



WAE のモニタリング

この章では、WAFS ネットワークにおける役割に関係なく Wide Area Application Engine (WAE) をモニタリングする方法について説明します。この章には、次の項があります。

- [WAE のモニタリング、11-2 ページ](#)
- [WAE のクリティカル ドライブのモニタリング、11-17 ページ](#)
- [システム ロギングとアラームの設定、11-21 ページ](#)



(注)

Cisco WAFS 3.0 ソフトウェアは、FE-511 File Engine と、WAE-611 および WAE-7326 Wide Area Application Engine で動作します。簡潔にするため、説明文の中や使用例のコマンド プロンプトの部分では、単に WAE と記述していますが、特に注釈がないかぎり、3 つのプラットフォームすべてに当てはまります。

この章で取り上げる CLI コマンドの完全な構文と使用方法の詳細については、『*Cisco WAFS 3.0 Command Reference*』を参照してください。

WAE のモニタリング

パフォーマンスの測定基準を設けたり、設定の微調整や追加の WAE の配置が必要となったときにその兆候を見極めたりするためには、WAE のモニタリングが非常に重要となります。ここでは、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) と WAFS ソフトウェア アラームを使用して WAE をモニタリングする方法について説明します。WAE のパフォーマンスをモニタリングするために、Cisco Discovery Protocol (CDP; シスコ検出プロトコル)、SNMP、WAFS ソフトウェア アラームをはじめとするいくつかのツールを使用できます。詳細については、次の項を参照してください。

- [CDP を使用した WAE のモニタリング、11-2 ページ](#)
- [SNMP を使用した WAE のモニタリング、11-2 ページ](#)
- [WAFS ソフトウェア アラームを使用した WAE のモニタリング、11-10 ページ](#)

CDP を使用した WAE のモニタリング

CDP は、すべてのシスコ製デバイス上で稼働するデバイス検出プロトコルです。CDP を使用すると、ネットワーク内の各デバイスは、ネットワーク内のその他のすべてのデバイスに定期的にメッセージを送信します。デバイスは、その他のデバイスが送信した定期的なメッセージを受信して、隣接デバイスについて学習し、それらのインターフェイスのステータスを判断します。

CDP を使用して、ネットワーク管理アプリケーションは、隣接デバイスのデバイス タイプと SNMP エージェント アドレスを学習できます。その後、アプリケーションは、ネットワーク内に SNMP クエリーを送信できます。また、CiscoWorks2000 は、起動後に WAE が送信した CDP パケットを認識することで、WAE を検出します。

WAE 関連の作業では、WAE プラットフォームの存在、タイプ、およびバージョンをシステム マネージャに通知できるように、WAE プラットフォームが CDP をサポートしている必要があります。

次の例では、単一の CLI コマンドを使用して、WAE 上の CDP 実装をイネーブルにしています。

```
WAE(config)# interface GigabitEthernet 1/0 cdp enable
```

SNMP を使用した WAE のモニタリング

Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) は、SNMP エージェントを介して WAE を外部モニタリングできる、相互運用可能な標準ベースのプロトコルです。

SNMP によって管理されるネットワークは、管理対象デバイス、エージェント、および管理システムの 3 つの基本コンポーネントから構成されます。

- 管理対象デバイスは、SNMP エージェントを持つネットワーク ノードで、管理対象ネットワークに常駐します。
- 管理対象デバイスは、管理情報を収集および格納し、SNMP を使用して、SNMP を使用する管理システムがこの情報を使用できるようにします。管理対象デバイスには、ルータ、アクセスサーバ、スイッチ、ブリッジ、ハブ、コンピュータ ホスト、およびプリンタが含まれます。
- SNMP エージェントは、管理対象デバイスに常駐するソフトウェア モジュールです。エージェントは、管理情報のうちローカルに関する知識を保持し、その情報を SNMP と互換可能な形式に変換します。SNMP エージェントは、MIB (Management Information Base; 管理情報ベース) からデータを収集します。MIB は、デバイス パラメータとネットワーク データに関する情報のリポジトリです。また、エージェントは、トラップ、つまり特定イベントの通知をマネージャに送信することもできます。

WAFS 3.x ソフトウェアを稼働する各 WAE には、WAE のデバイス設定とアクティビティに関する情報の収集を担当する SNMP エージェントがあります。事前に、SNMP 管理アプリケーションが管理ステーションに展開されていないと、この SNMP 情報にはアクセスできません。この SNMP 管理ステーションは、SNMP を使用して、WAE からの情報を取得するための SNMP Get 要求をデバイスエージェントに送信するため、*SNMP ホスト*と呼ばれています。

SNMP 管理ステーションとデバイスエージェント（WAE 上の SNMP エージェント）は、SNMP を使用して、次のように通信します。

1. SNMP 管理ステーション（SNMP ホスト）は、SNMP を使用して WAE に情報を要求します。
2. これらの SNMP 要求を受信すると、WAE 上のデバイス エージェントは、個々のデバイス（WAE）に関する情報を保持しているテーブルにアクセスします。このテーブル、またはデータベースが、MIB と呼ばれます。

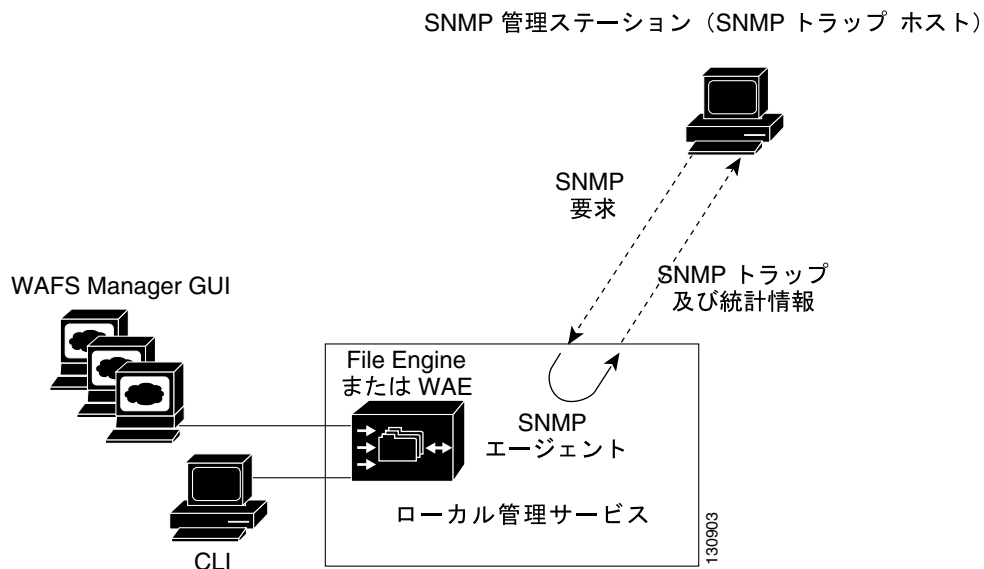


(注) WAE 上の SNMP エージェントは、異常な状況でのみ SNMP ホストとの通信を開始します。つまり、ホストに送信する必要のあるトラップがある場合にホストとの通信を開始します。この項目の詳細については、11-8 ページの「SNMP トラップを送信するための WAE の設定」を参照してください。

