可以使用下表中介绍的文件传输协议检索日志文件。您可以在 GUI 中创建或编辑日志订阅时设置协议，也可以通过在 CLI 中使用 `logconfig` 命令来设置协议。

| | |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>FTP 轮询</p> | <p>使用此类文件传输协议时，远程FTP客户端使用管理员级别或操作员级用户的用户名和口令来访问设备以检索日志文件。在配置日志订阅以使用FTP轮询方法时，您必须提供要保留的最大日志文件数量。在达到最大数量时，系统会删除最旧的文件。</p> |
| <p>FTP 推送</p> | <p>使用此类文件传输协议时，设备会定期将日志文件推送到远程计算机上的FTP服务器。订阅要求提供远程计算机上的用户名、口令和目标目录。系统会根据配置的滚动更新计划传输日志文件。</p> |
| <p>SCP 推送</p> | <p>使用此类文件传输协议时，设备会定期将日志文件推送到远程计算机上的SCP服务器。此方法要求远程计算机上的SSH SCP服务器使用SSH2协议。这种订阅需要提供远程计算机上的用户名、SSL密钥和目标目录。系统会根据配置的滚动更新计划传输日志文件。</p> |
| <p>系统日志推送</p> | <p>使用此类文件传输协议时，设备会将日志消息发送到远程系统日志服务器。此方法符合RFC 3164标准。您必须提交系统日志服务器的主机名并将UDP或TCP用于日志传输。默认使用的端口是514。在AsyncOS 14.1.0中，端口号范围为1-65535。可以为日志选择工具；但是，日志类型的默认值已在下拉菜单中预先选择。仅基于文本的日志可以使用系统日志推送传输。</p> <p>输入要发送到远程服务器的日志消息的最大大小。[对于TCP协议]最大消息大小值必须是一个介于1024和65535之间的整数，[对于UDP协议]最大消息大小值必须是一个介于1024和9216之间的整数</p> <p>使用TLS选项通过TLS连接将日志消息从思科安全邮件和Web管理器发送到远程系统日志服务器。</p> <p>Note 如果选择TLS选项，确保在思科安全邮件和Web管理器中添加有效的客户端证书，以便在思科安全邮件和Web管理器与远程系统日志服务器之间建立TLS连接。</p> |

| | |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Syslog Push</p> | <p>系统日志磁盘缓冲区 - [仅适用于 TCP 协议]: 选中此复选框可为系统日志推送日志订阅配置本地磁盘缓冲区，以允许思科安全邮件和 Web 管理器在远程系统日志服务器不可用时缓存日志事件。当系统日志服务器可用时，思科安全邮件和 Web 管理器开始将缓冲区中用于该日志订阅的所有数据发送到系统日志服务器。</p> <p>注:</p> <ul style="list-style-type: none"> • 在开始此程序之前，请确保系统日志服务器正在运行，以避免日志数据丢失。 • 确定本地磁盘缓冲区的大小，留出足够的空间来容纳系统日志服务器的最大预期停机时间。这可以避免日志数据丢失。 • 如果您有用于本地保留的辅助日志订阅，思科建议您取消辅助订阅，以便为主要订阅的本地磁盘缓冲区留出空间。 • 思科安全邮件和 Web 管理器在与系统日志服务器断开连接后，可能无法缓存前几秒的日志数据。这是由于 TCP 上的系统日志的特征所致。 • 默认系统日志磁盘缓冲区大小为 100 MB。允许的最大磁盘缓冲区大小为 1 GB。您可以输入以字节为单位的大小（1073741824）、兆字节（1M）或千兆字节（1G）。 |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

文件名和目录结构

AsyncOS 会根据日志订阅中指定的日志名称为每个日志订阅创建目录。目录中的日志文件名包含日志订阅中指定的文件名、启动日志文件时的时间戳和单字符的状态代码。以下示例显示有关目录和文件名的约定：

```
</Log_Name></Log_Filename>.@<timestamp>.<statuscode>
```

状态代码可以是 .c（表示“当前”）或 .s（表示“已保存”）。您只应传输具有已保存状态的日志文件。

日志回滚和传输计划

在创建日志订阅时，您为何时进行日志滚动更新、传输旧文件和创建新的日志文件指定触发因素。

从以下触发因素中进行选择：

- 文件大小
- 时间

- 按指定的时间间隔（以秒、分钟、小时或天为单位）
在输入值时仿照屏幕上的示例。
要输入复合时间间隔，例如两个半小时，请仿照示例 2h30m。
或
- 在您指定的每天时间
或
- 在您所选星期几的指定时间

在指定时间时使用 24 小时制，例如用 23:00 表示 11pm。

要在一天内安排多个滚动更新时间，请用逗号将时间隔开。例如，要在午夜和中午滚动更新日志，请输入 00:00, 12:00

将星号 (*) 用作通配符。例如，要在每个整点和半点滚动更新日志，请输入 *:00, *:30

在达到指定的限制（或达到第一个限制，如果您同时配置了基于文件大小的限制和基于时间的限制）时，日志文件会滚动更新。基于 FTP 轮询传输机制的日志订阅会创建文件并将其存储在设备的 FTP 目录中，直到检索文件为止或直到系统需要更多的日志文件空间为止。



Note 如果在达到下一个限制时滚动更新正在进行，则会跳过新的滚动更新。系统会记录错误，并发送警报。

日志文件中的时间戳

以下日志文件包括日志自身的开始和结束日期、AsyncOS 版本和 GMT 时差（在日志开头以秒为单位提供）：

- 邮件日志
- 安全列表/阻止列表日志
- 系统日志

默认启用的日志

安全管理设备经过预配置，并且已启用以下日志订阅。

Table 1: 预配置的日志订阅

| 日志名称 | 日志类型 | 检索方法 |
|----------|-----------|--------|
| cli_logs | CLI 审核日志 | FTP 轮询 |
| euq_logs | 垃圾邮件隔离区日志 | FTP 轮询 |

| 日志名称 | 日志类型 | 检索方法 |
|-------------------|----------------|--------|
| euqgui_logs | 垃圾邮件隔离区 GUI 日志 | FTP 轮询 |
| gui_logs | HTTP 日志 | FTP 轮询 |
| mail_logs | 文本邮件日志 | FTP 轮询 |
| reportd_logs | 报告日志 | FTP 轮询 |
| reportqueryd_logs | 报告查询日志 | FTP 轮询 |
| slbld_logs | 安全列表/阻止列表日志 | FTP 轮询 |
| smad_logs | SMA 日志 | FTP 轮询 |
| system_logs | 系统日志 | FTP 轮询 |
| trackerd_logs | 跟踪日志 | FTP 轮询 |

