测试和故障排除

本章包含以下部分：

使用测试邮件调试邮件流：追踪

您可以使用**系统管理 (System Administration) > 跟踪 (Trace)** 页面（与 CLI 中的 trace 命令等效）通过模拟发送测试邮件来利用系统调试邮件流。“跟踪”页面（和 **trace** CLI 命令）会模拟一封邮件被侦听程序接受，并会打印一份已被系统当前配置（包括未被确认的更改）“触发”或受其影响的功能摘要。测试消息实际上并未发送。“跟踪”页面（以及 **trace** CLI 命令）是一种强大的故障排除和调试工具，尤其是在结合邮件网关的许多高级功能的情况下，其功能会更强大。

Note 追踪不适用于测试文件信誉扫描。

“跟踪”页面（和 **trace** CLI 命令）会提示您提供下表所列的输入参数。

Table 1:“跟踪”页面的输入

值	说明	示例
源 IP 地址	输入远程客户端的 IP 地址，以模拟远程域的源。该地址可以是互联网协议版本 4 (IPv4) 或版本 6 (IPv6) 地址。 说明：trace 命令会提示用户输入 IP 地址和完全限定域名。它不会尝试根据该 IP 地址反查其是否与完全限定域名匹配。trace 命令不允许完全限定域名字段为空，因此不可能在 DNS 反向匹配不正确的情况下进行测试。	**203.45.98.109** **2001:0db8:85a3::8a2e:0370:7334**
源IP 的完全限定域名	输入完全限定远程域名以进行模拟。如果完全限定域名字段为空，则会对源 IP 地址执行反向 DNS 查找。	**smtp.example.com**
用于跟踪行为的监听程序	从系统内配置的监听程序列表中选择，作为模拟发送测试消息的目标。	**InboundMail**
网络所有者组织 ID	输入 网络所有者的唯一标识号，或让系统查找与源 IP 地址相关联的网络所有者 ID。如果用户通过 GUI 将网络所有者添加到发件人组，就能够查看此信息。	**34**
IP 信誉得分	输入要为被欺骗的域提供的 IP 信誉得分，或者允许系统查找与源 IP 地址关联的 IP 信誉得分。这有助于使用 IP 信誉得分对策略进行测试。请注意，手动输入的 IP 信誉得分不会传递至情景自适应扫描引擎(CASE)。有关详细信息，请参阅编辑侦听程序的 IP 信誉过滤得分阈值。	**-7.5**
信封发件人	输入测试消息的信封发件人。	**admin@example.net**
信封收件人	输入测试消息的收件人列表。使用逗号分隔多个条目。	**joe** **frank@example.com**
邮件正文	输入测试邮件的邮件正文，包括标题。在输入邮件正文时，请在分隔行末尾输入句号。请注意，“标题”也是邮件正文的一部分（由空行隔开），如果遗漏标题或格式输入不当，则可能导致无法达到预期的跟踪结果。	**To: 1@example.com** 发件人：ralph 主题：测试 **this is a test message** **.**

输入值后，请点击**开始跟踪 (Start Trace)**。将显示系统上配置的、对消息有影响的所有功能汇总。

用户可以从本地文件系统上传邮件内容。（在 CLI 中，用户可使用已上载至 **/configuration** 目录下的邮件正文进行测试。有关放置文件以导入邮件网关的详细信息，请参阅FTP、SSH 和 SCP 访问。）

汇总显示后，系统会提示用户查看结果消息并重新运行测试消息。如果输入另一封测试邮件，则“跟踪”页面和 trace 命令使用上表中您输入的任何先前值。

Note 按次序执行下表中所列的使用trace命令测试的配置项。这对了解功能配置之间的互相影响有很大帮助。例如，通过域映射功能转换的收件人地址在由RAT评估时会影响该地址。根据别名表对受RAT影响的收件人求值时，又会对该地址产生影响，等等。

Table 2: 执行跟踪时查看输出

trace 命令部分	**输出**
主机访问表 (HAT) 及邮件流策略处理	对用户指定的监听程序的主机访问表设置进行处理。系统报告HAT中与用户输入的远程IP地址及远程域名匹配的条目。用户可以查看默认邮件流策略和发件人组，以及与给定条目一致的内容。 如果邮件网关配置为拒绝连接（通过 REJECT 或 TCPREFUSE 访问规则），则 trace 命令会在处理过程中退出。 有关更多设置HAT参数的信息，请参阅了解预定义发件人组和邮件流策略。
信封发件人地址处理 这些部分汇总了邮件网关配置对用户提供的信封发件人的影响。（即邮件网关配置如何解释MAIL FROM 命令。）**trace** 命令会在此部分之前打印“**正在处理 MAIL FROM:** ”。	
默认域	如果用户指定某监听程序更改其接收消息的默认发件人域，则对信封发件人所作的任何更改都会显示在此部分中。 有关详细信息，请参阅配置网关以接收邮件。
伪装	如果用户指定要转换某消息的信封发件人，则所作更改会在此处注明。用户使用 **listenerconfig -> edit -> masquerade -> config subcommands** 子命令，在专用侦听程序上对信封发件人启用伪装。 有关详细信息，请参阅配置路由和传送功能。
信封收件人处理 这些部分汇总了邮件网关配置对用户提供的信封收件人的影响。（即，邮件网关的配置会如何解释RCPT TO 命令。）trace 命令会在此部分之前打印“正在处理收件人列表：”。	