3. デバイス エージェントは、MIB 内で指定された情報を見つけると、SNMP を使用して、その情報を SNMP 管理ステーションに送信します。

図 11-1 は、WAE に対するこれらの SNMP 動作を示しています。

図 11-1 SNMP コンポーネントと WAFS WAE との連携動作



SNMP のバージョンの違いについて

WAFS 3.x ソフトウェアは、次の SNMP のバージョンをサポートします。

- バージョン 1 (SNMPv1) SNMP の初期の実装です。機能の詳細については、RFC 1157 を参照してください。
- バージョン 2 (SNMPv2c) SNMP の 2 番目のリリースで、RFC 1902 に規定されています。データタイプ、カウンタサイズ、およびプロトコル動作が追加されています。
- バージョン 3 (SNMPv3) 最新バージョンの SNMP で、RFC 2271 ~ RFC 2275 に規定されています。

SNMP セキュリティ モデルおよびセキュリティ レベル

SNMPv1 および SNMPv2c には、ワイヤ上の SNMP パケットトラフィックの機密性を保持するためのセキュリティ（つまり、認証またはプライバシー）メカニズムがありません。その結果、ワイヤ上のパケットが検出され、SNMP コミュニティストリングが見破られてしまうことがあります。

SNMPv1 および SNMPv2c のセキュリティ上の欠点を解決するために、SNMPv3 では、ネットワークを経由するパケットを認証および暗号化することで、WAE への安全なアクセスを提供しています。WAFS 3.x ソフトウェアの SNMP エージェントは、SNMPv3 はもちろん、SNMPv1 と SNMPv2c もサポートします。

SNMPv3 で提供されるセキュリティ機能は、次のとおりです。

- メッセージの完全性 伝送中にパケットが一切妨害されていないことを保証します。
- 認証 有効な送信元からのメッセージであるかどうかを判別します。
- 暗号化 不正な送信元によってパケットが認識されてしまうのを防ぐため、パケットの内容をスクランブルします。

SNMPv3 は、セキュリティ モデルだけでなく、セキュリティ レベルも備えています。セキュリティ モデルは、ユーザと、ユーザが所属するグループに対して設定される認証プロセスです。セキュリティ レベルは、セキュリティ モデルの中で許容されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットの処理時に使用されるセキュリティ プロセスが決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2c、および SNMPv3 の 3 つです。

表 11-1 は、セキュリティ モデルとセキュリティ レベルの組み合わせをまとめたものです。

表 11-1 SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	プロセス
v1	noAuthNoPriv	コミュニティストリング	なし	ユーザ認証の照合にコミュニティストリングを使用します。
v2c	noAuthNoPriv	コミュニティストリング	なし	ユーザ認証の照合にコミュニティストリングを使用します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ認証の照合にユーザ名を使用します。
v3	AuthNoPriv	Message Digest 5 (MD5; メッセージダイジェスト 5) または Secure Hash Algorithm (SHA)	なし	Hash-Based Message Authentication Code (HMAC; ハッシュベースのメッセージ認証コード) -MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。
v3	AuthPriv	MD5 または SHA	あり	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。Cipher Block Chaining (CBC; 暗号ブロック連鎖) -Data Encryption Standard 56-bit (DES-56; データ暗号規格 56 ビット) に基づく、DES-56 暗号化 (パケット認証) を提供します。

SNMPv3 エージェントは、次のモードで使用できます。

- noAuthNoPriv モード パケットに対してオンになっているセキュリティ メカニズムはありません。
- AuthNoPriv モード プライバシー アルゴリズム (DES-56) を使用して、パケットを暗号化する必要はありません。
- AuthPriv モード パケットを暗号化する必要があります。プライバシーを保持するには、パケットに対して認証を実行する必要があります。

SNMPv3 を使用すれば、ユーザは、データが改ざんされる恐れを抱くことなく、SNMP エージェントから管理情報を安全に収集できます。また、WAE の設定を変更する SNMP set パケットなどの機密情報は、ワイヤ上で内容が露呈するのを防ぐために、暗号化することができます。グループベースの管理モデルでは、さまざまなユーザが異なるアクセス特権で同じ SNMP エージェントにアクセスすることができます。

サポートされる MIB

SNMP の WAFS 3.x ソフトウェア実装は、次の MIB をサポートします。

- ACTONA-ACTASTORE-MIB
- CISCO-CDP-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONTENT-ENGINE-MIB (一部。アラーム関連の MIB オブジェクトとディスク障害トラップのみ)
- ENTITY-MIB
- EVENT-MIB
- HOST-RESOURCES-MIB
- MIB-II
- SNMPv2

これらの MIB の詳細については、『Cisco WAFS 3.0 MIB Quick Reference』を参照してください。

MIB ファイルの WAE へのダウンロード

WAFS 3.x ソフトウェアを稼働する WAE によってサポートされる MIB はすべて、MIB ファイルを次の Cisco FTP サイトからダウンロードできます。

`ftp://ftp.cisco.com/pub/mibs/v2`

各 MIB に定義されている MIB オブジェクトは、上記 FTP サイトの MIB ファイルに、一目でわかる形で記述されています。

WAE の SNMP エージェントのイネーブル化

デフォルトでは、WAE の SNMP エージェントはディセーブルで、SNMP コミュニティ スtring は定義されていません。SNMP コミュニティ スtring は、WAE の SNMP エージェントへアクセスするときに、認証用のパスワードとして使用されます。認証されるには、WAE に送信された SNMP メッセージの Community Name フィールドが、WAE に定義された SNMP コミュニティ スtring に一致している必要があります。

SNMP コミュニティ スtring が WAE に定義されている場合、その WAE 上の SNMP エージェントはイネーブルです。WAFS Manager GUI または CLI を使用して、SNMP コミュニティ スtring を定義し、SNMP エージェントをイネーブルにすることができます。

CLI から、**snmp-server community** コマンドを使用します。たとえば、次のように入力します。

```
WAE(config)# snmp-server community comaccess
```

SNMP 要求に SNMPv3 プロトコルが使用されている場合は、次のステップで、SNMP ユーザ アカウントを定義します。このアカウントは、SNMP を使用して WAE にアクセスするために使用できます。WAE で SNMPv3 ユーザ アカウントを作成する方法の詳細については、[11-6 ページの「WAE の SNMP ユーザの定義」](#)を参照してください。

WAE の SNMP ユーザの定義

WAE に SNMP ユーザを定義する手順は、次のとおりです。

- SNMP 要求に SNMPv3 プロトコルが使用されている場合は、SNMP を使用して WAE にアクセスするために、少なくとも 1 つの SNMPv3 ユーザ アカウントを WAE に定義する必要があります。
- SNMPv1 または SNMPv2c セキュリティ モデルにしたがって定義されたグループは、SNMP ユーザには関連付けないでください。それらは、コミュニティ スtring だけに関連付ける必要があります。