所有预先配置的日志订阅的日志记录级别均设置为“信息”(Information)。有关日志级别的详细信息，请参阅[设置日志级别](#), on page 28。

您可以根据自己应用的许可证密钥配置其他日志订阅。有关创建和编辑日志订阅的信息，请参阅[日志订阅](#), on page 27。

日志类型

- [日志类型摘要](#), on page 6
- [使用配置历史记录日志](#), on page 10
- [使用 CLI 审核日志](#), on page 10
- [使用 FTP 服务器日志](#), on page 11
- [使用 HTTP 日志](#), on page 12
- [使用垃圾邮件隔离区日志](#), on page 12
- [使用垃圾邮件隔离区 GUI 日志](#), on page 13
- [使用文本邮件日志](#), on page 13
- [使用 NTP 日志](#), on page 19
- [使用报告日志](#), on page 19
- [使用报告查询日志](#), on page 20
- [使用安全列表/阻止列表日志](#), on page 20
- [使用 SMA 日志](#), on page 21
- [使用状态日志](#), on page 22
- [使用系统日志](#), on page 24
- [了解跟踪日志](#), on page 25

- [使用审核日志, on page 25](#)

日志类型摘要

日志订用可将日志类型与名称、日志记录级别及其他特性（例如文件大小和目标目录信息）相关联。允许除了配置历史记录日志外的所有日志类型的多个订用。日志类型决定日志中记录的数据。您在创建日志订用时选择日志类型。有关详细信息，请参阅[日志订用, on page 27](#)。

AsyncOS 会生成以下日志类型：

Table 2: 日志类型

| 日志类型 | 说明 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 身份验证日志 | 身份验证日志会记录成功的登录和不成功的登录尝试，这适用于在本地和外部经过身份验证的用户，以及通过 GUI 和 CLI 对安全管理设备的访问。 在调试和更详细的模式下，如果启用了外部验证，则所有 LDAP 查询都显示在这些日志中。 |
| 备份日志 | 备份日志自始至终记录备份过程。 有关备份计划的信息在 SMA 日志中。 |
| CLI审核日志 | CLI 审核日志会记录系统中的所有 CLI 活动。 |
| 配置历史记录日志 | 配置历史记录日志会记录以下信息：对安全管理设备进行的更改以及何时进行的更改。每次用户提交更改时，都会创建一份新的配置历史记录日志。 |
| FTP服务器日志 | FTP 日志记录了有关在接口上启用的 FTP 服务的信息。会记录连接详细信息和用户活动。 |
| GUI 日志 | GUI 日志包括 Web 界面、会话数据和用户访问的页面中的页面更新历史记录。您可以使用 <code>gui_log</code> 跟踪用户活动或调查用户在 GUI 中看到的错误。错误回溯通常在此日志中。 GUI 日志还包括有关 SMTP 事务的信息，例如有关通过邮件从设备发送的计划报告的信息。 |
| HTTP日志 | HTTP 日志会记录有关在接口上启用的 HTTP 服务和安全 HTTP 服务的信息。由于图形用户界面 (GUI) 是通过 HTTP 访问的，因此 HTTP 日志实质上是 CLI 审核日志的 GUI 等效版本。系统会记录会话数据（例如新的会话和过期的会话）以及在 GUI 中访问的页面。 |
| Haystack 日志 | Haystack 日志会记录跟踪数据处理的 Web 事务。 |
| 文本邮件日志 | 文本邮件日志会记录有关邮件系统操作（例如邮件接收、邮件传送尝试、打开和关闭连接、退回邮件等）的信息。 有关何时在邮件日志中包含附件名称的重要信息，请参阅 跟踪服务概述 。 |

| 日志类型 | 说明 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LDAP 调试日志 | <p>在“系统管理”(System Administration) > “LDAP”(LDAP) 中配置 LDAP 时，使用这些日志可调试问题。</p> <p>例如，这些日志会记录点击“测试服务器(Test Server)”和“测试查询(Test Queries)”按钮的结果。</p> <p>有关失败的 LDAP 身份验证的信息，请参阅身份验证日志。</p> |
| NTP 日志 | NTP 日志会记录设备与任何已配置的网络时间协议(NTP)服务器之间的对话。有关配置 NTP 服务器的信息，请参阅 配置系统时间 。 |
| 报告日志 | 报告日志会记录与集中报告服务的进程相关的操作。 |
| 报告查询日志 | 报告查询日志会记录与设备上运行的报告查询相关的操作。 |
| SMA 日志 | <p>SMA 日志会记录与常规安全管理设备进程相关的操作，不包括集中报告、集中跟踪和垃圾邮件隔离区服务的进程。</p> <p>这些日志包含有关备份计划的信息。</p> |
| SNMP 日志 | SNMP 日志会记录与 SNMP 网络管理引擎相关的调试消息。在跟踪或调试模式下，这包括对安全管理设备的 SNMP 请求。 |
| 安全列表/阻止列表日志 | 安全列表/阻止列表日志会记录有关安全列表/阻止列表设置和数据库的数据。 |
| 垃圾邮件隔离区 GUI 日志 | 垃圾邮件隔离区 GUI 日志会记录与垃圾邮件隔离区 GUI 相关联的操作，例如通过 GUI 进行的隔离区配置、最终用户身份验证和最终用户操作（例如放行邮件）。 |
| 垃圾邮件隔离区日志 | 垃圾邮件隔离区日志会记录与垃圾邮件隔离区流程相关联的操作。 |
| 状态日志 | 状态日志会记录 CLI 状态命令中找到的系统统计信息，包括 <code>status detail</code> 和 <code>dnsstatus</code> 。记录期限使用 <code>logconfig</code> 中的 <code>setup</code> 子命令设置。状态日志中的每个计数器或记录的速率为从上次重置计数器起至当前的值。 |
| 系统日志 | 系统日志会记录以下信息：启动信息、DNS 状态信息和用户使用 <code>commit</code> 命令键入的备注。系统日志可用于对设备的状态进行故障排除。 |
| 跟踪日志 | 跟踪日志记录了与跟踪服务过程关联的操作。跟踪日志是邮件日志的子集。 |
| 更新程序日志 | 有关服务更新的信息，例如时区更新。 |
| 升级日志 | 有关升级下载和安装的状态信息。 |

| 日志类型 | 说明 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 审核日志 | <p>审核日志记录 AAA（身份验证、授权和记帐）事件。</p> <p>某些审核日志详细信息如下：</p> <ul style="list-style-type: none"> • 用户 - 登录 • 用户 - 登录失败，密码不正确 • 用户 - 登录失败，用户名未知 • 用户 - 登录失败，账户到期 • 用户 - 注销 • 用户 - 锁定 • 用户 - 已激活 • 用户 - 密码更改 • 用户 - 密码重置 • 用户 - 安全设置/配置文件更改 • 用户 - 已创建 • 用户 - 已删除或修改 • 用户配置 - 用户所做的配置更改。 • 组/角色 - 删除或已修改 • 组/角色 - 权限更改 • 隔离区 - 对隔离区中的邮件执行的操作。 |

