使用 CLI 进行管理和监控

本章包含以下部分：

使用 CLI 进行管理和监控概述

使用 CLI 管理和监控邮件网关的过程包含以下类型的任务：

- 监控邮件活动。
  - 邮件网关在邮件管道中处理的邮件、收件人和退回收件人的原始数量。
  - 邮件传送或邮件退回的每小时速率基于过去 1 分钟、5 分钟或 15 分钟时段
- 监控系统资源。示例：
  - 内存使用率
  - 磁盘空间
  - 连接数
- 使用简单网络管理协议 (SNMP) 监控可能的系统功能障碍。示例：
  - 风扇故障
  - 更新失败
  - 异常高的邮件网关温度
- 管理管道中的邮件。示例：
  - 删除队列中的收件人
  - 将邮件重定向到另一台主机
  - 通过删除收件人或重定向邮件清除该队列
  - 暂停或恢复邮件接收、传送或工作队列处理

- 找到特定邮件

读取可用的监控组件

读取事件计数器

计数器提供系统中运行的各个事件的总数。对于每个计数器，可以查看自重置计数器以来、自上次系统重新启动以来以及在系统的整个生命周期中生成的事件总数。

每次发生事件时，计数器计数增加，其通过三个版本显示：

重置	自上次通过 resetcounters 命令重置计数器
正常运行时间	自上次系统重新启动
使用时间	在邮件网关整个生命周期中的总计

下表列出了在监控邮件网关时可用的计数器及其说明。

Note 这是完整的列表。显示的计数器因所选的显示选项或命令而异。此列表仅供参考。

Table 1: 计数器

统计信息	Description
Receiving	
接收的邮件数量	在接收队列中接收的邮件。
已经接收的收件人数量	所有已接收邮件的收件人。
生成的退回收件人数量	系统为其生成退回并将其插入传送队列中的收件人。
拒绝	
拒绝的收件人数量	由于收件人访问表 (RAT) 或意外协议协商（包括过早出现连接终止）而被拒绝接收到传送队列的收件人。

统计信息	Description
删除的邮件数量	由于过滤器丢弃操作条件匹配或已被 Sinkhole 排队侦听程序接收而被拒绝接收到传送队列中的邮件。定向到别名表中的 /dev/null 条目的邮件也被视为丢弃的邮件。被反垃圾邮件过滤功能（如果已在系统中启用）删除的邮件也会记入此计数器。
队列	软退回事件的数量 - 多次软退回的邮件具有多个软退回事件。
软退回事件的数量	
完成	全部硬退回的收件人、已传送收件人和已删除收件人的总计。从传送队列中删除的任何收件人。
已经完成的收件人数量	
硬退回的收件人数量	所有 DNS 硬退回、5XX 硬退回、过滤器硬退回、到期硬退信和其他硬退回的总计。将邮件传送给收件人的尝试失败，导致传送立即终止。
DNS 硬退回	尝试将邮件传送给收件人时遇到的 DNS 错误。
5XX 硬退回	当尝试将邮件传送给收件人时，目标邮件服务器返回“5XX”响应代码。
过期的硬退回	超出传送队列中允许的最长时间或最大连接尝试次数的邮件收件人。
内容过滤的硬退回	收件人传送已被匹配的过滤器bounce操作预占。被反垃圾邮件过滤功能（如果已在系统中启用）丢弃的邮件也会记入此计数器。
其他硬退回	在邮件传送或通过 bouncerecipients 命令明确退回邮件收件人期间出现的意外错误。
发送的收件人数量	邮件已成功传送给收件人。
已删除的收件人	通过 deleterecipients 命令明确删除的邮件收件人总数或全局取消订用命中数。
全局取消订用命中数	邮件收件人因匹配全局取消订用设置而被删除。
当前的 ID	分配给插入传送队列中的邮件的最后一个邮件ID。MID与邮件网关收到的每封邮件关联，并且可以在邮件日志中跟踪。MID 会在 231 处重置为零。
邮件ID(MID)	

统计信息	Description
注入连接 ID (ICID)	分配给侦听程序接口连接的最后注入连接 ID 。ICID 会在 231 处回滚（重置为零）。
传送连接 ID (DCID)	已分配给目标邮件服务器连接的最后传送连接 ID。DCID 会在 231 处回滚（重置为零）。

读取系统计量器

计量器会显示系统资源（如内存、磁盘空间或活动连接）的当前利用率。

下表列出了在监控邮件网关时可用的计量器及其说明。

Note 这是完整的列表。显示的计量器因所选的显示选项或命令而异。此列表仅供参考。

Table 2: 规格

统计信息	Description
系统计量器	
内存使用率	系统使用的物理随机访问内存的百分比。
CPU Utilization	CPU 使用率百分比
硬盘 I/O 使用率	使用的磁盘 I/O 的百分比。 **Note** 磁盘 I/O 利用率计量器不根据已知值的比例显示读数。相反，它会显示到目前为止系统发现的 I/O 利用率，并且根据上次重新启动以来的最大值进行调整。因此，如果计量器显示 100%，则表示系统达到启动以来最高级别的 I/O 利用率（不一定表示使用了整个系统 100% 的物理磁盘 I/O）。
资源节约	介于 0 和 60 或 999 之间的值。介于 0 和 60 之间的数字表示系统降低其接受邮件的程度，从而避免快速消耗关键系统资源。数字越高表示减少接受的程度越大。零表示不降低接受程度。如果此计量器显示999，则系统已进入“资源节约模式”，不会接受任何邮件。每当系统进入或退出资源节约模式时，都会发送警报邮件。
磁盘利用率：日志	用于日志的磁盘百分比，在状态日志中显示为 LogUsd，而在 XML 状态中显示为 log_used。
连接计量器	