SNMPv3 ユーザの定義

WAFS Manager GUI または CLI のどちらかを使用して、WAE に SNMPv3 ユーザ アカウントを定義できます。

CLI を使用して WAE (SNMP サーバ) に SNMPv3 ユーザ アカウントを定義するには、**snmp-server user** グローバル コンフィギュレーション コマンドを入力します。SNMP アクセスを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server user name group [auth {md5 password [priv password] | sha password [priv password]}
| remote octetstring [auth {md5 password [priv password] | sha password [priv password]}]]
```

次の例では、WAE に SNMPv3 ユーザ アカウントを作成しています。SNMPv3 ユーザは、名前が **acme** で、グループ **admin** に所属します。この SNMP ユーザ アカウントには認証パスワードが設定されていないため、WAE 上の SNMP エージェントは、このユーザからの SNMP 要求に対して認証を実行しません。

```
WAE(config)# snmp-server user acme admin
```

特定の MIB オブジェクトに関する SNMP トラップの設定

SNMP トラップがイネーブルの場合、WAE は、事前に定義された一連の SNMP トラップをモニタリングします。それらを [表 11-2](#) に示しています。

表 11-2 事前に定義された SNMP トラップ

MIB	トラップ
ACTONA-ACTASTORE-MIB	<ul style="list-style-type: none"> • isValid • daysLeft • esConTabIsConnected • esConnectedSessionCount • esCifsOpenFiles • esEvictedAge
EVENT-MIB	<ul style="list-style-type: none"> • mteTriggerFired • mteTriggerRising • mteTriggerFailure • mteEventSetFailure (未実装)
SNMPv2	<ul style="list-style-type: none"> • coldStart • authenticationFailure

snmp trigger グローバル コンフィギュレーション コマンドを使用すると、特定の設定に関連するその他の MIB オブジェクトについて追加の SNMP トラップを定義できます。トラップに対応する任意のサポート MIB から任意の MIB オブジェクトを選択できます。トラップは、さまざまなテストに基づいてトリガーできます。

- **absent** 最後のサンプリングの時点では存在していた指定した MIB オブジェクトが、現在のサンプリング時にはもはや存在していない。
- **equal** 指定した MIB オブジェクトの値が、指定したしきい値に等しい。
- **falling** 指定した MIB オブジェクトの値が、指定したしきい値を下回った。この状況に陥りトラップが生成された後は、サンプル対象の MIB オブジェクト値がしきい値を上回り、再び、下限しきい値を下回らないかぎり、同じ状況に対する別のトラップは生成されません。
- **greater-than** 指定した MIB オブジェクトの値が、指定したしきい値を超えた。
- **less-than** 指定した MIB オブジェクトの値が、指定したしきい値より小さい。
- **on-change** 指定した MIB オブジェクトの値が、最後のサンプリング以降に変更された。
- **present** 指定した MIB オブジェクトが、直前のサンプリング時には存在していなかったが、現在のサンプリング時には存在している。
- **rising** 指定した MIB オブジェクトの値が、指定したしきい値を上回った。この状況に陥りトラップが生成された後は、サンプル対象の MIB オブジェクト値がしきい値を下回り、再び、上限しきい値を上回らないかぎり、同じ状況に対する別のトラップは生成されません。

しきい値は、絶対サンプル タイプまたはデルタサンプル タイプに基づきます。絶対サンプル タイプでは、テストは 0 ~ 4294967295 までの固定小数点整数値に対して評価されます。デルタ サンプル タイプでは、テストは、現在のサンプリングと直前のサンプリングとの間の MIB オブジェクト値の差に対して評価されます。

SNMP トラップを設定したら、作成したイベント トラップを生成させるために、**snmp-server enable traps event** グローバル コンフィギュレーション コマンドを入力する必要があります。また、システムがリポートされても SNMP トラップ設定が失われないように、**snmp mib persist event** グローバル コンフィギュレーション コマンドを使用してイベントを持続的に設定し、**write mib-data EXEC** コマンドを使用して MIB データを保存する必要があります。

次の例は、MIB オブジェクト *esConTabIsConnected* のしきい値を作成し、Edge File Engine として動作する WAE から Core File Engine として動作する WAE への接続が失われたときにトラップが送信されるようにする方法を示しています。

```
WAE# snmp trigger create esConTabIsConnected ?
<60-600> The number of seconds to wait between trigger sample
wildcard Option to treat the MIB variable as wildcarded
WAE# snmp trigger create esConTabIsConnected wildcard 600 ?
absent          Absent existence test
equal           Equalality threshold test
falling         Falling threshold test
greater-than    Greater-than threshold test
less-than       Less-than threshold test
on-change       Changed existence test
present         Present present test
rising          Rising threshold test
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling ?
absolute Absolute sample type
delta          Delta sample type
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute ?
<0-4294967295> Falling threshold value
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 ?
LINE           Trigger-comment
mibvar1        Optional mib object to add to the notification
WAE# snmp trigger create esConTabIsConnected wildcard 600 falling absolute 1 "Lost the
connection with the core server."
WAE# configure
WAE(config)# snmp-server enable traps event
```

一旦、SNMP トラップを送信するように WAE を設定したら、`show snmp events EXEC` コマンドを使用して、この新たに作成されたトラップの結果を表示できます。

また、ユーザが作成した SNMP トラップは削除することもできます。次の例は、前出の例で作成し、*esConTabIsConnected* に対して設定されたトラップを削除する方法を示しています。

```
WAE# snmp trigger delete esConTabIsConnected
```

SNMP トラップを送信するための WAE の設定

WAFS Manager GUI または CLI のどちらかを使用して、SNMP トラップを送信するように WAE を設定できます。SNMP トラップを送信するように WAE を設定する場合は、次のガイドラインにしたがってください。

- SNMP ホストにトラップを受信させるには、設定する必要があるホストに対して、`snmp-server community` コマンド、および `snmp-server enable traps` コマンドと `snmp-server host` コマンドの両方を使用して、SNMP をイネーブルにする必要があります。
- デフォルトでは、SNMP エージェントはディセーブルで、コミュニティ スtring は設定されていません。

WAE で SNMP トラップを設定する手順は、次のとおりです。

ステップ 1 セキュリティ モデル グループ (SNMPv1、SNMPv2c、または SNMPv3) のいずれかを指定します。

```
snmp-server group name {v1 [notify name] [read name] [write name] | v2c [notify name] [read name]
[write name] | v3 {auth [notify name] [read name] [write name] | noauth [notify name] [read
name] [write name] | priv [notify name] [read name] [write name]}}
```

ステップ 2 WAE 上のすべての SNMP トラップをイネーブルにします。

```
WAE(config)# snmp-server enable traps
```

snmp-server enable traps コマンドを入力しないと、トラップは送信されません。すべての SNMP トラップまたは SNMP 認証トラップのみをディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3 WAE からの SNMP トラップを受信するホスト（複数可）を指定します。たとえば、コミュニティ スtring *public* を使用して、すべての SNMP トラップをホスト *192.168.2.160* へ送信するように WAE を設定します。

