



# CHAPTER 6

## CLI による管理およびモニタリング

Cisco IronPort アプライアンスには、ログを解析せずに電子メール動作をモニタするためのコマンドが用意されています。Cisco IronPort アプライアンスのモニタには、Command Line Interface (CLI; コマンドライン インターフェイス) と Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) のいずれかを使用できます。この章では、モニタリングおよび管理コマンドについて、また CLI を使ってそれらのコマンドにアクセスする方法について説明します。コンポーネントの多くは GUI から使用することもできます。GUI については、[第 7 章「GUI でのその他の作業」](#)を参照してください。

この章は、次の内容で構成されています。

- 「使用可能なモニタリング コンポーネントの読み取り」(P.6-231)
- 「CLI によるモニタリング」(P.6-239)
- 「電子メール キューの管理」(P.6-263)
- 「SNMP モニタリング」(P.6-280)

### 使用可能なモニタリング コンポーネントの読み取り

システムのモニタリングには、次の 3 つの主要コンポーネントがあります。

- カウンタ
- ゲージ
- レート

## カウンタの読み取り

カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リポート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。

カウンタは、イベントが発生するごとに増加し、次の 3 つのバージョンで表示されます。

<b>Reset</b>	resetcounters コマンドによる最後のカウンタ リセット以降
<b>Uptime</b>	最後のシステム リポート以降
<b>Lifetime</b>	Cisco IronPort アプライアンスの存続期間中の合計

表 6-1 に、Cisco IronPort アプライアンスをモニタするときに使用できるカウンタとその説明を示します。



(注)

これは、全体的なリストです。表示されるカウンタは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 6-1                   カウンタ

統計	説明
<b>Receiving</b>	
<b>Messages Received</b>	配信キューに受信されたメッセージ。
<b>Recipients Received</b>	受信されたすべてのメッセージの受信者。
<b>Generated Bounce Recipients</b>	システムによってバウンスが生成され、配信キューに挿入された対象の受信者。

表 6-1 カウンタ (続き)

統計	説明
<b>Rejection</b>	
<b>Rejected Recipients</b>	Recipient Access Table (RAT; 受信者アクセス テーブル) によって、または早期接続終了などの予期しないプロトコル ネゴシエーションによって配信キューへの受信を拒否された受信者。
<b>Dropped Messages</b>	フィルタ ドロップ アクションの一致によって配信キューへの受信を拒否されたメッセージ、またはブラック ホール キューイング リスナーによって受信されたメッセージ。エイリアス テーブル内の /dev/null エントリ宛てのメッセージは、ドロップされたメッセージと見なされます。アンチスパム フィルタリング (システムでイネーブルになっている場合) によってドロップされたメッセージも、このカウンタに計上されます。
<b>Queue</b>	
<b>Soft Bounced Events</b>	ソフト バウンス イベントの数。複数回ソフト バウンスしたメッセージには、複数のソフト バウンス イベントが設定されます。
<b>Completion</b>	
<b>Completed Recipients</b>	ハード バウンスされた受信者、配信された受信者、および削除された受信者の総合計。配信キューから削除されたすべての受信者。
<b>Hard Bounced Recipients</b>	DNS ハード バウンス、5XX ハード バウンス、フィルタ ハード バウンス、期限切れハード バウンス、およびその他のハード バウンスの総合計。受信者へのメッセージの配信に失敗し、配信がただちに終了となったものを表します。
<b>DNS Hard Bounces</b>	受信者へのメッセージの配信試行中に検出された DNS エラー。
<b>5XX Hard Bounces</b>	受信者へのメッセージの配信試行中に、宛先メールサーバから「5XX」応答コードが返されたものを表します。
<b>Expired Hard Bounces</b>	配信キューに許容されている最大時間、または最大接続試行回数を超えているメッセージ受信者。

表 6-1 カウンタ (続き)

統計	説明
<b>Filter Hard Bounces</b>	一致フィルタの bounce アクションによってプリエンプトされた受信者の配信。アンチスパム フィルタリング (システムでイネーブルになっている場合) によってドロップされたメッセージも、このカウンタに計上されます。
<b>Other Hard Bounces</b>	メッセージ配信中の予期しないエラー。または、メッセージ受信者が <code>bouncerecipients</code> コマンドによって明示的にバウンスされたものを表します。
<b>Delivered Recipients</b>	メッセージが正常に配信された受信者。
<b>Deleted Recipients</b>	<code>deleterecipients</code> コマンドによって明示的に削除されたメッセージ受信者、またはグローバル配信停止リストに合致するメッセージ受信者の合計。
<b>Global Unsubscribe Hits</b>	グローバル配信停止設定との一致により削除されたメッセージ受信者。
<b>Current IDs</b>	
<b>Message ID (MID)</b>	配信キューに挿入されたメッセージに割り当てられた最後のメッセージ ID。MID は、Cisco IronPort アプライアンスによって受信されたすべてのメッセージに関連付けられており、メール ログで追跡できます。MID は、 $2^{31}$ でゼロにリセットされます。
<b>Injection Connection ID (ICID)</b>	リスナー インターフェイスへの接続に割り当てられた最後のインジェクション接続 ID。ICID は $2^{31}$ でロール オーバー (ゼロにリセット) されます。
<b>Delivery Connection ID (DCID)</b>	宛先メール サーバへの接続に割り当てられた最後の配信接続 ID。DCID は $2^{31}$ でロール オーバー (ゼロにリセット) されます。