日志类型比较

下表总结了每种日志类型的特征。

Table 3: 日志类型比较

| | | | | | | 包含 | | | | | |
|--------|----|-----|-------|--------|--------|--------|--------|------|-------|-------|------|
| | 事务 | 无状态 | 记录为文本 | 记录为二进制 | 信头日志记录 | 定期状态信息 | 邮件接收信息 | 传送信息 | 单个硬退回 | 单个软退回 | 配置信息 |
| 身份验证日志 | | | | | | | | | | | |
| 备份日志 | | | | | | | | | | | |

| | | | | | | 包含 | | | | | |
|-------------|--|--|--|--|--|----|--|--|--|--|--|
| CLI 审核日志 | | | | | | | | | | | |
| 配置历史记录日志 | | | | | | | | | | | |
| FTP 服务器日志 | | | | | | | | | | | |
| HTTP 日志 | | | | | | | | | | | |
| Haystack 日志 | | | | | | | | | | | |
| 文本邮件日志 | | | | | | | | | | | |
| LDAP 调试日志 | | | | | | | | | | | |
| NTP 日志 | | | | | | | | | | | |
| 报告日志 | | | | | | | | | | | |
| 报告查询日志 | | | | | | | | | | | |
| SMA 日志 | | | | | | | | | | | |
| SNMP 日志 | | | | | | | | | | | |
| 安全列表/阻止列表日志 | | | | | | | | | | | |
| 垃圾邮件隔离区 GUI | | | | | | | | | | | |
| 垃圾邮件隔离区 | | | | | | | | | | | |
| 状态日志 | | | | | | | | | | | |
| 系统日志 | | | | | | | | | | | |

| | | | | | | 包含 | | | | | |
|--------|--|--|---|--|--|----|--|--|--|--|--|
| 跟踪日志 | | | | | | | | | | | |
| 更新程序日志 | | | | | | | | | | | |
| 审核日志 | | | . | | | | | | | | |

使用配置历史记录日志

配置历史记录日志包括配置文件以及列出用户名的附加部分、对用户配置中做出更改的位置的说明及用户在确认更改时输入的评论。每次用户提交更改时，都会创建一个包含更改后的配置文件的新日志。

示例

在本示例中，配置历史记录日志会显示用户（管理员）向定义允许哪些本地用户登录系统的表添加了访客用户。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
XML generated by configuration change.
Change comment: added guest user
User: admin
Configuration are described as:
  This table defines which local users are allowed to log into the system.
  Product: M160 Messaging Gateway(tm) Appliance
  Model Number: M160
  Version: 6.7.0-231
  Serial Number: 000000000ABC-D000000
  Number of CPUs: 1
  Memory (GB): 4
  Current Time: Thu Mar 26 05:34:36 2009
  Feature "Centralized Configuration Manager": Quantity = 10, Time Remaining = "25 days"
  Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"
  Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"
  Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"
  Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"
-->
<config>
```

使用 CLI 审核日志

下表介绍了 CLI 审核日志中记录的统计信息。

Table 4: CLI 审核日志统计信息

| 统计信息 | Description |
|------|-------------|
| 时间戳 | 数据的传输时间。 |

| 统计信息 | Description |
|------|----------------------------------------|
| PID | 输入命令的特定 CLI 会话的进程 ID。 |
| 邮件 | 消息包含输入的 CLI 命令、CLI 输出（包括菜单、列表等）和出现的提示。 |

示例

在本例中，CLI 审核日志显示用户对 PID 16434 输入以下 CLI 命令：`who`、`textconfig`。

```
Thu Sep  9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '
Thu Sep  9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n
=====
admin    Wed 11AM   3m 45s   10.1.3.14   tail\nadmin    02:32PM    0s        10.1.3.14
cli\nmail3.example.com> '
Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\nChoose the operation you want to perform:\n- NEW
- Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[ ]> '
```

使用 FTP 服务器日志

下表介绍了 FTP 服务器日志中记录的统计信息。

Table 5: FTP 服务器日志统计信息

| 统计信息 | Description |
|------|-----------------------------------------------|
| 时间戳 | 数据的传输时间。 |
| ID | 连接 ID。每个 FTP 连接的单独 ID。 |
| 邮件 | 日志条目的消息部分可以是日志文件状态信息或 FTP 连接信息（登录、上传、下载、注销等）。 |

示例

在本示例中，FTP 服务器日志记录了一个连接 (ID:1)。显示了传入连接的 IP 地址以及活动（上传和下载文件）和注销。

```
Wed Sep  8 18:03:06 2004 Info: Begin Logfile
Wed Sep  8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21
Wed Sep  8 18:03:06 2004 Info: Time offset from UTC: 0 seconds
Wed Sep  8 18:03:06 2004 Info: System is coming up
Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds
Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86
Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS
Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes
Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

使用 HTTP 日志

下表介绍了 HTTP 日志中记录的统计信息

Table 6: 在 HTTP 日志中记录的统计数据

| 统计信息 | Description |
|------|--------------------------------------|
| 时间戳 | 数据的传输时间。 |
| ID | 会话 ID。 |
| req | 连接的计算机的 IP 地址。 |
| 用户 | 连接的用户的用户名。 |
| 消息 | 有关所执行操作的信息。可能包括 GET 或 POST 命令或系统状态等。 |

示例

在本示例中，HTTP 日志显示 admin 用户与 GUI 的交互（例如运行“系统设置向导” [System Setup Wizard]）。

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443
Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80
Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443
Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds
Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303
Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190 HTTP/1.1
200
Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=190
HTTP/1.1 200
Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

使用垃圾邮件隔离区日志

下表介绍了垃圾邮件隔离区日志中记录的统计信息。

Table 7: 垃圾邮件隔离区日志统计信息

| 统计信息 | Description |
|------|------------------------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 消息包含所采取的操作（邮件被隔离、从隔离区放行等操作）。 |

示例

在本示例中，日志显示两封邮件（MID 8298624 和 MID 8298625）从隔离区放行到 admin@example.com。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

使用垃圾邮件隔离区 GUI 日志

下表 显示了在垃圾邮件隔离区 GUI 日志中记录的统计信息。

Table 8: 垃圾邮件隔离区 GUI 日志统计信息

| 统计信息 | Description |
|------|------------------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 该消息包括采取的措施，包括用户身份验证等等。 |