trace 命令部分	输出
默认域	如果用户指定某监听程序更改其接收消息的默认发件人域，则对信封收件人所作的任何更改都会显示在此部分中。 有关详细信息，请参阅配置网关以接收邮件。
域映射转换	域映射功能可将收件人地址转换为其他地址。如果用户指定了任何域映射更改，并且用户指定的收件人地址在更改范围内，则此部分中会显示出转换过程。 有关详细信息，请参阅配置路由和传送功能。
收件人访问表 (RAT)	除策略及参数外，此部分还会显示出与 RAT 内的条目匹配的每个信封收件人。（例如，指定某收件人忽略监听程序 RAT 中的限制。） 有关指定您接受的收件人的详细信息，请参阅配置网关以接收邮件。
别名表	此部分会显示出与邮件网关上配置的别名表内条目匹配的每个信封收件人（以及随后向一个或多个收件人地址的转换）。 有关详细信息，请参阅配置路由和传送功能。
入队前邮件操作 这些部分汇总了邮件网关在收到邮件正文后、将邮件列入工作队列之前，对每个邮件的影响。该处理工作在将最终的 **250 ok** 命令返回到远程 MTA 之前进行。 **trace** 命令在此部分之前列显“邮件正在处理：”。	
虚拟网关	**altsrchost** 命令基于信封发件人的完整地址、域/域名或 IP 地址的匹配，向指定接口分配消息。如果信封发件人与 **altsrchost** 命令中的条目相匹配，则该信息会显示在此部分中。 请注意，此时分配的虚拟网关地址可能会由以下消息过滤器的处理所覆盖。 有关详细信息，请参阅配置路由和传送功能。
退回配置文件	退回配置文件在处理过程中的三个不同时间使用。这是第一次出现。如果处理过程中要为监听程序分配退回配置文件，则会在此时分配。该信息会显示在此部分中。 有关详细信息，请参阅配置路由和传送功能。
工作队列操作 系统会对工作队列中的邮件执行以下一组功能。这组操作发生在客户端接收消息后、将消息列入目标队列等待发送之前。“工作队列中的邮件”由 status 和 status detail 命令进行报告。	

trace 命令部分	输出
伪装	如果用户指定要隐藏消息的收件人、发件人以及抄送标题（通过从监听程序输入的静态表或通过 LDAP 队列），则所作更改会在此处注明。用户使用 **listenerconfig -> edit -> masquerade -> config** 子命令，在专用侦听程序上对邮件信头启用伪装。 有关详细信息，请参阅配置路由和传送功能。
LDAP 路由	如果监听程序上启用了 LDAP 队列，则此部分会显示 LDAP 的接收结果、重编路由、伪装以及组队列。 有关详细信息，请参阅 LDAP 查询。
邮件过滤器处理	此时，通过测试消息对系统内启用的所有消息过滤器进行求值。对每个过滤器的规则求值，如果最终结果为“true”，则按顺序执行该过滤器内的每步操作。过滤器可能会包含其他过滤器，将其作为一种操作，且过滤器的嵌套是不受限的。如果规则评估为“false”，并且操作列表与 else 子句关联，则改为评估这些操作。此部分将会显示按顺序处理的消息过滤器的结果。 请参阅使用邮件过滤器实施邮件策略。
邮件策略处理 “邮件策略处理”(mail policy processing) 部分显示了反垃圾邮件、防病毒、病毒爆发过滤器功能以及您提供的所有收件人的声明时间戳。如果多个收件人与邮件安全管理器中的多条策略相匹配，则将为每条匹配的策略重复显示以下部分。字符串：“Message Going to”将定义收件人以及匹配的策略。	
反垃圾邮件	本部分显示未标记接受反垃圾邮件扫描处理的消息。如果要在消息送达监听程序之前，对消息进行反垃圾邮件扫描处理，则会在处理消息后显示返回的裁决。如果邮件网关配置为根据判定退回或丢弃邮件，则会列显该信息，并且 **trace** 命令处理将停止。 说明：如果反垃圾邮件扫描在系统内不可用，则跳过此步骤。如果反垃圾邮件扫描可用，但未使用功能键启用，则此部分同样会显示该信息。 请参阅管理垃圾邮件和灰色邮件。