统计信息	Description
当前的入站连接数	侦听程序接口的当前入站连接数。
当前的出站连接数	与目标邮件服务器的当前出站连接。
队列计量器	
正在处理的收件人	传送队列中的邮件收件人。未尝试发送的收件人和已尝试发送过的收件人的总计。
未尝试发送的收件人	有效收件人的子类别。队列中未尝试向其传送的邮件收件人。
已经尝试发送的收件人	有效收件人的子类别。队列中已尝试向其传送单位由于软退回事件而失败的邮件收件人。
工作队列中的邮件数量	在排队之前，等待由别名表扩展、伪装、反垃圾邮件、防病毒扫描、邮件过滤器和 LDAP 查询处理邮件数量。
隔离区中的邮件	任何隔离区中的独特邮件数量，加上已放行或删除但尚未执行操作的邮件。例如，如果放行病毒爆发中的所有隔离邮件，则病毒爆发的邮件总数将立即变为零，但是，此字段仍会反映隔离的邮件，直到传送所有这些邮件。
内存中的目标	内存中的目标域数量。对于具有需要传送的邮件的每个域，将在内存中创建目标对象。在传送了该域的所有邮件后，会将目标对象再保留 3 个小时。在 3 小时后，如果没有任何新邮件发往该域，则该对象将过期，因此不再报告该目标（例如，在 tophosts 命令中）。如果仅将邮件传送到一个域，此计数器将为“1”。如果您从未收到或发送任何邮件（或邮件网关在数小时内未处理任何邮件），则计数器将为“0”。 如果使用虚拟网关，则每个虚拟网关的目标域都将具有单独的目标对象。（例如，如果从 3 个不同的虚拟网关传送到 yahoo.com，yahoo.com 将统计为 3 个目标对象 ）。
已使用千字节	已使用的队列存储（按 KB 计）。
隔离区中的 KB 数	用于隔离的邮件的队列存储。该值的计算方式为：邮件大小加上每个收件人对应的 30 字节，并且根据上面统计的“隔离区中的邮件”进行求和。请注意，此计算通常会高估使用的空间。
可用千字节	剩余的队列存储（按 KB 计）。

读取已传送和已退回邮件的速率

所有速率均显示为在进行查询的特定时间点，每小时发生某个事件的平均速率。将为三个时间间隔计算速率：过去一 (1) 分钟、过去五 (5) 分钟和过去十五 (15) 分钟内的每小时平均速率。

例如，如果邮件网关在一分钟内收到 100 个收件人，则 1 分钟时间间隔的速率为每小时 6,000 个。5 分钟间隔的速率为每小时 1,200 个，而 15 分钟的速率为每小时 400 个。计算速率以指示当一分钟时段的速率继续时，该小时的平均速率是什么。因此，每分钟 100 封邮件会产生比 15 分钟 100 封邮件更高的速率。

下表列出了在监控邮件网关时可用的速率及其说明。

Note 这是完整的列表。显示的速率因所选的显示选项或命令而异。此列表仅供参考。

Table 3: 比率

统计信息	**Description**
接收的邮件数量	每小时将邮件插入传送队列的速率。
已经接收的收件人数量	每小时插入传送队列的所有邮件的收件人数的速率。
软退回事件的数量	每小时软退回事件数量的速率。（软退回多次的邮件具有多个软退回事件。）
已经完成的收件人数量	全部硬退回的收件人数量、已传送收件人和已删除收件人的总计的速率。从传送队列中删除的任何收件人都被视为已完成。
硬退回的收件人数量	每小时内所有 DNS 硬退回、5XX 硬退回、过滤器硬退回、到期硬退回和其他硬退回的总计的速率。导致传送立即终止的将邮件传送给收件人尝试失败被视为硬退回。
传送的收件人数量	每小时成功将邮件发送给收件人的速率。

使用 CLI 监控

监控邮件状态

您可能想要监控邮件网关上邮件操作的状态。status 命令将返回监控到的有关邮件操作的信息子集。统计数据以下列两种形式中的一种返回：计数器和计量器。计数器提供系统中运行的各个事件的总数。对于每个计数器，您可以查看自计数器重置以来、自系统上次重新引导以来以及在系统的整个生命周期所发生的事件总数。计量器会显示系统资源（如内存、磁盘空间或活动连接）的当前利用率。

有关每个项目的说明，请参阅使用 CLI 进行管理和监控概述, on page 1。

Table 4: 邮件状态

统计信息	Description
状态时间	显示当前系统时间和日期。
上次重置计数器	显示上次重置计数器的时间。
系统状态	在线、离线、接收暂停或传送暂停。请注意，仅当暂停所有侦听程序时，状态才会成为“接收暂停”。当所有侦听程序的接收和传送均暂停时，状态成为“离线”。
时间最长的邮件	显示等待由系统传送的时间最长的邮件。
功能	显示通过 featurekey 命令在系统上安装的任何特殊功能。

示例

```
mail3.example.com> status

Status as of:               Thu Oct 21 14:33:27 2004 PDT
Up since:                     Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset:         Never
System status:              Online
Oldest Message:              4 weeks 46 mins 53 secs
Counters:                      Reset          Uptime         Lifetime
  Receiving
    Messages Received      62,049,822         290,920      62,049,822
    Recipients Received    62,049,823         290,920      62,049,823
  Rejection
    Rejected Recipients     3,949,663          11,921       3,949,663
    Dropped Messages       11,606,037             219      11,606,037
  Queue
    Soft Bounced Events     2,334,552          13,598       2,334,552
  Completion
    Completed Recipients   50,441,741         332,625      50,441,741
  Current IDs
    Message ID (MID)                                      99524480
    Injection Conn. ID (ICID)                             51180368
    Delivery Conn. ID (DCID)                              17550674
Gauges:                                 Current
  Connections
    Current Inbound Conn.                     0
    Current Outbound Conn.                   14
  Queue
```

```
    Active Recipients                  7,166
    Messages In Work Queue                 0
    Messages In Quarantine            16,248
    Kilobytes Used                   387,143
      Kilobytes In Quarantine        338,206
    Kilobytes Free                39,458,745
mail3.example.com>
```

监控详细的邮件状态

status detail 命令返回有关邮件操作的完整受监控信息。返回的统计数据以下列三种类别中的一种返回：计数器、速率和计量器。计数器提供系统中运行的各个事件的总数。对于每个计数器，可以查看自重置计数器以来、自上次系统重新启动以来以及在系统的整个生命周期中生成的事件总数。计量器会显示系统资源（如内存、磁盘空间或活动连接）的当前利用率。所有速率均显示为在进行查询的特定时间点，每小时发生某个事件的平均速率。将为三个时间间隔计算速率：过去一(1)分钟、过去五 (5) 分钟和过去十五 (15) 分钟内的每小时平均速率。有关每个项目的说明，请参阅使用 CLI 进行管理和监控概述, on page 1。