## ゲージの読み取り

ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

表 6-2 に、Cisco IronPort アプライアンスをモニタするときを使用できるゲージとその説明を示します。



(注) これは、全体的なリストです。表示されるゲージは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 6-2 ゲージ

統計	説明
<b>System Gauges</b>	
<b>RAM Utilization</b>	システムによる物理 Random Access Memory (RAM; ランダム アクセス メモリ) の使用率。
<b>CPU Utilization</b>	CPU 使用率。
<b>Disk I/O Utilization</b>	ディスク I/O の使用率。  (注) Disk I/O Utilization ゲージには、既知の値の測定は表示されません。このゲージには、これまでにシステムで確認され、最後のレポート以降の最大値に対して測定された I/O 使用率が表示されます。したがって、ゲージに 100 % と表示されている場合、システムでは起動後最も高いレベルの I/O 使用率が発生しています (必ずしも、システム全体の 100 % の物理ディスク I/O を表すものではありません)。
<b>Resource Conservation</b>	0 ~ 60 または 999 の値。0 ~ 60 の数値は、重要なシステム リソースの急速な消費を防止するために、システムがメッセージの受け入れを減らしている度合いを表しています。数値が大きいほど、受け入れを減らす度合いが大きくなります。ゼロは、受け入れの減少がないことを示します。このゲージに 999 と表示されている場合、システムは「リソース節約モード」になっており、メッセージは受け入れられません。システムがリソース節約モードかどうかに関係なく、アラート メッセージは送信されます。
<b>Disk Utilization: Logs</b>	ログに使用されているディスクの割合。ステータスログには <code>logUsd</code> 、XML ステータスには <code>log_used</code> として表示されます。

表 6-2 ゲージ (続き)

統計	説明
<b>Connections Gauges</b>	
<b>Current Inbound Connections</b>	リスナー インターフェイスへの現在の着信接続。
<b>Current Outbound Connections</b>	宛先メール サーバへの現在の発信接続。
<b>Queue Gauges</b>	
<b>Active Recipients</b>	配信キュー内のメッセージ受信者。Unattempted Recipients と Attempted Recipients の合計。
<b>Unattempted Recipients</b>	Active Recipients のサブカテゴリ。配信がまだ試行されていない、キュー内のメッセージ受信者。
<b>Attempted Recipients</b>	Active Recipients のサブカテゴリ。試行されたものの、ソフトバウンス イベントによって失敗した配信の対象となっている、キュー内のメッセージ受信者。
<b>Messages in Work Queue</b>	キューに入る前に、エイリアス テーブル拡張、マスカレード、アンチスパム、アンチウイルス スキャン、メッセージフィルタ、および LDAP クエリーによる処理を待つメッセージの数。
<b>Messages in Quarantine</b>	検疫エリア内にあるメッセージに、解放または削除されたが実際の処理がまだ行われていないメッセージを足した一意の数。たとえば、Outbreak からすべての検疫対象メッセージを解放すると、Outbreak の合計メッセージ数はただちにゼロになりますが、このフィールドでは、完全に配信されるまでの検疫対象メッセージが反映されます。

表 6-2 ゲージ (続き)

統計	説明
<b>Destinations in Memory</b>	<p>メモリ内の宛先ドメインの数。メッセージの配信先となる各ドメインに対して、宛先オブジェクトがメモリ内に作成されます。そのドメインに対するすべてのメールが配信された後、宛先オブジェクトは 3 時間保持されます。3 時間のうちに、そのドメインに対して新しいメッセージがバインドされなければ、オブジェクトは期限切れとなり、宛先は (toposts コマンドなどで) 報告されなくなります。1 つのドメインだけにメールを配信する場合、このカウンタは「1」になります。メッセージを送信したことがない (または、長い時間アプライアンスによってメッセージが処理されていない) 場合、カウンタは「0」になります。</p> <p>仮想ゲートウェイを使用している場合、各仮想ゲートウェイの宛先ドメインには別個の宛先オブジェクトが作成されます (たとえば、3 つの異なる仮想ゲートウェイから yahoo.com に配信している場合、yahoo.com が 3 つの宛先オブジェクトとしてカウントされます)。</p>
<b>Kilobytes Used</b>	使用されるキュー ストレージ (キロバイト単位)。
<b>Kilobytes in Quarantine</b>	<p>検疫対象メッセージに使用されるキュー ストレージ。メッセージサイズと、上記の Messages in Quarantine にカウントされている受信者ごとに 30 バイトを足した値になります。この計算では通常、使用されるスペースが過大に見積もられます。</p>
<b>Kilobytes Free</b>	残りのキュー ストレージ (キロバイト単位)。

## レートを読み取り

すべてのレートは、クエリーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。

たとえば、IronPort アプライアンスが 1 分で 100 の受信者を受信すると、1 分間隔に対するレートは 1 時間あたり 6,000 となります。5 分間隔に対するレートは 1 時間あたり 1,200 となり、15 分間隔に対するレートは 1 時間あたり 400 となります。レートは、1 分間のレートが継続した場合の 1 時間あたりの平均レートを示すように計算されます。したがって、1 分で 100 件のメッセージのほうが 15 分で 100 件のメッセージよりもレートは高くなります。

表 6-3 に、Cisco IronPort アプライアンスをモニタするときを使用できるレートとその説明を示します。



(注)

これは、全体的なリストです。表示されるレートは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 6-3 レート

