Managing and Monitoring Using the CLI

This chapter contains the following sections:

- Overview of Managing and Monitoring Using the CLI, on page 1
- Reading the Available Components of Monitoring, on page 2
- Monitoring Using the CLI, on page 7
- Managing the Email Queue, on page 17
- Monitoring System Health and Status Using SNMP, on page 26

Overview of Managing and Monitoring Using the CLI

Managing and monitoring the email gateway using the CLI includes these types of tasks:

- Monitoring message activity.
  - The raw number of messages, recipients, and bounce recipients that the email gateway is processing in the email pipeline
  - The hourly rate of message delivery or message bounces based on the last one-minute, five-minute, or fifteen-minute period
- Monitoring system resources. Examples:
  - Memory usage
  - Disk space
  - Number of connections
- Monitoring possible system disfunction using the Simple Network Management Protocol (SNMP). Examples:
  - Fan failure
  - Update failure
  - Abnormally high email gateway temperature
- Managing email within the pipeline. Examples:
  - Deleting recipients in the queue
  - Redirecting messages to another host
  - Clear the queue by deleting recipients or redirecting the messages
  - Suspend or resume email receiving, delivery, or work queue processing
  - Locate specific messages

Reading the Available Components of Monitoring

- Reading the Event Counters, on page 2
- Reading the System Gauges, on page 4
- Reading the Rates of Delivered and Bounced Messages, on page 6

Reading the Event Counters

Counters provide a running total of various events in the system. For each counter, you can view the total number of events that have occurred since the counter was reset, since the last system reboot, and over the system's lifetime.

Counters increment each time an event occurs and are displayed in three versions:

Reset	Since the last counter reset with the resetcounters command
Uptime	Since the last system reboot
Lifetime	Total through the lifetime of the email gateway

The following table lists the available counters and their description when monitoring the email gateway.

Note This is the entire list. The displayed counters vary depending on which display option or command you choose. Use this list as a reference.

Table 1: Counters

Statistic	Description
Receiving	Messages received into the delivery queue.
Messages Received	
Recipients Received	Recipients on all received messages.
Generated Bounce Recipients	Recipients for which bounces have been generated by the system and inserted into the delivery queue.
Rejection	Recipients that have been denied receiving into the delivery queue due to the Recipient Access Table (RAT), or unexpected protocol negotiation including premature connection termination.
Rejected Recipients	

Statistic	Description
Dropped Messages	Messages that have been denied receiving into the delivery queue due to a filter drop action match or have been received by a Sinkhole queuing listener. Messages directed to /dev/null entries in the alias table also are considered dropped messages. Messages dropped by anti-spam filtering (if it has been enabled on the system) also increment this counter.
Queue	
Soft Bounced Events	Number of soft bounce events — a message that soft bounces multiple times has multiple soft bounce events.
Completion	
Completed Recipients	Total of all hard bounced recipients, delivered recipients, and deleted recipients. Any recipient that is removed from the delivery queue.
Hard Bounced Recipients	Total of all DNS hard bounces, 5XX hard bounces, filter hard bounces, expired hard bounces and other hard bounces. A failed attempt to deliver message to a recipient that results in immediate termination of that delivery.
DNS Hard Bounces	DNS error encountered while trying to deliver a message to a recipient.
5XX Hard Bounces	The destination mail server returned a “5XX” response code while trying to deliver a message to a recipient.
Expired Hard Bounces	Message recipients that have exceeded the maximum time allowed in the delivery queue or the maximum number of connection attempts.
Filter Hard Bounces	Recipient delivery has been preempted by a matching filter bounce action. Messages dropped by anti-spam filtering (if it has been enabled on the system) also increment this counter.
Other Hard Bounces	An unexpected error during message delivery or a message recipient was explicitly bounced via the bouncerecipients command.
Delivered Recipients	Message successfully delivered to a recipient.
Deleted Recipients	Total of message recipients explicitly deleted via the deleterecipients command or was a Global Unsubscribe Hit.
Global Unsubscribe Hits	Message recipient was deleted due to a matching global unsubscribe setting.
Current IDs	

Statistic	Description
Message ID (MID)	The last Message ID to have been assigned to a message inserted into the delivery queue. A MID is associated with every message received by the email gateway and can be tracked in mail logs. The MID resets to zero at 231.
Injection Connection ID (ICID)	The last Injection Connection ID to have been assigned to a connection to a listener interface. The ICID rolls over (resets to zero) at 231.
Delivery Connection ID (DCID)	The last Delivery Connection ID to have been assigned to a connection to a destination mail server. The DCID rolls over (resets to zero) at 231.