示例

```
mail3.example.com> status detail
Status as of:           Thu Jun 30 13:09:18 2005 PDT
Up since:                Thu Jun 23 22:21:14 2005 PDT (6d 14h 48m 4s)
Last counter reset:             Tue Jun 29 19:30:42 2004 PDT
System status:                  Online
Oldest Message:                 No Messages
Feature - IronPort Anti-Spam:  17 days
Feature - Sophos:               Dormant/Perpetual
Feature - Outbreak Filters: Dormant/Perpetual
Feature - Central Mgmt:         Dormant/Perpetual
Counters:                        Reset          Uptime        Lifetime
  Receiving
    Messages Received       2,571,967          24,760       3,113,176
    Recipients Received     2,914,875          25,450       3,468,024
    Gen. Bounce Recipients      2,165               0           7,451
  Rejection
    Rejected Recipients     1,019,453             792       1,740,603
    Dropped Messages        1,209,001              66       1,209,028
  Queue
    Soft Bounced Events        11,236               0          11,405
  Completion
    Completed Recipients    2,591,740          49,095       3,145,002
      Hard Bounced Recipients   2,469               0           7,875
        DNS Hard Bounces          199               0           3,235
        5XX Hard Bounces        2,151               0           4,520
        Expired Hard Bounces      119               0             120
        Filter Hard Bounces         0               0               0
        Other Hard Bounces          0               0               0
      Delivered Recipients  2,589,270          49,095       3,137,126
      Deleted Recipients            1               0               1
        Global Unsub. Hits          0               0               0
    DomainKeys Signed Msgs         10               9              10
  Current IDs
    Message ID (MID)                                          7615199
    Injection Conn. ID (ICID)                                 3263654
    Delivery Conn. ID (DCID)                                  1988479
Rates (Events Per Hour):      1-Minute       5-Minutes      15-Minutes
  Receiving
```

```
    Messages Received              180              300              188
    Recipients Received            180              300              188
  Queue
    Soft Bounced Events              0                0                0
  Completion
    Completed Recipients           360              600              368
      Hard Bounced Recipients        0                0                0
      Delivered Recipients         360              600              368
Gauges:                                Current
  System
    RAM Utilization                              1%
    CPU Utilization
      MGA                                        0%
      AntiSpam                                   0%
      AntiVirus                                  0%
    Disk I/O Utilization                         0%
    Resource Conservation                        0
  Connections
    Current Inbound Conn.                        0
    Current Outbound Conn.                       0
  Queue
    Active Recipients                            0
      Unattempted Recipients                     0
      Attempted Recipients                       0
    Messages In Work Queue                       0
    Messages In Quarantine                      19
    Destinations In Memory                       3
    Kilobytes Used                             473
      Kilobytes In Quarantine                  473
    Kilobytes Free                     39,845,415
```

Note 新安装的邮件网关中可能存在这样的情况：最早的邮件计数器显示邮件，但是实际上计数器中未显示任何收件人。如果远程主机正在连接且接收邮件的速度非常缓慢（即接收一封邮件需花费数分钟的时间），您可能会发现收件人接收的计数器显示“0”，但是最早的邮件计数器显示“1”。这是因为时间最长的邮件计数器会显示正在进行的邮件。如果连接最终断开，则会重置计数器。

监控邮件主机的状态

如果您怀疑特定收件人主机存在传送问题或要在虚拟网关地址上收集信息，则hoststatus 命令会显示此信息。hoststatus 命令会返回有关与特定收件人主机相关的邮件操作的监控信息。该命令要求您输入要返回的主机信息的域。此外还提供在 AsyncOS 缓存中存储的 DNS 信息以及从收件人主机返回的最后一个错误。返回的数据是从上一个 resetcounters 命令运行以来累加的。返回的统计数据以下列两种类别显示：计数器和计量器。有关每个项目的说明，请参阅使用CLI进行管理和监控概述, on page 1。

此外，还会返回特定于 hoststatus 命令的其他数据。

***Table 5: hoststatus* 命令中的其他数据**

统计信息	Description
挂起的出站连接	与目标邮件主机的挂起或“起始”连接，与开放和有效连接相对。挂起的出站连接是尚未到达协议问候阶段的连接。

统计信息	Description
时间最长的邮件	此域传送队列中时间最长的有效收件人的时限。此计数器对于确定邮件在队列中由于软退回事件和/或关闭的主机而无法传送的时间非常有用。
最后的行为	每次尝试向该主机传送邮件时，此字段便会更新。
已排序的 IP 地址	此字段包含 IP 地址的 TTL（生存时间）、根据 MX 记录的首选项以及实际地址。MX 记录会指定域的邮件服务器 IP 地址。一个域可以有多个 MX 记录。每个 MX 记录邮件服务器均分配有优先级。具有最低优先级数字的 MX 记录将成为首选项。
最后的 5XX 错误	此字段包含主机返回的最新“5XX”状态代码和说明。该项仅在存在 5XX 错误时显示。
MX 记录	MX 记录会指定域的邮件服务器 IP 地址。一个域可以有多个 MX 记录。每个 MX 记录邮件服务器均分配有优先级。具有最低优先级数字的 MX 记录将成为首选项。
此主机的 SMTP 路由	如果为此域定义了 SMTP 路由，它们将列出在此处。
最后的 TLS 错误	此字段包含有关最近传出 TLS 连接错误的说明以及邮件网关尝试建立的 TLS 连接类型。仅当出现 TLS 错误时，才会显示该信息。

虚拟网关

仅当设置了虚拟网关地址时，才会显示以下虚拟网关信息（请参阅配置网关以接收邮件）。

***Table 6: hoststatus* 命令中的其他虚拟网关数据**

统计信息	Description
主机 up/down	与同名全局 hoststatus 字段具有相同的定义 - 根据虚拟网关地址跟踪。
最后的行为	与同名全局 hoststatus 字段具有相同的定义 - 根据虚拟网关地址跟踪。
收件人	此字段还对应与全局 hoststatus 命令相同的定义。有效收件人字段 - 按虚拟网关地址跟踪。
最后的 5XX 错误	此字段包含主机返回的最新 5XX 状态代码和说明。该项仅在存在 5XX 错误时显示。

示例

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com
Host mail status for: 'aol.com'
Status as of:          Tue Mar 02 15:17:32 2010
```

