CHAPTER 5

ロギング

Cisco IronPort電子メール セキュリティ アプライアンスの重要な機能に、ロギング機能があります。AsyncOS は多くのログ タイプを生成し、さまざまなタイプの情報を記録できます。ログ ファイルには、システムの各種コンポーネントによる通常のアクティビティとエラーの記録が保持されます。この情報は、Cisco IronPort アプライアンスをモニタするときや、パフォーマンスのトラブルシューティングまたはチェックを行うときに役立つ場合があります。

この章は、次の内容で構成されています。

概要

ここでは、次の項目について説明します。

ログ ファイルおよびログ サブスクリプションについて

ログは、AsyncOS の電子メール動作に関する重要な情報を収集する、簡潔で効率的な方法です。これらのログには、IronPort アプライアンスでのアクティビティに関する情報が記録されます。情報は、バウンス ログや配信ログなど、表示するログによって異なります。

ほとんどのログは、プレーン テキスト（ASCII）形式で記録されますが、配信ログはリソースの効率性を保つためにバイナリ形式で記録されます。ASCII テキスト情報は、任意のテキスト エディタで読み取ることができます。

IronPort は、複数の IronPort アプライアンスからのログに対応するオフボックスの集中化レポーティングおよびトラッキング ツールを提供しています。詳細については、IronPort の担当者にお問い合わせください。

ログ サブスクリプションでは、ログ タイプに名前、ロギング レベル、およびその他の制約事項（サイズや宛先情報など）を関連付けます。同じログ タイプに対して複数のサブスクリプションが許可されます。

ログ タイプ

ログ タイプは、メッセージ データ、システム統計情報、バイナリまたはテキスト データなど、生成されたログにどの情報が記録されるかを示します。ログ タイプは、ログ サブスクリプションを作成するときに選択します。詳細については、「ログ サブスクリプション」（P.5-212）を参照してください。

IronPort AsyncOS for Email では、次のログ タイプが生成されます。

表 5-1　ログ タイプ

ログ	説明
IronPort テキスト メール ログ	テキスト メール ログには、電子メール システムの動作に関する情報が記録されます。たとえば、メッセージの受信、メッセージの配信試行、接続のオープンとクローズ、バウンス、TLS 接続などです。
qmail 形式メール ログ	qmail 形式の配信ログには、次の配信ログと同じく電子メール システムの動作に関する情報が記録されますが、保存は qmail 形式です。

表 5-1　ログ タイプ（続き）

ログ	説明
配信ログ	配信ログには、IronPort アプライアンスの電子メール配信動作に関する重要な情報が記録されます。たとえば、配信試行時の各受信者の配信やバウンスに関する情報などです。ログ メッセージは「ステートレス」です。つまり、関連付けられたすべての情報が各ログ メッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログ メッセージを参照する必要がありません。配信ログは、リソースの効率性を保つためにバイナリ形式で記録されます。配信ログ ファイルを XML または Comma-Separated Values（CSV）形式に変換するには、提供されるユーティリティを使用して事後処理する必要があります。変換ツールは、次の場所にあります。 `http://support.ironport.com`
バウンス ログ	バウンス ログには、バウンスされた受信者の情報が記録されます。バウンスされた受信者ごとに記録される情報には、メッセージ ID、受信者 ID、Envelope From アドレス、Envelope To アドレス、その受信者のバウンスの理由、および受信者ホストからの応答コードなどが含まれます。また、バウンスされた各受信者メッセージの一定量を記録するように選択することもできます。この量はバイトで定義され、デフォルトはゼロです。
ステータス ログ	このログ ファイルには、`status detail` および `dnsstatus` などの CLI ステータス コマンドで検出されたシステムの統計情報が記録されます。記録期間は、`logconfig` の `setup` サブコマンドを使用して設定します。ステータス ログに報告される各カウンタまたはレートは、カウンタが最後にリセットされてからの値です。
ドメイン デバッグ ログ	ドメイン デバッグ ログには、Cisco IronPort アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このログ タイプは、特定の受信者ホストに関する問題のデバッグに使用できます。ログ ファイルに記録する SMTP セッションの合計数を指定する必要があります。セッションが記録されるにつれ、この数は減少していきます。ログ サブスクリプションを削除または編集することによって、すべてのセッションが記録される前にドメイン デバッグを停止できます。

表 5-1　ログ タイプ（続き）

ログ	説明
インジェクション デバッグ ログ	インジェクション デバッグ ログには、Cisco IronPort アプライアンスと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネット上の Cisco IronPort アプライアンスとホスト間の通信に関する問題をトラブルシューティングするのに役立ちます。
システム ログ	システム ログには、ブート情報、DNS ステータス情報、および `commit` コマンドを使用してユーザが入力したコメントが記録されます。システム ログは、アプライアンスの基本的な状態をトラブルシューティングするのに役立ちます。
CLI 監査ログ	CLI 監査ログには、システム上のすべての CLI アクティビティが記録されます。
FTP サーバ ログ	FTP ログには、インターフェイスでイネーブルになっている FTP サービスの情報が記録されます。接続の詳細とユーザ アクティビティが記録されます。
HTTP ログ	HTTP ログには、インターフェイスでイネーブルになっている HTTP サービス、セキュア HTTP サービス、またはその両方のサービスに関する情報が記録されます。Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）には HTTP を介してアクセスするので、HTTP ログは表面上 CLI 監査ログと同等の GUI です。GUI でアクセスされたセッション データ（新規セッション、期限切れセッション）およびページが記録されます。
NTP ログ	NTP ログには、設定されている任意の Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバとアプライアンス間の会話が記録されます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」の章の「Editing the Network Time Protocol (NTP) Configuration (Time Keeping Method)」を参照してください。

表 5-1　ログ タイプ（続き）

ログ	説明
LDAP デバッグ ログ	LDAP デバッグ ログは、LDAP インストールのデバッグを目的としています（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください）。ここには、Cisco IronPort アプライアンスが LDAP サーバに送信しているクエリーについての有益な情報が記録されます。
アンチスパム ログ	アンチスパム ログには、最新のアンチスパム ルールのアップデート受信に関するステータスなど、システムのアンチスパム スキャン機能のステータスが記録されます。また、Context Adaptive Scanning Engine に関するすべてのログもここに記録されます。
アンチスパム アーカイブ	アンチスパム スキャン機能をイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。これは、mbox 形式のログファイルとなります。アンチスパム エンジンの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Spam」の章を参照してください。
アンチウイルス ログ	アンチウイルス ログには、最新のアンチウイルス アイデンティティ ファイルのアップデート受信に関するステータスなど、システムのアンチウイルス スキャン機能のステータスが記録されます。
アンチウイルス アーカイブ	アンチウイルス エンジンをイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。これは、mbox 形式のログファイルとなります。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Virus」の章を参照してください。

表 5-1　ログ タイプ（続き）

ログ	説明
スキャン ログ	スキャン ログには、スキャン エンジンに関するすべての LOG および COMMON メッセージが保持されます（『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「System Administration」の章の「Alerts」を参照してください）。これは一般に、アプリケーションの障害、送信されたアラート、失敗したアラート、およびログ エラー メッセージになります。このログは、システム全体のアラートには適用されません。
IronPort スパム検疫ログ	IronPort スパム検疫ログには、IronPort スパム検疫プロセスに関連付けられたアクションが記録されます。
IronPort スパム検疫 GUI ログ	IronPort スパム検疫ログには、GUI を介した設定、エンド ユーザ認証、およびエンド ユーザ アクション（電子メールの解放など）を含む、IronPort スパム検疫に関連付けられたアクションが記録されます。
SMTP 会話ログ	SMTP 会話ログには、着信および発信 SMTP 会話のすべての部分が記録されます。
セーフリスト/ブロックリスト ログ	セーフリスト/ブロックリスト ログには、セーフリスト/ブロックリストの設定に関するデータとデータベースが記録されます。
レポーティング ログ	レポーティング ログには、集中化レポーティング サービスのプロセスに関連付けられたアクションが記録されます。
レポーティング クエリー ログ	レポーティング クエリー ログには、アプライアンスで実行されるレポーティング クエリーに関連付けられたアクションが記録されます。
アップデータ ログ	アップデータ ログには、McAfee アンチウイルス定義のアップデートなど、システム サービスのアップデートに関するイベントが記録されます。
トラッキング ログ	トラッキング ログには、トラッキング サービスのプロセスに関連付けられたアクションが記録されます。トラッキング ログは、メール ログのサブセットです。
認証ログ	認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