示例

在本示例中，日志显示了成功的身份验证、登录和注销：

Table 9: 垃圾邮件隔离区 GUI 日志示例

| |
|--------------------------------------------------------------------------------------------|
| Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82 |
| Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83 |
| Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin |
| Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO session:10.251.23.228 |
| Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO session:10.251.23.228 |
| Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin |

使用文本邮件日志

这些日志包含邮件接收、邮件传送和退回的详细信息。这些日志是重要的信息来源，可帮助了解特定邮件的传送情况和分析系统性能。

这些日志不需要任何特殊配置。但是，必须正确配置系统才能查看附件名称，而且不一定会记录附件名称。有关详细信息，请参阅[跟踪服务概述 \(Tracking Service Overview\)](#)。

下表介绍了文本邮件日志中显示的信息。

Table 10: 文本邮件日志统计信息

| 统计信息 | Description |
|------|--------------------------------------------------------------------------------|
| ICID | 注入连接 ID。这是与系统建立的单个 SMTP 连接的数字标识符。可以通过一个 SMTP 连接将单封邮件或成千上万封邮件发送到系统。 |
| DCID | 传输连接 ID。这是与另一台服务器建立的单个 SMTP 连接的数字标识符，用于传送一封至成千上万封邮件，每封邮件的部分或全部 RID 在单个邮件传输中传送。 |
| RCID | RPC 连接 ID。这是与垃圾邮件隔离区建立的单个 RPC 连接的数字标识符。该标识符用于在邮件进出垃圾邮件隔离区时跟踪邮件。 |
| MID | 消息 ID。使用此 ID 跟踪流经日志的邮件。 |
| RID | 收件人 ID。系统会为每个邮件收件人分配 ID。 |
| New | 新连接已发起。 |
| 开始 | 已开始新的邮件。 |

文本邮件日志示例

使用以下示例作为解释日志文件的指南。



Note 日志文件中的各行未编号。在此处对它们进行编号仅用于示例演示。

Table 11: 文本邮件日志详细信息

| | |
|---|------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes |
| 2 | Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5 |
| 3 | Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com> |
| 4 | Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com> |

| | |
|----|---------------------------------------------------------------------------------------------|
| 5 | Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com> |
| 6 | Mon Apr 17 19:59:59 2003 Info: ICID 5 close |
| 7 | Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25 |
| 8 | Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0] |
| 9 | Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0] |
| 10 | Mon Mar 31 20:11:03 2003 Info: DCID 8 close |

下表 可用作阅读上一日志文件的指南。

Table 12: 文本邮件日志详细信息示例

| 行号 | 说明 |
|----|-------------------------------------------------------------------------|
| 1 | 发起到系统的新连接并分配注入 ID (ICID) “5”。该连接在管理 IP 接口上收到，并从地址为 10.1.1.209 的远程主机上发起。 |
| 2 | 在从客户端发出 MAIL FROM 命令后，为邮件分配了邮件 ID (MID) “6”。 |
| 3 | 识别和接受发件人地址。 |
| 4 | 识别收件人，并且分配收件人 ID (RID) “0”。 |
| 5 | 接受 MID 5，将其写入磁盘并确认。 |
| 6 | 接收成功，接收连接断开。 |
| 7 | 邮件传送过程开始。系统为其分配了从 192.168.42.42 到 10.5.3.25 的传输连接 ID (DCID) “8”。 |
| 8 | 开始到 RID “0” 的邮件传送。 |
| 9 | 从 MID 6 到 RID “0” 的传送成功。 |
| 10 | 传送连接断开。 |

文本邮件日志条目示例

以下示例根据各种情况显示日志条目。

邮件接收

发送给单个收件人的一封邮件注入设备中。已成功传输该邮件。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com (1.2.3.4)
  address 2.3.4.5 reverse dns host unknown verified no
Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970
Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>
Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID '<37gva9$5uvbhe@mail.example.com>'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative
Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery
Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4
Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]
Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close
Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0] [('X-SBRS',
  'None')]
Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery
Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

成功的邮件传送示例

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address 63.251.108.110
Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]
Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]
Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

不成功的邮件传输（硬退回）

具有两个收件人的一封邮件注入设备中。传送后，目标主机返回5XX错误，这表示邮件未能传送到任何一个收件人。设备会通知发件人，并从队列中删除收件人。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address 64.81.204.225
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

最终成功传送的软退回示例

一封邮件注入设备中。在第一次尝试传输时，邮件被软退回并且排队等候将来传输。第二次尝试时，邮件被成功传送。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address 63.251.108.110
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23 2003
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
```



```
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

邮件扫描结果 (scanconfig)

如果使用 `scanconfig` 命令确定当邮件无法分解为各组成部分时（在删除附件时）的行为，如以下提示所述：

```
If a message could not be deconstructed into its component parts in order to remove specified
attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[3]>
```

以下是邮件日志中的指示：

在无法分解邮件时 `scanconfig` 设置为 `deliver`。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>
Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'
Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:36:29 2004 Info: ICID 44784 close
Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'
Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus
Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

在无法分解邮件时 `scanconfig` 设置为 `drop`。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

包含附件的邮件

在本例中，条件为“邮件正文包含”的内容过滤器已配置为支持附件名称识别：

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes
Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0
Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e5f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
```

```

policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery

```

请注意，三个附件中的第二附件采用 Unicode 格式。在无法显示 Unicode 的终端上，这些附件以引用的可打印格式显示。

生成的或重写的邮件

诸如重写/重定向操作等某些功能（`alt-rcpt-to` 过滤器、反垃圾邮件收件人重写、`bcc()` 操作、防病毒重定向等操作）会创建新邮件。在查看日志时，您可能需要检查结果并添加其他 MID 和 DCID。条目可能如下所示：

```

Tue Jun 1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
或者：
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antisipam
Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter 'testfilt'

```



Note “重写的”条目可以出现在日志中的行之后，指明使用新 MID。

将邮件发送到垃圾邮件隔离区

在用户将邮件发送到隔离区时，邮件日志会跟踪进出隔离区的移动，使用 RCID（RPC 连接 ID）标识 RPC 连接。在以下邮件日志中，邮件被标记为垃圾邮件并发送到垃圾邮件隔离区：