```
Host up/down:         up
Counters:
  Queue
    Soft Bounced Events                         0
  Completion
    Completed Recipients                        1
      Hard Bounced Recipients                   1
        DNS Hard Bounces                        0
        5XX Hard Bounces                        1
        Filter Hard Bounces                     0
        Expired Hard Bounces                    0
        Other Hard Bounces                      0
      Delivered Recipients                      0
      Deleted Recipients                        0
Gauges:
  Queue
    Active Recipients                           0
      Unattempted Recipients                    0
      Attempted Recipients                      0
    Connections
      Current Outbound Connections              0
      Pending Outbound Connections              0
Oldest Message        No Messages
Last Activity         Tue Mar 02 15:17:32 2010
Ordered IP addresses: (expiring at Tue Mar 02 16:17:32 2010)
    Preference   IPs
    15           64.12.137.121    64.12.138.89     64.12.138.120
    15           64.12.137.89     64.12.138.152    152.163.224.122
    15           64.12.137.184    64.12.137.89     64.12.136.57
    15           64.12.138.57     64.12.136.153    205.188.156.122
    15           64.12.138.57     64.12.137.152    64.12.136.89
    15           64.12.138.89     205.188.156.154  64.12.138.152
    15           64.12.136.121    152.163.224.26   64.12.137.184
    15           64.12.138.120    64.12.137.152    64.12.137.121
MX Records:
    Preference   TTL        Hostname
    15           52m24s     mailin-01.mx.aol.com
    15           52m24s     mailin-02.mx.aol.com
    15           52m24s     mailin-03.mx.aol.com
    15           52m24s     mailin-04.mx.aol.com
    Last 5XX Error:
    ----------
    550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
 (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
    ----------
Last TLS Error:             Required - Verify
    ----------
    TLS required, STARTTLS unavailable
    (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
Virtual gateway information:
===========================================================
example.com (PublicNet_017):
    Host up/down:         up
    Last Activity         Wed June 22 13:47:02 2005
    Recipients            0
```

Note 仅在使用 altsrchost 功能时，才会显示虚拟网关地址信息。

确定邮件队列的组成

要获取有关邮件队列的即时信息并确定特定收件人主机是否存在传送问题（例如队列组成），请使用 tophosts 命令。tophosts 命令将返回队列中前 20 个收件人主机的列表。可以按不同的统计数据排列该列表，包括有效收件人、输出连接、传送的收件人、软退回事件和硬退回的收件人。有关每个项目的说明，请参阅使用 CLI 进行管理和监控概述, on page 1。

示例

```
mail3.example.com> tophosts

Sort results by:
1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Soft Bounced Events
5. Hard Bounced Recipients
[1]> 1
Status as of:         Mon Nov 18 22:22:23 2003
                    Active    Conn.   Deliv.   Soft      Hard
#  Recipient Host   Recip     Out     Recip.   Bounced   Bounced
1  aol.com          365       10      255      21         8
2  hotmail.com      290        7      198      28        13
3  yahoo.com        134        6      123      11        19
4  excite.com        98        3       84       9         4
5  msn.com           84        2       76      33        29
mail3.example.com>
```

显示实时活动

邮件网关提供实时监控功能，以便查看系统中邮件活动的进度。rate 命令会返回有关邮件操作的实时监控信息。信息按您指定的时间间隔定期更新。使用 Ctrl+C 组合键可停止 **rate** 命令。

该数据显示在下表中：

***Table 7: rate* 命令中的数据**

统计信息	**Description**
入站连接数量	入站连接的数量。
出去的TCP连接数	出站连接的数量。
已经接收的收件人数量	系统中接收的收件人总数。
完成的收件人	完成的收件人总数。
△	自上次数据更新以来，已接收收件人与已完成收件人之间的差异。
使用的队列	邮件队列的大小（以 KB 计）。

示例

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1
Hit Ctrl-C to return to the main prompt.
Time     Connections Recipients          Recipients              Queue
             In    Out   Received    Delta  Completed    Delta     K-Used
23:37:13    10     2   41708833        0   40842686        0         64
23:37:14     8     2   41708841        8   40842692        6        105
23:37:15     9     2   41708848        7   40842700        8         76
23:37:16     7     3   41708852        4   40842705        5         64
23:37:17     5     3   41708858        6   40842711        6         64
23:37:18     9     3   41708871       13   40842722       11         67
23:37:19     7     3   41708881       10   40842734       12         64
23:37:21    11     3   41708893       12   40842744       10         79
^C
```

hostrate 命令会返回有关特定邮件主机的实时监控信息。此信息是 status detail 命令的子集。（请参阅监控详细的邮件状态, on page 8。）

***Table 8: hostrate* 命令中的数据**

统计信息	Description
主机状态	特定主机的当前状态：运行、关闭或未知。
当前出站连接数	当前与主机的出站连接数量。
队列中正在处理的收件人	队列中发送到特定主机的有效收件人总数。
队列中正在处理的收件人增量	自上次已知主机状态以来，队列中发送到特定主机的有效收件人总数的差异。
传送的收件人增量	自上次已知主机状态以来，队列中发送到特定主机的已传送收件人总数的差异。
硬退回收件人增量	自上次已知主机状态以来，队列中发送到特定主机的硬退回收件人总数的差异。
软退回事件增量	自上次已知主机状态以来，队列中发送到特定主机的软退回收件人总数的差异。

使用 Ctrl+C 组合键可停止 hostrate 命令。

示例

```
mail3.example.com> hostrate
Recipient host:
[]> aol.com
Enter the number of seconds between displays.
[10]> 1
    Time    Host  CrtCncOut  ActvRcp ActvRcp  DlvRcp HrdBncRcp SftBncEvt
```

```
           Status                       Delta   Delta      Delta      Delta
23:38:23        up          1          0       0        4          0          0
23:38:24        up          1          0       0        4          0          0
23:38:25        up          1          0       0       12          0          0
^C
```

监控入站邮件连接

您可能希望监控连接到邮件网关的主机，以识别大量发件人或对系统的入站连接进行故障排除。topin 命令提供连接到系统的远程主机的快照。它会显示一个表，其中每个行对应连接到特定侦听程序的每个远程 IP 地址。从同一 IP 地址到不同侦听程序的两个连接会在下表中产生 2 个行，该表描述了使用 topin 命令时显示的字段。

***Table 9: topin* 命令中的数据**

统计信息	**Description**
远程主机名	远程主机的主机名，衍生自反向 DNS 查找。
远程 IP 地址	远程主机的 IP 地址。
监听程序	接收连接的邮件网关上侦听程序的昵称。
入站连接数量	在命令运行时打开的来自具有指定 IP 地址的远程主机的并发连接数。

系统会执行反向 DNS 查找来查找远程主机名，然后执行正向 DNS 查找来验证该名称。如果正向查找不会产生原始 IP 地址，或者如果反向 DNS 查询失败，则该表会在主机名列中显示 IP 地址。有关发件人验证过程的详细信息，请参阅验证发件人。

