



## CLI による管理およびモニタリング

この章は、次の項で構成されています。

- [CLI を使用した管理およびモニタリングの概要](#) (1 ページ)
- [使用可能なモニタリング コンポーネントの読み取り](#) (2 ページ)
- [CLI を使用したモニタリング](#) (8 ページ)
- [電子メール キューの管理](#) (19 ページ)
- [SNMP を使用したシステムの状態のモニタリング](#) (29 ページ)

### CLI を使用した管理およびモニタリングの概要

CLI を使用した E メールセキュリティ アプライアンスの管理およびモニタリングには次のようなタスクがあります。

- メッセージ アクティビティのモニタリング。
  - アプライアンスが電子メール パイプラインで処理している未処理メッセージ、受信者、バウンス受信者の数
  - 最後の 1 分、5 分、または 15 分の間隔に基づくメッセージ配信またはバウンス メッセージの時間レート
- システム リソースのモニタリング。次に、例を示します。
  - メモリ使用量
  - ディスク容量
  - 接続数
- 簡易ネットワーク管理プロトコル (SNMP) を使用する、システムの機能障害のモニタリング。次に、例を示します。
  - ファン障害
  - 更新の失敗
  - 異常に高いアプライアンスの温度
- パイプライン内の電子メールの管理。次に、例を示します。

- キュー内の受信者の削除
- 別のホストへのメッセージのリダイレクト
- 受信者の削除またはメッセージのリダイレクトによるキューのクリア
- 電子メールの受信、送信、またはワーク キュー処理の一時停止または再開
- 特定のメッセージの検索

## 使用可能なモニタリング コンポーネントの読み取り

- [イベントカウンタの読み取り \(2 ページ\)](#)
- [システム ゲージの読み取り \(4 ページ\)](#)
- [配信およびバウンスされたメッセージのレートの読み取り \(7 ページ\)](#)

### イベント 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、最後のシステム再起動以降、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。

リセット	<b>resetcounters</b> コマンドによる最後のカウンタ リセット以降
Uptime	最後のシステム再起動以降
保存期間 (Lifetime)	Cisco アプライアンスの存続期間中の合計

次の表に、Cisco アプライアンスをモニタするときに表示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 1: カウンタ

統計	説明
Receiving	配信キューに受信されたメッセージ。
Messages Received	
Recipients Received	受信されたすべてのメッセージの受信者。

統計	説明
Generated Bounce Recipients	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。
Rejection	
拒否した受信者	受信者アクセス テーブル (RAT) 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。
ドロップされたメッセージ	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。
キュー (Queue)	
ソフトバウンスしたイベント数	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。
Completion	
完了した受信者	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。
ハードバウンスされた受信者	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。
DNS ハードバウンス	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。
5XX ハードバウンス	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。
期限切れハードバウンス	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。

統計	説明
フィルタ ハード バウンス	一致フィルタの bounce アクションによってプリエンブ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。
その他のハード バウンス	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。
配信された受信者	メッセージが正常に配信された受信者。
削除された受信者	<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。
Global Unsubscribe Hits	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。
現在の ID	
Message ID (MID)	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 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、231 でゼロにリセットされます。
Injection Connection ID (ICID)	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 231 でロールオーバー (ゼロにリセット) されます。
Delivery Connection ID (DCID)	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 231 でロールオーバー (ゼロにリセット) されます。

## システム 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。

次の表に、Cisco 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 2: ゲージ

統計	説明
System Gauges	
RAM Utilization	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。
CPU Utilization	CPU の使用状況のパーセンテージ。
Disk I/O Utilization	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、最後の再起動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)。
Resource Conservation	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耗を防止するために、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。
Disk Utilization: Logs	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 LogUsd、XML ステータスには log_used として表示されます。
Connections Gauges	
現在のインバウンド接続	リスナー インターフェイスへの現在の着信接続。
現在のアウトバウンド接続	宛先メール サーバへの現在の発信接続。
Queue Gauges	
アクティブ受信者	配信キュー内のメッセージ受信者。Unattempted Recipients と Attempted Recipients の合計。
Unattempted Recipients	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。