統計	説明
<b>Messages Received</b>	1 時間あたりに配信キューに挿入されるメッセージのレート。
<b>Recipients Received</b>	1 時間あたりに配信キューに挿入されるすべてのメッセージに対する受信者数のレート。
<b>Soft Bounced Events</b>	1 時間あたりのソフト バウンス イベント数のレート (複数回ソフト バウンスしたメッセージには、複数のソフト バウンス イベントが設定されます)。
<b>Completed Recipients</b>	ハード バウンスされた受信者、配信された受信者、および削除された受信者の総合計のレート。配信キューから削除された受信者は、完了済みと見なされます。
<b>Hard Bounced Recipients</b>	1 時間あたりの DNS ハード バウンス、5XX ハード バウンス、フィルタ ハード バウンス、期限切れハード バウンス、およびその他のハード バウンスの総合計のレート。ハード バウンスとは、受信者へのメッセージの配信試行に失敗し、その配信がただちに終了されることをいいます。
<b>Delivered Recipients</b>	受信者に正常に配信された 1 時間あたりのメッセージ数のレート。



# CLI によるモニタリング

ここでは、次の内容について説明します。

- 「電子メール ステータスのモニタリング」 (P.6-239)
- 「詳細な電子メール ステータスのモニタリング」 (P.6-242)
- 「メール ホストのステータスのモニタリング」 (P.6-247)
- 「電子メール キューの構成の確認」 (P.6-253)
- 「リアルタイム アクティビティの表示」 (P.6-255)
- 「着信電子メール接続のモニタリング」 (P.6-258)
- 「DNS ステータスの確認」 (P.6-261)
- 「電子メール モニタリング カウンタのリセット」 (P.6-262)

## 電子メール ステータスのモニタリング

Cisco IronPort アプライアンスにおける電子メール動作のステータスをモニタすることが必要になることがあります。status コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返された統計情報は、カウンタとゲージのいずれかの形式で表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リポート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

各項目の説明については、「使用可能なモニタリング コンポーネントの読み取り」 (P.6-231) を参照してください。

表 6-4 メール ステータス

統計	説明
Status as of	現在のシステム日時を表示します。
Last counter reset	カウンタが最後にリセットされた時刻を表示します。

表 6-4 メール ステータス (続き)

統計	説明
<b>System status</b>	online、offline、receiving suspended、または delivery suspended。ステータスが receiving suspended になるのは、すべてのリスナーが一時停止した場合のみです。すべてのリスナーに対する受信と配信が一時停止されると、ステータスは offline になります。
<b>Oldest Message</b>	システムによる配信を待つ、最も古いメッセージを表示します。
<b>Features</b>	featurekey コマンドによってシステムにインストールされた特別な機能を表示します。

## 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:
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>

```

## 詳細な電子メール ステータスのモニタリング

status detail コマンドは、電子メール動作についてモニタされた詳細な情報を返します。返された統計情報は、カウンタ、レート、およびゲージのいずれかのカテゴリで表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リポート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。すべてのレートは、クエ

リーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。各項目の説明については、「[使用可能なモニタリング コンポーネントの読み取り](#)」(P.6-231) を参照してください。

## 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 - Virus 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



(注)

新たにインストールされたアプライアンスでは、最も古いメッセージカウンタにメッセージが示される場合がありますが、実際にはカウンタに示される受信者はありません。リモートホストが接続されており、メッセージの受信が非常に遅い（つまり、メッセージを受信するまでに数分かかる）場合には、受信された受信者カウンタに「0」と表示され、最も古いメッセージカウンタに「1」と表示されることがあります。これは、最も古いメッセージカウンタに進行中のメッセージが表示されるためです。接続が最終的にドロップされると、カウンタはリセットされます。

## メールホストのステータスのモニタリング

特定の受信者ホストへの配信に問題があると思われる場合や、仮想ゲートウェイアドレスに関する情報を収集する場合には、`hoststatus` コマンドを実行するとそれらの情報を表示できます。`hoststatus` コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。コマンドには、取得するホスト情報のドメインを入力する必要があります。**AsyncOS** キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した `resetcounters` コマンドからの累積です。返される統計情報は、カウンタとゲージの 2 つのカテゴリに表示されます。各項目の説明については、「[使用可能なモニタリングコンポーネントの読み取り](#)」(P.6-231) を参照してください。

また、`hoststatus` コマンドに固有のその他のデータも返されます。

表 6-5 `hoststatus` コマンドのその他のデータ

統計	説明
<b>Pending Outbound Connections</b>	開いている接続や作業中の接続とは対照的な、宛先メール ホストへの保留中、または「初期」接続。Pending Outbound Connections は、プロトコルのグリーティングの段階にまだ達していない接続です。
<b>Oldest Message</b>	このドメインに対する配信キュー内で最も古いアクティブ受信者の経過時間。このカウンタは、ソフトバウンス イベントやホストの停止によって配信できない、キュー内のメッセージの経過時間を判断するのに役立ちます。
<b>Last Activity</b>	このフィールドは、そのホストにメッセージ配信が試みられるたびに更新されます。
<b>Ordered IP Addresses</b>	このフィールドには、IP アドレスの Time To Live (TTL; 存続可能時間)、MX レコードに応じた IP アドレスの優先順位、および実際のアドレスが表示されます。MX レコードは、ドメインに対するメール サーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。
<b>Last 5XX error</b>	このフィールドには、ホストから返された最新の「5XX」ステータスコードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。
<b>MX Records</b>	MX レコードは、ドメインに対するメール サーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。
<b>SMTP Routes for this host</b>	このドメインに対して SMTP ルートが定義されている場合は、ここに表示されます。
<b>Last TLS Error</b>	このフィールドには、最新の発信 TLS 接続エラーの説明と、アプライアンスが確立を試みた TLS 接続のタイプが表示されます。このフィールドが表示されるのは、TLS エラーが存在する場合のみです。

## 仮想ゲートウェイ

次に示す仮想ゲートウェイ情報は、仮想ゲートウェイ アドレスを設定している場合のみ表示されます (『Cisco IronPort AsyncOS for Email Configuration Guide』の「Configuring the Gateway to Receive Email」を参照してください)。

表 6-6 hoststatus コマンドのその他の仮想ゲートウェイ データ

統計	説明
Host up/down	同じ名前のグローバル hoststatus フィールドと同じ定義。仮想ゲートウェイ アドレスごとに追跡されます。
Last Activity	同じ名前のグローバル hoststatus フィールドと同じ定義。仮想ゲートウェイ アドレスごとに追跡されます。
Recipients	このフィールドも、グローバル hoststatus コマンドの定義に対応します。Active Recipients フィールド：仮想ゲートウェイ アドレスごとに追跡されます。
Last 5XX error	このフィールドには、ホストから返された最新の 5XX ステータス コードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。

## 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
```