Reading the System Gauges

Gauges show the current utilization of a system resource such as memory, disk space, or active connections.

The following table lists the available gauges and their description when monitoring the email gateway.

Note This is the entire list. The displayed gauges will vary depending upon which display option or command you choose. Use this list as a reference.

Table 2: Gauges

Statistic	Description
System Gauges	
RAM Utilization	Percentage of physical RAM (Random Access Memory) being used by the system.
CPU Utilization	Percentage of CPU usage.
Disk I/O Utilization	Percentage of Disk I/O being used. **Note** The Disk I/O Utilization gauge does not display a reading against a scale of a known value. Rather, it displays the I/O utilization the system has seen thus far and scales against the maximum value since the last reboot. So, if the gauge displays 100%, the system is experiencing the highest level of I/O utilization seen since boot (which may not necessarily represent 100% of the physical Disk I/O of the entire system).

Statistic	Description
Resource Conservation	A value between 0 and 60 or 999 . Numbers from 0 to 60 represent the degree to which the system is decreasing its acceptance of messages in order to prevent the rapid depletion of critical system resources. Higher numbers represent a higher degree of decreased acceptance. Zero represents no decrease in acceptance. If this gauge displays 999 , the system has entered "Resource Conservation mode," and it will accept no messages. Alert messages are sent whenever the system enters or exits Resource Conservation mode.
Disk Utilization: Logs	Percentage of disk being used for logs, displayed as LogUsd in the status logs and log_used in the XML status.
Connections Gauges	
Current Inbound Connections	Current inbound connections to the listener interfaces.
Current Outbound Connections	Current outbound connections to destination mail servers.
Queue Gauges	
Active Recipients	Message recipients in the delivery queue. Total of Unattempted Recipients and Attempted Recipients.
Unattempted Recipients	A subcategory of Active Recipients. Message recipients in queue for which delivery has not yet been attempted.
Attempted Recipients	A subcategory of Active Recipients. Message recipients in queue for which delivery has been attempted but failed due to a Soft Bounces Event.
Messages in Work Queue	The number of messages waiting to be processed by alias table expansion, masquerading, anti-spam, anti-virus scanning, message filters, and LDAP queries prior to being enqueued.
Messages in Quarantine	The unique number of messages in any quarantine, plus messages that have been released or deleted but not yet acted upon. For example, if you release all quarantined messages from Outbreak, the total messages for Outbreak would become zero immediately, but this field still reflects the quarantined messages until they were all delivered.

Statistic	Description
Destinations in Memory	The number of destinations domains in memory. For each domain with a message destined to be delivered, a destination object is created in memory. After all the mail for that domain has been delivered, the destination object is retained for another 3 hours. After 3 hours, if no new messages are bound for that domain, the object is expired so that the destination is no longer reported (for example, in the tophosts command). If you are delivering mail only to one domain, this counter will be "1." If you have never received or sent any messages (or no messages have been processed by the email gateway in many hours), the counter will be "0." If you are using Virtual Gateways, destination domains for each Virtual Gateway will have a separate destination object. (For example, yahoo.com will count as 3 destination objects if you are delivering to yahoo.com from 3 different Virtual Gateways).
Kilobytes Used	Queue storage used in kilobytes.
Kilobytes in Quarantine	Queue storage used for quarantined messages. The value is calculated as the message size plus 30 bytes for each recipient, totaled for the "Messages in Quarantine" as counted above. Note that this calculation will usually *overestimate* the space used.
Kilobytes Free	Queue storage remaining in kilobytes.