統計	説明
Attempted Recipients	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。
Messages in Work Queue	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。
Messages in Quarantine	隔離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 からすべての隔離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隔離対象メッセージが反映されます。
Destinations in Memory	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つのドメインにだけメールを配信している場合は、このカウンタが「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。  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)。
Kilobytes Used	使用されるキュー ストレージ (キロバイト単位)。
Kilobytes in Quarantine	隔離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。
Kilobytes Free	残りのキュー ストレージ (キロバイト単位)。

## 配信およびバウンスされたメッセージのレートの読み取り

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、Cisco アプライアンスが1分間に100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件のメッセージの方が15分で100件のメッセージよりもレートは高くなります。

次の表に、Cisco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 3: レート

統計	説明
Messages Received	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。
Recipients Received	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。
Soft Bounced Events	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）。
Completed Recipients	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。
Hard Bounced Recipients	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。
Delivered Recipients	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を使用したモニタリング

- [電子メールステータスのモニタリング \(8 ページ\)](#)
- [詳細な電子メールステータスのモニタリング \(9 ページ\)](#)
- [メールホストのステータスのモニタリング \(11 ページ\)](#)
- [電子メールキューの構成の確認 \(14 ページ\)](#)
- [リアルタイムアクティビティの表示 \(14 ページ\)](#)
- [着信電子メール接続のモニタリング \(16 ページ\)](#)
- [DNSステータスの確認 \(17 ページ\)](#)
- [電子メールモニタリングカウンタのリセット \(18 ページ\)](#)
- [アクティブなTCP/IPサービスの識別 \(19 ページ\)](#)

## 電子メールステータスのモニタリング

Cisco 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、最後のシステム再起動以降、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、[CLIを使用した管理およびモニタリングの概要 \(1 ページ\)](#) を参照してください。

表 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。
System status	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。
Oldest Message	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。
機能	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:
  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、最後のシステム再起動以降、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、[CLIを使用した管理およびモニタリングの概要 \(1 ページ\)](#) 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 - 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表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処理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、[CLIを使用した管理およびモニタリングの概要（1ページ）](#)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 5: `hoststatus` コマンドのその他のデータ

統計	説明
Pending Outbound Connections	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ンティングの段階にまだ達していない接続です。
Oldest Message	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、ソフトバウンズ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。
Last Activity	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。

統計	説明
Ordered IP Addresses	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。
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。
MX Records	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。
SMTP Routes for this host	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。
Last TLS Error	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

次の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ず（電子メールを受信するためのゲートウェイの設定を参照してください）。

表 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 <code>hoststatus</code> フィールドと同じ定義。Virtual Gateway アドレスごとに追跡されます。
最後のアクティビティ (Last Activity)	同じ名前のグローバル <code>hoststatus</code> フィールドと同じ定義。Virtual Gateway 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 <code>hoststatus</code> 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、`altsrhost` 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、[CLIを使用した管理およびモニタリングの概要（1 ページ）](#) 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 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。

次の表に、表示されるデータを示します。

表 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。

統計	説明
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。
差分 (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 \(9 ページ\)](#) を参照）。

表 8: hostrate コマンドのデータ

統計	説明
Host Status	特定のホストの現在のステータス (up、down、または unknown)。
Current Connections Out	ホストに対する現在の発信接続数。
Active Recipients in Queue	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。
Active Recipients in Queue Delta	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。
Delivered Recipients Delta	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。

統計	説明
Hard Bounced Recipients Delta	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。
Soft Bounce Events Delta	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   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
```

## 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 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 つの接続は、topin コマンドを使用して表示されるフィールドについて説明する、次の表の 2 行になります。

表 9: topin コマンドのデータ

統計	説明
Remote Hostname	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。
Remote IP Address	リモートホストの IP アドレス。
listener	接続を受信している、Cisco アプライアンス上のリスナーのニックネーム。
Connections In	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、[送信者の検証](#)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、最後のシステム再起動以降、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。

次の表に、使用可能なカウンタを示します。

表 10: `dnsstatus` コマンドのデータ

統計	説明
DNS 要求	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。
ネットワーク要求	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。
Cache Hits	レコードが検出されて返された、DNS キャッシュへの要求。
Cache Misses	レコードが検出されなかった、DNS キャッシュへの要求。

統計	説明
Cache Exceptions	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。
Cache Expired	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



**注意** クラウドEメールセキュリティ アプライアンスでは、電子メール モニタリング カウンタをリセットしないようにすることを推奨します。

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。[\[システムステータス \(System Status\)\]](#) ページを参照してください。

## 例

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

## アクティブな TCP/IP サービスの識別

Eメールセキュリティアプライアンスで使用されるアクティブな TCP/IP サービスを識別するには、コマンドラインインターフェイスで `tcpsservices` コマンドを使用します。

## 電子メール キューの管理

Cisco 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、Cisco 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（[電子メールの受信と配信の一時停止](#)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 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リ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、Cisco 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（[電子メールの受信と配信の一時停止](#)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 Cisco AsyncOS をオンライン状態にした後でのみ開始されます。

## 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.
```