ログ タイプの特徴

表 5-2 に、各ログ タイプの特徴をまとめます。

表 5-2　ログ タイプの比較

	記載内容												
	トランザクション	ステートレス	テキストとして記録	mbox ファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個々のハード バウンス	個々のソフト バウンス	インジェクション SMTP 会話	ヘッダー ロギング	配信 SMTP 会話
IronPort メール ログ	•		•			•	•	•	•	•		•	
qmail 形式配信 ログ		•			•		•	•	•			•	
配信ログ		•			•		•	•	•			•	
バウンス ログ	•		•						•	•		•	
ステータス ログ		•	•			•							
ドメインデバッグ ログ	•		•					•	•	•			•
インジェクション デバッグ ログ	•		•				•				•		
システム ログ	•		•			•							
CLI 監査ログ	•		•			•							
FTP サーバ ログ	•		•			•							
HTTP ログ	•		•			•							
NTP ログ	•		•			•							
LDAP ログ	•		•										
アンチスパム ログ	•		•			•							

表 5-2　ログ タイプの比較（続き）

	記載内容													
	トランザクション	ステートレス	テキストとして記録	mbox ファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個々のハード バウンス	個々のソフト バウンス	インジェクション SMTP 会話	ヘッダー ロギング	配信 SMTP 会話
アンチスパム アーカイブ ログ				•									
アンチウイルス ログ	•		•			•							
アンチウイルス アーカイブ				•									
スキャン ログ	•		•			•							
IronPort スパム検疫	•		•			•							
IronPort スパム検疫 GUI	•		•			•							
セーフリスト/ブロックリスト ログ	•		•			•							
レポーティング ログ	•		•		•								
レポーティング クエリー ログ	•		•		•								
アップデータ ログ			•										
トラッキング ログ	•				•	•	•	•	•	•		•	
認証ログ	•		•										

ログ取得方法

ログ ファイルは、次のいずれかのファイル転送プロトコルに基づいて取得できます。ログ サブスクリプション プロセス中に GUI または `logconfig` コマンドを使用して、ログ サブスクリプションの作成や編集を行いながらプロトコルを設定します。

表 5-3　ログ転送プロトコル

FTP ポーリング	この方法では、管理者ユーザまたはオペレータ ユーザのユーザ名とパスワードを使用して、リモート FTP クライアントから Cisco IronPort アプライアンスにアクセスしてログ ファイルを取得します。FTP ポーリング方法を使用するようにログ サブスクリプションを設定する場合は、保有するログ ファイルの最大数を指定する必要があります。最大数に達すると、最も古いファイルが削除されます。
FTP プッシュ	この方法では、リモート コンピュータ上の FTP サーバに定期的にログ ファイルをプッシュします。サブスクリプションには、リモート コンピュータ上のユーザ名、パスワード、および宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。「ログ サブスクリプションのパスワードのロードについての注意事項」（P.8-351）も参照してください。
SCP プッシュ	この方法では、リモート コンピュータ上の SCP サーバに定期的にログ ファイルをプッシュします。この方法には、SSH1 または SSH2 プロトコルを使用するリモート コンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、リモート コンピュータ上のユーザ名、SSH キー、および宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。
syslog プッシュ	この方法では、ログ メッセージをリモートの syslog サーバに送信します。この方法は、RFC 3164 に準拠しています。syslog サーバのホスト名を送信し、ログの転送に UDP または TCP を使用するように選択する必要があります。使用するポートは 514 です。ログのファシリティは選択できますが、ログ タイプのデフォルトはドロップダウン メニューであらかじめ選択されています。syslog プッシュを使用して転送できるのは、テキストベースのログだけです。

ログ ファイル名とディレクトリ構造

IronPort AsyncOS は、ログ サブスクリプション名に基づいて各ログ サブスクリプションのディレクトリを作成します。ディレクトリ内の実際のログ ファイル名は、ユーザが指定したログ ファイル名、ログ ファイルが開始されたときのタイムスタンプ、および単一文字のステータス コードで構成されます。ログのファイル名は、次の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

ステータス コードは、.c（現在の意）または .s（保存済みの意）になります。saved（保存済み）ステータスのログ ファイルだけを転送するようにしてください。

ログのロールオーバーおよび転送スケジュール

ログ サブスクリプションは、最初に到達したユーザ指定の限度、つまり最大ファイル サイズまたは最大時間に基づいてログ ファイルを作成し、転送（ロールオーバー）します。FTP ポーリング転送メカニズムに基づいたログ サブスクリプションでは、ファイルが作成されると、それらのファイルが取得されるか、システムでログ ファイル用にさらにスペースが必要になるまで、Cisco IronPort アプライアンスの FTP ディレクトリにそれらのファイルが保存されます。詳細については、Appendix A, “Accessing the Appliance” を参照してください。

デフォルトでイネーブルになるログ

IronPort アプライアンスは、次のログ サブスクリプションがデフォルトでイネーブルになった状態で事前に設定されています（適用したライセンス キーによって、その他のログが設定される場合があります）。

表 5-4　事前に設定されるログ サブスクリプション

ログ番号	ログ サブスクリプション名	ログ タイプ	取得方法
1	antispam	アンチスパム ログ	FTP ポーリング
2	antivirus	アンチウイルス ログ	FTP ポーリング
3	asarchive	アンチスパム アーカイブ	FTP ポーリング
4	authentication	認証ログ	FTP ポーリング
5	avarchive	アンチウイルス アーカイブ	FTP ポーリング

表 5-4　事前に設定されるログ サブスクリプション（続き）

ログ番号	ログ サブスクリプション名	ログ タイプ	取得方法
6	bounces	バウンス ログ	FTP ポーリング
7	cli_logs	CLI 監査ログ	FTP ポーリング
8	encryption	暗号化	FTP ポーリング
9	error_logs	IronPort テキスト メール ログ	FTP ポーリング
10	euq_logs	IronPort スパム検疫ログ	FTP ポーリング
11	euqgui_logs	IronPort スパム検疫 GUI ログ	FTP ポーリング
12	ftpd_logs	FTP サーバ ログ	FTP ポーリング
13	gui_logs	HTTP ログ	FTP ポーリング
14	mail_logs	IronPort テキスト メール ログ	FTP ポーリング
15	reportd_logs	レポーティング ログ	FTP ポーリング
16	reportingqueryd_logs	レポーティング クエリー ログ	FTP ポーリング
17	scanning	スキャン ログ	FTP ポーリング
18	slbld_logs	セーフリスト/ブロック リスト ログ	FTP ポーリング
19	sntpd_logs	NTP ログ	FTP ポーリング
20	status	ステータス ログ	FTP ポーリング
21	system_logs	システム ログ	FTP ポーリング
22	trackerd_logs	トラッキング ログ	FTP ポーリング
23	updater_logs	アップデータ ログ	FTP ポーリング

エラーだけが含まれるように 1 に設定された error_logs を除き、事前に設定されるすべてのログ サブスクリプションのログ レベルは 3 になります。詳細については、「ログ レベル」（P.5-213）を参照してください。新規のログ サブスクリプションの作成、または既存のログ サブスクリプションの変更については、「ログ サブスクリプション」（P.5-212）を参照してください。

ログ タイプ

ここでは、次の内容について説明します。

ログ ファイル内のタイムスタンプ

次のログ ファイルには、ログ自体の開始日と終了日、AsyncOS のバージョン、および GMT オフセット（秒単位でログの始まりにのみ表示）が含まれます。

- アンチウイルス ログ
- LDAP ログ
- システム ログ
- メール ログ

IronPort テキスト メール ログの使用

これらのログに、特別な設定は必要ありません。これらのログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。ステータス情報も、1 分ごとにメール ログに書き込まれます。これらのログは、特定のメッセージの配信を理解し、システム パフォーマンスを分析するうえで有益な情報源となります。

表 5-5 に、テキスト メール ログに表示される情報を示します。

表 5-5　テキスト メール ログの統計情報

統計	説明
ICID	Injection Connection ID（インジェクション接続 ID）。システムに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが送信されます。
DCID	Delivery Connection ID（配信接続 ID）。別のサーバに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが配信されます。1 つのメッセージ送信で一部または全部の RID が一緒に配信されます。
RCID	RPC Connection ID（RPC 接続 ID）。IronPort スパム検疫に対する個々の RPC 接続を表す数値 ID です。この ID を使用して、IronPort スパム検疫との間で送受信されるメッセージを追跡します。
MID	Message ID（メッセージ ID）：この ID を使用して、ログを通過するメッセージを追跡します。

表 5-5　テキスト メール ログの統計情報（続き）

統計	説明
RID	Recipient ID（受信者 ID）：各メッセージ受信者に ID が割り当てられます。
New	新規の接続が開始されました。
Start	新規のメッセージが開始されました。