Reading the Rates of Delivered and Bounced Messages

All rates are shown as the average rate an event occurs per hour at the specific point in time the query is made. Rates are calculated for three intervals, the average rate per hour over the past one (1) minute, the past five (5) minutes, and the past fifteen (15) minutes.

For example, if the email gateway receives 100 recipients in a single minute, then the rate for the 1 minute interval will be 6,000 per hour. The rate for the 5-minute interval will be 1,200 per hour, and the 15-minute rate will be 400 per hour. The rates are calculated to indicate what the average rate for the hour would be if the rate for the one minute period continued. Therefore, 100 messages each minute would yield a higher rate than 100 messages over 15 minutes.

The following table lists the available rates and their description when monitoring the email gateway.

Note This is the entire list. The displayed rates will vary depending upon which display option or command you choose. Use this list as a reference.

Table 3: Rates

Statistic	Description
Messages Received	Rate of messages inserted into the delivery queue per hour.

Statistic	Description
Recipients Received	Rate of the number of recipients on all messages inserted into the delivery queue per hour.
Soft Bounced Events	Rate of the number of soft bounce events per hour. (A message that soft bounces multiple times has multiple soft bounce events.)
Completed Recipients	Rate of the total of all hard bounced recipients, delivered recipients and deleted recipients. Any recipient that is removed from the delivery queue is considered completed.
Hard Bounced Recipients	Rate of the total of all DNS hard bounces, 5XX hard bounces, filter hard bounces, expired hard bounces and other hard bounces per hour. A failed attempt to deliver a message to a recipient that results in immediate termination of that delivery is a hard bounce.
Delivered Recipients	Rate of messages successfully delivered to a recipient per hour.

Monitoring Using the CLI

- Monitoring the Email Status, on page 7
- Monitoring Detailed Email Status, on page 8
- Monitoring the Status of a Mail Host, on page 10
- Determining the Make-up of the Email Queue, on page 12
- Displaying Real-time Activity, on page 13
- Monitoring Inbound Email Connections, on page 14
- Checking the DNS Status, on page 15
- Resetting Email Monitoring Counters, on page 16
- Identifying Active TCP/IP Services, on page 17

Monitoring the Email Status

You may want to monitor the status of email operations on the email gateway. The status command returns a subset of the monitored information about email operations. The statistics returned displayed in one of two fashions: counters and gauges. Counters provide a running total of various events in the system. For each counter, you can view the total number of events that have occurred since the counter was reset, since the last system reboot, and over the system's lifetime. Gauges show the current utilization of a system resource such as memory, disk space, or active connections.

For a description of each item, see Overview of Managing and Monitoring Using the CLI, on page 1.

Table 4: Mail Status

Statistic	Description
Status as of	Displays the current system time and date.
Last counter reset	Displays the last time the counters were reset.

Statistic	Description
System status	Online, offline, receiving suspended, or delivery suspended. Note that the status will be "receiving suspended" only when *all* listeners are suspended. The status will be "offline" when receiving and delivery are suspended for *all* listeners.
Oldest Message	Displays the oldest message waiting to be delivered by the system.
Features	Displays any special features installed on the system by the featurekey command.

Example

```
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>
```

Monitoring Detailed Email Status

The status detail command returns complete monitored information about email operations. The statistics returned are displayed in one of three categories: counters, rates, and gauges. Counters provide a running total of various events in the system. For each counter, you can view the total number of events that have occurred since the counter was reset, since the last system reboot, and over the system's lifetime. Gauges show the current utilization of a system resource such as memory, disk space, or active connections. All rates are shown as the average rate an event occurs per hour at the specific point in time the query is made. Rates are calculated for three intervals, the average rate per hour over the past one (1) minute, the past five (5) minutes, and the

past fifteen (15) minutes. For a description of each item, see Overview of Managing and Monitoring Using the CLI, on page 1.