## キュー内のメッセージのリダイレクト

`redirectrecipients` コマンドを使用すると、電子メール配信キュー内のすべてのメッセージを別のリレーホストにリダイレクトできます。受信者を、このホストから大量のSMTPメールを受け入れる準備ができていないホストまたはIPアドレスにリダイレクトすると、メッセージがバウンスするだけでなく、メールが失われる可能性もあることに注意してください。



**注意** メッセージを、`/dev/null` を宛先とする受信側ドメインにリダイレクトすると、メッセージが失われます。メールをこのようなドメインにリダイレクトしても、CLIに警告は表示されません。メッセージをリダイレクトする前に、受信側ドメインがあるかどうかSMTPルートを確認してください。

### 例

次に、すべてのメールを `example2.com` ホストにリダイレクトする例を示します。

```
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.
```

## キュー内の受信者に基づいたメッセージの表示

`showrecipients` コマンドを使用すると、電子メール配信キューからのメッセージが受信者ホストまたはEnvelope Fromアドレスごとに表示されます。また、キュー内のすべてのメッセージを表示することもできます。

### 例

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

```

[0]      [0]      8243@example.com
1532    1230    user123456@ironport.com Testing
[0]      [0]      1820@example.com
1531    1230    user123456@ironport.com Testing
[0]      [0]      9595@example.com
1518    1230    user123456@ironport.com Testing
[0]      [0]      8778@example.com
1535    1230    user123456@ironport.com Testing
[0]      [0]      1703@example.com
1533    1230    user123456@ironport.com Testing
[0]      [0]      3052@example.com
1536    1230    user123456@ironport.com Testing
[0]      [0]      511@example.com

```

次に、すべての受信者ホストへのキュー内のメッセージの例を示します。

## 電子メール配信の一時停止



**注意** アプライアンスでは、電子メール配信を一時停止/再開しないことをお勧めします。

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、Cisco AsyncOS を配信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が、`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、システムを再起動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再起動する場合は、`resumedel` コマンドを使用して再起動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



**注意** クラウドEメールセキュリティ アプライアンスでは、電子メール配信を一時停止したり、再開したりしないようにすることを推奨します。

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

### 構文

```
resumedel
```

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

## 電子メールの受信の一時停止



**注意** クラウドEメールセキュリティ アプライアンスでは、リスナーを一時停止/再開しないことをお勧めします。

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、システムを再起動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再起動する場合、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>
```

## 電子メールの受信の再開



**注意** クラウドEメールセキュリティアプライアンスでは、リスナーを一時停止/再開しないことをお勧めします。

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

### 構文

```
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>
```

## 電子メールの配信と受信の再開

`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ス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>
```

## ワークキューの休止



**注意** クラウドEメールセキュリティアプライアンスでは、ワークキューを一時停止しないことをお勧めします。

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、スパム対策、およびウイルス対策スキャンエンジンの処理は、すべて「ワークキュー」で実行されます。処理フローについては[ルーティングおよび配信機能の設定](#)を、「ワークキュー内のメッセージ」ページの説明については[システムゲージの読み取り \(4 ページ\)](#)を参照してください。`workqueue` コマンドを使用して、ワーク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ワーク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、ワーク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。

ワーク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、ワーク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、ワーク 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。これを行うには、`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隔離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、ワークキュー、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 `configuration` 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、隔離エリア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。メッセージがワークキュー、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) シスコのスパム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 を使用したシステムの状態のモニタリング