IronPort テキスト メール ログの解釈

ログ ファイルを解釈するためのガイドとして、次のサンプルを使用してください。

（注）　ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

表 5-6　テキスト メール ログの詳細

1	Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes
2	Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5
3	Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>
4	Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>
5	Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>
6	Mon Apr 17 19:59:59 2003 Info: ICID 5 close
7	Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25
8	Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]
9	Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10	Mon Mar 31 20:11:03 2003 Info: DCID 8 close

前述のログ ファイルを読み取るためのガイドとして、表 5-7 を使用してください。

表 5-7　テキスト メール ログの例の詳細

行番号	説明
1.	システムへの新しい接続が開始され、Injection ID（ICID; インジェクション ID）「5」が割り当てられます。この接続は、管理 IP インターフェイスで受信され、リモート ホスト 10.1.1.209 から開始されました。
2.	クライアントから MAIL FROM コマンドが実行された後、メッセージに Message ID（MID; メッセージ ID）「6」が割り当てられました。
3.	送信者アドレスが識別され、受け入れられます。
4.	受信者が識別され、Recipient ID（RID; 受信者 ID）「0」が割り当てられます。
5.	MID 5 が受け入れられ、ディスクに書き込まれ、承認されます。
6.	受信に成功し、受信接続がクローズします。
7.	次に、メッセージ配信プロセスが開始されます。192.168.42.42 から 10.5.3.25 への配信に、Delivery Connection ID（DCID; 配信接続 ID）「8」が割り当てられます。
8.	RID「0」へのメッセージ配信が開始されます。
9.	MID 6 から RID「0」への配信に成功します。
10.	配信接続がクローズします。

テキスト メール ログ エントリの例

次に、さまざまな状況に基づいたいくつかのサンプル ログ エントリを示します。

メッセージのインジェクションおよび配信

1 人の受信者に対するメッセージが Cisco IronPort アプライアンスにインジェクトされます。メッセージは正常に配信されます。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface
mail.example.com (1.2.3.4) address 2.3.4.5 reverse dns host unknown
verified no

Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None

Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970

Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From:
<someone@foo.com>

Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To:
<user@example.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from
<someone@foo.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative

Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface
1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID
200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID
200257070 to RID [0] [('X-SBRS', 'None')]
```

```
Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

正常なメッセージ配信

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11
address 63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

失敗したメッセージ配信（ハード バウンス）

2 人の受信者が指定されたメッセージが Cisco IronPort アプライアンスにインジェクトされます。配信時に、宛先ホストが 5*XX* エラーを返します。このエラーは、メッセージをいずれの受信者にも配信できないことを示します。Cisco IronPort アプライアンスは、送信者に通知して、キューからそれらの受信者を削除します。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11
address 64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0,
1]

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0
- Unknown address error ('550', ['<george@yourdomain.com>... Relaying
denied']) []

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0
- Unknown address error ('550', ['<jane@yourdomain.com>... Relaying
denied']) []

Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

ソフト バウンスの後の正常な配信

メッセージが Cisco IronPort アプライアンスにインジェクトされます。最初の配信試行で、メッセージはソフト バウンスして、その後の配信キューに入れられます。2 回めの試行でメッセージは正常に配信されます。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11
address 63.251.108.110

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0,
1]

Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0
- Unknown address error ('466', ['Mailbox temporarily full.'])[]

Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon
Mar 31 20:01:23 2003

Mon Mar 31 20:01:28 2003 Info: DCID 5 close

Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet
address 172.17.0.113

Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID
[0]

Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

scanconfig コマンドのメッセージ スキャン結果

`scanconfig` コマンドを使用して、メッセージの構成要素を分解できない場合（添付ファイルを削除する場合）のシステムの動作を決定できます。オプションは、`Deliver`、`Bounce`、または `Drop` です。

次に、scanconfig を Deliver に設定した IronPort テキスト メール ログの例を示します。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From:
<test@virus.org>

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To:
<joe@example.com>

Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID
'<137398.@virus.org>'

Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test
#22'

Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from
<test@virus.org>

Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem:
Continuation line seen before first header

Tue Aug 3 16:36:29 2004 Info: ICID 44784 close

Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive
'EICAR-AV-Test'

Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by
antivirus

Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

次に、scanconfig を drop に設定した IronPort テキスト メール ログの例を示します。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To:
<joe@example.com>

Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID
'<392912.@virus.org>'
```

```
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test
#22'

Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from
<test@virus.org>

Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem:
Continuation line seen before first header

Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by
filter 'drop_zip_c'

Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done

Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

生成またはリライトされたメッセージに対するログ エントリ

リライト/リダイレクト アクションなどの一部の機能（`alt-rcpt-to` フィルタ、アンチスパム RCPT リライト、`bcc()` アクション、アンチウイルス リダイレクションなど）によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じて MID や、場合によっては DCID を追加します。次のようなエントリが可能です。

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by
bcc filter 'nonetest'
```

または

```
Tue Jan  6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by
alt-rcpt-to-filter filter 'testfilt'
```

「rewritten」エントリについては、ログ内で新しい MID の使用を示す行の後に表示される点に注目してください。

IronPort スパム検疫エリアに送信されたメッセージ

メッセージを検疫エリアに送信すると、メール ログでは、RPC 接続を識別する RPC Connection ID（RCID; RPC 接続 ID）を使用して、検疫エリアとの間の移動が追跡されます。次のメール ログでは、スパムとしてタグが付けられたメッセージが IronPort スパム検疫に送信されています。

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From:
<HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.
chase.com>'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream
home - Now make it a reality'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from
<HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for
per-recipient policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam
suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine

Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative

Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery

Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID
2317877 to local IronPort Spam Quarantine

Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
```

```
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877

Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

IronPort 配信ログの使用

配信ログには、AsyncOS の電子メール配信動作に関する重要な情報が記録されます。ログ メッセージは「ステートレス」です。つまり、関連するすべての情報が各ログ メッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログ メッセージを参照する必要がありません。

配信ログには、受信者ごとの電子メール配信動作に関連するすべての情報が記録されます。すべての情報は、論理的にレイアウトされ、IronPort が提供するユーティリティを使用して変換した後は、人による読み取りが可能になります。変換ツールは、次の場所にあります。
`http://support.ironport.com`

配信ログは、リソースの効率性を保つためにバイナリ形式で記録され、転送されます。次の表に、配信ログに記録される情報を示します。

表 5-8　配信ログの統計情報

統計	説明
Delivery status	success（メッセージは正常に配信されました）または bounce（メッセージはハード バウンスされました）
Del_time	配信時間。
Inj_time	インジェクション時間。`del_time` - `inj_time` = 受信者メッセージがキューに留まっていた時間。
Bytes	メッセージ サイズ
Mid	メッセージ ID
Ip	受信者ホスト IP 受信者メッセージを受信またはバウンスしたホストの IP アドレス
From	Envelope From（Envelope Sender または MAIL FROM としても知られます）
Source_ip	送信元ホスト IP 着信メッセージのホストの IP アドレス
Code	受信者ホストからの SMTP 応答コード
Reply	受信者ホストからの SMTP 応答メッセージ

表 5-8　配信ログの統計情報（続き）

統計	説明
Rcpt Rid	受信者 ID。受信者 ID は <0> から始まります。複数の受信者が指定されたメッセージには、複数の受信者 ID が付きます。
To	Envelope To
Attempts	配信試行回数

配信ステータスが bounce であった場合は、次の追加情報が配信ログに表示されます。

表 5-9　配信ログのバウンス情報

統計	説明
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Code	受信者ホストからの SMTP 応答コード
Error	受信者ホストからの SMTP 応答メッセージ

ログヘッダーを設定している場合（「メッセージ ヘッダーのロギング」（P.5-218）を参照）、ヘッダー情報は配信情報の後に表示されます。

表 5-10　配信ログのヘッダー情報

統計	説明
Customer_data	ログに記録されるヘッダーの始まりを示す XML タグ
Header Name	ヘッダーの名前
Value	ログに記録されるヘッダーの内容

配信ログ エントリの例

ここでは、さまざまな配信ログ エントリの例を示します。

正常なメッセージ配信

```
<success del_time="Fri Jan 09 15:34:20.234 2004" inj_time="Fri Jan 09
15:33:38.623 2004" bytes="202" mid="45949" ip="10.1.1.1"
from="campaign1@yourdomain.com" source_ip="192.168.102.1" code="250"
reply="sent">