Example

```
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 A case could exist in a newly installed email gateway where the oldest message counter shows a message but, in fact, there are no recipients shown in counters. If the remote host is connecting and in the process of receiving a message very slowly (that is, it takes minutes to receive a message), you might see that the recipients received counter displays " 0 " but the oldest message counter displays " 1 ." This is because the oldest message counter displays messages in progress. The counter will be reset if the connection is eventually dropped.

Monitoring the Status of a Mail Host

If you suspect delivery problems to a specific recipient host or you want to gather information on a Virtual Gateway address, the hoststatus command displays this information. The hoststatus command returns monitoring information about email operations relating to a specific recipient host. The command requires that you enter the domain of the host information to be returned. DNS information stored in the AsyncOS cache and the last error returned from the recipient host is also given. Data returned is cumulative since the last resetcounters command. The statistics returned are displayed in two categories: counters and gauges. For a description of each item, see Overview of Managing and Monitoring Using the CLI, on page 1.

In addition, these other data are returned specific to the hoststatus command.

Table 5: Additional Data in the hoststatus Command

Statistic	Description
Pending Outbound Connections	Pending, or "embryonic" connections to the destination mail host, as opposed to open and working connections. Pending Outbound Connections are connections which have not yet gotten to the protocol greeting stage.
Oldest Message	The age of the oldest active recipient in the delivery queue for this domains. This counter is useful for determining the age of a message in the queue that cannot be delivered because of soft bounce events and/or a downed host.
Last Activity	This field is updated each time a message delivery is attempted to that host.
Ordered IP Addresses	This field contains the TTL (time to live) for IP addresses, their preference according to MX records, and the actual addresses. An MX record designates the mail server IP address for a domain. A domain may have multiple MX records. Each MX record mail server is assigned a priority. The MX record with the lowest priority number is given preference.
Last 5XX error	This field contains the most recent "5XX" status code and description returned by the host. This is only displayed if there is an 5XX error.

Statistic	Description
MX Records	An MX record designates the mail server IP address for a domain. A domain may have multiple MX records. Each MX record mail server is assigned a priority. The MX record with the lowest priority number is given preference.
SMTP Routes for this host	If SMTP routes are defined for this domain, they are listed here.
Last TLS Error	This field contains a description of the the most recent outgoing TLS connection error and the type of TLS connection that the email gateway tried to establish. This is only displayed if there is a TLS error.

Virtual Gateway

The following Virtual Gateway information is only displayed if you have set up Virtual Gateway addresses (see Configuring the Gateway to Receive Email.)

Table 6: Additional Virtual Gateway Data in the hoststatus Command

Statistic	Description
Host up/down	Same definition as global hoststatus field of the same name — tracked per Virtual Gateway address.
Last Activity	Same definition as global hoststatus field of the same name — tracked per Virtual Gateway address.
Recipients	This field also corresponds to the same definition as the global hoststatus command. Active Recipients field — tracked per Virtual Gateway address.
Last 5XX error	This field contains the most recent 5XX status code and description returned by the host. This is only displayed if there is a 5XX error.

Example

```
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 The Virtual Gateway address information only appears if you are using the altsrchost feature.

Determining the Make-up of the Email Queue

To get immediate information about the email queue and determine if a particular recipient host has delivery problems — such as a queue buildup — use the tophosts command. The tophosts command returns a list of the top 20 recipient hosts in the queue. The list can be sorted by a number of different statistics, including active recipients, connections out, delivered recipients, soft bounced events, and hard bounced recipients. For a description of each item, see Overview of Managing and Monitoring Using the CLI, on page 1.

Example

```
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>
```

Displaying Real-time Activity

The email gateway offers real-time monitoring, which allows you to view the progress of email activity on the system. The rate command returns real-time monitoring information about email operations. The information is updated on a periodic interval as specified by you. Use Control-C to stop the **rate** command.

The data shown are listed in the following table:

Table 7: Data in the rate Command

Statistic	Description
Connections In	Number of inbound connections.
Connections Out	Number of outbound connections.
Recipients Received	Total number of recipients received into the system.
Recipients Completed	Total number of recipients completed.
Delta	The difference change in Received and Completed recipients since the last data update.
Queue Used	Size of the message queue in kilobytes.

Example

```
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
```

The hostrate command returns real-time monitoring information about a specific mail host. This information is a subset of the status detail command. (See Monitoring Detailed Email Status, on page 8.)