**(注)**

仮想ゲートウェイ アドレス情報は、altsrchoost 機能を使用している場合のみ表示されます。

## 電子メール キューの構成の確認

電子メール キューに関する現在の情報を取得し、特定の受信者ホストに配信の問題（キューの増大など）があるかどうかを判断するには、`tophosts` コマンドを使用します。`tophosts` コマンドは、キュー内の上位 20 の受信者のリストを返します。リストは、アクティブ受信者、発信接続、配信済み受信者、ソフトバウンス イベント、およびハードバウンスされた受信者など、さまざまな統計情報別にソートできます。各項目の説明については、「[使用可能なモニタリング コンポーネントの読み取り](#)」(P.6-231) を参照してください。

## 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>
```



## リアルタイム アクティビティの表示

Cisco IronPort アプライアンスではリアルタイム モニタリングが可能であり、システムにおける電子メール アクティビティの進捗状況を確認できます。rate コマンドは、電子メール動作に関するリアルタイム モニタリング情報を返します。この情報は、ユーザが指定した間隔で定期的に更新されます。rate コマンドを停止するには、Ctrl+C を使用します。

表 6-7 に、表示されるデータを示します。

表 6-7 rate コマンドのデータ

統計	説明
Connections In	着信接続の数。
Connections Out	発信接続の数。
Recipients Received	システムに受信された受信者の合計数。
Recipients Completed	完了した受信者の合計数。
Delta	最後のデータ アップデート以降変化した、Received 受信者数および Completed 受信者数の差異。
Queue Used	メッセージ キューのサイズ (キロバイト単位)。

## 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 コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。この情報は、status detail コマンドのサブセットです（「[詳細な電子メール ステータスのモニタリング](#)」(P.6-242) を参照）。

表 6-8 hostrate コマンドのデータ

統計	説明
<b>Host Status</b>	特定のホストの現在のステータス (up、down、または unknown)。
<b>Current Connections Out</b>	ホストに対する現在の発信接続数。
<b>Active Recipients in Queue</b>	キュー内の特定のホストに対するアクティブ受信者の合計数。
<b>Active Recipients in Queue Delta</b>	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するアクティブ受信者の合計数の差異。
<b>Delivered Recipients Delta</b>	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対する配信済み受信者の合計数の差異。
<b>Hard Bounced Recipients Delta</b>	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するハード バウンスされた受信者の合計数の差異。
<b>Soft Bounce Events Delta</b>	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するソフト バウンスされた受信者の合計数の差異。

hostrate コマンドを停止するには、Ctrl+C を使用します。

## 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 0	up	1	0	0	4	0	
23:38:24 0	up	1	0	0	4	0	
23:38:25 0	up	1	0	0	12	0	

^C

## 着信電子メール接続のモニタリング

大量の送信者を識別するため、またはシステムへの着信接続をトラブルシューティングするために、Cisco IronPort アプライアンスに接続しているホストのモニタが必要になる場合があります。topin コマンドは、システムに接続しているリモートホストのスナップショットを示します。このスナップショットには、特定のリスナーに接続しているリモート IP アドレスごとに 1 つの行を持つテーブルが表示されます。同じ IP アドレスから異なるリスナーへの 2 つの接続に対

しては、テーブルに 2 つの行が作成されます。表 6-9 に、`topin` コマンドを使用したときに表示されるフィールドの説明を示します。

**表 6-9 topin コマンドのデータ**

統計	説明
<b>Remote Hostname</b>	リモートホストのホスト名。リバース DNS ルックアップによって取得されます。
<b>Remote IP Address</b>	リモートホストの IP アドレス。
<b>listener</b>	接続を受信している、Cisco IronPort アプライアンス上のリスナーのニックネーム。
<b>Connections In</b>	コマンドが実行されたときに開いていた、指定の IP アドレスを持つリモートホストからの同時接続数。

システムは、リバース DNS ルックアップによってリモートホスト名を検索してから、フォワード DNS ルックアップによってその名前を検証します。フォワードルックアップで元の IP アドレスにならない場合、またはリバース DNS ルックアップに失敗した場合、テーブルのホスト名カラムには IP アドレスが表示されます。送信者検証プロセスの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Sender Verification」を参照してください。

## 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

## DNS ステータスの確認

`dnsstatus` コマンドは、DNS ルックアップおよびキャッシュ情報の統計を表示するカウンタを返します。カウンタごとに、そのカウンタの最後のリセット以降、最後のシステム リポート以降、およびシステムの存続期間中に発生したイベントの合計数を表示できます。

表 6-10 に、使用可能なカウンタを示します。

表 6-10 `dnsstatus` コマンドのデータ

統計	説明
<b>DNS Requests</b>	ドメイン名を解決するためのシステム DNS キャッシュに対する上位レベルの非反復要求。
<b>Network Requests</b>	DNS 情報を取得するためのネットワーク（非ローカル）への要求。
<b>Cache Hits</b>	レコードが検出されて返された、DNS キャッシュへの要求。
<b>Cache Misses</b>	レコードが検出されなかった、DNS キャッシュへの要求。
<b>Cache Exceptions</b>	レコードが検出されたものの、ドメインが不明である、DNS キャッシュへの要求。
<b>Cache Expired</b>	レコードが検出された、DNS キャッシュへの要求。  キャッシュでは、使用状況が考慮され、古すぎるレコードは破棄されます。  Time To Live (TTL; 存続可能時間) を超えていても、多くのエントリがキャッシュに存在する場合があります。これらのエントリは使用されない限り、期限切れカウンタには含まれません。キャッシュがフラッシュされると、有効なエントリと無効（古すぎる）エントリの両方が削除されます。フラッシュ動作によって、期限切れカウンタが変更されることはありません。

## 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>
```