```
WAE(config)# snmp-server host 192.168.2.160 public
```



(注) SNMP トラップを送信するには、少なくとも 1 台の SNMP トラップ ホストを設定する必要があります。1 つの WAE に最大 8 台の SNMP ホストを設定できます。

ステップ 4 WAE 上の SNMP エージェントをイネーブルにし、WAE 上の SNMP エージェントにアクセスしたときの認証用のパスワードとしてコミュニティ スtring を割り当てます。たとえば、パスワードとして *comaccess* を指定します。

```
WAE(config)# snmp-server community comaccess
```



ヒント WAE へ送信された SNMP メッセージは、メッセージ内の Community Name フィールドが、ここで定義したコミュニティ スtring と一致していなければ、認証されません。

snmp-server community string グローバル コンフィギュレーション コマンドは、SNMPv1、SNMPv2c、および SNMPv3 に対応したビューベースのアクセス コントロールを提供しますが、異なるバージョン間の下位互換性も引き続き提供します。

WAE の SNMP エージェントのディセーブル化

WAE の SNMP エージェントをディセーブルにするには、**no snmp-server** グローバル コンフィギュレーション コマンドを入力します。

```
WAE(config)# no snmp-server
```

SNMP エージェントをディセーブルにし、以前に定義したコミュニティ スtring を削除するには、**no snmp-server community** グローバル コンフィギュレーション コマンドを入力します。

```
WAE(config)# no snmp-server community
```

WAE の SNMP トラップのディセーブル化

WAE のすべての SNMP トラップをディセーブルにするには、`no snmp-server enable traps` グローバル コンフィギュレーション コマンドを入力します。

```
WAE(config)# no snmp-server enable traps
```

MIB-II SNMP 認証トラップの送信をディセーブルにするには、`no snmp-server enable traps snmp authentication` コマンドを入力する必要があります。

WAFS ソフトウェア アラームを使用した WAE のモニタリング

従来、SNMP は、SNMP トラップを生成することでエラー状態をレポートします。WAFS 3.x では、[11-2 ページの「SNMP を使用した WAE のモニタリング」](#)に説明するとおり、このモニタリングメカニズムを引き続き使用しています。

WAFS 3.x は、Node Health Manager の機能をサポートしています。この機能を使用して、WAFS アプリケーションは、エラーやその他の重大な状態に注意を引くためのアラームを発信できます。Node Health Manager は、このようなアラームのデータ リポジトリであり、WAE 上でモニタリングされているアプリケーション、サービス（たとえば、CIFS サービス）、リソース（たとえば、ディスク ドライブ）に関するヘルス情報とアラーム情報を集約します。たとえば、この新しい機能は、モニタリング対象のアプリケーション（たとえば、CIFS キャッシング サービス）が WAE 上で稼働しているかどうかを判断するためのメカニズムを提供します。これらのアラームは、WAFS ソフトウェアアラームと呼ばれています。

次の WAE アプリケーションは、WAFS ソフトウェアアラームを生成できます。

- Node Health Manager（アラーム過負荷状態と Node Manager の稼働状態）
- サービス障害に対応する Node Manager（モニタ対象のアプリケーションの稼働状態）
- ディスク障害に対応するシステム モニタ（sysmon）

WAE 上で発信されたアラームは、[表 11-3](#) に示す CLI コマンドを使用して一覧できます。SNMP トラップは、すべての発信およびクリアされたアラームについて送信されます。送信される SNMP トラップのタイプは、アラームによって変わります。

いくつかの CLI コマンドを使用して、WAFS ソフトウェアアラームの原因（問題の原因）を系統立てて調べることができます。これらの CLI コマンドを使用すると、膨大な WAFS ソフトウェア ログに目を通すことなく、問題の原因を特定できます。

表 11-3 show alarms コマンドのリスト

CLI コマンド	説明	詳細
show alarms	現時点で、WAE 上で発信されたすべての WAFS ソフトウェア アラーム（クリティカル、メジャー、およびマイナーの各アラーム）のリストを表示します。	11-13 ページの「WAFS ソフトウェア アラームに関する情報の表示」 を参照してください。
show alarms critical	現在、WAE 上で発信された WAFS ソフトウェア クリティカル アラームのみのリストを表示します。	11-13 ページの「WAFS ソフトウェア アラームに関する情報の表示」 を参照してください。
show alarms major	現在、WAE 上で発信された WAFS ソフトウェア メジャー アラームのみのリストを表示します。	11-13 ページの「WAFS ソフトウェア アラームに関する情報の表示」 を参照してください。

表 11-3 show alarms コマンドのリスト (続き)

CLI コマンド	説明	詳細
show alarms minor	現在、WAE 上で発信された WAFS ソフトウェアマイナー アラームのみのリストを表示します。	11-13 ページの「WAFS ソフトウェアアラームに関する情報の表示」を参照してください。
show alarms detail	現在、発信された WAFS ソフトウェアアラームに関する詳細を表示します。	11-14 ページの「WAFS ソフトウェアアラームに関する詳細情報の表示」を参照してください。
show alarms history	WAE 上で発信およびクリアされた WAFS ソフトウェアアラームの履歴を表示します。CLI は、最近 100 個のアラームの発信およびクリア イベントを保持します。	11-14 ページの「WAFS ソフトウェアアラームの履歴の表示」を参照してください。
show alarms status	現在、WAE 上で発信された WAFS ソフトウェアアラーム数を表示します。また、アラーム過負荷状態とアラーム過負荷設定値も一覧します。	11-16 ページの「WAFS ソフトウェアアラームのステータスの表示」を参照してください。



(注) WAFS ソフトウェアアラームに関する情報は、CLI または SNMP を使用して入手できます。

アラームの重大度レベル

WAFS ソフトウェアアラームには 3 つのレベルがあります。表 11-4 を参照してください。

表 11-4 WAFS ソフトウェアアラームのアラーム重大度レベル

アラームのレベル	説明
クリティカル	WAE を経由する既存のトラフィックに影響し、致命的である (WAE は、回復してトラフィックの処理を継続することができない) と見なされるアラーム。
メジャー	メジャーなサービス (たとえば、CIFS キャッシュ サービス) がダメージを受けたか、失われたことを示すアラーム。このサービスを回復するために、緊急に対処する必要があります。ただし、その他のノードコンポーネントは十分に機能しており、既存のサービスには最小限の影響しかありません。
マイナー	サービスには影響しない状態が発生したが、深刻な障害が発生するのを防ぐために修正処置が必要なことを示すアラーム。

show alarms history EXEC コマンドの出力には、WAFS ソフトウェアアラームの重大度が示されます。

WAE# show alarms history