示例

```
mail3.example.com> topin

Status as of:                  Sat Aug 23 21:50:54 2003
#  Remote hostname            Remote IP addr.   listener        Conn. In
1  mail.remotedomain01.com    172.16.0.2        Incoming01            10
2  mail.remotedomain01.com    172.16.0.2        Incoming02            10
3  mail.remotedomain03.com    172.16.0.4        Incoming01             5
4  mail.remotedomain04.com    172.16.0.5        Incoming02             4
5  mail.remotedomain05.com    172.16.0.6        Incoming01             3
6  mail.remotedomain06.com    172.16.0.7        Incoming02             3
7  mail.remotedomain07.com    172.16.0.8        Incoming01             3
8  mail.remotedomain08.com    172.16.0.9        Incoming01             3
9  mail.remotedomain09.com    172.16.0.10       Incoming01             3
10 mail.remotedomain10.com    172.16.0.11       Incoming01             2
11 mail.remotedomain11.com    172.16.0.12       Incoming01             2
12 mail.remotedomain12.com    172.16.0.13       Incoming02             2
13 mail.remotedomain13.com    172.16.0.14       Incoming01             2
14 mail.remotedomain14.com    172.16.0.15       Incoming01             2
15 mail.remotedomain15.com    172.16.0.16       Incoming01             2
16 mail.remotedomain16.com    172.16.0.17       Incoming01             2
17 mail.remotedomain17.com    172.16.0.18       Incoming01             1
18 mail.remotedomain18.com    172.16.0.19       Incoming02             1
19 mail.remotedomain19.com    172.16.0.20       Incoming01             1
20 mail.remotedomain20.com    172.16.0.21       Incoming01             1
```

检查 DNS 状态

dnsstatus 命令会返回一个计数器，以显示 DNS 查找统计数据和缓存信息。对于每个计数器，可以查看自上次重置计数器以来、自上次系统重新启动以来以及在系统生命周期中的事件总数。

下表列出了可用的计数器。

***Table 10: dnsstatus* 命令中的数据**

统计信息	**Description**
DNS 请求	发送到用于解析域名的系统 DNS 缓存的顶级非递归请求。
网络请求数	发送到用于检索 DNS 信息的网络（非本地）的请求。
缓存命中数	发送到在其中找到并返回记录的 DNS 缓存的请求。
缓存丢失数	发送到在其中未找到记录的 DNS 缓存的请求。
缓存排斥数	发送到在其中找到记录但域未知的 DNS 缓存的请求。
缓存过期	发送到在其中找到记录的 DNS 缓存的请求。 在缓存中，考虑使用，并且由于过于陈旧而放弃。 许多条目可存在于缓存中，即使它们的生存时间 (TTL) 已过也是如此。只要这些条目未使用，它们就不会包含在到期计数器中。当清理缓存时，有效和无效（过旧）条目都会被删除。刷新操作不会更改到期计数器。

示例

```
mail3.example.com> dnsstatus
Status as of: Sat Aug 23 21:57:28 2003
Counters:                    Reset          Uptime        Lifetime
  DNS Requests         211,735,710       8,269,306     252,177,342
  Network Requests     182,026,818       6,858,332     206,963,542
  Cache Hits           474,675,247      17,934,227     541,605,545
  Cache Misses         624,023,089      24,072,819     704,767,877
  Cache Exceptions      35,246,211       1,568,005      51,445,744
  Cache Expired            418,369           7,800         429,015
mail3.example.com>
```

重置邮件监控计数器

Caution 建议避免在云邮件安全设备上重置邮件监控计数器。

resetcounters 命令会重置累加的邮件监控计数器。重置会影响全局计数器以及每个主机计数器。重置不会影响与重试计划相关的传送队列中的邮件计数器。

Note 还可以在 GUI 中重置计数器。请参阅“系统状态”(System Status) 页面。

示例

```
mail3.example.com> resetcounters
Counters reset: Mon Jan 01 12:00:01 2003
```

识别有效的 TCP/IP 服务

要识别邮件网关使用的有效 TCP/IP 服务，请在命令行界面使用 tcpservices 命令。

管理邮件队列

通过思科 AsyncOS，可以对邮件队列中的邮件执行操作。可以删除、退回、暂停或重定向邮件队列中的邮件。还可以找到、删除和存档队列中的旧邮件。

删除队列中的收件人

如果不希望传送给特定收件人或要清除邮件队列，请使用 deleterecipients 命令。deleterecipients 命令支持通过删除等待传送的特定收件人来管理邮件传送队列。要删除的收件人将通过作为收件人目标的收件人主机或邮件发件人（由邮件信封的“信封发件人”(Envelope From) 行中指定的特定地址确定）来识别。此外，可以同时删除传送队列中的所有邮件。

Note 要执行 deleterecipients 功能，建议将邮件网关置于离线状态或暂停传送（请参阅暂停邮件接收和传送）。

Note 尽管该功能在所有状态下均受支持，但是在执行该功能期间可能会传送一些邮件。

收件人主机和发件人的匹配必须是完全相同的字符串匹配。不接受通配符。deleterecipients 命令会返回已删除邮件的总数。此外，如果配置了邮件日志订用（仅限 IronPort 文本格式），则邮件删除事件会记录为单独的行。

示例

```
mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
```

```
3. All.
[1]>
```

邮件网关提供了各种选项来根据需要删除收件人。以下示例显示按收件人主机删除收件人、按信封发件人地址删除收件人以及删除队列中的所有收件人。

按收件人域删除

```
Please enter the hostname for the messages you wish to delete.
[]> example.com
Are you sure you want to delete all messages being delivered to "example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

按 Envelope From 地址删除

```
Please enter the Envelope From address for the messages you wish to delete.
[]> mailadmin@example.com
Are you sure you want to delete all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

全部删除

```
Are you sure you want to delete all messages in the delivery queue (all active recipients)?
 [N]> Y
Deleting messages, please wait.
1000 messages deleted.
```

退回队列中的收件人

与 deleterecipients 命令一样，bouncerecipients 命令允许通过硬退回等待传送的特定收件人来管理邮件传送队列。邮件退回遵循在 bounceconfig 命令中指定的常规退回邮件配置。

Note 要执行 bouncerecipients 功能，建议将邮件网关置于离线状态或暂停传送（请参阅暂停邮件接收和传送）。

Note 尽管该功能在所有状态下均受支持，但是在执行该功能期间可能会传送一些邮件。

收件人主机和发件人的匹配必须是完全相同的字符串匹配。不接受通配符。bouncerecipients 命令会返回退回邮件的总数。

Note bouncerecipients 功能是资源密集型，可能需要几分钟才能完成。如果处于离线或暂停传送状态，则仅在通过 resume 命令将思科 AsyncOS 恢复为在线状态之后，才会开始退回邮件的实际发送（如果开启硬退回生成）。