## 電子メール モニタリング カウンタのリセット

`resetcounters` コマンドは、累積する電子メール モニタリング カウンタをリセットします。リセットは、グローバル カウンタとホスト単位のカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。



(注) GUI で、カウンタをリセットすることもできます。[「\[System Status\] ページ \(P.2-66\)」](#) を参照してください。



## 例

```
mail3.example.com> resetcounters
```

```
Counters reset: Mon Jan 01 12:00:01 2003
```

# 電子メール キューの管理

IronPort AsyncOS では、電子メール キュー内のメッセージに対する動作を実行できます。電子メール キュー内のメッセージは、削除、バウンス、一時停止、またはリダイレクトすることができます。また、キュー内の古いメッセージを検索、削除、およびアーカイブすることもできます。

## キュー内の受信者の削除

特定の受信者が配信されていない場合や、電子メール キューをクリアする場合には、`deleterecipients` コマンドを使用します。`deleterecipients` コマンドでは、配信を待つ特定の受信者を削除することによって、電子メール配信キューを管理できます。削除される受信者は、受信者の宛先である受信者ホストによって、または、メッセージエンベロープの **Envelope From** 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージ（すべてのアクティブ受信者）を一度に削除することもできます。



(注)

---

`deleterecipients` 機能を実行するには、IronPort アプライアンスをオフラインまたは配信一時停止の状態にすることを推奨します（「[IronPort アプライアンスをメンテナンス状態にする](#)」(P.8-317) を参照）。

---



(注)

---

この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

---

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルドカードは使用できません。deleterecipients コマンドは、削除されるメッセージの合計数を返します。また、メール ログ サブスクリプション (IronPort テキスト形式のみ) が設定されている場合、メッセージの削除は別個の行としてログに記録されます。

## 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]>
```

Cisco IronPort アプライアンスには、必要に応じて受信者を削除するための各種のオプションが用意されています。次に、受信者ホスト別の受信者の削除、Envelope From アドレスによる削除、およびキュー内のすべての受信者の削除の例を示します。

## 受信者ドメインによる削除

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.

## Envelope From アドレスによる削除

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.

## すべて削除

```
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.
```

## キュー内の受信者のバウンス

`deleterecipients` コマンドと同様に、`bouncerecipients` コマンドでは、配信を待つ特定の受信者をハードバウンスすることによって、電子メール配信キューを管理できます。メッセージのバウンスは、`bounceconfig` コマンドに指定された通常のバウンスメッセージ設定に従います。



**(注)** `bouncerecipients` 機能を実行するには、**IronPort** アプライアンスをオフラインまたは配信一時停止の状態にすることを推奨します（「[IronPort アプライアンスをメンテナンス状態にする](#)」(P.8-317) を参照）。



**(注)** この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルドカードは使用できません。`bouncerecipients` コマンドは、バウンスされたメッセージの合計数を返します。



**(注)** `bouncerecipients` 機能ではリソースが集中的に使用され、完了までに数分かかる場合があります。オフラインまたは配信一時停止の状態の場合は、バウンスメッセージの実際の送信（ハードバウンス生成がオンの場合）は、`resume` コマンドを使用して **IronPort AsyncOS** をオンライン状態にした後でのみ開始されません。

## 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]>
```

バウンスされる受信者は、宛先受信者ホストによって、またはメッセージエンベロープの **Envelope From** 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージを一度にバウンスすることもできます。

## 受信者ホストによるバウンス

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.

## Envelope From アドレスによるバウンス

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.