Table 8: Data in the hostrate Command

Statistic	Description
Host Status	Current status of the specific host: up, down, or unknown.
Current Connections Out	Current number of outbound connections to the host.
Active Recipients in Queue	Total number of active recipients to the specific host in queue.
Active Recipients in Queue Delta	Difference in the total number of active recipients to the specific host in queue since the last known host status.
Delivered Recipients Delta	Difference in the total number of delivered recipients to the specific host in queue since the last known host status.
Hard Bounced Recipients Delta	Difference in the total number of hard bounced recipients to the specific host in queue since the last known host status.
Soft Bounce Events Delta	Difference in the total number of soft bounced recipients to the specific host in queue since the last known host status.

Use Control-C to stop the hostrate command.

Example

```
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
```

Monitoring Inbound Email Connections

You may want to monitor hosts that are connecting to the email gateway to identify the large volume senders or to troubleshoot inbound connections to the system. The topin command provides a snapshot of the remote hosts connecting to the system. It displays a table with one row for each remote IP address connecting to a specific listener. Two connections from the same IP address to different listeners results in 2 rows in the following table describes the fields displayed when using the topin command.

Table 9: Data in the topin Command

Statistic	Description
Remote Hostname	Hostname of the remote host, derived from Reverse DNS lookup.
Remote IP Address	IP address of the remote host.
listener	Nickname of the listener on the email gateway that is receiving the connection.
Connections In	The number of concurrent connections from the remote host with the specified IP address open at the time when the command is run.

The system does a reverse DNS lookup to find the remote hostname, and then a forward DNS lookup to validate the name. If the forward lookup does not result in the original IP address, or if the reverse DNS lookup fails, the table displays the IP address in the hostname column. For more information about the process of sender verification, see Verifying Senders.

Example

```
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
```

Checking the DNS Status

The dnsstatus command returns a counter displaying statistics of DNS lookup and cache information. For each counter, you can view the total number of events since the counter was last reset, since the last system reboot, and over the lifetime of the system.

The following table lists the available counters.

Table 10: Data in the dnsstatus Command

Statistic	Description
DNS Requests	A top-level, non-recursive request to the system DNS cache to resolve a domain name.
Network Requests	A request to the network (non-local) to retrieve DNS information.
Cache Hits	A request to the DNS cache where the record was found and returned.
Cache Misses	A request to the DNS cache where the record was not found.
Cache Exceptions	A request to the DNS cache where the record was found but the domain was unknown.
Cache Expired	A request to the DNS cache where the record was found in the cache, considered for use, and discarded because it was too old. Many entries can exist in the cache even though their time to live (TTL) has been exceeded. As long as these entries are not used, they will not be included in the expires counter. When the cache is flushed, both valid and invalid (too old) entries are deleted. A flush operation does not change the expires counter.

Example

```
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>
```

Resetting Email Monitoring Counters

Caution It is recommended that you avoid resetting email monitoring counters on Cloud Email Security appliances.

The resetcounters command resets cumulative email monitoring counters. The reset affects global counters as well as per host counters. The reset does not affect the counters on messages in the delivery queue related to retry schedules.

Note You can also reset the counters in the GUI. See System Status Page.

Example

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

Identifying Active TCP/IP Services

To identify active TCP/IP services used by your email gateway, use the tcpservices command in the command line interface.

Managing the Email Queue

Cisco AsyncOS allows you to perform operations on messages in the email queue. You can delete, bounce, suspend, or redirect messages in the email queue. You can also locate, remove, and archive older messages in your queue.

Deleting Recipients in Queue

If particular recipients are not being delivered or to clear the email queue, use the deleterecipients command. The deleterecipients command allows you to manage the email delivery queue by deleting specific recipients waiting for delivery. Recipients to be deleted are identified by either the recipient host that the recipient is destined for, or the message sender identified by the specific address given in the Envelope From line of the message envelope. Alternately, you can delete all messages in the delivery queue (all active recipients) at once.

Note To perform the deleterecipients function, it is recommended that you place the email gateway in an offline state or suspended delivery (see Suspending Email Receiving and Delivery).