```

Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To: <stevell@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pemailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make it
a reality'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local Spam
Quarantine
Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done

```

使用 NTP 日志

下表 显示了 NTP 日志中记录的统计信息。

Table 13: NTP 日志中记录的统计信息

| 统计信息 | 说明 |
|------|------------------------------------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 消息包含对服务器的简单网络时间协议 (SNTP) 查询或 adjust: 消息。 |

示例

在本例中，NTP 日志显示了两次轮询 NTP 主机的设备。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652
Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152
Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

使用报告日志

下表 显示了报告日志中记录的统计信息。

Table 14: 报告日志统计信息

| 统计信息 | Description |
|------|------------------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 该消息包括采取的措施，包括用户身份验证等等。 |

示例

在本例中，报告日志显示了在信息日志级别设置的设备。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692
Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds
Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41
Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692
Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

使用报告查询日志

下表 显示了报告查询日志中记录的统计信息。

Table 15: 报告查询日志统计信息

| 统计信息 | Description |
|------|------------------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 该消息包括采取的措施，包括用户身份验证等等。 |

示例

在本例中，报告查询日志显示了从 2007 年 8 月 29 日到 10 月 10 日，运行每日传出邮件流量查询的设备。

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTEN
T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI
PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints
None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from 0
to 2 sort_ascendin
g=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constra
ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning results
from 0 to 2 sort
_ascending=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

使用安全列表/阻止列表日志

下表 显示了在安全列表/阻止列表日志中记录的统计信息。

Table 16: 安全列表/阻止列表日志统计信息

| 统计信息 | Description |
|------|------------------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 该消息包括采取的措施，包括用户身份验证等等。 |

示例

在本示例中，安全列表/阻止列表日志显示每两隔小时创建数据库快照的设备。它还显示了何时将发件人添加到数据库中。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version: 6.0.0-425
SN: XXXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC: 10800 seconds
Fri Sep 28 14:22:33 2007 Info: System is coming up.
Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.
.....
Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.
Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.
Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

使用 SMA 日志

下表显示了在 SMA 日志中记录的统计信息。

Table 17: SMA 日志统计信息

| 统计信息 | Description |
|------|------------------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 该消息包括采取的措施，包括用户身份验证等等。 |

示例

在本示例中，SMA 日志显示从邮件安全设备下载跟踪文件的集中跟踪服务，并显示从邮件安全设备下载报告文件的集中报告服务。

```
Wed Oct 3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202244Z_20071003T202544Z.s
Wed Oct 3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T202443Z_20071003T202743Z.s
Wed Oct 3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202544Z_20071003T202844Z.s
Wed Oct 3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T202743Z_20071003T203043Z.s
Wed Oct 3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from 172.29.0.15
- /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz
Wed Oct 3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202844Z_20071003T203144Z.s
Wed Oct 3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from 172.29.0.17
- /reporting/ou
```

```
tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz
Wed Oct 3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T203043Z_20071003T203343Z.s
```

使用状态日志

状态日志记录 CLI 状态命令中的系统统计信息，包括 `status`、`status detail` 以及 `dnsstatus` 命令。记录期限使用 `logconfig` 中的 `setup` 子命令设置。状态日志中的每个计数器或记录的速率为从上次重置计数器起至当前的值。

Table 18: 状态日志统计信息

| 统计信息 | 说明 |
|------------|-----------------|
| CPULd | CPU 利用率。 |
| DskIO | 磁盘 I/O 利用率。 |
| RAMUtil | RAM 利用率。 |
| QKUsd | 已用的队列空间 (KB)。 |
| QKFre | 可用的队列空间 (KB)。 |
| CrtMID | 邮件 ID (MID)。 |
| CrtICID | 注入连接 ID (ICID)。 |
| CRTDCID | 传送连接 ID (DCID)。 |
| InjMsg | 注入的邮件数量。 |
| InjRcp | 注入的收件人数量。 |
| GenBncRcp | 生成的退回收件人数量。 |
| RejRcp | 拒绝的收件人数量。 |
| DrpMsg | 丢弃的邮件数量。 |
| SftBncEvnt | 软退回的事件数量。 |
| CmpRcp | 已完成的收件人数量。 |
| HrdBncRcp | 硬退回的收件人数量。 |
| DnsHrdBnc | DNS 硬退回数量。 |
| 5XXHrdBnc | 5XX 硬退回数量。 |
| FltrHrdBnc | 过滤器硬退回数量。 |

| 统计信息 | 说明 |
|------------|-----------------------|
| ExpHrdBnc | 过期硬退回数量。 |
| OtrHrdBnc | 其他硬退回数量。 |
| DlvRcp | 已传送的收件人数量。 |
| DelRcp | 已删除的收件人数量。 |
| GlbUnsbHt | 全局取消订阅命中数。 |
| ActvRcp | 正在处理的收件人数量。 |
| UnatmptRcp | 未尝试的收件人数量。 |
| AtmptRcp | 已尝试的收件人数量。 |
| CrtCncIn | 当前的进站连接数。 |
| CrtCncOut | 当前的出站连接数。 |
| DnsReq | DNS 请求数。 |
| NetReq | 网络请求数。 |
| CchHit | 缓存命中数。 |
| CchMis | 缓存丢失数。 |
| CchEct | 缓存异常数。 |
| CchExp | 缓存过期。 |
| CPUTTm | 应用使用的 CPU 时间。 |
| CPUETm | 自应用启动以来经过的时间。 |
| MaxIO | 邮件进程每秒的最大磁盘 I/O 操作数量。 |
| RamUsd | 分配的内存（字节）。 |
| SwIn | 换入的内存。 |
| SwOut | 换出的内存。 |
| SwPgIn | 页入的内存。 |
| SwPgOut | 页出的内存。 |
| MMLen | 系统中的邮件总数。 |
| DstInMem | 内存中的目标对象数。 |

| 统计信息 | 说明 |
|-----------|---------------------------------------|
| ResCon | 资源节省 tarpit 值。对传入邮件的接受延迟此秒数，因为系统负载很重。 |
| WorkQ | 工作队列中的邮件数量。 |
| QuarMsgs | 系统隔离区中各邮件的数量（出现在多个隔离区中的邮件只计算一次）。 |
| QuarQKUsd | 系统隔离区邮件已使用的空间 (KB)。 |
| LogUsd | 已使用的日志分区百分比。 |
| CASELd | CASE 扫描已使用的 CPU 百分比。 |
| TotalLd | CPU 总利用率。 |
| LogAvail | 可用于日志文件的磁盘空间量。 |
| EuQ | 垃圾邮件隔离区中的邮件数量。 |
| EuQRls | 垃圾邮件隔离区放行队列中的邮件数量。 |

示例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318
  DrpMsg 7437 SftBncEvt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc
0 ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp
0 CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct
15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen 0 DstInMem 4
ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail
17G EuQ 0 EuQRls 0
```

使用系统日志

下表显示了在系统日志中记录的统计信息。

Table 19: 系统日志统计信息

| 统计信息 | Description |
|------|-------------|
| 时间戳 | 数据的传输时间。 |
| 消息 | 记录的事件。 |

示例

在本示例中，系统日志显示了一些提交条目，包括发出提交命令的用户的名称和输入的备注。

```
Wed Sep 8 18:02:45 2004 Info: Version: 6.0.0-206 SN: XXXXXXXXXXXX-XXX
Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds
Wed Sep 8 18:02:45 2004 Info: System is coming up
Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache
```



```

Wed Sep  8 18:02:49 2004 Info: DNS cache bootstrapped
Wed Sep  8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Passphrase
Wed Sep  8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW
Thu Sep  9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds
Thu Sep  9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI log
    for examples
Thu Sep  9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.