## すべてバウンス

Are you sure you want to bounce all messages in the queue? [N]> **Y**

```
Bouncing messages, please wait.
```

```
1000 messages bounced.
```

## 電子メール配信の一時停止

メンテナンスやトラブルシューティングのために電子メールの配信を一時的に停止するには、`suspenddel` コマンドを使用します。`suspenddel` コマンドは、IronPort AsyncOS を配置一時停止の状態にします。この状態には、次のような特徴があります。

- 発信電子メール配信は停止されます。
- 着信電子メール接続は受け入れられます。
- ログ転送は続行します。
- CLI はアクセス可能のままになります。

`suspenddel` コマンドを実行すると、開いていた発信接続が閉じられ、新規の接続は開かれません。`suspenddel` コマンドはただちに開始され、確立しているすべての接続を正常に閉じることができます。配信一時停止の状態から通常の動作に戻すには、`resumedel` コマンドを使用します。



(注)

---

「`delivery suspend`」状態は、システムをリブートしても保持されます。`suspenddel` コマンドを使用してからアプライアンスをリブートする場合は、`resumedel` コマンドを使用してリブートしてから配信を再開する必要があります。

---

## 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.
```

## 電子メール配信の再開

`resumedel` コマンドは、`suspenddel` コマンドの使用後に IronPort AsyncOS を通常の動作状態に戻します。

## 構文

```
resumedel
```

```
mail3.example.com> resumedel
```

```
Mail delivery resumed.
```

## 受信の一時停止

すべてのリスナーに対して 電子メールの受信を一時停止するには、`suspendlistener` コマンドを使用します。受信が一時停止されている間、システムはリスナーの特定のポートへの接続を受け入れません。



これは、このリリースの AsyncOS で変更された動作です。以前のリリースでは、システムは接続を受け入れ、次のように応答してから接続解除していました。

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



(注)

「receiving suspend」状態は、システムをリブートしても保持されます。suspendlistener コマンドを使用してからアプライアンスをリブートする場合、リスナーでメッセージの受信を再開するには、resumelister コマンドを使用する必要があります。

## 構文

```
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>
```

## 受信の再開

`resumedlistener` コマンドは、`suspendlistener` コマンドの使用後に IronPort AsyncOS を通常の動作状態に戻します。

### 構文

```
resumelister

mail3.example.com> resumelister

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>
```

## 配信および受信の再開

resume コマンドは、配信と受信の両方を再開します。

### 構文

```
resume

mail3.example.com> resume

Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

## 電子メールの即時配信スケジュール

delivernow コマンドを使用すると、後で配信するようにスケジュールされた受信とホストをただちに再試行できます。delivernow コマンドでは、キュー内の電子メールに即時配信を再スケジュールすることができます。down のマークが付いたすべてのドメインと、スケジュールされたメッセージまたはソフトバウンズされたメッセージが、即時配信のキューに入れられます。

delivernow コマンドは、キュー内の（スケジュールされた、およびアクティブな）すべての受信者または特定の受信者に対して呼び出すことができます。特定の受信者を選択する際は、即時配信をスケジュールする受信者のドメイン名を入力する必要があります。システムは、文字列全体の文字と長さを照合します。

### 構文

```
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>
```

## 作業キューの休止

LDAP 受信者アクセス、マスカレード、LDAP 再ルーティング、メッセージフィルタ、アンチスパム、およびアンチウイルス スキャン エンジンの処理は、すべて「作業キュー」で実行されます。処理フローについては『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」、および「Messages in Work Queue」ゲージの説明については表 6-2 (P.235) を参照してください。workqueue コマンドを使用して、作業キュー部分のメッセージ処理を手動で休止することができます。

たとえば、多くのメッセージが作業キュー内にあるときに、LDAP サーバの設定を変更する必要があるとします。おそらく、LDAP 受信者アクセス クエリーに基づいて、メッセージをバウンスからドロップに切り替えようとしています。または、キューを休止して、最新のアンチウイルス スキャン エンジンの定義ファイルを手動で確認 (antivirusupdate コマンドを使用) する可能性もあります。workqueue コマンドを使用すると、作業キューを休止してから再開することで、処理を停止した状態で他の設定変更を行うことができます。

作業キューを休止してから再開すると、そのイベントがログに記録されます。次に例を示します。

```
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
```

次の例では、作業キューが中止されます。

```
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
```

**(注)**

---

理由の入力は任意です。理由を入力しないと、その理由は [Manually paused by user] としてログに記録されます。

---

次の例では、作業キューが再開されます。

```
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
```

## 古いメッセージの検索およびアーカイブ

時折、古くなったメッセージが配信できずに、キューに留まっていることがあります。これらのメッセージは削除したり、アーカイブしたりすることができます。これには、`showmessage` CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージを表示します。`oldmessage` CLI コマンドを使用すると、システム上の最も古い非検疫メッセージが表示されます。その後は、任意で `removemessage` を使用して、所定のメッセージ ID に対応するメッセージを安全に削除できます。このコマンドでは、作業キュー、再試行キュー、または宛先キュー内のメッセージのみを削除できます。メッセージがこれらのキューのいずれにもない場合は、削除できません。

また、`archivemessage[mid]` CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージをコンフィギュレーションディレクトリ内の `mbox` ファイルにアーカイブすることもできます。

`oldmessage` コマンドを使用して、システム検疫内のメッセージのメッセージ ID を取得することはできません。ただし、メッセージ ID がわかっている場合は、指定のメッセージを表示したり、アーカイブしたりすることができます。メッセージが作業キュー、再試行キュー、または宛先キューにないと、`removemessage` コマンドでメッセージを削除することはできません。