<rcpt rid="0" to="alsdfj.ajsdfl@alsdfj.d2.qa25.qa" attempts="1" />

</success>
```

配信ステータス バウンス

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05
08:28:32.929 2003" bytes="4074" mid="94157762" ip="0.0.0.0"
from="campaign1@yourdomain.com" source_ip="192.168.102.1 "reason="5.1.0 -
Unknown address error" code="550" error="["Requested action not taken:
mailbox unavailable"]">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

ログヘッダー付きの配信ログ エントリ

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28
15:55:17.696 2003" bytes="139" mid="202" ip="10.1.1.13"
from="campaign1@yourdomain.com" source_ip="192.168.102.1" code="250"
reply="sent">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

IronPort バウンス ログの使用

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。表 5-11 に、バウンス ログに記録される情報を示します。

表 5-11　バウンス ログの統計情報

統計	説明
Timestamp	バウンス イベントの時刻
Log level	このバウンス ログの詳細レベル
Bounce type	Bounced または Delayed（ハードバウンスまたはソフトバウンスなど）
MID/RID	メッセージ ID および受信者 ID
From	Envelope From
To	Envelope To
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Response	受信者ホストからの SMTP 応答コードおよびメッセージ

また、ログに記録するメッセージ サイズを指定しているか、ログヘッダーを設定している（「メッセージ ヘッダーのロギング」（P.5-218）を参照）場合、メッセージおよびヘッダー情報はバウンス情報の後に表示されます。

表 5-12　バウンス ログのヘッダー情報

Header	ヘッダー名およびヘッダーのコンテンツ。
Message	ログに記録されるメッセージのコンテンツ。

バウンス ログ エントリの例

ソフトバウンスされた受信者（バウンス タイプ = Delayed）

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>


Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

ハードバウンスされた受信者（バウンス タイプ = Bounced）

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0
From:<campaign1@yourdomain.com> To:<user2@sampledomain.com>


Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no
such active account.'])"
```

メッセージ本文およびログヘッダー付きのバウンス ログ

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>

Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers:
['xname: userID2333']' Message: Message-Id:


<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```

（注）　テキスト文字列 \015\012 は、改行を表します（CRLF など）。

IronPort ステータス ログの使用

ステータス ログには、`status`、`status detail`、および `dnsstatus` を含む CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、`logconfig` の `setup` サブコマンドを使用して設定します。ステータス ログに報告される各カウンタまたはレートは、カウンタが最後にリセットされてからの値です。

ステータス ログの読み取り

表 5-13 に、ステータス ログ ラベルと、一致するシステム統計情報を示します。

表 5-13　ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率
DskIO	Disk I/O 使用率
RAMUtil	RAM 使用率
QKUsd	使用されているキュー（キロバイト単位）
QKFre	空いているキュー（キロバイト単位）
CrtMID	Message ID（MID; メッセージ ID）
CrtICID	Injection Connection ID（ICID; インジェクション接続 ID）
CRTDCID	Delivery Connection ID（DCID; 配信接続 ID）
InjMsg	インジェクトされたメッセージ
InjRcp	インジェクトされた受信者
GenBncRcp	生成されたバウンス受信者
RejRcp	拒否された受信者
DrpMsg	ドロップされたメッセージ
SftBncEvnt	ソフト バウンスされたイベント
CmpRcp	完了した受信者

表 5-13　ステータス ログの統計情報（続き）

統計	説明
HrdBncRcp	ハード バウンスされた受信者
DnsHrdBnc	DNS ハード バウンス
5XXHrdBnc	5XX ハード バウンス
FltrHrdBnc	フィルタ ハード バウンス
ExpHrdBnc	期限切れハード バウンス
OtrHrdBnc	その他のハード バウンス
DlvRcp	配信された受信者
DelRcp	削除された受信者
GlbUnsbHt	グローバル配信停止リストとの一致数
ActvRcp	アクティブ受信者
UnatmptRcp	未試行受信者
AtmptRcp	試行受信者
CrtCncIn	現在の着信接続
CrtCncOut	現在の発信接続
DnsReq	DNS 要求
NetReq	ネットワーク要求
CchHit	キャッシュ ヒット
CchMis	キャッシュ ミス
CchEct	キャッシュ例外
CchExp	キャッシュ期限切れ
CPUTTm	アプリケーションが使用した合計 CPU 時間
CPUETm	アプリケーションが開始されてからの経過時間
MaxIO	メール プロセスに対する 1 秒あたりの最大ディスク I/O 動作
RamUsd	割り当て済みのメモリ（バイト単位）
SwIn	スワップインされたメモリ
SwOut	スワップアウトされたメモリ
SwPgIn	ページインされたメモリ
SwPgOut	ページアウトされたメモリ

表 5-13　ステータス ログの統計情報（続き）

統計	説明
MMLen	システム内の合計メッセージ数
DstInMem	メモリ内の宛先オブジェクト数
ResCon	リソース保持の tarpit 値（大量のシステム負荷により、着信メールの受け入れがこの秒数だけ遅延します）
WorkQ	作業キューにある現在のメッセージ数
QuarMsgs	システム検疫にある個々のメッセージ数（複数の検疫エリアに存在するメッセージは 一度だけカウントされます）
QuarQKUsd	システム検疫メッセージによって使用されるキロバイト
LogUsd	使用されるログ パーティションの割合
AVLd	アンチウイルス スキャンで使用される CPU の割合
CmrkLd	Cloudmark アンチスパム スキャンで使用される CPU の割合
SophLd	Sophos アンチスパム スキャンで使用される CPU の割合
McafLd	McAfee アンチウイルス スキャンで使用される CPU の割合
CASELd	CASE スキャンで使用される CPU の割合
TotalLd	CPU の合計消費量
LogAvail	ログ ファイルに使用できるディスク スペース
EuQ	IronPort スパム検疫内の推定メッセージ数
EuqRls	IronPort スパム検疫解放キュー内の推定メッセージ数

ステータス ログの例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0
QKFre 8388608 CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp
14230 GenBncRcp 12 RejRcp 6318 DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813
HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc 0 ExpHrdBnc 1 OtrHrdBnc
0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0
CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis
504791 CchEct 15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350
RAMUsd 21528056 MMLen 0 DstInMem 4 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd
0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail 17G EuQ 0 EuqRls 0
```

IronPort ドメイン デバッグ ログの使用

ドメイン デバッグ ログには、Cisco IronPort アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このログ タイプは主に、特定の受信者ホストに関する問題のデバッグに使用されます。

表 5-14　ドメイン デバッグ ログの統計情報

統計	説明
Timestamp	バウンス イベントの時刻
Log level	このバウンス ログの詳細レベル
From	Envelope From
To	Envelope To
Reason	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
Response	受信者ホストからの SMTP 応答コードおよびメッセージ

ドメイン デバッグ ログの例

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL
FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT
TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END
WITH "." ON A LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

IronPort インジェクション デバッグ ログの使用

インジェクション デバッグ ログには、Cisco IronPort アプライアンスと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントと Cisco IronPort アプライアンス間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、[Sent to]（接続ホストに送信）または [Rcvd from]（接続ホストから受信）に分類されます。

記録するホストの会話を指定するには、IP アドレス、IP 範囲、ホスト名、または部分ホスト名を指定する必要があります。IP 範囲内で接続している IP アドレスがすべて記録されます。部分ドメイン内のホストがすべて記録されます。システムは、接続している IP アドレスに対してリバース DNS ルックアップを実行して、ホスト名に変換します。DNS に対応する PTR レコードがない IP アドレスは、ホスト名に一致しません。

記録するセッション数も指定する必要があります。

インジェクション デバッグ ログ内の各行には、表 5-15 に示す情報が含まれます。

表 5-15　インジェクション デバッグ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
ICID	インジェクション接続 ID は、別のログ サブスクリプションで同じ接続に関連付けることができる固有識別子です。
Sent/Received	「Sent to」と記された行は、接続ホストに送信された実際のバイトです。「Rcvd from」と記された行は、接続ホストから受信した実際のバイトです。
IP Address	接続ホストの IP アドレス。

インジェクション デバッグ ログの例

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220
postman.example.com ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go
ahead\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject:
Test Subject\015\012From: Sender <sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the
content of the message'

Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com\015\012'
```

IronPort システム ログの使用

表 5-16　システム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	ログに記録されたイベント。

システム ログの例

次のシステム ログの例は、commit を実行したユーザの名前と入力されたコメントを含む、いくつかの commit エントリを示しています。

```
Wed Sep  8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXX-XXX

Wed Sep  8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep  8 18:02:45 2004 Info: System is coming up

Wed Sep  8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep  8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep  8 18:13:30 2004 Info: PID 608: User admin commit changes:
SSW:Password

Wed Sep  8 18:17:23 2004 Info: PID 608: User admin commit changes:
Completed Web::SSW

Thu Sep  9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep  9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added
a second CLI log for examples

Thu Sep  9 08:51:53 2004 Info: PID 1237: User admin commit changes:
Removed example CLI log.
```