```

了解跟踪日志

跟踪日志记录了有关 AsyncOS 的邮件操作的信息。此类日志消息包含在邮件日志中。

消息跟踪组件使用跟踪日志构建消息跟踪数据库。由于构建数据库的过程中会使用日志文件，因此跟踪日志是动态的。跟踪日志中的信息不是供人类阅读或分析的。

为了提高资源效率，跟踪日志以二进制格式记录和传输。信息以符合逻辑的方式列出，在使用思科提供的实用程序转换后可供人员阅读。转换工具位于以下网址：<http://tinyurl.com/3c5l8r>。

使用审核日志

审核日志记录 AAA（身份验证、授权和记帐）事件。大多数信息处于“调试”或“跟踪”级别。

审核日志条目示例：

- 在本例中，日志显示了用户（例如 **admin**）何时：
 - 已登录设备的 Web 界面。
 - 已从设备的 Web 界面注销。

```

Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Event: Successful login
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session established
successfully
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: User logged out
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session terminated

```

- 在本例中，日志显示用户（例如 **admin**）输入了 `logconfig` CLI 命令。

```

Thu Oct 8 13:33:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User input was 'logconfig'
Thu Oct 8 13:33:46 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User input was 'Enter'

```

- 在本例中，日志显示用户（例如 **admin**）查看了设备的旧 Web 界面上的 GUI 页面。

```

Thu Oct 8 13:35:07 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /network/dns, Event: User visited the web page.

```

- 在本例中，日志显示使用 Web 界面将新用户（例如 **admin**）添加到了设备，但未提交更改。

```
Thu Oct 8 13:36:30 2020 Info: Appliance: maill.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Added
user "admin" and changes
will reflect after commit.
Thu Oct 8 13:37:22 2020 Info: Appliance: maill.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Deleted
user "admin" and changes
will reflect after commit.
```

- 在本例中，日志显示用户（例如 admin）放弃了在设备的 Web 界面上未提交的所有更改。

```
Thu Oct 8 13:39:44 2020 Info: Appliance: maill.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /commit, Event: User discarded all uncommitted changes.
```

- 在本例中，日志显示用户（例如 admin）放弃了所有未通过 CLI 提交的更改。

```
Thu Oct 8 13:41:38 2020 Info: Appliance: maill.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User discarded all uncommitted changes.
```

- 在本例中，日志显示用户（例如 admin）对 Web UI 会话超时进行了配置更改。



注释 通过查看“配置历史日志” (Configuration History Logs) 或启用审核日志的调试模式，可以查看在设备中进行的配置更改的更多详细信息。

```
Thu Oct 8 13:45:46 2020 Info: Appliance: maill.example.com, User: admin,
Event: The following configuration changes were committed with comment - 'N/A'
Thu Oct 8 13:45:46 2020 Info: * [standalone] Number of seconds before the Web UI session
times out.
```

- 在本例中，日志显示了由于身份验证失败，AsyncOS API 无法获取日志订阅。

```
Thu Oct 8 13:52:28 2020 Debug: 08/Oct/2020 13:52:28 +0000 Error - Code: 401,
Details: Unauthorized (No permission -- see authorization schemes)
Thu Oct 8 13:52:28 2020 Info: Appliance: maill.example.com, Interaction Mode: API,
User: admin, Role: Role Not Available, Source IP: 192.168.1.1, Destination IP:
192.168.2.2,
Location: GET /sma/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: User is not
valid.
```

- 在本例中，日志显示了由于身份验证成功，AsyncOS API 可以获取日志订阅。

```
Thu Oct 8 13:52:37 2020 Info: Appliance: maill.example.com, Interaction Mode: API,
User: admin, Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Location: GET /sma/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: API Access
Success.
```

- 在本例中，日志显示：

- 使用 CLI 将新用户（例如 admin）添加到了设备，但未提交更改。
- 使用 CLI 在设备中更新了现有用户帐户详细信息，但未提交更改。

```
Thu Oct 8 13:42:48 2020 Info: Appliance: maill.example.com, Interaction Mode: CLI,
User: admin, Source IP: 192.168.1.1, Event: Added user "hops" and changes will
reflect
after commit
Thu Oct 8 13:43:26 2020 Info: Appliance: maill.example.com, Interaction Mode: CLI,
```

```
User: admin,
Source IP: 192.168.1.1, Event: Updated user "hops" and changes will reflect after
commit
```

- 在本例中，日志显示用户（例如 admin）在设备的新 Web 界面上执行了邮件跟踪搜索。

```
User: admin,
Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Location: GET /sma/api/v2.0/message-tracking/messages?startDate=2020-10-12T00:00:00.000Z
&endDate=2020-10-12T04:13:00.000Z&ciscoHost=All_Hosts&searchOption=messages&offset=0&limit=100
HTTP/1.0,
Event: API Access Success.
```



注释 在设备的新 Web 界面上执行的操作（例如，跟踪，报告或隔离搜索）会根据用于这些操作的相应 API 记录为日志。

日志订用

- [配置日志订用, on page 27](#)
- [在 GUI 中创建日志订用, on page 29](#)
- [配置日志记录的全局设置, on page 30](#)
- [滚动更新日志订用, on page 31](#)
- [配置主机密钥, on page 33](#)