Note Although the function is supported in all states, certain messages may be delivered while the function is taking place.

Matches to recipient hosts and senders must be identical string matches. Wild cards are not accepted. The deleterecipients command returns the total number of messages deleted. In addition, if a mail log subscription (IronPort text format only) is configured, the message deletion is logged as a separate line.

Example

```
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]>
```

The email gateway gives you various options to delete recipients depending upon the need. The following example show deleting recipients by recipient host, deleting by Envelope From Address, and deleting all recipients in the queue.

Delete by Recipient Domain

```
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.
```

Delete by Envelope From Address

```
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.
```

Delete All

```
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.
```

Bouncing Recipients in Queue

Similar to the deleterecipients command, the bouncerecipients command allows you to manage the email delivery queue by hard bouncing specific recipients waiting for delivery. Message bouncing follows regular bounce message configuration as specified in the bounceconfig command.

Note To perform the bouncerecipients function, it is recommended that you place the email gateway in an offline state or suspended delivery (see Suspending Email Receiving and Delivery).

Note Although the function is supported in all states, certain messages may be delivered while the function is taking place.

Matches to recipient hosts and senders must be identical string matches. Wild cards are not accepted. The bouncerecipients command returns the total number of messages bounced.

Note The bouncerecipients function is resource-intensive and may take several minutes to complete. If in offline or suspended delivery state, the actual sending of bounce messages (if hard bounce generation is on) will begin only after Cisco AsyncOS is placed back into the online state by using the resume command.

Example

```
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]>
```

Recipients to be bounced are identified by either the destination recipient host or the message sender identified by the specific address given in the Envelope From line of the message envelope. Alternately, all messages in the delivery queue can be bounced at once.

Bounce by Recipient Host

```
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.
```

Bounce by Envelope From Address

```
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.
```

Bounce All

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

Redirecting Messages in Queue

The redirectrecipients commands allow you to redirect all messages in the email delivery queue to another relay host. Please note that 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.

Caution Redirecting messages to a receiving domain that has /dev/null as its destination results in the loss of messages. The CLI does not display a warning if you redirect mail to such a domain. Check the SMTP route for the receiving domain before redirecting messages.

Example

The following example redirects all mail to the example2.com host.

```
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.
```

Showing Messages Based on Recipient in Queue

Use the showrecipients command to show messages from the email delivery queue by recipient host or Envelope From address. You can also show all messages in the queue.

Example

```
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
```

The following example shows messages in the queue for all recipient hosts.

Suspending Email Delivery

Caution It is recommended that you avoid suspending and resuming email delivery on us appliances.

To temporarily suspend email delivery for maintenance or troubleshooting, use the suspenddel command. The suspenddel command puts Cisco AsyncOS into suspended delivery state. This state is characterized by the following:

- Outbound email delivery is halted.
- Inbound email connections are accepted.
- Log transfers continue.
- The CLI remains accessible.

The suspenddel command lets open outbound connections close, and it stops any new connections from opening. The suspenddel command commences immediately, and allows any established connections to successfully close. Use the resumedel command to return to regular operations from the suspended delivery state.

Note The "delivery suspend" state is preserved across system reboots. If you use the suspenddel command and then reboot the email gateway, you must resume delivery after the reboot using the resumedel command.

Example

```
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.
```

Resuming Email Delivery

Caution It is recommended that you avoid suspending and resuming email delivery on Cloud Email Security appliances.

The resumedel command returns Cisco AsyncOS to normal operating state after using the suspenddel command.

Syntax

resumedel

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

Suspending Receiving Email

Caution It is recommended that you avoid suspending and resuming listeners on Cloud Email Security appliances.

To temporarily suspend all listeners from receiving email, use the suspendlistener command. While receiving is suspended, the system does not accept connections to the specific port of the listener.

This behavior has changed in this release of AsyncOS. In previous releases, the system would accept connections, respond with the following responses and disconnect:

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

- QMQP: ZService not available

Note The “receiving suspend” state is preserved across system reboots. If you use the suspendlistener command and then reboot the email gateway, you must use the resumelistener command before the listener will resume receiving messages.