IronPort CLI 監査ログ

表 5-17　CLI 監査ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
PID	コマンドが入力された特定の CLI セッションのプロセス ID。
Message	メッセージは、入力された CLI コマンド、CLI 出力（メニュー、リストなど）、および表示されるプロンプトで構成されます。

CLI 監査ログの例

次の CLI 監査ログの例は、`who` および `textconfig` CLI コマンドが入力された PID 16434 の情報を示しています。

```
Thu Sep  9 14:35:55 2004 Info: PID 16434: User admin entered 'who';
prompt was '\nmail3.example.com> '

Thu Sep  9 14:37:12 2004 Info: PID 16434: User admin entered
'textconfig'; prompt was '\nUsername  Login Time  Idle Time  Remote Host
What\n========  ==========  =========  ===========  ====\nadmin     Wed
11AM    3m 45s     10.1.3.14    tail\nadmin     02:32PM     0s
10.1.3.14    cli\nmail3.example.com> '

Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt
was '\nThere are no text resources currently defined.\n\n\nChoose the
operation you want to perform:\n- NEW - Create a new text resource.\n-
IMPORT - Import a text resource from a file.\n[]> '
```

IronPort FTP サーバ ログの使用

表 5-18　FTP サーバ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
ID	接続 ID。FTP 接続ごとの別個の ID。
Message	ログ エントリのメッセージ セクションは、ログファイル ステータス情報、または FTP 接続情報（ログイン、アップロード、ダウンロード、ログアウトなど）になります。

FTP サーバ ログの例

次の FTP サーバ ログの例には、接続（ID:1）が記録されています。着信接続の IP アドレスのほか、アクティビティ（ファイルのアップロードとダウンロード）およびログアウトが示されています。

```
Wed Sep  8 18:03:06 2004 Info: Begin Logfile

Wed Sep  8 18:03:06 2004 Info: Version: 4.0.0-206 SN:
00065BF3BA6D-9WFWC21

Wed Sep  8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep  8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on
172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS

Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes

Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

IronPort HTTP ログの使用

表 5-19　HTTP ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
ID	セッション ID
req	接続マシンの IP アドレス
user	接続ユーザのユーザ名
Message	実行されたアクションに関する情報。GET コマンド、POST コマンド、またはシステム ステータスなどが含まれる場合があります。

HTTP ログの例

次の HTTP ログの例は、管理者ユーザと GUI の対話（システム設定ウィザードの実行など）を示しています。

```
Wed Sep  8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting
to https port 443

Wed Sep  8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep  8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep  8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep  8 11:17:24 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg POST /system_administration/system_setup_wizard
HTTP/1.1 303

Wed Sep  8 11:17:25 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /system_administration/ssw_done HTTP/1.1 200

Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /monitor/incoming_mail_overview HTTP/1.1 200
```

```
Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin
&height=190 HTTP/1.1 200

Wed Sep  8 11:18:46 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipie
ntsin&height=190 HTTP/1.1 200

Wed Sep  8 11:18:49 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /monitor/quarantines HTTP/1.1 200
```

IronPort NTP ログの使用

表 5-20　NTP ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、サーバへの Simple Network Time Protocol (SNTP; 簡易ネットワーク タイム プロトコル) クエリーまたは adjust: メッセージで構成されます。

NTP ログの例

次の NTP ログの例は、アプライアンスから NTP ホストへの 2 度のポーリングを示しています。

```
Thu Sep  9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset
-652

Thu Sep  9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us
next_poll: 4096

Thu Sep  9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset
-1152

Thu Sep  9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us
next_poll: 4096
```

IronPort アンチスパムの使用

表 5-21　アンチスパム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、アンチスパム アップデートの確認と結果（エンジンまたはアンチスパム ルールのアップデートが必要であったかどうかなど）で構成されます。

アンチスパム ログの例

次のアンチスパム ログの例は、アンチスパム エンジンによる、スパム定義のアップデートおよび CASE アップデートの確認を示しています。

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) :
case-daemon: server successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) :
startup: Region profile: Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy:
Fuzzy plugin v7 successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) :
uribllocal: running URI blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config:
Finished loading configuration
```

IronPort アンチウイルス ログの使用

表 5-22　アンチウイルス ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、アンチウイルス アップデートの確認と結果（エンジンまたはウイルス定義のアップデートが必要であったかどうかなど）で構成されます。

アンチウイルス ログの例

次のアンチウイルス ログの例は、Sophos アンチウイルス エンジンによる、ウイルス定義（IDE）とエンジン自体のアップデートの確認を示しています。

```
Thu Sep  9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep  9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine
update needed

Thu Sep  9 14:18:04 2004 Info: Current IDE serial=2004090902. No update
needed.
```

このログを一時的に DEBUG レベルに設定すると、アンチウイルス エンジンが所定のメッセージについて特定の結果を返した理由を診断するのに役立ちます。DEBUG ロギング情報は冗長です。使用の際は注意してください。

IronPort スパム検疫ログの使用

表 5-23　IronPort スパム ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、実行されたアクション（メッセージの検疫、検疫エリアからの解放など）で構成されます。

IronPort スパム検疫ログの例

次のログの例は、検疫から admin@example.com にメッセージ（MID 8298624）が解放されていることを示しています。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for
all

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624
(skipping work queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to
admin@example.com

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625
(skipping work queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to
admin@example.com
```

IronPort スパム検疫 GUI ログの使用

表 5-24　IronPort スパム GUI ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	メッセージは、ユーザ認証などの実行されたアクションで構成されます。

IronPort スパム検疫 GUI ログの例

次のログの例は、成功した認証、ログイン、およびログアウトを示しています。

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port
82

Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1,
port 83

Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin

Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

IronPort LDAP デバッグ ログの使用

表 5-25　LDAP デバッグ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻
Message	LDAP デバッグ メッセージ。

LDAP デバッグ ログの例

（注）　ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

```
1    Thu Sep  9 12:24:56 2004 Begin Logfile

2    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

3    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

4    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

5    Thu Sep  9 12:28:08 2004 LDAP: Clearing LDAP cache

6    Thu Sep  9 13:00:09 2004 LDAP: Query
     '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun
     (sun.qa:389)

7    Thu Sep  9 13:00:09 2004 LDAP: After substitute, query is
     '(&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d000
     02b.loc@ldap.route.local.add00002.qa))'

8    Thu Sep  9 13:00:09 2004 LDAP: connecting to server

9    Thu Sep  9 13:00:09 2004 LDAP: connected
```

```
10   Thu Sep  9 13:00:09 2004 LDAP: Query
     (&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d0000
     2b.loc@ldap.route.local.add00002.qa)) returned 1 results

11   Thu Sep  9 13:00:09 2004 LDAP: returning: [<LDAP:>]
```

前述のログ ファイルを読み取るためのガイドとして使用してください。

表 5-26　LDAP デバッグ ログの例の詳細

行番号	説明
1.	ログ ファイルが開始されます。
2. **3.** **4.**	リスナーは、明確に「sun.masquerade」という LDAP クエリーによって、マスカレードに LDAP を使用するように設定されています。 アドレス employee@routing.qa が LDAP サーバで検索され、一致が検出されます。その結果のマスカレード アドレスは employee@mail.qa であり、マスカレードの設定によってこのアドレスがメッセージ ヘッダー、エンベロープ送信者、またはその両方に書き込まれます。
5.	ユーザは手動で `ldapflush` を実行しています。
6.	クエリーは、sun.qa、ポート 389 に送信されます。クエリー テンプレートは (&(ObjectClass={g})(mailLocalAddress={a})) です。 {g} は、発信側フィルタ（rcpt-to-group または mail-from-group ルール）で指定されたグループ名に置換されます。 {a} は、当該のアドレスに置換されます。
7. **8.**	ここで代入（前述のとおり）が実行されます。LDAP サーバに送信される前のクエリーはこのようになります。
9.	サーバへの接続がまだ確立されていないので、接続します。

表 5-26　LDAP デバッグ ログの例の詳細（続き）

行番号	説明
10.	サーバに送信されるデータです。
11.	結果は、確実に空になります。つまり、1 つのレコードが返されますが、クエリーはフィールドを要求していないので、データは報告されません。これらは、データベースに一致があるかどうかをクエリーでチェックするときに、グループ クエリーと許可クエリーの両方に使用されます。

セーフリスト/ブロックリスト ログの使用

表 5-27 に、セーフリスト/ブロックリスト ログに記録される統計情報を示します。

表 5-27　セーフリスト/ブロックリスト ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

セーフリスト/ブロックリスト ログの例

次のセーフリスト/ブロックリスト ログの例は、アプライアンスによって 2 時間ごとにデータベースのスナップショットが作成されていることを示しています。送信者がデータベースに追加された時刻も表示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007
Info: Version: 6.0.0-425 SN: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007
Info: Time offset from UTC: 10800 seconds Fri Sep 28 14:22:33 2007 Info:
System is coming up.

Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been
created.

Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been
created.
```

```
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been
created.

Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been
created.

Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been
created.

.........................

Mon Oct  1 14:16:09 2007 Info: SLBL: The database snapshot has been
created.

Mon Oct  1 14:37:39 2007 Info: SLBL: The database snapshot has been
created.

Mon Oct  1 15:31:37 2007 Warning: SLBL: Adding senders to the database
failed.

Mon Oct  1 15:32:31 2007 Warning: SLBL: Adding senders to the database
failed.

Mon Oct  1 16:37:40 2007 Info: SLBL: The database snapshot has been
created.
```