(注)

IronPort スпам検疫内のメッセージに対しては、これらのキュー管理コマンドを実行できません。

## 構文

```
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>
```

## 構文

```
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>
```

## システム内のメッセージのトラッキング

findevent CLI コマンドは、オンボックスのメール ログ ファイルを使用して、システム内のメッセージのトラッキング（追跡）プロセスを容易にします。findevent CLI コマンドを使用すると、メッセージ ID の検索、またはサブジェクト ヘッダー、エンベロープ送信者、またはエンベロープ受信者に対する正規表現の一致検索によって、メール ログから特定のメッセージを検索できます。



現在のログ ファイルやすべてのログ ファイルの結果を表示することも、ログ ファイルを日付別で表示することもできます。ログ ファイルを日付別で表示する場合は、特定の日付か、日付の範囲を指定できます。

ログを表示するメッセージを識別した後は、`findevent` コマンドによって、分裂情報（分裂したログ メッセージ、バウンス、およびシステム生成メッセージ）を含む、そのメッセージ ID に対するログ情報を表示できます。次に、`findevent` CLI コマンドで、サブジェクト ヘッダーに「**confidential**」とあるメッセージの受信と配信を追跡する例を示します。

```
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
```

## SNMP モニタリング

IronPort AsyncOS オペレーティング システムは、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) を使ったシステム ステータスのモニタリングをサポートしています。これには、IronPort のエンタープライズ MIB、ASYNCOS-MAIL-MIB が含まれます。ASYNCOS-MAIL-MIB を使用することで、管理者は、システムの状態をモニタしやすくなります。また、

このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています (SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください)。次の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作 (コンフィギュレーション) は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。
- このサービスをイネーブルにするには、パスワード認証と DES 暗号化を伴う SNMPv3 の使用が必須です (SNMPv3 の詳細については、RFC 2571 ~ 2575 を参照してください)。SNMP システム ステータスのモニタリングをイネーブルにするには、少なくとも 8 文字の SNMPv3 パスフレーズを設定する必要があります。最初に SNMPv3 パスフレーズを入力するときは、確認のためにそのパスフレーズを再入力する必要があります。次に snmpconfig コマンドを実行するときは、コマンドにこのフレーズが「記憶」されています。
- SNMPv3 ユーザ名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティ スtring を設定する必要があります。コミュニティ スtring は、public にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- トラップを使用するには、SNMP マネージャ (AsyncOS には含まれていません) が実行中であり、その IP アドレスがトラップ ターゲットとして入力されている必要があります (ホスト名を使用できますが、その場合、トラップは DNS が動作しているときに限り機能します)。

snmpconfig コマンドを使用して、アプライアンスの SNMP システム ステータスを設定します。インターフェイスの値を選択し、設定し終わると、アプライアンスは SNMPv3 GET 要求に応答します。これらのバージョン 3 要求には、一致するパスワードが含まれている必要があります。デフォルトでは、バージョン 1 および 2 要求は拒否されます。イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティ スtring が含まれている必要があります。

## MIB ファイル

IronPort システムには、「Structure of Management Information」(SMI) ファイルとして「エンタープライズ」MIB が装備されています。

- ASYNCOS-MAIL-MIB.txt : IronPort アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- IRONPORT-SMI.txt : IronPort の SNMP 管理対象製品における ASYNCOS-MAIL-MIB の役割を定義します。

これらのファイルは、Cisco IronPort アプライアンスに付属のドキュメンテーション CD に収録されています。また、IronPort カスタマー サポートを通じてこれらのファイルを要求することもできます。

## ハードウェア オブジェクト

Intelligent Platform Management Interface Specification (IPMI) 準拠のハードウェア センサーが温度、ファン スピード、および電源モジュール ステータスを報告します。

表 6-11 に、どのモデルでどのハードウェア派生オブジェクトをモニタリングに使用できるかを示します。表示されている数字は、モニタできるオブジェクトのインスタンスの数です。たとえば、C10 アプライアンスの 3 つのファン、および C300/C600/X1000 アプライアンスの 6 つのファンについてクエリーを送信できます。

表 6-11 IronPort アプライアンスごとのハードウェア オブジェクトの数

モデル	CPU 温度	周囲 温度	バック プレーン 温度	ライザー 温度	ファン	電源ス テータス	ディスク ステータス	NIC リンク
C10/100	1	1	0	0	3	0	2	2
C30/C60	0	0	0	0	0	0	2 (C60 は 4)	3

表 6-11 IronPort アプライアンスごとのハードウェア オブジェクトの数 (続き)

モデル	CPU 温度	周囲 温度	バック プレーン 温度	ライザー 温度	ファン	電源ス テータス	ディスク ステータス	NIC リンク
C300/ C600/ X1000	2	1	1	1	6	2	4 (C300 は 2)	3 (ファイバー インターフェ イス搭載の C600 と X1000 の場合は 5)
C350/ C650/ X1050	2	1	0	0	4	2	4 (C350 は 2)	3 (ファイバー インターフェ イス搭載の C650 と x1050 の場合は 5)