trace 命令部分	输出
防病毒	此部分注明未标记为由防病毒扫描处理的邮件。如果要在消息送达监听程序之前，对消息进行防病毒扫描处理，则会在处理消息后显示返回的裁决。如果邮件网关配置为“清除”受感染邮件，则会注明该信息。如果该设备配置为根据判定退回或丢弃消息，则会显示出该信息，且 trace 命令的处理停止。 注意：如果防病毒扫描在系统内不可用，则跳过此步骤。如果防病毒扫描可用，但未使用功能键启用，则此部分同样会显示该信息。 请参阅防病毒。
内容过滤器处理	系统上启用的所有内容过滤器此时都会由测试邮件进行评估。对每个过滤器的规则求值，如果最终结果为“true”，则按顺序执行该过滤器内的每步操作。过滤器可能会包含其他过滤器，将其作为一种操作，且过滤器的嵌套是不受限的。此部分会列显按顺序处理的内容过滤器的结果。 请参阅内容过滤器。
病毒爆发过滤器处理	此部分指明，包含附件的邮件将要绕过病毒爆发过滤器功能。如果邮件将由收件人的病毒爆发过滤器处理，邮件将被处理和评估。如果该邮件网关配置为根据判定隔离、退回或丢弃消息，则会显示出该信息，且处理会停止。 请参阅病毒爆发过滤器。
页脚印戳	此部分指明是否将页脚文本资源追加到邮件。并显示了文本资源名称。请参阅文本资源中邮件免责声明标记。
发送操作 以下部分注明传送邮件时发生的操作。在此部分之前，trace 命令将显示“队列中等待发送的邮件”。	
根据域和用户进行全局退订	如果任何被指定为 trace 命令输入的收件人与全局退订功能中所列的收件人、收件人域或 IP 地址相匹配，则所有退订的收件人地址都会显示在此部分中。 请参阅配置路由和传送功能。

trace 命令部分	输出
发件人域信誉	显示被发件人域的信誉判定阻止的邮件的处理结果。 以下是处理结果的示例： • 信誉：不确定 • 域有效期：33 年 9 个月 6 天 • 类别：不适用 • 操作：邮件已丢弃
最终结果 全部处理过程显示后，用户会收到最终结果的提示。在 CLI 中，针对问题“是否要查看生成的邮件”回答 **y**，以查看生成的邮件。	

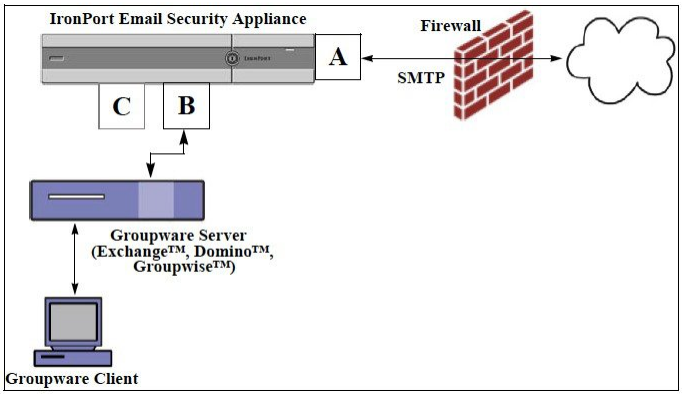
使用侦听程序测试邮件网关

通过“Sinkhole”侦听程序，可以测试您的邮件生成系统，同时还可以粗略衡量接收性能。sinkhole 侦听程序的两种类型是排队和非排队。

- 排队侦听程序会将邮件保存到队列，然后立即将其删除。如果希望衡量您的邮件生成系统的整个注入部分的性能，请使用排队侦听程序。
- 非排队侦听程序会接受邮件，然后立即将其删除，不进行保存。如果希望排除邮件生成系统与邮件网关之间的连接故障，请使用非排队侦听程序。

例如，在下图中，可以创建 sinkhole 侦听程序“C”来镜像标记为“B”的专用侦听程序。非排队版本会测试从组件客户端到组件服务器再到邮件网关的系统性能路径。排队版本会测试相同的路径以及邮件网关使邮件入队并为通过 SMTP 传送而做准备的能力。

Figure 1: 企业网关的 ***Sinkhole*** 侦听程序



在以下示例中，使用 listenerconfig 命令在管理接口上创建名为 Sinkhole_1 的 sinkhole 排队侦听程序。然后，编辑侦听程序的主机访问表 (HAT) 以接受来自以下主机的连接：

- **yoursystem.example.com**
- **10.1.2.29**
- **badmail.tst**
- **.tst**

Note 最后的条目 .tst 用于配置侦听程序，以便 .tst 域中的任何主机都可以向名为 Sinkhole_1 的侦听程序发送邮件。

示例

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> new

Please select the type of listener you want to create.

1. Private

2. Public

3. Sinkhole

[2]> 3

Do you want messages to be queued onto disk? [N]> y

Please create a name for this listener (Ex: "OutboundMail"):

[]> Sinkhole_1

Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1
```

```
Choose a protocol.

1. SMTP

2. QMQP

[1]> 1

Please enter the IP port for this listener.

[25]> 25

Please specify the systems allowed to relay email through the IronPort C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are allowed.

Separate multiple entries with commas.