示例

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
```

目标收件人主机或邮件信封的信封发件人行所示的特定地址识别的邮件发件人可对要退回的收件人进行识别。另外，可以一次性退回传送队列中的所有邮件。

按收件人主机退回

```
Please enter the hostname for the messages you wish to bounce.
[]> example.com
Are you sure you want to bounce all messages being delivered to "example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

按 Envelope From 地址退回

```
Please enter the Envelope From address for the messages you wish to bounce.
[]> mailadmin@example.com
Are you sure you want to bounce all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

全部退回

```
Are you sure you want to bounce all messages in the queue? [N]> Y
Bouncing messages, please wait.
1000 messages bounced.
```

重定向队列中的邮件

redirectrecipients 命令允许邮件传送队列中的所有邮件重定向至另一个中继主机。请注意，将收件人重定向至未准备好从此主机接受大量 SMTP 邮件的主机或 IP 地址会导致退回邮件，并且可能导致邮件丢失。

Caution 将邮件重定向至目标为 /dev/null 的接收域会导致邮件丢失。如果您将邮件重定向至这种域，那么 CLI 就不会显示警告。在重定向邮件之前，请检查接收域的 SMTP 路由。

示例

以下示例将所有邮件重定向至 example2.com 主机。

```
mail3.example.com> redirectrecipients
Please enter the hostname or IP address of the machine you want to send all mail to.
[]> example2.com
WARNING: redirecting recipients to a host or IP address that is not prepared to accept large
 volumes of SMTP mail from this host will cause messages to bounce and possibly result in
the loss of mail.
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
Redirecting messages, please wait.
246 recipients redirected.
```

根据队列中的收件人显示邮件

使用 showrecipients 命令按收件人主机或信封发件人地址显示邮件传送队列中的邮件。还可以显示队列中的所有邮件。

示例

```
mail3.example.com> showrecipients
Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 3
Showing messages, please wait.
MID/     Bytes/    Sender/                 Subject
[RID]    [Atmps]   Recipient
1527     1230      user123456@ironport.com Testing
[0]      [0]       9554@example.com
1522     1230      user123456@ironport.com Testing
[0]      [0]       3059@example.com
1529     1230      user123456@ironport.com Testing
[0]      [0]       7284@example.com
1530     1230      user123456@ironport.com Testing
[0]      [0]       8243@example.com
1532     1230      user123456@ironport.com Testing
[0]      [0]       1820@example.com
1531     1230      user123456@ironport.com Testing
[0]      [0]       9595@example.com
1518     1230      user123456@ironport.com Testing
[0]      [0]       8778@example.com
1535     1230      user123456@ironport.com Testing
[0]      [0]       1703@example.com
1533     1230      user123456@ironport.com Testing
[0]      [0]       3052@example.com
1536     1230      user123456@ironport.com Testing
[0]      [0]       511@example.com
```

以下示例显示所有收件人主机队列中的邮件。

暂停邮件传送

Caution 建议避免在设备上暂停和恢复邮件传送。

要临时暂停邮件传送以进行维护或故障排除，请使用 suspenddel 命令。suspenddel 命令将思科 AsyncOS 置为暂停传送状态。此状态具有以下特征：

- 停止出站邮件传送。
- 接受入站邮件连接。
- 继续日志传输。
- CLI 保持可访问。

suspenddel 命令可使打开的出站连接关闭，并阻止打开任何新的连接。suspenddel 命令会立即开始，并允许成功关闭任何已建立的连接。使用 resumedel 命令从暂停传送状态恢复为正常操作。

Note 在系统重新启动过程中会保留“传送暂停”状态。如果使用 suspenddel 命令，然后重新启动邮件网关，则必须在重新启动后使用 resumedel 命令恢复传送。

示例

```
mail3.example.com> suspenddel
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

恢复邮件传送

Caution 建议避免在云邮件安全设备上暂停和恢复邮件传送。

resumedel 命令会在使用 suspenddel 命令后将思科 AsyncOS 恢复为正常操作状态。

语法

resumedel

```
mail3.example.com> resumedel
Mail delivery resumed.
```

暂停接收邮件

Caution 建议避免在云邮件安全设备上暂停和恢复侦听程序。

要临时暂停所有侦听程序接收邮件，请使用 suspendlistener 命令。当暂停接收时，系统不会接受与侦听程序特定端口的连接。

此行为在此 AsyncOS 版本中已更改。在以前的版本中，系统会接受连接，做出以下响应并断开连接：

- SMTP: 421 *hostname* Service not available, closing transaction channel
- QMQP: ZService not available

Note 在系统重新启动过程中会保留“接收暂停”状态。如果使用 suspendlistener 命令，然后重新启动邮件网关，则必须使用 resumelistener 命令，然后才使侦听程序恢复接收邮件。

语法

```
suspendlistener mail3.example.com> suspendlistener
Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>
```

恢复接收邮件

Caution 建议避免在云邮件安全设备上暂停和恢复侦听程序。

resumelistener 命令会在使用 suspendlistener 命令后将思科 AsyncOS 恢复为正常操作状态。

语法

```
resumelistener
```

```
mail3.example.com> resumelistener
Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
```

```
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Receiving resumed.
mail3.example.com>
```

恢复邮件的传送和接收

恢复命令将恢复传送和接收。

语法

```
resume
```

```
mail3.example.com> resume
Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

安排邮件立即传送

对于安排延迟交付的收件人和主机，可以使用 delivernow 命令立即重试。delivernow 命令允许重新安排立即传送队列中的邮件。记下的所有域和任何已安排或软退回的邮件都会排队以进行立即传送。

可以调用 delivernow 命令用于队列（已安排和活动）中的所有收件人或特定收件人。当选择特定收件人时，必须输入安排立即传送的收件人的域名。系统会匹配整个字符串的字符和长度。

语法

```
delivernow
```

```
mail3.example.com> delivernow
Please choose an option for scheduling immediate delivery.
1. By recipient host
2. All messages
[1]> 1
Please enter the domain to schedule for immediate delivery.
[]> recipient.example.com
Rescheduling all messages to recipient.example.com for immediate delivery.
mail3.example.com>
```

暂停工作队列

Caution 建议避免在云邮件安全设备上暂停工作队列。

LDAP 收件人访问处理、伪装、LDAP 重新路由、邮件过滤器、反垃圾邮件和防病毒扫描引擎都在“工作队列”中执行。有关处理流程，请参阅配置路由和传送功能，有关“工作队列中的邮

件”(Messages in Work Queue) 计量器的说明，请参阅读取系统计量器, on page 4。可以使用 workqueue 命令手动暂停邮件处理的工作队列部分。

例如，假设要更改 LDAP 服务器配置的配置，而许多邮件都在工作队列中。或许您要从退回转换到根据 LDAP 收件人访问查询来删除邮件。又或许您要暂停队列，同时手动检查最新的防病毒扫描引擎定义文件（通过 antivirusupdate 命令）。通过 workqueue 命令可以暂停和恢复工作队列，以在执行其他配置更改时停止处理。

当暂停和恢复工作队列时，系统会记录事件。例如，