**注意** クラウド E メールセキュリティ アプライアンスでは、SNMP を設定しないことをお勧めします。

AsyncOS オペレーティング システムは、SNMP (シンプル ネットワーク管理プロトコル) を使用したシステム 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)。以下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。
- SNMPv3 をイネーブルにする場合、メッセージ認証と暗号化は必須です。暗号化アルゴリズムには AES (推奨) または DES を指定できます。認証アルゴリズムには SHA-1 (推奨)

または MD5 を指定できます。次に `snmpconfig` コマンドを実行するときは、コマンドにこのパスフレーズが「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 SHA -A ironport mail.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティストリングを設定する必要があります。コミュニティストリングは、`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)。

アプライアンスに対して SNMP モニタリングをイネーブルにして設定するには、`snmpconfig` コマンドを使用します。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、一致するパスフレーズ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トリングが含まれている必要があります。

## MIB ファイル

Cisco E メールセキュリティアプライアンス用の次の MIB ファイルは、<http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html> から入手できます。使用可能な最新の MIB ファイルを使用します。

- ASYNCOs-MAIL-MIB.txt : Cisco 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。
- AsyncOS SMI.txt (IRONPORT-SMI.txt) : Cisco コンテンツセキュリティ製品で ASYNCOs-MAIL-MIB の役割を定義する「管理情報構造」(SMI) ファイル。

## 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によって、温度、ファン速度、電源モジュールステータスなどの情報が報告されます。

ハードウェアステータスをポーリングして、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。

アプライアンスの電源モジュールの数や動作温度の範囲などの情報については、モデルのハードウェアガイドを参照してください。ハードウェアガイドの場所については、[資料](#)を参照してください。

## ハードウェア トラップ

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。

たとえば、C170 アプライアンスで次のしきい値に達すると、トラップが送信されます。

表 11: C170 アプライアンスのハードウェア 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
C170	90C	47C	NA	NA	0 RPM	ステータスの変化	ステータスの変化	ステータスの変化

アプライアンスで使用可能なトラップおよびしきい値を表示するには、コマンドラインインターフェイスで `snmpconfig` コマンドを実行します。

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、複数のファンまたは電源モジュールを持つアプライアンスで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。

### 関連項目

- 例： `snmpconfig` コマンド (31 ページ)

## 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Eメールセキュリティアプライアンス）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、SNMP管理コンソールソフトウェアが稼働するホストに送信します。

SNMPトラップを有効にして設定するには、`snmpconfig` コマンドを使用します。

複数のトラップターゲットの指定方法：トラップターゲットの入力を求められたときに、カンマで区切ったIPアドレスを10個まで入力できます。

### 例： `snmpconfig` コマンド

次の例では、C690 ハードウェア アプライアンスで `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を有効にしています。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。

```

esa.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 ]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: esa.example.com)
[ 1 ]>
Which port shall the SNMP daemon listen on interface "Management"?
[ 161 ]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
[ 1 ]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[ 1 ]> 2
Enter the SNMPv3 authentication passphrase.
[ ]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[ ]>
Enter the SNMPv3 privacy passphrase.
[ ]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[ ]>
Service SNMP V1/V2c requests?
[ N ]> Y
Enter the SNMP V1/V2c community string.
[ironport]> public
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]>
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]> 203.0.113.1
Enter the Trap Community string.
[ironport]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded      Disabled
2. FIPSMODEDisableFailure      Enabled
3. FIPSMODEEnableFailure       Enabled
4. FailoverHealthy             Enabled
5. FailoverUnhealthy           Enabled
6. RAIDStatusChange           Enabled
7. connectivityFailure         Disabled
8. fanFailure                  Enabled
9. highTemperature             Enabled
10. keyExpiration              Enabled
11. linkUpDown                 Enabled
12. memoryUtilizationExceeded  Disabled
13. powerSupplyStatusChange    Enabled
14. resourceConservationMode    Enabled
15. updateFailure              Enabled
Do you want to change any of these settings?
[ N ]> Y
Do you want to disable any of these traps?
[ Y ]> n

```



```
Do you want to enable any of these traps?
[Y]> y
Enter number or numbers of traps to enable. Separate multiple numbers with
commas.
[]> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
Enter the System Contact string.
[snmp@localhost]> esa-admin@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: esa-admin@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
esa.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
esa.example.com>
```

例: `snmpconfig` コマンド