[]> yoursystem.example.com, 10.1.2.29, badmail.tst, .tst

Do you want to enable rate limiting per host? (Rate limiting defines
the maximum number of recipients per hour you are willing to receive from a remote
domain.) [N]> n

Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control: No

Spam Detection Enabled: No

Virus Detection Enabled: Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Would you like to change the default host access policy? [N]> n

Listener Sinkhole_1 created.

Defaults have been set for a Sinkhole Queuing listener.

Use the listenerconfig->EDIT command to customize the listener.

Currently configured listeners:
```

```
1. Sinkhole_1 (on Management, 192.168.42.42) SMTP Port 25 Sinkhole Queuing

2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public

3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>
```

Note 请记得要发出 commit 命令，这些更改才能生效。

在配置了黑洞排队侦听程序并修改了 HAT 以接受来自注入系统的连接后，请使用注入系统向邮件网关发送邮件。使用 status、status detail 和 rate 命令监控系统性能。也可以通过图形用户界面 (GUI) 来监控系统。有关详细信息，请参阅：

- 使用 CLI 监控
- GUI 中的其他任务

排除网络故障

如果怀疑邮件网关存在网络连接问题，请先确认邮件网关工作正常。

测试邮件网关的网络连接

Procedure

步骤 1 连接到系统并以管理员身份登录。成功登录后，将显示以下信息：

```
Last login: day month date hh:mm:ss from IP address

Copyright (c) 2001-2003, IronPort Systems, Inc.

AsyncOS x.x for Cisco


Welcome to the Cisco Messaging Gateway Appliance(tm)
```

步骤 2 使用 status 或 status detail 命令。

```
mail3.example.com> status
```

或

```
mail3.example.com> status detail
```

status 命令将返回监控到的有关邮件操作的信息子集。返回的统计信息分为两类：计量器和测量器。有关邮件操作的完整监控信息（包括速率），请使用 status detail 命令。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。（有关详细信息，请参阅使用 CLI 监控。）

步骤 3 使用 `mailconfig` 命令向已知的工作地址发送邮件。

`mailconfig` 命令会生成一种可读文件，包括邮件网关可用的所有配置设置。尝试将文件从邮件网关发送到已知工作邮件地址，以确认邮件网关可以通过网络发送邮件。

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send the
configuration file.


Separate multiple addresses with commas.

[]> user@example.com

Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig. [N]> y


The configuration file has been sent to user@example.com.

mail3.example.com>
```

故障排除

确认邮件网关在网络中处于活动状态后，请使用以下命令查明所有网络问题。

- 可以使用 `netstat` 命令显示网络连接（包括传入和传出）、路由表和大量网络接口统计信息，包括以下信息：
  - 活动套接字列表
  - 网络接口状态
  - 路由表内容
  - 侦听队列的大小
  - 数据包流量信息

- 可以使用 `diagnostic -> network -> flush` 命令清空所有网络相关的缓存。
- 可以使用 `diagnostic -> network -> arpshow` 命令显示系统 ARP 缓存。
- 可以使用 `packetcapture` 命令解释和显示 TCP/IP 及其他正在通过计算机连接到的网络传送或接收的数据包。

  要使用 `packetcapture`，请设置网络接口和过滤器。过滤器使用相同的命令格式 UNIX `tcpdump` 命令。使用 start 开始数据包捕获，使用 stop 停止数据包捕获。停止捕获之后，需要使用 SCP 或 FTP 从 /pub/captures 目录下载文件。有关详细信息，请参阅运行数据包捕获, on page 24。
- 使用 `ping` 命令到达已知工作主机，以确认邮件网关在网络中具有活动连接，并且能够到达特定网段。

  使用 `ping` 命令可以测试网络主机与邮件网关的连接。

```
mail3.example.com> ping

Which interface do you want to send the pings from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Please enter the host you wish to ping.

[]> anotherhost.example.com

Press Ctrl-C to stop.

PING anotherhost.example.com (x.x.x.x): 56 data bytes

64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms

64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms

^C

--- anotherhost.example.com ping statistics ---

11 packets transmitted, 11 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

Note 您必须使用 Control-C 才能结束 ping 命令。

- 使用 `traceroute` 命令测试网络主机与邮件网关的连接性并调试网络跳的路由问题。

```
mail3.example.com> traceroute

Which interface do you want to trace from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Please enter the host to which you want to trace the route.

[]> 10.1.1.1

Press Ctrl-C to stop.

traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets

1 gateway (192.168.0.1) 0.202 ms 0.173 ms 0.161 ms

2 hostname (10.1.1.1) 0.298 ms 0.302 ms 0.291 ms

mail3.example.com>
```

- 使用 `diagnostic -> network -> smtpping` 命令测试远程 SMTP 服务器。
- 使用 `nslookup` 命令检查 DNS 功能。

  `nslookup` 命令可以确认邮件网关能够到达并解析来自工作 DNS（域名服务）服务器的主机名和 IP 地址。

```
mail3.example.com> nslookup

Please enter the host or IP to resolve.