```
Sun Aug 17 20:01:36 2003 Info: work queue paused, 1900 msgs S
Sun Aug 17 20:01:39 2003 Info: work queue resumed, 1900 msgs
```

在以下示例中，工作队列将暂停：

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:02:30 2003 GMT
Status:   Operational
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
- PAUSE - Pause the work queue
- RATE - Display work queue statistics over time
[]> pause
Manually pause work queue?  This will only affect unprocessed messages.  [N]> y
Reason for pausing work queue:
[]> checking LDAP server
Status as of:  Sun Aug 17 20:04:21 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
```

Note 输入原因是可选操作。如果不输入原因，系统会将原因记录为“由用户手动暂停”。

在以下示例中，工作队列将恢复：

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:42:10 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
- RESUME - Resume the work queue
- RATE - Display work queue statistics over time
[]> resume
Status:   Operational
Messages: 1243
```

查找并存档较早的邮件

有时，由于无法传送，旧邮件会保留在队列中。您可能希望删除和存档这些邮件。为此，请使用 showmessage CLI 命令显示给定邮件 ID 的邮件。使用 oldmessage CLI 命令显示系统中最早的非隔离邮件。然后，您可以选择性使用 removemessage 安全删除给定邮件 ID 的邮件。此命令仅可删除工作队列、重试队列或目标队列中的邮件。如果邮件不在任何这些队列中，则其无法删除。

您还可以使用 archivemessage[mid] CLI 命令将给定邮件 ID 的邮件存档到配置目录中的 mbox 文件内。

您无法使用 oldmessage 命令获取隔离区中某个邮件的邮件 ID。但是，如果知道邮件 ID，则可以显示或存档指定的邮件。由于邮件不在工作队列、重试队列或目标队列中，因此无法通过removemessage命令删除该邮件。

Note 您无法在思科垃圾邮件隔离区中对邮件执行其中任何队列管理命令。

语法

```
archivemessage
```

```
example.com> archivemessage
Enter the MID to archive and remove.
[0]> 47
 MID 47 has been saved in file oldmessage_47.mbox in the configuration directory
example.com>
```

语法

```
oldmessage
```

```
example.com> oldmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from example.com ([172.16.0.102])
  by example.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@example.com
To: 4031@test.example2.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@example.com>
```

跟踪系统中的邮件

findevent CLI 命令可简化使用 onbox 邮件日志文件跟踪系统中的邮件的过程。findevent CLI 命令允许通过搜索邮件ID或根据主题信头、信封发件人或信封收件人匹配的正则表达式来搜索整个邮件日志中的特定邮件。可以显示当前日志文件或所有日志文件的结果，也可以按日期显示日志文件。按日期查看日志文件时，可以指定某个日期或日期范围。

确定要查看其日志的邮件后，findevent命令会显示该邮件ID的日志信息，包括拆分信息（拆分日志邮件、退回和系统生成的邮件）。以下示例显示了 findevent CLI 命令如何跟踪主题信头中包含“Confidential”的邮件的接收和传送情况：

```
example.com>
findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
```

```
4. Search by envelope TO
[1]> 3
Enter the regular expression to search for.
[]> confidential
Currently configured logs:
1. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to use for message tracking.
[]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 3
The following matching message IDs were found. Please choose one to
show additional log information:
1. MID 4 (Tue Jul 31 17:37:35 2007) sales: confidential
[1]> 1
Tue Jul 31 17:37:32 2007 Info: New SMTP ICID 2 interface Data 1 (172.19.1.86) address
10.251.20.180 reverse dns host unknown verified no
Tue Jul 31 17:37:32 2007 Info: ICID 2 ACCEPT SG None match ALL SBRS None
Tue Jul 31 17:37:35 2007 Info: Start MID 4 ICID 2
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 From: <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 RID 0 To: <ljohnson@example02.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 Subject 'sales: confidential'
Tue Jul 31 17:37:35 2007 Info: MID 4 ready 4086 bytes from <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 matched all recipients for per-recipient policy DEFAULT
 in the inbound table
Tue Jul 31 17:37:35 2007 Info: ICID 2 close
Tue Jul 31 17:37:37 2007 Info: MID 4 interim verdict using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 interim AV verdict using Sophos CLEAN
Tue Jul 31 17:37:37 2007 Info: MID 4 antivirus negative
Tue Jul 31 17:37:37 2007 Info: MID 4 queued for delivery
Tue Jul 31 17:37:37 2007 Info: Delivery start DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: Message done DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: MID 4 RID [0] Response '/null'
Tue Jul 31 17:37:37 2007 Info: Message finished MID 4 done
```

使用 SNMP 监控系统运行状况和状态

⚠

Caution 建议避免在云邮件安全设备上配置 SNMP。

AsyncOS 操作系统通过 SNMP（简单网络管理协议）支持系统状态监控。此版本可实现 RFC 1213 和 1907 中定义的 MIB-II 只读子网。（有关 SNMP 的详细信息，请参阅 RFC 1065、1066 和 1067。）请注意：

- 默认情况下，SNMP 已**关闭**。
- 在启用 SNMP 时，使用的默认版本为 SNMPv3。
- 不执行 SNMP 设置操作（配置）。
- AsyncOS 支持 SNMPv1、v2 和 v3。
- 用于身份验证和加密的密码应不同。加密算法必须仅为 AES。身份验证算法必须仅为 SHA-1。在您下次运行 snmpconfig 命令时，该命令会“记住”您的密码。
- SNMPv3 用户名为：v3get

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a SHA -A ironport mail.example.com
```

- 如果仅使用 SNMPv1 或 SNMPv2，则必须设置社区字符串。社区字符串的默认值不是 public。
- 对于 SNMPv1 和 SNMPv2，必须指定在其中接受 SNMP GET 请求的网络。
- 如果使用 SNMPv3，则必须选择下表中显示的任一受支持安全级别：