```

Op Sev Alarm ID           Module/Submodule      Instance
-----
1 R Cr svcdisabled        nodemgr               smbd
2 C Mi servicedead        nodemgr               smbd
3 R Mi servicedead        nodemgr               smbd
4 C Mi servicedead        nodemgr               actastor_watchdog
5 R Mi servicedead        nodemgr               actastor_watchdog
6 C Mi servicedead        nodemgr               actastor_watchdog
7 R Mi servicedead        nodemgr               actastor_watchdog

```

Op - Operation: R-Raised, C-Cleared
 Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor

アラーム過負荷

WAE は、Node Health Manager からの着信アラーム レートを追跡できます。着信アラーム レートが High Water Mark (HWM; 最高水準点) を超えると、WAE はアラーム過負荷状態になります。WAE がアラーム過負荷状態になると、次の状況が発生します。

- それ以降のアラーム発信およびクリア動作に関する SNMP トラップは、一時停止されます。raise alarm-overload アラームと clear alarm-overload アラームに対応するトラップが送信されません。ただし、raise alarm-overload アラームが発信されてから clear alarm-overload アラームが発信されるまでの間に行われたアラーム動作に関するトラップは一時停止されます。
- アラーム過負荷発信およびクリア通知は、阻止されます。
- 着信アラーム レートが Low Water Mark (LWM; 最低水準点) を下回るレベルまで減少しても、WAE はアラーム過負荷状態のままです。

アプリケーションがアクティブかどうかの追跡

Node Health Manager は、WAE 上で作成されたアプリケーション (たとえば、プリント サーバ アプリケーション) が稼働しているかどうかを追跡します。Node Health Manager は作成されたアプリケーションが停止していることを検出すると、アラームを発信します。Node Health Manager がそのアプリケーションからのキープアライブを受信しなかった場合、アプリケーションに障害が発生したと見なされます。

アプリケーションに障害が発生すると、Node Health Manager はサービス障害アラームを発信してその状態をレポートし、その後、サービスを再起動します。しばらくの間 (通常 10 秒間) サービスが継続して稼働すると、サービス障害アラームはクリアされます。

アプリケーションが再起動後に再び障害が発生した場合は、引き続きサービス障害アラームが発信され、Node Health Manager はアプリケーションの再起動を試みます。通常、再起動は、Node Health Manager によって最大 10 回まで試行されます。Node Health Manager は、そのサービスについてサービス無効アラームを発信した後、サービス障害アラームをクリアし、サービスの再起動を止めます。

サービスを再起動するには、一旦、機能の設定を解除し、再度設定しなおす必要があります。たとえば、NTP サービスの場合は、`no ntp server hostname | IP address` グローバル コンフィギュレーション コマンドを入力して NTP サービスの設定を解除し、その後、`ntp server hostname | IP address` グローバル コンフィギュレーション コマンドを入力して NTP サービスを設定し直します。

WAE での SNMP アラーム トラップの設定

WAE では、特定のアラーム状態に対して SNMP トラップを生成するように設定することができます。WAE では、次の条件に基づいて、SNMP アラーム トラップの生成を設定できます。

- アラームの重大度 (クリティカル、メジャー、またはマイナー)
- アクション (アラームが発信されたかクリアされたか)

表 11-5 は、WAFS 3.0 ソフトウェアでも使用できる CISCO-CONTENT-ENGINE-MIB に含まれている 6 つの一般的なアラーム トラップを示しています。

表 11-5 一般的なアラーム トラップ

アラーム トラップ名	重大度	アクション	WAE でのアラーム トラップをイネーブルにする CLI コマンド
cceAlarmCriticalRaised	クリティカル	発信	snmp-server enable traps alarm raise-critical
cceAlarmCriticalCleared	クリティカル	クリア	snmp-server enable traps alarm clear-critical
cceAlarmMajorRaised	メジャー	発信	snmp-server enable traps alarm raise-major
cceAlarmMajorCleared	メジャー	クリア	snmp-server enable traps alarm clear-major
cceAlarmMinorRaised	マイナー	発信	snmp-server enable traps alarm raise-minor
cceAlarmMinorCleared	マイナー	クリア	snmp-server enable traps alarm clear-minor



(注) デフォルトでは、これらの 6 つの一般的なアラーム トラップはディセーブルです。

これらの 6 つの一般的なアラーム トラップにより、SNMP と Node Health Manager との間の整合性が保たれます。6 つのアラーム トラップは、WAFS CLI を使用して個別にイネーブルまたはディセーブルにすることができます。snmp-server enable traps グローバル コンフィギュレーション コマンドには、alarm オプションが含まれます。

```
WAE(config)# snmp-server enable traps alarm ?
clear-critical  Enable clear-critical alarm trap
clear-major     Enable clear-major alarm trap
clear-minor     Enable clear-minor alarm trap
raise-critical  Enable raise-critical alarm trap
raise-major     Enable raise-major alarm trap
raise-minor     Enable raise-minor alarm trap
```

次の例では、クリティカル アラームがクリアされた場合に SNMP トラップを生成するように WAE (SNMP サーバ) を設定します。

```
WAE(config)# snmp-server enable traps alarm clear-critical
```

WAFS ソフトウェア アラームに関する情報の表示

現在、WAE について発信されているすべてのクリティカル、メジャー、およびマイナーの各アラームに関する情報を表示するには、show alarms EXEC コマンドを使用します。WAE 上で現在、発信されたアラームがない場合は、出力に None と示されます。

```
WAE# show alarms
```

```
Critical Alarms:
```

```
-----
```

Alarm ID	Module/Submodule	Instance
1 svcdisabled	nodemgr	smbd

```
Major Alarms:
```

```
-----
```

```
None
```

```
Minor Alarms:
```

```
-----
```

```
None
```

また、次のように、現在 WAE で発信されている WAFS ソフトウェア アラームのうち、指定したレベルのみの情報を表示することもできます。

- **show alarm critical** EXEC コマンドを使用すると、クリティカル アラームに関する情報だけを表示できます。
- **show alarm major** EXEC コマンドを使用すると、メジャー アラームに関する情報だけを表示できます。
- **show alarm minor** EXEC コマンドを使用すると、マイナー アラームに関する情報だけを表示できます。



(注) アラームのさまざまな重大度レベル(クリティカル、メジャー、マイナー)の詳細については、[表 11-4](#) を参照してください。

WAFS ソフトウェア アラームに関する詳細情報の表示

現在、発信されている SNMP アラームに関する詳細を表示するには、**show alarm detail** EXEC コマンドを使用します。このコマンドを使用すると、特定のアラームに関する詳細情報を取得できます。

WAE# **show alarms detail**

Critical Alarms:

Alarm ID	Module/Submodule	Instance
1	svcdisabled	nodemgr
	Mar 20 00:38:21.222 IST, Processing Error Alarm, #000013, 2000:330001	
	nodemgr: The smbd service has been disabled.	

Major Alarms:

None

Minor Alarms:

None

WAFS ソフトウェア アラームの履歴の表示

WAE 上で以前発信およびクリアされた WAFS ソフトウェア アラームの履歴を表示するには、**show alarms history** EXEC コマンドを使用します。

WAE# **show alarms history**

Op	Sev	Alarm ID	Module/Submodule	Instance
1	R	Cr	svcdisabled	nodemgr
2	C	Mi	servicedead	nodemgr
3	R	Mi	servicedead	nodemgr
4	C	Mi	servicedead	nodemgr
5	R	Mi	servicedead	nodemgr
6	C	Mi	servicedead	nodemgr
7	R	Mi	servicedead	nodemgr

Op - Operation: R-Raised, C-Cleared

Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor

アラームに関する、より詳細な情報を表示するには、**show alarms history detail support EXEC** コマンドを入力します。

```

WAE# show alarms history detail support
  Op Sev Alarm ID          Module/Submodule      Instance
-----
  Op Sev Alarm ID          Module/Submodule      Instance
-----
  1 R Cr svcdisabled        nodemgr               smbd
Mar 20 00:38:21.224 IST, ProcessingError Alarm, #000013, 2000:330001
  nodemgr: The smbd service has been disabled.