[]> example.com


Choose the query type:

1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>

A=192.0.34.166 TTL=2d
```

Table 3: 检查 ***DNS*** 功能：查询类型

A	主机的互联网地址
CNAME	别名的规范名称
MX	邮件交换器
NS	用于指定区域的名称服务器
PTR	如果查询是互联网地址，则指主机名，否则，是指向其他信息的指针
SOA	域名的“start-of-authority”信息
TXT	文本信息

- 使用 CLI 的 `tophosts` 命令或 GUI，并按“活动收件人”进行排序。

  `tophosts` 命令返回队列中前 20 个收件人主机的列表。此命令可帮助您确定是否已将网络连接问题隔离至您尝试向其发送邮件的单个或一组主机。（有关详细信息，请参阅中的“确定邮件队列的构成”。）

```
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

ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1 aol.com36510255218

2 hotmail.com29071982813

3 yahoo.com13461231119

4 excite.com9838494

5 msn.com8427633 29

^C
```

- “向下钻取”以使用 tophosts 命令结果中列出的顶部域中的 `hoststatus` 命令。

`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。此外，还会提供 AsyncOS 缓存中存储的 DNS 信息以及从收件人主机返回的最后一条错误。返回的数据是从上一个 `resetcounters` 命令运行以来累加的。（有关详细信息，请参阅监控邮件主机的状态。）

对排名靠前的域使用 `hoststatus` 命令可以将 DNS 解析性能问题隔离到邮件网关或互联网。例如，如果顶部的活动收件人主机的 `hoststatus` 命令显示了许多待定出站连接，则尝试确定该特定主机是否已关闭或无法到达，或者邮件网关是否无法连接到全部或大多数主机。

- 检查防火墙权限。

  邮件网关可能需要打开以下所有端口才能正常工作：端口 20、21、22、23、25、53、80、123、443 和 628。（请参阅防火墙资讯。）

- 从网络中的邮件网关向 dnscheck@ironport.com 发送邮件

  将邮件从网络内部发送至 dnscheck@ironport.com 以在系统上执行基本的 DNS 检查。自动回复邮件将对以下四种测试的结果和详细信息加以回应。

DNS PTR 记录 - “信封发件人”的 IP 地址与域的 PTR 记录是否匹配？

DNS A 记录 - 域的 PTR 记录与“信封发件人”的 IP 地址是否匹配？

HELO 匹配 - `SMTP HELO` 命令中列出的域与“信封发件人”的 DNS 主机名是否匹配？

邮件服务器接受延迟退回邮件 - `SMTP HELO` 命令中列出的域是否具有解析该域的 IP 地址的 MX 记录？

排除侦听程序故障

如果您怀疑注入邮件存在问题，请采用以下战略方法：

- 确认您正在从其注入的 IP 地址，然后使用 `listenerconfig` 命令检查允许的主机。

  是否允许 IP 地址连接到您创建的侦听程序？使用 `listenerconfig` 命令检查侦听程序的主机访问表 (HAT)。使用以下命令打印侦听程序的 HAT：

  ```
  listenerconfig -> edit -> listener_number -> hostaccess -> print
  ```

  HAT 可以配置为通过 IP 地址、IP 地址块、主机名或域拒绝连接。有关详细信息，请参阅“指定允许连接的主机”。

  您还可以使用 `limits` 子命令检查侦听程序允许的最大连接数：

  ```
  listenerconfig -> edit -> listener_number -> limits
  ```

- 在您从其注入的计算机中，使用 Telnet 或 FTP 手动连接到邮件网关。例如：

  ```
  injection_machine% telnet appliance_name
  ```

  您还可以使用邮件网关中的 `telnet` 命令从侦听程序连接到实际邮件网关设备：

  ```
  mail3.example.com> telnet

  Please select which interface you want to telnet from.

  1. Auto
  ```

```
2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 3

Enter the remote hostname or IP.

[]> 193.168.1.1

Enter the remote port.

[25]> 25

Trying 193.168.1.1...

Connected to 193.168.1.1.

Escape character is '^]'.
```

如果无法从一个接口连接到另一个接口，可能是邮件网关的管理接口以及 Data1 和 Data2 接口连接到网络的方式有问题。有关详细信息，请参阅FTP、SSH 和 SCP 访问。您可以使用 telnet 登录到侦听程序的端口 25 并手动输入 SMTP 命令（如果您熟悉该协议）。

- 检查 IronPort 文本邮件日志和注入调试日志，以检查是否存在接收错误。

  注入调试日志记录邮件网关与连接到系统的指定主机之间的 SMTP 会话。注入调试日志对于排除邮件网关与从互联网发起连接的客户端之间的通信问题很有帮助。该日志记录两个系统之间传送的所有字节并将这些字节分类为“已发送至”连接主机或“接收自”连接主机。

  有关详细信息，请参阅使用文本邮件日志和使用注入调试日志。

排除从设备传送邮件的故障

如果您怀疑从邮件网关传送邮件存在问题，请采用以下战略方法：

- 确定问题是否是域特定的问题。

  使用 `tophosts` 命令获取有关邮件队列的即时信息并确定特定收件人域是否存在传送问题。

  按“正在处理的收件人数量”排序时返回的域是否有问题？

  按“出站连接数量”分类时，是否有任何域达到了为侦听程序指定的最大连接数？侦听程序默认的最大连接数为 600。默认的系统范围最大连接数为 10,000（通过 `deliveryconfig` 命令设置）。您可以使用以下命令检查侦听程序的最大连接数：