レポーティング ログの使用

表 5-28 に、レポーティング ログに記録される統計情報を示します。

表 5-28　レポーティング ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング ログの例

次のレポーティング ログの例は、情報ログ レベルに設定されたアプライアンスを示しています。

```
Wed Oct  3 13:39:53 2007 Info: Period minute using 0 (KB)

Wed Oct  3 13:39:53 2007 Info: Period month using 1328 (KB)

Wed Oct  3 13:40:02 2007 Info: Update 2 registered appliance at
2007-10-03-13-40

Wed Oct  3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not
found: 1692

Wed Oct  3 13:40:53 2007 Info: Period hour using 36800 (KB)

Wed Oct  3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct  3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct  3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct  3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533
seconds

Wed Oct  3 13:41:02 2007 Info: Update 2 registered appliance at
2007-10-03-13-41

Wed Oct  3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not
found: 1692

Wed Oct  3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct  3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct  3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct  3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct  3 13:42:03 2007 Info: Update 2 registered appliance at
2007-10-03-13-42
```

レポーティング クエリー ログの使用

表 5-29 に、レポーティング クエリー ログに記録される統計情報を示します。

表 5-29　レポーティング クエリー ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング クエリー ログの例

次のレポーティング クエリー ログの例は、アプライアンスによって、2007 年 8 月 29 日から 10 月 10 日までの期間で毎日の発信メール トラフィック クエリーが実行されていることを示しています。

```
Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804480.

Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610229
for ['MAIL_OUTGOING_TRAFFIC_SUMMARY.

DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTEN

T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI

PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29
to 2007-10-01 with key constraints

 None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM']
returning results from 0 to 2 sort_ascendin

g=False.

Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610229.
```

```
Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610230
for ['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM

ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range
2007-08-29 to 2007-10-01 with key constra

ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES']
returning results from 0 to 2 sort

_ascending=False.

Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

アップデータ ログの使用

表 5-30　アップデータ ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、システム サービス アップデート情報のほか、AsyncOS によるアップデートの確認と、スケジュールされている次回アップデートの日時で構成されます。

アップデータ ログの例

次のログの例は、アプライアンスが新規の McAfee アンチウイルス定義でアップデートされていることを示しています。

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update
11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for
mcafee
```

```
Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server
manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:12:52 2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files

Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:17:52 2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:22:52 2008
```

トラッキング ログについて

トラッキング ログには、AsyncOS の電子メール動作に関する情報が記録されます。ログ メッセージは、メール ログに記録されたメッセージのサブセットです。

トラッキング ログは、メッセージ トラッキング データベースを作成するため、メッセージ トラッキング コンポーネントで使用されます。ログ ファイルはデータベースの作成プロセスで消費されるので、トラッキング ログは一過性のものになります。トラッキング ログの情報は、人による読み取りや解析を目的とした設計になっていません。

トラッキング ログは、リソースの効率性を保つためにバイナリ形式で記録され、転送されます。情報は、論理的にレイアウトされ、IronPort が提供するユーティリティを使用して変換した後は人による読み取りが可能になります。変換ツールは、次の URL にあります。
`http://tinyurl.com/3c5l8r`

認証ログの使用

認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

表 5-31　認証ログの統計情報

統計	説明
Timestamp	バイトが送信された時刻。
Message	メッセージは、アプライアンスにログインしようとしたユーザのユーザ名と、そのユーザが正常に認証されたかどうかという情報で構成されます。

認証ログの例

次のログの例は、「admin」、「joe」、および「dan」というユーザによるログイン試行を示しています。

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX
```

```
Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds

Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

ログ サブスクリプション

ここでは、次の項目について説明します。

ログ サブスクリプションの設定

[System Administration] の [Log Subscriptions] ページ（または CLI の `logconfig` コマンド）を使用して、ログ サブスクリプションを設定します。ログ サブスクリプションによって、エラーを含む AsyncOS アクティビティの情報

を保存するログ ファイルが作成されます。ログ サブスクリプションは、別のコンピュータに配信（プッシュ）、または別のコンピュータから取得（ポーリング）されます。一般に、ログ サブスクリプションには次の属性があります。

表 5-32　ログ ファイルの属性

属性	説明
Log type	記録される情報のタイプと、ログ サブスクリプションの形式を定義します。詳細については、表 5-1「ログ タイプ」（P.162）を参照してください。
Name	今後の参照に使用するログ サブスクリプションのニックネーム。
Log level	ログ サブスクリプションごとに詳細のレベルを設定します。
Retrieval method	ログ サブスクリプションを Cisco IronPort アプライアンスから転送する方法を定義します。
Log filename	ディスクに書き込むときのファイルの物理名に使用されます。複数の Cisco IronPort アプライアンスを使用している場合、ログ ファイルを生成したシステムを識別するため、ログ ファイル名を固有にする必要があります。
Maximum File Size	ファイルの最大サイズ。このサイズに到達すると、ローリング オーバーされます。

ログ レベル

ログ レベルによって、ログに送信される情報量が決定します。ログには、5 つの詳細レベルのいずれかを設定できます。詳細レベルを高くするほど大きいログ ファイルが作成され、システムのパフォーマンスが低下します。詳細レベルの高い設定には、詳細レベルの低い設定に保持されるすべてのメッセージと、その他のメッセージも含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。

（注）　ログ レベルは、すべてのメール ログ タイプに対して選択できます。

表 5-33　ログ レベル

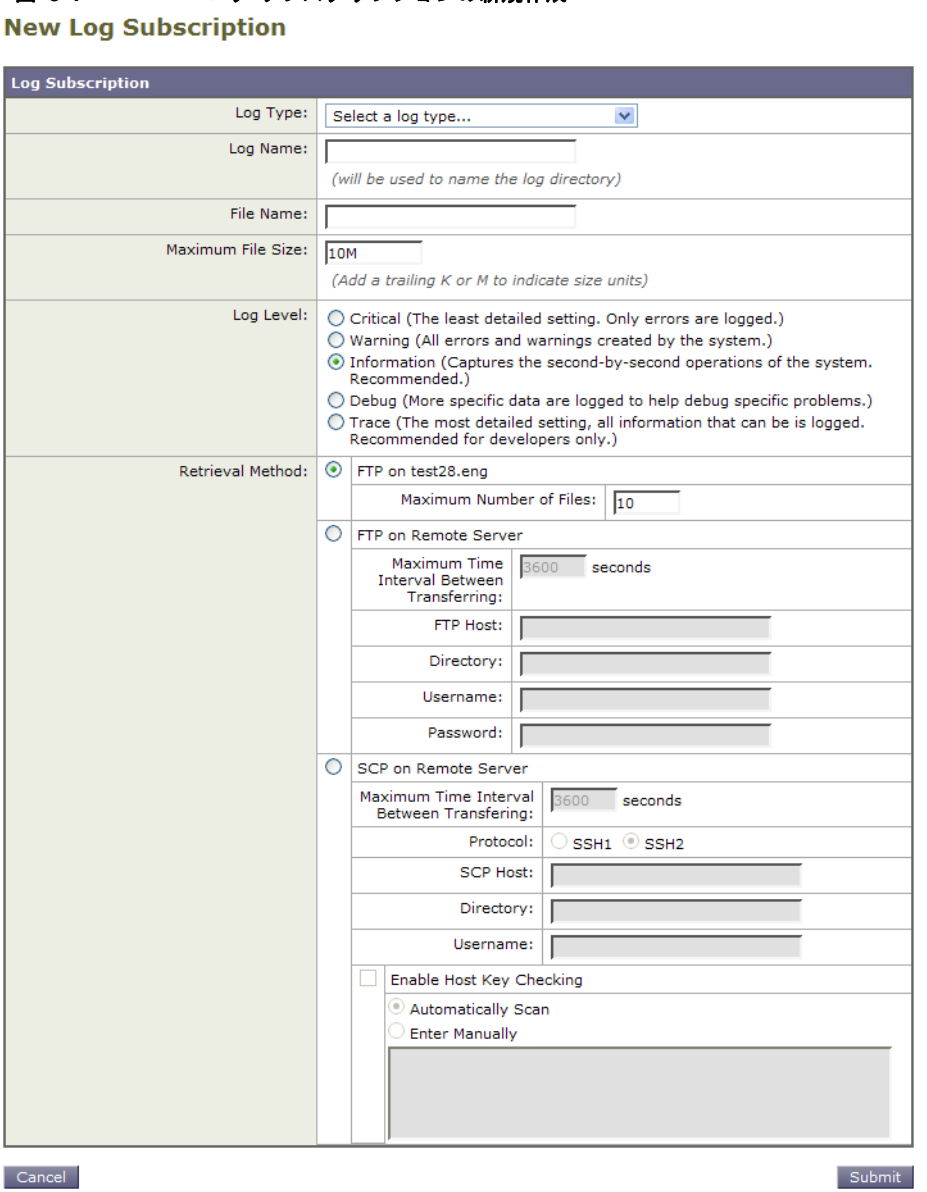
ログ レベル	説明
Critical	詳細レベルの最も低い設定。エラーだけがログに記録されます。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできませんが、ログ ファイルがすぐには最大サイズに達しなくなります。このログ レベルは、syslog レベル「Alert」と同等です。
Warning	システムによって作成されたすべてのエラーと警告。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできません。このログ レベルは、syslog レベル「Warning」と同等です。
Information	情報設定では、システムの秒単位の動作がキャプチャされます。たとえば、接続のオープンや配信試行などです。Information レベルは、ログに推奨される設定です。このログ レベルは、syslog レベル「Info」と同等です。
Debug	エラーの原因を調べるときは、Debug ログ レベルを使用します。この設定は一時的に使用し、後でデフォルト レベルに戻します。このログ レベルは、syslog レベル「Debug」と同等です。
Trace	Trace ログ レベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログ レベルは、syslog レベル「Debug」と同等です。