  /alm/crit/nodemgr/-service name-/svcdisabled:

    -service name- service has been disabled.

  Explanation:
  The node manager tried restarting the specified service but
  the service kept restarting. The number of restarts has
  exceeded an internal limit and the service has been
  disabled.

  Action:
  The device may have to be reloaded for the service to be
  reenabled.

  2 C Mi servicedead        nodemgr               smbd
Mar 20 00:38:21.222 IST, ProcessingError Alarm, #000003, 2000:330004
  nodemgr: The smbd service died.

  /alm/min/nodemgr/-service_name-/servicedead:

    -service name- service died.

  Explanation:
  The node manager found the specified service to be dead.
  Attempts will be made to restart this service.

  Action:
  Examine the syslog for messages relating to cause of service
  death. The alarm will be cleared if the service stays
  alive and does not restart in a short while.

  3 R Mi servicedead        nodemgr               smbd
Mar 20 00:38:00.031 IST, ProcessingError Alarm, #000003, 2000:330004
  nodemgr: The smbd service died.

  /alm/min/nodemgr/-service_name-/servicedead:

    -service name- service died.

  Explanation:
  The node manager found the specified service to be dead.
  Attempts will be made to restart this service.

  Action:
  Examine the syslog for messages relating to cause of service
  death. The alarm will be cleared if the service stays
  alive and does not
  .
  .
  .
Op - Operation: R-Raised, C-Cleared
Sev - Severity: Cr-Critical, Ma-Major, Mi-Minor

```

WAFS ソフトウェア アラームのステータスの表示

WAE 上で現在発信されているアラームの総数を表示するには、`show alarms status EXEC` コマンドを入力します。次の出力例は、現在の発信されている WAFS ソフトウェア アラーム数を示しています。また、出力には、アラーム過負荷設定値（たとえば、過負荷検出が現在 WAE 上でイネーブルかディセーブルか）に関する情報も含まれます。

```
WAE# show alarms status

Critical Alarms :          1
Major Alarms    :          0
Minor Alarms    :          0

Overall Alarm Status : Critical
Device is NOT in alarm overload state.

Device enters alarm overload state @ 10 alarms/sec.
Device exits alarm overload state @ 1 alarms/sec.
Overload detection is ENABLED.
```

WAE のクリティカル ドライブのモニタリング

適切に動作させるには、WAE が disk00 という名前のディスク ドライブを持っている必要があります。また、WAE は、SYSFS（システム ファイル システム）の第 1 パーティションを含むディスク ドライブを持っていないなりません。SYSFS パーティションは、システム ログ（syslog）と内部デバッグ ログを含む、ログ ファイルを格納するために使用されます。また、WAE 上のイメージ ファイルとコンフィギュレーション ファイルを格納するために使用される場合もあります。disk00 は、第 1 SYSFS パーティションを内包している場合もあれば、第 2 ディスクの disk01 に常駐している場合もあります。どちらの場合も、disk00 ディスクと、SYSFS の第 1 パーティションを含むディスクは、**クリティカル ドライブ**と呼ばれ、WAE を適切に動作させるために必要です。

WAE がブートされ、システムの起動時にクリティカル ドライブが検出されなかった場合、WAE 上の WAFS システムはサービス低下状態で稼働します。実行時にクリティカル ドライブのいずれかが不良な状態に陥ると、WAFS システムはアプリケーションの機能不良、機能停止、または強制終了などの兆候を示すことがあります。また、WAFS システム自体が機能停止したり、強制終了したりする場合もあります。このような場合は、WAE 上のクリティカル ドライブをモニタリングし、ディスク ドライブ エラーを Cisco TAC に報告する必要があります。

WAFS システムでは、ディスク デバイス エラーは、次のイベントのいずれかとして定義されています。

- Linux カーネルによって表示された SCSI または IDE デバイス エラー。
- EIO エラー コードが戻されて失敗した、アプリケーションによるディスク デバイス アクセス（たとえば、open(2)、read(2)、write(2)などのシステム コール）
- 起動時には存在していたが、実行時にアクセス不能なディスク デバイス。

ディスク ステータスは、フラッシュ メモリ（不揮発性ストレージ）に記録されます。WAE ディスク デバイス上でエラーが発生したときには、SYSFS パーティションがまだ損傷していない場合はメッセージがシステム ログ（syslog）に書き込まれ、WAE に SNMP が設定されている場合は SNMP トラップが生成されます。

ディスク エラー処理しきい値の指定

WAE では、ディスク デバイス エラー処理しきい値を定義できます。ディスク デバイスのエラー数が指定したしきい値に達すると、該当するディスク デバイスは自動的に不良としてマーキングされます。デフォルトでは、このしきい値は 10 に設定されています。WAFS システムは、すぐには、不良ディスク デバイスの使用を中止せず、次のリポート後に不良ディスク ドライブの使用を中止するだけです。

デフォルトのしきい値を変更するには、**disk error-handling threshold** グローバル コンフィギュレーション コマンドを使用します。ディスク ドライブが決して不良としてマーキングされないようにする場合は、0 を指定します。

指定されたしきい値を超えると、WAE は、このイベントを記録するか、またはリポートします。不良ディスク ドライブがクリティカルドライブで、自動リロード機能（**disk error-handling reload** コマンド）がイネーブルの場合は、WAFS ソフトウェアがそのディスク ドライブを不良としてマーキングし、WAE は自動的にリロードされます。WAE がリロードされた後、syslog メッセージと SNMP トラップが生成されます。

デフォルトでは、WAE 上の自動リロード機能はディセーブルになっています。自動リロード機能をイネーブルにするには、**disk error-handling reload** グローバル コンフィギュレーション コマンドを使用します。自動リロード機能をイネーブルにした後、再度ディセーブルにするには、**no disk error-handling reload** グローバル コンフィギュレーション コマンドを使用します。

次の例では、特定のディスクドライブ（たとえば、disk00）で 5 つのディスクドライブエラーが発生したら、そのディスクドライブが自動的に不良としてマーキングされます。