  ```
  listenerconfig -> edit -> listener_number -> limits
  ```

  侦听程序的连接数是否受 `destconfig` 命令（或者系统最大数或虚拟网络地址）的进一步限制？使用此命令检查 `destconfig` 连接限制：

  ```
  destconfig -> list
  ```

- 使用 `hoststatus` 命令。

使用结果（通过 tophosts 命令列出）中列出的顶部域上的 hoststatus 命令“向下钻取”。

主机是否可用并接受连接？

给定主机的某个特定 MX 记录邮件服务器是否存在问题？

如果指定的主机存在 5XX 错误（永久负完成回复），则 hoststatus 命令会报告该主机返回的最后一个“5XX”状态代码和说明。如果与主机的最后一个传出 TLS 连接失败，则 hoststatus 命令会显示失败的原因。

- 配置和/或检查域调试、退回和文本邮件日志来检查收件人主机是否可用。

  域调试日志记录邮件网关与指定收件人主机之间的 SMTP 会话期间的客户端和服务器通信。此日志文件类型可用来调试特定收件人主机存在的问题。

  有关详细信息，请参阅使用域调试日志。

  退回日志记录与每个已退回收件人有关的所有信息。

  有关详细信息，请参阅使用退回日志。

  文本邮件日志包含邮件接收、邮件传送和退回的详细信息。这些日志是非常有用的信息来源，可用于了解特定邮件的传输及分析系统性能。

  有关详细信息，请参阅使用文本邮件日志。

- 使用 telnet 命令从邮件网关连接到问题域：

```
mail3.example.com> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Enter the remote hostname or IP.
[]> problemdomain.net
Enter the remote port.

[25]> 25
```

- 您可以使用 tlsverify 命令按需建立出站 TLS 连接并调试有关目的域的所有 TLS 连接问题。要创建连接，请指定要验证的域和目标主机。AsyncOS 根据“必需（验证）”(Required [Verify]) TLS 设置检查 TLS 连接。

```
mail3.example.com> tlsverify
```

```
Enter the TLS domain to verify against:

[]> example.com

Enter the destination host to connect to. Append the port (example.com:26) if you are

not connecting on port 25:

[example.com]> mxe.example.com:25

Connecting to 1.1.1.1 on port 25.

Connected to 1.1.1.1 from interface 10.10.10.10.

Checking TLS connection.

TLS connection established: protocol TLSv1, cipher RC4-SHA.

Verifying peer certificate.

Verifying certificate common name mxe.example.com.

TLS certificate match mxe.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.

TLS verification completed.
```

排除性能问题

如果您怀疑邮件网关存在性能问题，请采用以下策略方法：

- 使用 rate 和 `hostrate` 命令检查当前的系统活动。

  rate 命令会返回有关邮件操作的实时监控信息。有关详细信息，请参阅显示实时活动。

  `hostrate` 命令会返回特定主机的实时监控信息。

- 使用 status 命令再次确认历史速率，以检查是否存在性能降低问题。
- 使用 `status detail` 命令检查 RAM 利用率。

  您可以使用 `status detail` 命令快速查看系统的 RAM、CPU 和磁盘 I/O 利用率。

Note RAM 利用率应始终少于 45%。如果 RAM 利用率超过 45%，邮件网关将进入“资源节约模式；”该模式会启动“后退”算法以防止资源的超订用并发出以下邮件警报：

```
This system (hostname: hostname) has entered a 'resource conservation' mode in order
to
prevent the rapid depletion of critical system resources.
```