GUI でのログ サブスクリプションの作成

ログ サブスクリプションを作成するには、次の手順を実行します。

ステップ 1　[Log Subscription] ページで [Add Log Subscription] をクリックします。次の [New Log Subscription] ページが表示されます。

図 5-1　ログ サブスクリプションの新規作成



ステップ 2　ログ タイプを選択し、ログ名（ログ ディレクトリ用）とログ ファイル自体の名前を入力します。

ステップ 3　最大ファイル サイズとログ レベルを指定します。

ステップ 4　ログの取得方法を設定します。

ステップ 5　変更を送信し、保存します。

ログ サブスクリプションの編集

ログ サブスクリプションを編集するには、次の手順を実行します。

ステップ 1　[Log Subscriptions] ページの [Log Name] カラムにあるログ名をクリックします。[Edit Log Subscription] ページが表示されます。

ステップ 2　ログ サブスクリプションを変更します。

ステップ 3　変更を送信し、保存します。

ロギングに対するグローバル設定

システムは、IronPort テキスト メール ログおよび IronPort ステータス ログ内にシステムの測定を定期的に記録します。[System Administration] > [Log Subscriptions] ページの [Global Settings] セクションにある [Edit Settings] ボタン（または、CLI の `logconfig -> setup` コマンド）を使用して、次の情報を設定します。

- システムの測定頻度。これは、システムが測定を記録するまで待機する時間（秒単位）です。
- メッセージ ID ヘッダーを記録するかどうか。
- リモート応答ステータス コードを記録するかどうか。
- 元のメッセージのサブジェクト ヘッダーを記録するかどうか。
- メッセージごとにログに記録するヘッダーのリスト。

すべての IronPort ログには、次の 3 つのデータを任意で記録できます。

1. Message-ID

このオプションを設定すると、可能な場合はすべてのメッセージのメッセージ ID ヘッダーがログに記録されます。このメッセージ ID は、受信したメッセージから取得される場合と、AsyncOS 自体で生成される場合があります。次の例を参考にしてください。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

2. Remote Response

   このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次の例を参考にしてください。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as
9C8B425DA7'
```

   リモート応答文字列は、SMTP 会話配信時の DATA コマンドへの応答後に受信される、人が読み取ることのできるテキストです。この例では、接続ホストが data コマンドを実行した後のリモート応答が、「queued as 9C8B425DA7」となります。

```
[...]