いずれのモデルでも、SNMP を使用してディスク ドライブの状態とネットワーク インターフェイスのリンク ステータスをモニタできます。

## ハードウェア トラップ

表 6-12 に、ハードウェア トラップが送信される温度およびハードウェアの条件を示します。

表 6-12 ハードウェア トラップ：温度およびハードウェアの条件

モデル	高温 (CPU)	高温 (周囲)	高温 (バック プレーン)	高温 (ラ イザー)	ファン 障害	電源 モジュール	RAID	リンク
C10/ C100	90C	47C	NA	NA	0 RPM	ステータス 変更	ステータス 変更	ステータス 変更
C30/ C60	NA	NA	NA	NA	NA	NA	ステータス 変更	ステータス 変更
C300/ C600/ X1000	90C	47C	72C	62C	0 RPM	ステータス 変更	ステータス 変更	ステータス 変更
C350/ C650/ X1050	90C	47C	NA	NA	0 RPM	ステータス 変更	ステータス 変更	ステータス 変更

ステータス変更トラップは、ステータスが変更されると送信されます。ファン障害および高温トラップは、5 秒ごとに送信されます。その他のトラップは、障害条件アラームトラップです。これらのトラップは、ステータスが（良好から障害へ）変更されたときに一度だけ送信されます。ハードウェアステータステーブルにポーリングを送信して、致命的な状況になる前に潜在的なハードウェア障害を識別することを推奨します。重大値の 10 % 以内の温度を不安原因と考えることができます。

障害条件アラームトラップは、個々のコンポーネントの致命的な障害を示しますが、システム全体の障害の原因になるとは限りません。たとえば、C600 アプライアンスで 1 つのファンまたは電源モジュールに障害が発生しても、アプライアンスは動作し続けます。

## SNMP トラップ

SNMP には、1 つまたは複数の条件が満たされたときに管理アプリケーション（通常は、SNMP 管理コンソール）に知らせるためのトラップ（または通知）を送信する機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワークパケットです。トラップは、SNMP エージェント（この場合は Cisco IronPort アプライアンス）である条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、標準の SNMP トラップポートであるポート 162 経由で送信します。次の例では、トラップターゲット `snmp-monitor.example.com` およびトラップコミュニティストリングが入力されています。これは、IronPort アプライアンスから SNMP トラップを受信する SNMP 管理コンソールソフトウェアを実行しているホストです。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブルまたはディセーブルに）できます。トラップターゲットの入力を求められたときに、複数のトラップターゲットを指定するには、カンマで区切った IP アドレスを 10 個まで入力できます。

## CLI の例

次の例では、`snmpconfig` コマンドを使用して、ポート 161 の「PublicNet」インターフェイスで SNMP をイネーブルにしています。バージョン 3 のパスフレーズが入力され、確認のために再入力されています。システムは、バージョン 1 および 2 要求を処理するように設定されており、これらのバージョン 1 および 2 か

らの GET 要求に対してコミュニティ ストリング `public` が入力されています。トラップ ターゲット `snmp-monitor.example.com` が入力されています。最後に、システムの場所と連絡先情報が入力されています。

```
mail3.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? [N]> y
```

```
Please choose an IP interface for SNMP requests.
```

```
1. Data 1 (192.168.1.1/24: mail3.example.com)
```

```
2. Data 2 (192.168.2.1/24: mail3.example.com)
```

```
3. Management (192.168.44.44/24: mail3.example.com)
```

```
[1]>
```

```
Enter the SNMPv3 passphrase.
```

```
>
```

```
Please enter the SNMPv3 passphrase again to confirm.
```

```
>
```

```
Which port shall the SNMP daemon listen on?
```

```
[161]>
```

```
Service SNMP V1/V2c requests? [N]> y
```

```
Enter the SNMP V1/V2c community string.
```

```
[ ]> public
```

```
From which network shall SNMP V1/V2c requests be allowed?
```

```
[192.168.2.0/24]>
```

```
Enter the Trap target (IP address recommended). Enter "None" to  
disable traps.
```

```
[None]> 10.1.1.29
```

```
Enter the Trap Community string.
```

```
[ ]> tcomm
```

```
Enterprise Trap Status
```

- |                     |         |
|---------------------|---------|
| 1. RAIDStatusChange | Enabled |
| 2. fanFailure       | Enabled |



```
3. highTemperature           Enabled
4. keyExpiration             Enabled
5. linkDown                  Enabled
6. linkUp                    Enabled
7. powerSupplyStatusChange  Enabled
8. resourceConservationMode  Enabled
9. updateFailure            Enabled
```

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

```
Do you want to disable any of these traps? [Y]>
```

```
Enter number or numbers of traps to disable. Separate multiple
numbers with commas.
```

```
[ ]> 1,8
```

```
Enterprise Trap Status
```

```
1. RAIDStatusChange         Disabled
2. fanFailure                Enabled
3. highTemperature           Enabled
4. keyExpiration             Enabled
5. linkDown                  Enabled
6. linkUp                    Enabled
```

```
7. powerSupplyStatusChange      Enabled
8. resourceConservationMode      Disabled
9. updateFailure                 Enabled
```

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

Enter the System Location string.

```
[Unknown: Not Yet Configured]> Network Operations Center - west; rack
#31, position 2
```

Enter the System Contact string.

```
[snmp@localhost]> Joe Administrator, x8888
```

Current SNMP settings:

Listening on interface "Data 1" 192.168.2.1/24 port 161.

SNMP v3: Enabled.

SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.

SNMP v1/v2 Community String: public

Trap target: 10.1.1.29

Location: Network Operations Center - west; rack #31, position 2

System Contact: Joe Administrator, x8888

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