配置日志订用

日志订用会创建在思科内容安全设备或远程位置存储的单个日志文件。系统会对日志订用进行推送（传输到另一台计算机）或轮询（从设备检索）。通常，日志订用具有以下属性：

Table 20: 日志文件属性

| 属性 | 说明 |
|---------------------------------|-------------------------------------------------------------------|
| 日志类型 | 定义记录的信息类型以及日志订用的格式。有关详细信息，请参阅 日志类型摘要, on page 6 。 |
| 名称 | 您提供的供自己将来参考的日志订用描述性名称。 |
| 日志文件名 (Log Filename) | 文件写入磁盘时的实际名称。如果系统包括多台内容安全设备，请使用唯一的日志文件名来标识生成该日志文件的设备。 |
| 按文件大小滚动 (Rollover by File Size) | 文件在滚动更新之前可以达到的最大大小。 |
| 按时间滚动 (Rollover by Time) | 何时根据时间滚动更新日志文件。请参阅 日志回滚和传输计划, on page 3 的选项。 |

| 属性 | 说明 |
|-------------------------|-----------------------------------------------------|
| 速率限制 | 在指定的时间范围内（以秒为单位），设置日志文件中记录的最大事件数。 默认时间范围值为 10 秒。 |
| 日志级别 (Log Level) | 每个日志订用的详细信息级别。 |
| 检索方法 (Retrieval Method) | 用于从设备传输日志文件的方法。 |

使用管理设备 (Management Appliance) > 系统管理 (System Administration) > 日志订阅 (Log subscriptions) 页面（或 CLI 中的 `logconfig` 命令）配置日志订阅。系统会提示您输入日志类型，如 [日志类型摘要, on page 6](#) 所示。对于大多数日志类型，系统会要求您为日志订阅选择日志级别 (*log level*)。



Note 仅限配置历史记录日志：如果您预期从配置历史记录日志加载配置，请注意不能加载包含已屏蔽口令的配置。在管理设备 (Management Appliance) > 系统管理 (System Administration) > 日志订阅 (Log subscriptions) 页面上，当系统提示您是否要在日志中包括口令时选择是 (Yes)。如果您在 CLI 中使用 `logconfig` 命令，请在出现提示时键入 `y`。

设置日志级别

日志级别决定日志中提供的信息量。日志可以是五种级别中的一种。与简略的日志级别设置相比，详细的日志级别设置会创建更大的日志文件，且对系统性能有更大的影响。详细的日志级别设置包括简略的日志级别设置中包含的所有消息以及其他消息。随着详细级别的提升，系统性能会逐渐下降。




Note 您可以为每种日志类型指定不同的日志记录级别。

Table 21: 日志级别

| 日志级别 | 说明 |
|------------------|----------------------------------------------------------------------------------------------------|
| 严重 | 仅记录错误。这是最简略的日志级别设置。在此日志级别，您无法监控性能和重要设备活动；但是，日志文件不会像在详细日志级别那样快速达到最大大小。此日志级别类似于系统日志级别“警报” (Alert)。 |
| 警告 | 记录所有系统错误和警告。在此日志级别，您无法监控性能和重要设备活动。日志文件比在“严重” (Critical) 日志级别更快达到最大大小。此日志级别类似于系统日志级别“警告” (Warning)。 |
| 信息 (Information) | 记录系统的每一秒钟的操作。例如，会记录打开的连接和传送尝试。信息级别是推荐日志设置。此日志级别类似于系统日志级别“信息” (Info)。 |

| 日志级别 | 说明 |
|------|------------------------------------------------------------------------------------------------|
| 调试 | 比在“信息”日志级别记录的信息更详细。在对错误进行故障排除时，请使用“调试”(Debug)日志级别。暂时使用此设置，然后恢复到默认级别。此日志级别类似于系统日志级别“调试”(Debug)。 |
| 跟踪 | 记录所有可用的信息。建议仅将“跟踪”日志级别供开发人员使用。使用此级别会造成严重的系统性能下降，建议不要使用。此日志级别类似于系统日志级别“调试”(Debug)。 |

在 GUI 中创建日志订阅

- 步骤 1** [仅限新 Web 界面] 在安全管理设备中，点击  加载旧 Web 界面。
- 步骤 2** 在管理设备 (Management Appliance) > 系统管理 (System Administration) > 日志订阅 (Log Subscriptions) 页面上，点击添加日志订阅 (Add Log Subscription)。
- 步骤 3** 选择日志类型，并输入日志目录的日志名称和日志文件本身的名称。
- 步骤 4** 如果适用，请指定最大文件大小。
- 步骤 5** 如果适用，请指定滚动更新日志的日期、当天时间或时间间隔。有关详细信息，请参阅 [日志回滚和传输计划, on page 3](#)。
- 步骤 6** 如果适用，请在指定的时间范围内（以秒为单位）指定日志文件中记录的最大事件数。
- 步骤 7** 如果适用，请指定日志级别。
- 步骤 8** （仅限配置历史记录日志）选择是否在日志中包括口令。
Note 您不能加载包含已屏蔽口令的配置。如果您预期从配置历史记录日志加载配置，请选择“是”以在日志中包括口令。
- 步骤 9** 配置日志检索方法。
- 步骤 10** 提交并确认更改。

编辑日志订阅

- 步骤 1** 单击“日志订阅”(Log Subscriptions) 页面上的“日志名称”(Log Name) 列中的日志名称。
- 步骤 2** 更新日志订阅。
- 步骤 3** 提交并确认更改。

配置日志记录的全局设置

系统会在文本邮件日志和状态日志中定期记录系统指标。使用“日志订阅”(Log Subscriptions)页面的“全局设置”(Global Settings)部分中的编辑设置按钮(或CLI中的logconfig -> setup命令)配置以下设置:

- 系统在记录指标之间等待的时长(以秒为单位)
- 是否记录邮件ID标题
- 是否记录远程响应状态代码
- 是否记录原始邮件的主题标题
- 应该为每个邮件记录的信头

所有思科内容安全设备日志可以有选择地包括以下三项:

- 邮件ID: 如果配置了此选项, 则每个邮件都会记录其邮件ID信头(如果有)。此邮件ID可能来自收到的邮件或可能由AsyncOS生成。例如:

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

- 远程响应: 如果配置了此选项, 将记录每封邮件的远程响应状态代码(如果可用)。例如:

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
```

远程响应字符串是在传输SMTP对话期间响应DATA命令后收到的人类可读的文本。在本例中, 在连接主机发出数据命令后的远程响应是“queued as 9C8B425DA7”。