```
RAM utilization for this system has exceeded the resource conservation threshold of
45%.
The allowed injection rate for this system will be gradually decreased as RAM
utilization approaches 60%.
```

仅当利用传送性能较差的设备进行攻击性注入时才会出现这种情况。如果遇到 RAM 利用率超过 45% 的情况，请检查队列中的邮件数并查看特定域是否已关闭或无法传送（通过 `hoststatus` 或 `hostrate` 命令）。此外，还要检查系统的状态并确保传送未处于挂起状态。如果停止注入后 RAM 利用率仍然很高，请与思科客户支持联系。

- 问题是否特定于某个域？

  使用 `tophosts` 命令获取有关邮件队列的即时信息并确定特定收件人域是否存在传送问题。

  检查队列的大小。您可以删除、退回、挂起或重定向邮件队列中的邮件，以管理其大小或处理有问题的特定域的收件人。有关详细信息，请参阅管理邮件队列。使用如下命令：

  - `deleterecipients`
  - `bouncerecipients`
  - `redirectrecipients`
  - `suspenddel / resumedel`
  - `suspendlistener / resumelistener`

  使用 `tophosts` 命令检查软退回和硬退回的数量。按“软退回的事件”（选项 4）或“硬退回的收件人”（选项5）进行分类。如果特定域存在性能问题，请使用上述命令管理到该域的传送。

Web 界面外观和呈现问题

请参阅覆盖 Internet Explorer 兼容模式。

回应警报

-
- 对“其他磁盘使用量接近配额”的警报进行故障排除 , on page 19

对“其他磁盘使用量接近配额”的警报进行故障排除

问题

您收到“其他磁盘使用量接近配额”的警报。

解决方案

您可以增加配额或删除文件。请参阅管理“其他”配额的磁盘空间。

对硬件问题进行故障排除

硬件邮件网关前面板和/或后面板上的指示灯指示邮件网关设备的运行状况和状态。有关这些指示灯的说明，请参阅硬件指南，例如《思科 *x90s* 系列内容安全设备的安装和维护指南》，可通过以下网址获取：
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html。

这些文档中还会介绍邮件网关规格，例如温度范围。

远程重置邮件网关电源

如果邮件网关需要硬重置，您可以使用第三方智能平台管理接口 (IPMI) 工具远程重新启动邮件网关机箱。

限制

- 远程电源重新启动仅适用于特定硬件。

  有关特定信息，请参阅启用远程电源循环。

- 如果您希望能够使用此功能，必须在需要使用该功能之前提前将其启用。

  有关详细信息，请参阅启用远程电源循环。

- 仅支持以下 IPMI 命令：
  - **`status, on, off, cycle, reset, diag, soft`**
  - 发出不支持的命令将导致“权限不足”错误。

准备工作

- 使用 IPMI 版本 2.0 获取并设置可用于管理设备的实用程序。
- 了解如何使用受支持的 IPMI 命令。请参阅 IPMI 工具的文档。

Procedure

步骤 1 使用 IPMI 向分配到“远程重启”端口（之前配置）的 IP 地址发出支持的电源循环命令，以及所需的凭证。

例如，从支持 IPMI 的 UNIX 类型计算机中可能发出如下命令：

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

其中，**`192.0.2.1`** 是分配到远程电源重新启动端口的 IP 地址，**`remoteresetuser`** 和 password 是您在启用此功能时输入的凭证。

步骤 2 等待至少十一分钟，以便邮件网关重启。

使用技术支持

虚拟邮件网关技术支持

获取虚拟邮件网关技术支持的要求在思科内容安全虚拟设备安装指南（可从 http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html 获得）中进行了介绍。

从邮件网关提交或更新支持案例

准备工作

- 如果问题紧急，请勿使用此方法。请改为使用思科客户支持中列出的方法之一与支持人员联系。

  仅当遇到类似请求信息或者您有解决方法但希望采用备选方案的问题时再使用以下过程。

- 考虑获取帮助的其他选项：
  - 知识库
  - 思科支持社区
- 要直接从邮件网关访问思科技术支持，您的 Cisco.com 用户 ID 必须与此邮件网关的服务协议合同相关联。要查看当前与您的 Cisco.com 配置文件相关的服务合同列表，请访问位于 https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do 的 Cisco.com 配置文件管理器。如果没有 Cisco.com 用户 ID，请注册一个。请参阅注册思科账户。

  请务必要将您的 Cisco.com 用户 ID 和支持合同 ID 保存在一个安全的位置。

- 使用此过程创建支持案例时，系统会将邮件网关配置文件发送给思科客户支持人员。如果您不希望发送邮件网关配置，可以使用另一种方法联系客户支持部门。
- 在集群配置中，支持请求及其保存的值是计算机特定的。
- 邮件网关必须联网并且能够发送邮件。
- 如果您要发送某个现有案例的相关信息，确保您有案例编号。

Procedure

步骤 1 登录到邮件网关。

步骤 2 依次选择**帮助和支持 (Help and Support)** > **联系技术支持 (Contact Technical Support)**。

步骤 3 完成表格。

步骤 4 单击**发送 (Send)**。

Note 必须在邮件网关上保存 CCO 用户 ID 和上次输入的合同 ID 以供日后使用。

启用思科技术支持人员远程访问

只有思科客户帮助部门才能使用这些方法访问您的邮件网关。

- 启用对网络连接邮件网关的远程访问 , on page 22