Syntax

```
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>
```

Resuming Receiving Email

Caution It is recommended that you avoid suspending and resuming listeners on Cloud Email Security appliances.

The resumelistener command returns Cisco AsyncOS to normal operating state after using the suspendlistener command.

Syntax

```
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>
```

Resuming Delivery and Receiving of Email

The resume command resumes both delivery and receiving.

Syntax

```
resume
```

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

Scheduling Email for Immediate Delivery

Recipients and hosts that are scheduled for later delivery can be immediately retried by using the delivernow command. The delivernow command allows you to reschedule email in the queue for immediate delivery. All domains that are marked down and any scheduled or soft bounced messages are queued for immediate delivery.

The delivernow command can be invoked for all recipients or specific recipients in the queue (scheduled and active). When selecting specific recipients, you must enter the domain name of the recipients to schedule for immediate delivery. The system matches the entire string for character and length.

Syntax

```
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>
```

Pausing the Work Queue

Caution It is recommended that you avoid pausing the work queue on Cloud Email Security appliances.

Processing for LDAP recipient access, masquerading, LDAP re-routing, Message Filters, anti-spam, and the anti-virus scanning engine are all performed in the "work queue." Refer to Configuring Routing and Delivery Features for the processing flow and Reading the System Gauges, on page 4 for a description of the "Messages in Work Queue" gauge. You can manually pause the work queue portion of message processing using the workqueue command.

For example, assume that you wanted to change the configuration of an LDAP server configuration while many messages are in the work queue. Perhaps you want to switch from bouncing to dropping messages based on an LDAP recipient access query. Or perhaps you want to pause the queue while you manually check for the latest anti-virus scanning engine definition files (via the antivirusupdate command).The workqueue command allows you to pause and resume the work queue to stop processing while you perform other configuration changes.

When you pause and resume the work queue, the event is logged. For example

```
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
```

In the following example, the work queue is paused:

```
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 Entering a reason is optional. If you do not enter a reason, the system logs the reason as " Manually paused by user ."

In this example, the work queue is resumed:

```
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
```

Locating and Archiving Older Messages

Sometimes older messages remain in the queue because they could not be delivered. You may want to remove and archive these messages. To do this, use the showmessage CLI command to to display the message for the given message ID. Use the oldmessage CLI command to display the oldest non-quarantine message on the system. You can then optionally use the removemessage to safely remove the message for the given message ID. This command can only remove messages that are in the work queue, retry queue, or a destination queue. If the message is in none of these queues, it cannot be removed.

You can also use the archivemessage[mid] CLI command to archive the message for a given message ID into an mbox file in the configuration directory.

You cannot use the oldmessage command to get the message ID for a message in a quarantine. However, if you know the message ID, you can show or archive the specified message. Since the message is not in the

work queue, retry queue, or a destination queue, you cannot remove the message with the removemessage command.

Note You cannot perform any of these queue management commands on a message in the Cisco Spam Quarantine.

Syntax

```
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>
```

Syntax

```
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>
```

Tracking Messages Within the System

The findevent CLI command simplifies the process of tracking messages within the system using the onbox mail log files. The findevent CLI command allows you to search through the mail logs for a particular message by searching for a message ID or a regular expression match against the subject header, envelope sender or envelope recipient. You can display results for the current log file, all the log files, or display log files by date. When you view log files by date, you can specify a date or a range of dates.

After you identify the message you want to view logs for, the findevent command displays the log information for that message ID including splintering information (split log messages, bounces and system generated messages). The following example shows the findevent CLI command tracking the receiving and delivery a message with “confidential” in the subject header:

```
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
```

Monitoring System Health and Status Using SNMP

Caution It is recommended that you avoid configuring SNMP on Cloud Email Security appliances

The AsyncOS operating system supports system status monitoring via SNMP (Simple Network Management Protocol). This release implements a read-only subset of MIB-II as defined in RFCs 1213 and 1907. (For more information on SNMP, see RFCs 1065, 1066, and 1067.) Please note:

- SNMP is **off** by default.
- When SNMP is enabled, the default version used is SNMPv3.
- SNMP SET operations (configuration) are not implemented.
- AsyncOS supports SNMPv1, v2, and v3.
- Passphrases for authentication and encryption should be different. The encryption algorithm must be AES only. The authentication algorithm must be SHA-1 only. The snmpconfig command “remembers” your passphrases the next time you run the command.
- The SNMPv3 username is: v3get

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

- If you use only SNMPv1 or SNMPv2, you must set a community string. The community string does not default to public .
- For SNMPv1 and SNMPv2, you must specify a network from which SNMP GET requests are accepted.

- If you use SNMPv3, you must select any one of the supported security levels shown in the following table:

Security Level	Authentication	Privacy
noAuthNoPriv	Yes The authentication is done using the SNMPv3 username.	No
authNoPriv	Yes The authentication is done using the SNMPv3 authentication passphrase.	No
authPriv	Yes The authentication is done using the SNMPv3 authentication passphrase.	Yes The privacy is activated using the SNMPv3 privacy passphrase.

- If you enable both SNMPv2 and SNMPv3, you must select the required version for traps.
- To use traps, an SNMP manager (not included in AsyncOS) must be running and its IP address entered as the trap target. (You can use a hostname, but if you do, traps will only work if DNS is working.)

Use the snmpconfig command to enable and configure SNMP monitoring for the email gateway. After you choose and configure values for an interface, the email gateway responds to SNMPv3 GET requests. These version 3 requests must include a matching passphrase. By default, version 1 and 2 requests are rejected. If enabled, version 1 and 2 requests must have a matching community string.

MIB Files

The following MIB files for email gateways are available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html. Use the latest available MIB files.

- ASYNCOS-MAIL-MIB.txt — an SNMPv2 compatible description of the Enterprise MIB for email gateways.
- AsyncOS-SMI.txt (IRONPORT-SMI.txt) — a “Structure of Management Information” (SMI) file that defines the role of the ASYNCOS-MAIL-MIB in Cisco content security products.

Hardware Objects

Hardware sensors conforming to the Intelligent Platform Management Interface Specification (IPMI) report information such as temperature, fan speed, and power supply status.

It is a good idea to poll for the hardware status and identify possible hardware failures before they become critical. Temperatures within 10 per cent of the critical value may be a cause for concern.

For information such as the number of power supplies and the range of operating temperatures for your email gateway, see the hardware guide for your model. For the location of hardware guides, see Documentation.

Hardware Traps

Status change traps are sent when the status changes. Fan Failure and high temperature traps are sent every 5 seconds. The other traps are failure condition alarm traps — they are sent once when the state changes (healthy to failure).

For example, on C170 email gateways, traps are sent if the following thresholds are reached:

Table 11: Hardware Traps on C170 Email Gateways: Temperature and Hardware Conditions

Model	High Temp (CPU)	High Temp (Ambient)	High Temp (Backplane)	High Temp (Riser)	Fan Failure	Power Supply	RAID	Link
C170	90C	47C	NA	NA	0 RPMs	Status Change	Status Change	Status Change

To see the available traps and threshold values on your email gateway, run the snmpconfig command from the command-line interface.

Note that failure condition alarm traps represent a critical failure of the individual component, but may not cause a total system failure. For example, a single fan or power supply can fail on an email gateway with multiple fans or power supplies and the email gateway will continue to operate.

Related Topics

- Example: snmpconfig Command , on page 28

SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administration application (an SNMP management console, typically) when one or more conditions have been met. Traps are network packets that contain data relating to a component of the system sending the trap. Traps are generated when a condition has been met on the SNMP agent (in this case, the email gateway). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it to the host running the SNMP management console software.

To enable and configure SNMP traps, use the snmpconfig command.

To specify multiple trap targets: when prompted for the trap target, you may enter up to 10 comma separated IP addresses.

Example: snmpconfig Command

In the following example, the snmpconfig command is used on a C690 hardware email gateway to enable SNMP on the “PublicNet” interface on port 161. The community string public is entered for GET requests from versions 1 and 2.

```
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
```