安全等级	身份验证	隐私
noAuthNoPriv	支持 身份验证使用 SNMPv3 用户名完成。	不支持
authNoPriv	支持 身份验证使用 SNMPv3 身份验证口令完成。	不支持
authPriv	支持 身份验证使用 SNMPv3 身份验证口令完成。	支持 使用 SNMPv3 隐私密码激活隐私。

- 如果同时启用 SNMPv2 和 SNMPv3，则必须为陷阱选择所需的版本。
- 要使用陷阱，必须运行 SNMP 管理器（AsyncOS 中未包括）并输入其 IP 地址作为陷阱目标。（可以使用主机名，但是如果这样，陷阱仅在 DNS 正常运行时才有效。）

使用 snmpconfig 命令以启用并配置邮件网关 SNMP 监控。选择并配置接口的值以后，邮件网关会响应 SNMPv3 GET 请求。这些第 3 版请求必须包含匹配密码。默认情况下，拒绝版本 1 和版本 2 请求。如果已启用，则版本 1 和版本 2 请求必须具有匹配的社区字符串。

MIB 文件

以下邮件网关的 MIB 文件可在 http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html 找到。使用最新可用的 MIB 文件。

- ASYNCOS-MAIL-MIB.txt - 邮件网关的 Enterprise MIB 的 SNMPv2 兼容说明。
- AsyncOS-SMI.txt (IRONPORT-SMI.txt) - 一种“管理信息结构”(SMI) 文件，用于定义思科内容安全产品中 ASYNCOS-MAIL-MIB 的角色。

硬件对象

符合智能平台管理接口规格 (IPMI) 的硬件传感器会报告温度、风扇速度以及电源状态等信息。

在问题变得严重之前，轮询硬件状态并识别可能的硬件故障是明智之举。距离临界值 10% 以内的温度可能会产生令人担心的问题。

有关邮件网关电源数量和工作温度范围等信息，请参阅对应您的设备型号的指南。有关硬件指南的位置，请参阅文档。

硬件陷阱

状态改变时，发送状态更改陷阱。每隔 5 秒发送一次风扇故障和高温陷阱。其他陷阱是故障条件警报陷阱 - 当状态更改（从正常变为故障）时，就会发送一次。

例如，在 C170 邮件网关上，如果达到以下阈值，会发送陷阱：

Table 11: C170 **邮件网关上的硬件陷阱：温度和硬件条件**

型号	高温 (CPU)	高温（环境）	高温（背板）	高温（侧板）	风扇故障	电源	RAID	链接
C170	90C	47C	不适用	不适用	0 RPM	状态更改	状态更改	状态更改

要查看您邮件网关上的可用陷阱和阈值，请从命令行接口运行 snmpconfig 命令。

请注意，故障条件警报陷阱表示单个组件的严重故障，但是可能不会导致整个系统故障。例如，邮件网关上多个风扇或电源中的单个风扇或电源发生故障，而邮件网关仍会继续运行。

相关主题

- 示例：snmpconfig 命令 , on page 27

SNMP 陷阱

当满足一个或多个条件时，SNMP 能够发送陷阱或通知来告知管理应用（通常是 SNMP 管理控制台）。陷阱是网络数据包，其中包含与发送陷阱的系统的组件相关的数据。满足 SNMP 代理（在这种情况下，为邮件网关）上的条件后，则会生成陷阱。在满足条件后，SNMP 代理就会形成 SNMP 数据包并将其发送到运行 SNMP 管理控制台软件的主机。

要启用并配置 SNMP 陷阱，可使用 snmpconfig 命令。

要指定多个陷阱目标：提示陷阱目标时，最多可以输入 10 个逗号分隔的 IP 地址。

示例：snmpconfig 命令

在以下示例中，snmpconfig 命令用于 C690 硬件邮件网关以在 161 端口上的“PublicNet”接口上启用 SNMP。对 GET 请求输入版本 1 和 2 的社区字符串 public。

```
mail1.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> setup

Do you want to enable SNMP? [Y]>
SNMP default version is V3
```

```
Choose an IP interface for SNMP requests.
1. Management (10.10.4.5/27: mail1.example.com) [1]>

Which port shall the SNMP daemon listen on?
[161]>

Select SNMPv3 security level:
1. noAuthNoPriv - Authentication is done using the SNMPv3 username, and no privacy is
activated.
2. authNoPriv - Authentication is done using the SNMPv3 authentication passphrase, and no
privacy is activated.
3. authPriv - Authentication is done using the SNMPv3 authentication passphrase, and privacy
 is activated using the SNMPv3 privacy passphrase.
[3]>

Select SNMPv3 authentication type:
1. SHA
[1]>

Select SNMPv3 privacy protocol:
1. AES
[1]>

Enter the SNMPv3 authentication passphrase.
[]>

The SNMPv3 passphrase must be at least 8 characters.

Enter the SNMPv3 authentication passphrase.
[]>

Enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Enter the SNMPv3 privacy passphrase again to confirm.
[]>
Warning: The same authentication and privacy passwords reduce the security of the system.

Do you want to set other passwords? [Y]> n

Service SNMP V1/V2c requests? [N]> Y

Enter the SNMP V1/V2c community string.
[ironport]>

Shall SNMP V2c requests be serviced from IPv4 addresses? [Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate multiple networks
 with commas.
[127.0.0.1/32]>

Select the version for SNMP traps:
1. 2c
2. 3
[2]>

Enter the Trap target as a host name, IP address or list of IP addresses separated by commas
 (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 10.10.0.28

Enterprise Trap Status
```

```
1. CPUUtilizationExceeded Disabled
2. FIPSModeDisableFailure Enabled
3. FIPSModeEnableFailure Enabled
4. FailoverHealthy Enabled
5. FailoverUnhealthy Enabled
6. connectivityFailure Disabled
7. keyExpiration Enabled
8. linkUpDown Enabled
9. memoryUtilizationExceeded Disabled
10. resourceConservationMode Enabled
11. updateFailure Enabled

Do you want to change any of these settings? [N]>

Enter the System Location string.
[Unknown: Not Yet Configured]>

Enter the System Contact string.
[snmp@localhost]>

Current SNMP settings:
Listening on interface "Management" 10.10.4.5/27 port 161.
SNMP v3: Enabled.
Security level: authPriv
Authentication Protocol: SHA
Encryption Protocol: AES
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32,fe::1/64.
SNMP v1/v2 Community String: ironport
Trap version: V3
Trap target: 10.10.0.28
Location: Unknown: Not Yet Configured
System Contact: snmp@localhost

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
mail1.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。