- 启用对无直接网络连接的邮件网关的远程访问 , on page 23
- 禁用远程访问 , on page 24
- 禁用技术支持隧道 , on page 23
- 检查支持连接的状态 , on page 24

启用对网络连接邮件网关的远程访问

支持部门可通过此过程在邮件网关与 **upgrades.ironport.com** 服务器之间创建的 SSH 隧道访问邮件网关。

准备工作

确定一个可以从互联网访问的端口。默认端口为 。允许在大多数防火墙配置下通过此端口进行连接。

Procedure

步骤 1 登录到邮件网关。

步骤 2 从 GUI 窗口的右上角，依次选择**帮助和支持 (Help and Support)** > **远程访问 (Remote Access)**。

步骤 3 单击**启用 (Enable)**。

步骤 4 输入信息：

选项	说明
种子字符串	种子字符串用于生成一个安全的共享密钥，思科客户支持要使用该密码访问此邮件网关。
安全隧道	选中该复选框以使用安全隧道进行远程访问连接。 输入该连接的端口。 默认端口为 25 ，该端口在大多数环境中都适用。

步骤 5 单击**提交 (Submit)**。

What to do next

当不再需要远程访问支持人员时，请参阅禁用技术支持隧道 , on page 23。

启用对无直接网络连接的邮件网关的远程访问

对于没有直接互联网连接的设备，可以通过连接至互联网的第二台邮件网关进行访问。

准备工作

- 邮件网关必须能够通过端口 22 连接到第二台连网邮件网关。
- 在已连接互联网的邮件网关上，按照启用对网络连接邮件网关的远程访问 , on page 22中的过程创建通往该邮件网关的支持隧道。

Procedure

步骤 1 在请求支持的邮件网关的命令行界面中，输入 **techsupport** 命令。

步骤 2 输入 **sshaccess**。

步骤 3 按照提示操作。

What to do next

当不再需要支持人员的远程访问时，请参阅以下内容：

- 禁用远程访问 , on page 24
- 禁用技术支持隧道 , on page 23

禁用技术支持隧道

已启用的 techsupport 隧道连续 7 天保持连接到 upgrades.ironport.com。7 天之后，建立的连接虽然不会断开，但一旦断开就无法重新连接至该隧道。

要手动禁用隧道，请执行以下操作：

Procedure

步骤 1 登录到邮件网关。

步骤 2 从 GUI 窗口的右上角，依次选择**帮助和支持 (Help and Support)** > **远程访问 (Remote Access)**。

步骤 3 单击**禁用 (Disable)**。

禁用远程访问

使用 techsupport 命令创建的远程访问账户将保持活动状态，直到将其禁用为止。

Procedure

步骤 1 在命令行界面中，输入 techsupport 命令。

步骤 2 输入 sshaccess。

步骤 3 输入 disable。

检查支持连接的状态

Procedure

步骤 1 在命令行界面中，输入 techsupport 命令。

步骤 2 输入 status。

运行数据包捕获

数据包捕获允许支持人员查看邮件网关接收和发出的TCP/IP数据及其他数据包。这样，支持人员就可以调试网络设置，并知道哪些网络流量到达该邮件网关或者离开该邮件网关。

Procedure

步骤 1 依次选择**帮助和支持 (Help and Support) > 数据包捕获 (Packet Capture)**。

步骤 2 指定数据包捕获设置：

a) 在**数据包捕获设置 (Packet Capture Settings)** 屏幕中，单击**编辑设置 (Edit Settings)**。

b) （可选）输入数据包捕获的持续时间、限制和过滤器。

您的支持代表可能会提供这些设置的相关指导。

如果您输入了捕获的持续时间却没有指定时间单位，AsyncOS 默认使用秒。

在**过滤器**部分：

- 自定义过滤器可以使用 UNIX tcpdump 命令支持的任何语法，例如 host 10.10.10.10 && port 80。
- 客户端 IP 是连接到邮件网关的计算机的 IP 地址，例如通过邮件网关发送邮件的邮件客户端。

- 服务器 IP 是指邮件网关连接的计算机（例如邮件网关传送邮件至的 Exchange 服务器）的 IP 地址。
- 您可以使用客户端和服务器 IP 地址跟踪特定客户端与特定服务器之间的流量，将邮件网关置于中间。

c) 单击**提交 (Submit)**。

步骤 3 单击**开始捕获 (Start Capture)**。

- 一次只能运行一个捕获操作。
- 运行数据包捕获时，数据包捕获页面会显示当前统计数据，例如文件大小和逝去的时间，让您能够看到进行中的捕获状态。
- GUI 只显示 GUI 中开始的数据包捕获，而不显示从 CLI 开始的数据包捕获。同样地，CLI 只显示 CLI 中开始的当前数据包捕获的运行状态。
- 数据包捕获文件分为 10 个部分。如果数据包捕获结束前文件到达最大大小限制，那么该文件最早的部分将会被删除（数据丢弃），新的部分从当前的数据包捕获数据开始。一次只能丢弃数据包捕获文件的 1/10。
- 两次会话期间保留 GUI 中开始的正在运行的捕获。（当会话终止时，CLI 中开始的正在运行的捕获会停止。）

步骤 4 允许捕获操作运行指定的时间，或者如果您让捕获无限运行，则可以单击**停止捕获 (Stop Capture)**停止捕获。

步骤 5 访问数据包捕获文件：

- 在**管理数据包捕获文件 (Manage Packet Capture Files)** 列表中单击该文件，然后单击**下载文件 (Download File)**。
- 使用 FTP 或 SCP 访问邮件网关 captures 子目录中的文件。

What to do next

将该文件提供给支持部门：

- 如果您允许远程访问您的邮件网关，技术人员可以使用 FTP 或 SCP 访问数据包捕获文件。请参阅启用思科技术支持人员远程访问 , on page 22。
- 通过邮件形式将该文件发送给支持部门。