250 ok hostname

250 Ok: queued as 9C8B425DA7
```

   文字列の先頭にある空白や句読点（および、250 応答の場合は OK 文字）は除去されます。文字列の末尾については、空白だけが除去されます。たとえば、IronPort アプライアンスはデフォルトで、DATA コマンドに対して 250 Ok: Message MID accepted という文字列で応答します。したがって、リモート ホストが別の IronPort アプライアンスである場合は、文字列「Message MID accepted」がログに記録されます。

3. Original Subject Header

このオプションをイネーブルにすると、各メッセージの元のサブジェクト ヘッダーがログに記録されます。

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2

Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>

Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>

Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'

Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

メッセージ ヘッダーのロギング

場合によっては、メッセージがシステムを通過するときに、メッセージのヘッダーの存在と内容を記録する必要があります。[Log Subscriptions Global Settings] ページ（または、CLI の `logconfig` -> `logheaders` サブコマンド）に、記録するヘッダーを指定します。Cisco IronPort アプライアンスは、指定されたメッセージ ヘッダーを IronPort テキスト メール ログ、IronPort 配信ログ、および IronPort バウンス ログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。

（注） システムは、ロギングに指定したヘッダーに関係なく、メッセージの記録処理中に随時、メッセージに存在するすべてのヘッダーを評価します。

（注） SMTP プロトコルについての RFC は、`http://www.faqs.org/rfcs/rfc2821.html` にあります。この RFC には、ユーザ定義のヘッダーが規定されています。

（注）　logheaders コマンドを使用してヘッダーをログに記録するように設定している場合、ヘッダー情報は配信情報の後に表示されます。

表 5-34　ログ ヘッダー

Header name	ヘッダーの名前
Value	ログに記録されるヘッダーの内容

たとえば、ログに記録するヘッダーとして「date, x-subject」を指定すると、メール ログに次の行が表示されます。

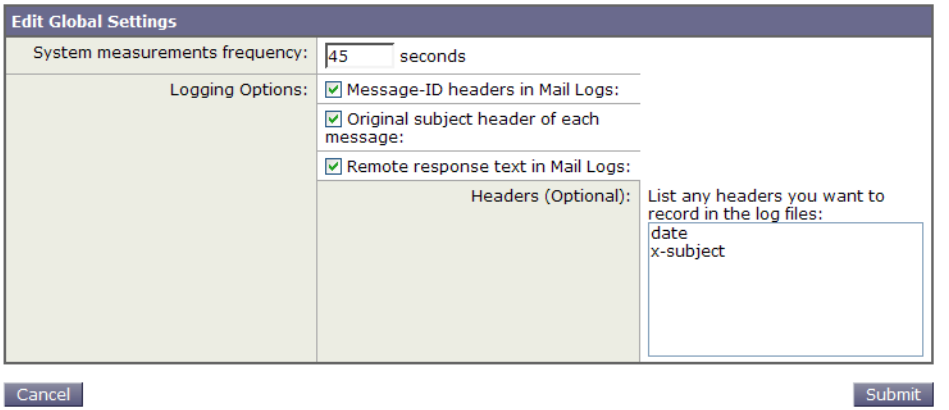
```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this
header')]
```

GUI を使用したロギングのグローバル設定

ロギングのグローバル設定を行うには、次の手順を実行します。

ステップ 1　[Log Subscriptions] ページの [Global Settings] セクションにある [Edit Settings] ボタンをクリックします。[Log Subscriptions Global Settings] ページが表示されます。

図 5-2　ログ サブスクリプションのグローバル設定



ステップ 2　システム測定頻度、メール ログにメッセージ ID ヘッダーを加えるかどうか、リモート応答を加えるかどうか、および各メッセージの元のサブジェクト ヘッダーを加えるかどうかを指定します。

ステップ 3　ログに加えるその他のヘッダーを入力します。

ステップ 4　変更を送信し、保存します。

ログ サブスクリプションのロール オーバー

IronPort AsyncOS は、[Log Subscriptions Global Settings] ページ（または CLI の `logconfig` コマンド）での設定に基づいてログ ファイルをロール オーバーします。また、[Log Subscriptions] ページの [Rollover Now] ボタンをクリックするか、`rollovernow` コマンドを使用することによって、必要に応じてログ ファイルをロールオーバーできます。IronPort AsyncOS がログ ファイルをロール オーバーすると、次のことが行われます。

- ロールオーバーのタイムスタンプで新規のログ ファイルが作成され、文字「`c`」の拡張子によって現在のファイルとして指示されます。
- 現在のログ ファイルが、保存済みを示す文字「`s`」の拡張子付きに名前変更されます。
- 新たに保存されたログ ファイルがリモート ホストに転送されます（プッシュ ベースの場合）。

- 同じサブスクリプションから以前に失敗したログ ファイルが転送されます（プッシュ ベースの場合）。
- 保持するファイルの合計数を超えた場合は、ログ サブスクリプション内の最も古いファイルが削除されます（ポーリング ベースの場合）。

GUI を使用したログ サブスクリプションのロール オーバー

ログ サブスクリプションをロール オーバーするには、次の手順を実行します。

ステップ 1　[Log Subscriptions] ページで、ロール オーバーするログの右側のチェックボックスをオンにします。

ステップ 2　任意で、[All] チェックボックスをオンにして、すべてのログをロールオーバー対象として選択できます。

ステップ 3　ロールオーバー対象として 1 つまたは複数のログを選択すると、[Rollover Now] ボタンがイネーブルになります。[Rollover Now] ボタンをクリックして、選択したログをロール オーバーします。

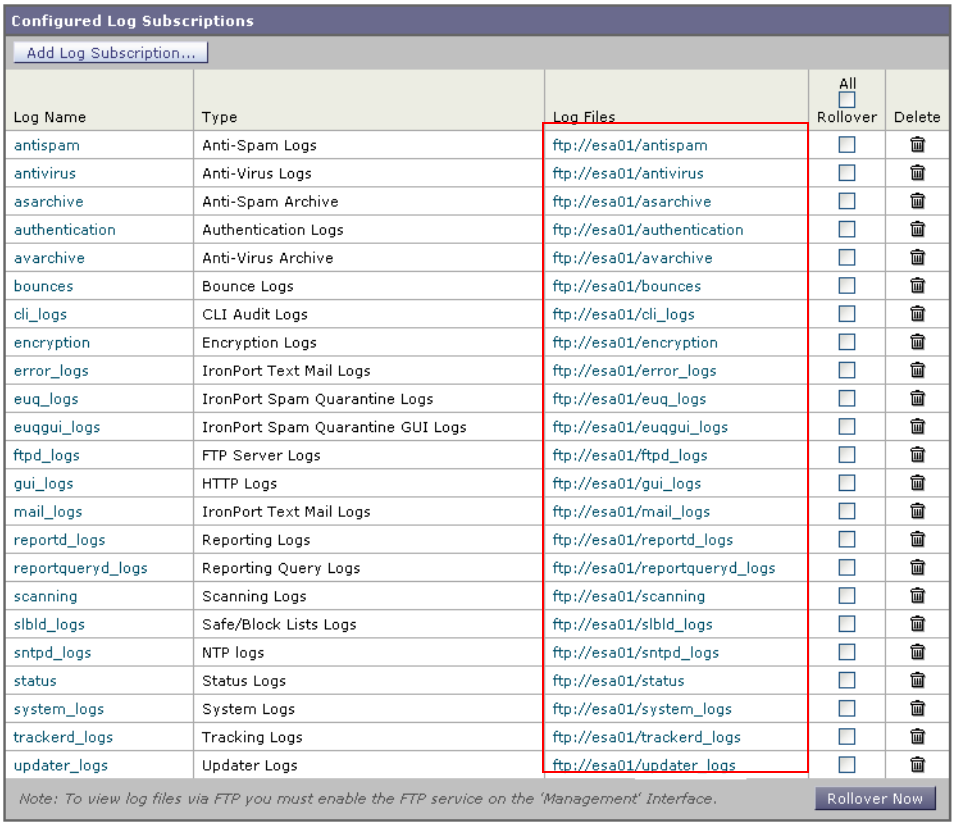
CLI を使用したログ サブスクリプションのロール オーバー

`rollovernow` コマンドを使用すると、一度にすべてのログ ファイルをロール オーバーするか、リストから特定のログ ファイルを選択することができます。

GUI での最近のログ エントリの表示

GUI を介してログ ファイルを表示するには、[Log Subscriptions] ページのテーブルの [Log Files] カラムにあるログ サブスクリプションをクリックします。ログ サブスクリプションへのリンクをクリックすると、パスワードの入力を求められてから、そのサブスクリプションに対するログ ファイルの一覧が表示されます。次に、いずれかのログ ファイルをクリックして、ブラウザに表示したり、ディスクに保存したりすることができます。GUI を介してログを表示するには、管理インターフェイスで FTP サービスをイネーブルにしておく必要があります。

図 5-3　ログ サブスクリプションのグローバル設定



CLI での最近のログ エントリの表示（tail コマンド）

AsyncOS では、アプライアンスに設定されたログの最新エントリを表示する `tail` コマンドをサポートしています。`tail` コマンドを実行し、現在設定されているログのうち、表示するログの番号を選択します。Ctrl+ C を押して、`tail` コマンドを終了します。

例

次に、tail コマンドを使用してシステム ログを表示する例を示します（このログは、特に commit コマンドによるユーザのコメントを追跡します）。また、tail コマンドでは、パラメータとして表示するログの名前 tail mail_logs が受け入れられています。

```
mail3.example.com> tail


Currently configured logs:

1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll

4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll

6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll

7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll

8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll

9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll

10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP
Poll

11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval:
FTP Poll

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll

13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll

14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
```

```
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll

16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP
Poll

17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll

18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll

19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll

20. "status" Type: "Status Logs" Retrieval: FTP Poll

21. "system_logs" Type: "System Logs" Retrieval: FTP Poll

22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll

23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll



Enter the number of the log you wish to tail.

[]> 19



Press Ctrl-C to stop.

Sat May 15 12:25:10 2008 Info: PID 274: User system commit changes:
Automated Update for Quarantine Delivery Host

Sat May 15 23:18:10 2008 Info: PID 19626: User admin commit changes:

Sat May 15 23:18:10 2008 Info: PID 274: User system commit changes:
Updated filter logs config

Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes:
Receiving suspended.

^Cmail3.example.com>
```

ホスト キーの設定

`logconfig -> hostkeyconfig` サブコマンドを使用して、IronPort アプライアンスから他のサーバにログをプッシュするときに、SSH で使用するホスト キーを管理します。SSH サーバには、秘密キーと公開キーの 2 つのホスト キーが必要です。秘密ホスト キーは SSH サーバにあり、リモート マシンから読み取ることはできません。公開ホスト キーは、SSH サーバと対話する必要のある任意のクライアント マシンに配信されます。

（注） ユーザ キーを管理するには、「セキュア シェル（SSH）キーの管理」（P.8-357）を参照してください。

`hostkeyconfig` サブコマンドによって、次の機能が実行されます。

表 5-35　ホスト キーの管理：サブコマンドのリスト

コマンド	説明
New	新しいキーを追加します。
Edit	既存のキーを変更します。
Delete	既存のキーを削除します。
Scan	ホスト キーを自動的にダウンロードします。
Print	キーを表示します。
Host	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに配置される値です。
Fingerprint	システム ホスト キーのフィンガープリントを表示します。
User	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

次の例では、AsyncOS によってホスト キーがスキャンされ、ホスト用に追加されます。

```
mail3.example.com> logconfig


Currently configured logs:

[ list of logs ]


Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]> hostkeyconfig


Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]


Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.
```

```
- DELETE - Remove a key.

- SCAN - Automatically download a host key.

- PRINT - Display a key.

- HOST - Display system host keys.

- FINGERPRINT - Display system host key fingerprints.

- USER - Display system user keys.

[]> scan


Please enter the host or IP address to lookup.

[]> mail3.example.com


Choose the ssh protocol type:

1. SSH1:rsa

2. SSH2:rsa

3. SSH2:dsa

4. All

[4]>


SSH2:dsa

mail3.example.com ssh-dss

[ key displayed ]
```

```
SSH2:rsa

mail3.example.com ssh-rsa

[ key displayed ]


SSH1:rsa

mail3.example.com 1024 35

[ key displayed ]


Add the preceding host key(s) for mail3.example.com? [Y]>


Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

2. mail3.example.com ssh-rsa [ key displayed ]

3. mail3.example.com 1024 35 [ key displayed ]


Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.

- DELETE - Remove a key.

- SCAN - Automatically download a host key.

- PRINT - Display a key.

- HOST - Display system host keys.
```

```
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>

Currently configured logs:
[ list of configured logs ]

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>

mail3.example.com> commit
```