```
WAE(config)# disk error-handling threshold 5
```

手動による WAE ディスクドライブのマーキングとマーキングの解除

WAE のディスクドライブは、良好なドライブ（正常に稼働しており、使用中のドライブ）としてマーキングするか、または、不良ドライブ（正常に稼働しておらず、`reload` コマンドの実行後には使用されないドライブ）としてマーキングできます。

disk01 を不良としてマーキングし、WAE をリロードしてから、disk01 を良好としてマーキングし再び使用できるようにする手順は、次のとおりです。

1. `disk mark EXEC` コマンドを入力して、disk01 を不良としてマーキングします。

```
WAE# disk mark disk01 bad
disk01 is marked as bad.
It will be not used after reload.
```

2. `show disks details EXEC` コマンドを入力して、ディスクに関する詳細を表示します。この時点では、disk01 は WAE のブート後にマーキングされたため、アスタリスク付きで表示されます。disk01 が `Normal`（現在使用中）としてレポートされたことがわかります。

```
WAE# show disks details
Physical disk information:

disk00: Normal                (h00 c00 i00 100 - DAS)    76324MB( 74.5GB)
disk01: Normal                (h01 c00 i00 100 - DAS)    76324MB( 74.5GB) (*)
```

(*) Disk drive won't be used after reload.

Mounted filesystems:

MOUNT POINT	TYPE	DEVICE	SIZE	INUSE	FREE	USE%
/	root	/dev/root	34MB	28MB	6MB	82%
...						

3. `reload EXEC` コマンドを実行して、WAE をリロードします。メッセージが表示されたら、`Enter` キーを押して、リロードを続行します。WAE がリロードされた後、不良ディスクドライブとしてマーキングされた disk01 は使用されません。

```
WAE# reload
Proceed with reload?[confirm]
...
```

4. リロードが完了したら、`show disks details EXEC` コマンドを入力して、ディスクに関する詳細を表示します。WAE のリポート後、disk01 は不良として検出されなかったため、この時点では、disk01 は `Not used` として表示されます。

```
WAE# show disks details
Physical disk information:

disk00: Normal                (h00 c00 i00 100 - DAS)    76324MB( 74.5GB)
disk01: Not used
```

(*) Disk drive won't be used after reload.

...

5. **disk mark EXEC** コマンドを入力して、disk01 を良好としてマーキングします。

```
WAE# disk mark disk01 good
disk01 is marked as good.
It will be used after reload.
```

6. ここで、**show disks details EXEC** コマンドを入力して、disk01 が `Not used` としてマーキングされていることを確認します。**reload EXEC** コマンドを実行して、WAE をリロードします。メッセージが表示されたら、**Enter** キーを押して、リロードを続行します。WAE がリロードされた後、良好なディスクドライブとしてマーキングされた disk01 は再び使用されます。**show disks details** コマンドを入力して、このことを確認します。

```
WAE# show disks details
Physical disk information:

    disk00: Normal                (h00 c00 i00 100 - DAS)    76324MB( 74.5GB)
    disk01: Not used
    ...

WAE# reload
Proceed with reload?[confirm]
...
WAE# show disks details

Physical disk information:

    disk00: Normal                (h00 c00 i00 100 - DAS)    76324MB( 74.5GB)
    disk01: Normal                (h01 c00 i00 100 - DAS)    76324MB( 74.5GB)
    ...
```

SMART を使用したディスクヘルスの予防的なモニタリング

Self Monitoring, Analysis, and Reporting Technology (SMART) を使用すると、ディスクの「健康状態」を監視して、その故障を未然に防止することができます。SMART は、ハードドライブ診断情報と、切迫しているディスク障害に関する情報を提供します。

SMART は、ほとんどのディスクベンダーによってサポートされており、ディスクがどの程度健全であるかを判断するために使用される標準的な方式です。SMART の属性には、複数の読み取り専用属性（たとえば、power on hours [使用時間] 属性、load and unload count [ロード / アンロード回数] 属性）があります。これらの属性は、WAFS ソフトウェアに、切迫したディスク障害を示すことのある動作状況や環境状況に関する情報を提供します。

SMART のサポートは、ベンダーによって異なります。次の 2 つの異なる WAE (WAE A および WAE B) で入力した `show disk SMART-info EXEC` コマンドの出力例に示すとおり、各ベンダーがサポートする SMART 属性セットは異なります。これらの 2 つの WAE は、それぞれ異なるベンダーによって製造されたハードディスクを内蔵しています。

```
WAEA# show disks SMART-info
=== disk00 ===
Device: IBM          IC35L036UCD210-0 Version: S5BS
Serial number:      22222222
Device type: disk
Transport protocol: Fibre channel (FCP-2)
Local Time is: Sun Jan  2 03:14:16 2005 Etc
Device supports SMART and is Enabled
Temperature Warning Disabled or Not Supported
SMART Health Status: OK

=== disk01 ===
disk01: Not present

WAEB# show disk SMART-info
Disk 01:
=====
Device Model:      HITACHI_DK23BA-20
Serial Number:    111111
Firmware Version: 00E0A0D2
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
SMART overall-health self-assessment test result: PASSED
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG      VALUE WORST THRESH TYPE      WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000d   100   083   050   Pre-fail     -         677
  3 Spin_Up_Time            0x0007   100   100   050   Pre-fail     -          0
  4 Start_Stop_Count        0x0032   100   100   050   Old_age      -        249
  5 Reallocated_Sector_Ct   0x0033   099   099   010   Pre-fail     -         30
<cr>
```

より詳細な情報を表示するには、`show disk SMART-info details EXEC` コマンドを入力します。`show disk SMART-info` コマンドと `show disk SMART-info details` コマンドの出力は、ディスクベンダーとドライブテクノロジーのタイプ (IDE または SCSI ディスクドライブ) によって異なります。

SMART 属性はベンダーによって異なるとは言え、大半の SMART 属性を解釈する共通の方法があります。各 SMART 属性は、正規化された現在値としきい値を持ちます。現在値がしきい値を越えると、ディスクは「故障」したと見なされます。WAFS ソフトウェアは、SMART 属性をモニタリングし、syslog メッセージ、SNMP トラップ、およびアラームを使用して、切迫した障害をサポートします。`show tech-support EXEC` コマンドの出力には、SMART 情報も含まれます。

システム ログイングとアラームの設定

WAFS システムに関する情報は、キャプチャし、接続されたコンソール、WAE のディスク、または別のホスト マシンに送信できます。ここでは、システム ログイングとアラーム レポートを WAE に設定する手順について説明します。ここで説明する内容は、次のとおりです。

- [WAE でのシステム ログイングについて、11-21 ページ](#)
- [ログイングに使用されるプライオリティ レベル、11-22 ページ](#)
- [コンソールへのシステム ログイングの設定、11-22 ページ](#)
- [WAE ディスクへのシステム ログイングの設定、11-23 ページ](#)
- [リモート ホストへのシステム ログイングの設定、11-24 ページ](#)
- [WAFS アラームの設定、11-25 ページ](#)



(注)

この章では、システム メッセージまたはアラーム メッセージについては取り上げていません。これらのメッセージの詳細については、『Cisco WAFS 3.0 System Messages』を参照してください。

WAE でのシステム ログイングについて

システム ログ ファイル (syslog) の特定のパラメータを設定するには、システム ログイング機能を使用します。このファイルには、認証エントリ、特権レベル、および管理の詳細情報が含まれています。システム ログ ファイルは、システム ファイル システム (SYSFS) パーティションに */local/syslog.txt* として配置されます。

デフォルトでは、システム ログイングは WAE 上でイネーブルです。表 11-6 は、システム ログイングのデフォルト設定値をまとめたものです。

表 11-6 システム ログイングのデフォルト設定値

設定値	デフォルト設定値
コンソール用メッセージのプライオリティ	warning (警告)
ディスク ログ ファイル用メッセージのプライオリティ	debug (デバッグ)
ホスト用メッセージのプライオリティ	warning (警告)
ログ ファイルの場所	<i>/local/syslog.txt</i>
ログ ファイルのリサイクル サイズ	10,000,000 バイト

ログイングに使用されるプライオリティ レベル

システム ログ情報をコンソールまたは WAE ディスクのどちらかに送信するように設定したかに関わらず、収集および送信するメッセージの重大度レベルを識別する必要があります。表 11-7 は、プライオリティ レベルとその意味をまとめたものです。

表 11-7 ログにおけるメッセージのプライオリティ

プライオリティ	レベル	説明
緊急	0	システムを使用できません。
アラート	1	すぐに措置が必要です。
クリティカル	2	システム内に危険な状態が存在します。
エラー	3	システム内にエラー状態が存在します。
警告	4	システム内に警告すべき状態が存在します。
通知	5	システムは正常に動作していますが、深刻な状態が存在します。
情報	6	情報メッセージです。
デバッグ	7	デバッグメッセージです。

コンソールへのシステム ログイングの設定

システム ログイングは、さまざまなレベルのメッセージ (プライオリティ レベル) をコンソールへ送信するように設定できます。プライオリティ オプションは、表 11-7 に定義されています。

コンソールへのシステム ログイングを設定し、コンソールに送信する必要のあるさまざまなレベルのメッセージを指定するには、`logging console priority` グローバル コンフィギュレーション コマンドを使用します。