```
[...]
250 ok hostname
250 Ok: queued as 9C8B425DA7
```

系统会从字符串开头剥离空白区域、标点符号和“OK”字符(在250响应情况下)。仅从字符串末尾剥离空白区域。例如, 默认情况下, 思科内容安全设备使用以下字符串来响应DATA命令: 250 Ok: Message MID accepted。因此, 如果远程主机是另一个思科内容安全设备, 则会记录“Message MID accepted”。

- 原始主题标题: 启用此选项时, 每封邮件的原始主题标题均包括在日志中。

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

日志记录邮件信头

有时, 当邮件通过系统时, 有必要记录邮件信头的存在性及其内容。您可以在“日志订阅全局设置”(Log Subscriptions Global Settings)页面上(或通过CLI中的logconfig -> logheaders子命令)指定要记录的标题。设备会在文本邮件日志和跟踪日志中记录指定的邮件标题。如果信头存在, 则系统会记录信头的名称和值。如果没有信头, 则不会在日志中记录任何信息。



Note 在处理要记录的邮件的过程中，系统会评估存在于邮件中的所有信头，不管是否为日志记录指定了信头都是如此。



Note SMTP 协议的 RFC 位于 <http://www.faqs.org/rfcs/rfc2821.html> 并定义用户定义的信头。



Note 如果已通过 `logheaders` 命令配置了要记录的信头，则在传输信息之后将显示信头信息：

Table 22: 日志信头

| 信头名称 | 信头的名称 |
|------|----------|
| 值 | 已记录信头的内容 |

例如，指定 “`date, x-subject`” 作为要记录的标题会导致以下行出现在邮件日志中：

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0] [('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

通过使用 GUI 配置日志记录的全局设置

步骤 1 单击“日志订阅” (Log Subscriptions) 页面的“全局设置” (Global Settings) 部分中的编辑设置 (**Edit Settings**) 按钮。

步骤 2 指定系统指标频率、是否要将邮件 ID 标题包括在邮件日志中、是否包括远程响应以及包括每封邮件的原始主题标题。

有关这些设置的详细信息，请参阅[配置日志记录的全局设置, on page 30](#)。

步骤 3 输入要在日志中包含的任何其他信头。用逗号分隔每个条目。

步骤 4 提交并确认更改。

滚动更新日志订用

在滚动更新日志文件时，AsyncOS 会执行以下操作：

- 使用滚动更新操作的时间戳创建新的日志文件，并使用字母 “**c**” 扩展名指定该文件为最新文件
- 将最新的日志文件重命名为具有字母 “**s**” 扩展名，表示已保存
- 将新保存的日志文件传输到一台远程主机（如果基于推送）
- 从同一订用传输以前不成功的任何日志文件（如果基于推送）

- 在超过要保存的文件总数时，删除日志订阅中的最旧文件（如果基于轮询）

后续操作

滚动更新日志订阅中的日志

请参阅 [日志回滚和传输计划](#), on page 3。

使用 GUI 立即滚动更新日志

步骤 1 在“日志订阅” (Log Subscriptions) 页面上，选中要滚动更新的日志右侧的复选框。

步骤 2 （可选）通过选中全部 (All) 复选框选择滚动更新所有日志。

步骤 3 点击立即滚动更新 (Rollover Now) 按钮。

What to do next

- [滚动更新日志订阅中的日志](#), on page 32
- [通过 CLI 立即滚动更新日志](#), on page 32

通过 CLI 立即滚动更新日志

使用 rollovernow 命令同时滚动更新所有日志文件，或从列表中选择特定的日志文件。

查看 GUI 中最新的日志条目

您可以通过 GUI 查看日志文件，方法是在“日志订阅” (Log Subscriptions) 页面上点击表的“日志名称” (Log Name) 列中的日志订阅。点击日志订阅的链接时，系统会提示您输入口令。该订阅的日志文件列表随即出现。您可以点击其中一个日志文件，以便在浏览器中查看或将其保存到磁盘。您必须在“管理” (Management) 接口上启用 FTP 服务才可以在 GUI 中查看日志。

查看日志中的最新条目（tail 命令）

AsyncOS 支持 tail 命令，该命令会显示在设备上配置的日志的最新条目。发出 tail 命令并选择当前配置的日志的编号以查看它。按 Ctrl-C 可从 tail 命令中退出。



Note 您无法通过使用 tail 命令查看配置历史记录日志。您必须使用 FTP 或 SCP。

示例

在以下示例中，tail 命令用于查看系统日志。tail 命令还接受将日志名称视为参数，例如：tail system_logs


```

Welcome to the M600 Messaging Gateway(tm) Appliance
example.srv> tail
Currently configured logs:
1. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
2. "euq_logs" Type: "Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "Text Mail Logs" Retrieval: FTP Poll
6. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
7. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
8. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
9. "smad_logs" Type: "SMA Logs" Retrieval: FTP Poll
10. "system_logs" Type: "System Logs" Retrieval: FTP Poll
11. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 10
Press Ctrl-C to stop.
Thu Sep 27 00:18:56 2007 Info: Begin Logfile
Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN: 001143583D73-FT9GP61
Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds
Thu Sep 27 00:18:47 2007 Info: System is coming up.
Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64] Host is down' to
'172.16.0.3' looking up 'downloads.cisco.com'
Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:
Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:
^Cexample.srv>
    
```

配置主机密钥

将日志从思科内容安全设备推送到其他服务器时，使用 `logconfig -> hostkeyconfig` 子命令管理与 SSH 配合使用的主机密钥。SSH 服务器必须具有一对主机密钥：一个私钥和一个公钥。专用主机密钥驻留在 SSH 服务器上，无法被远程计算机读取。公共主机密钥可分配给需要与 SSH 服务器交互的任何客户端计算机。



Note 要管理用户密钥，请参阅邮件安全设备用户指南或在线帮助中的“管理安全外壳 (SSH) 密钥”。

`hostkeyconfig` 子命令会执行以下功能：

Table 23: 管理主机密钥 - 子命令列表

| 命令 | 说明 |
|--------|-----------|
| New | 添加新密钥。 |
| Edit | 修改现有密钥。 |
| Delete | 删除现有密钥。 |
| Scan | 自动下载主机密钥。 |
| Print | 显示密钥。 |

| 命令 | 说明 |
|-------------|-----------------------------------------------------------------------------------|
| 主机 | 显示系统主机密钥。这是要放置在远程系统的“known_hosts”文件中的值。 |
| Fingerprint | 显示系统主机密钥指纹。 |
| User | 显示将日志推送到远程计算机的系统账户的公共密钥。这是在设置 SCP 推送订用时出现的同一密钥。这是要放置在远程系统的“authorized_keys”文件中的值。 |

示例

在以下示例中，这些命令扫描主机密钥并为主机添加密钥：

```
mail3.example.com> logconfig
Currently configured logs:
[ list of logs
]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[> hostkeyconfig
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[> scan
Please enter the host or IP address to lookup.
[> mail3.example.com
Choose the ssh protocol type:
1. SSH2:rsa
2. SSH2:dsa
3. All
[3]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed
]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed
]
Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed
]
2. mail3.example.com ssh-rsa [ key displayed
]
3. mail3.example.com 1024 35 [ key displayed
]
```

```
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
Currently configured logs:
[ list of configured logs
]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
mail3.example.com> commit
```


当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。