```
logging console { enable | priority loglevel }
```

システム情報を接続されたコンソールにログイングする手順は、次のとおりです。

- ステップ 1 コンソール ログイングを設定し、ログする情報のプライオリティ レベルを識別します。デフォルトのプライオリティ レベルは警告です。

```
WAE(config)# logging console priority loglevel
```

次の例では、プライオリティ レベルをコンソール ログイングに対してアラートに設定しています。

```
WAE(config)# logging console priority alert
```

- ステップ 2 コンソール ログイングをイネーブルにします。

```
WAE(config)# logging console enable
```



(注) WAE からリモート ホスト (この場合は、コンソール) への syslog メッセージは、ポート 514 ではなく、ポート 10000 から送信されます。

次の例は、ファイル内のテキストの最後の数行だけをリストする `type-tail EXEC` コマンドを使用して、`syslog.txt` ファイル内の最後の数行を示しています。

```
WAE# type-tail syslog.txt
Mar 23 23:08:39 wae511-1 last message repeated 4 times
Mar 23 23:18:39 wae511-1 last message repeated 4 times
Mar 23 23:23:38 wae511-1 last message repeated 2 times
Mar 23 23:27:41 wae511-1 Nodemgr: %CE-NODEMGR-5-330027: pid 18529 exits
Mar 23 23:27:41 wae511-1 Nodemgr: %CE-NODEMGR-5-330048: DEBUG: respawn_count = 6,
period: 4516536.250000
Mar 23 23:27:41 wae511-1 Nodemgr: %CE-NODEMGR-5-330040: Start service 'mingetty'
using: '/ruby/bin/startmingetty.sh' with pid: 20218
Mar 23 23:27:44 wae511-1 login: %CE-UTILLIN-3-801060: PAM unable to
dlopen(/lib/security/pam_winbind.so)
Mar 23 23:27:44 wae511-1 login: %CE-UTILLIN-3-801060: PAM [dlerror:
/lib/security/pam_winbind.so: cannot open shared object file: No such file or
directory]
Mar 23 23:27:44 wae511-1 login: %CE-UTILLIN-3-801060: PAM adding faulty module:
/lib/security/pam_winbind.so
Mar 23 23:27:47 wae511-1 login: %CE-SYSUTL-5-800003: admin login on ttyS0
```

WAE ディスクへのシステム ログिंगの設定

システム ログिंगは、さまざまなレベルのメッセージ（プライオリティ レベル）をディスクへ送信するように設定できます。ディスクへのシステム ログिंगを設定し、ディスクに送信する必要のあるさまざまなレベルのメッセージを指定するには、`logging disk priority` グローバル コンフィギュレーション コマンドを使用します。

```
logging disk {enable | filename filename | priority loglevel | recycle size}
```

これらの項目を指定したら、ディスク ログिंगをイネーブルにする必要があります。

システム情報を WAE ディスクにログングする手順は、次のとおりです。

- ステップ 1** ディスク ログングを設定し、情報の送信先となるログ ファイルのファイル名（最大 255 文字）を指定します。

```
WAE(config)# logging disk filename filename
```

次の例は、`syslog.txt` ログ ファイルへのディスク ログングを示しています。

```
WAE(config)# logging disk filename syslog.txt
```

- ステップ 2** ログする情報の各プライオリティ レベルを識別します。デフォルトのプライオリティは、デバッグです。

```
WAE(config)# logging disk priority name
```

次の例では、ディスク ログングに対してクリティカル プライオリティ レベルを設定しています。

```
WAE(config)# logging disk priority critical
```

- ステップ 3** ログ ファイルが上書きされる（もっとも古い情報が最初に上書きされる）前の最大サイズ（1,000,000 ~ 50,000,000 バイト）を定義します。

```
WAE(config)# logging disk recycle size
```

ステップ 4 ディスク ログイングをイネーブルにします。

```
WAE(config)# logging disk enable
```

リモート ホストへのシステム ログイングの設定

さまざまなレベルのメッセージを最大 8 台のリモート syslog ホストへ送信するように WAE を設定できます。各 syslog ホストは、異なるレベルのイベント メッセージを受信できます。各ホストは、ネットワーク上で到達可能でなければなりません。

帯域幅とその他のリソースの消費量を制限するために、リモート syslog ホストへのメッセージにレートリミットを設けることができます。この制限を越えると、指定されたリモート syslog ホストはメッセージを廃棄します。デフォルトのレートリミットはありません。デフォルトでは、すべての syslog メッセージがすべての設定済みの syslog ホストに送信されます。レートリミットを越えると、すべての CLI EXEC の Shell login コマンドに対して、「message of the day」(motd)が表示されます。



(注) syslog ホストの冗長性は、WAE 上に複数の syslog ホストを設定し、設定済みの各 syslog ホストに同じプライオリティ コードを割り当てることで、必然的に実現できます (たとえば、「クリティカル」レベル 2 のプライオリティ コードを、sylog ホスト 1、sylog ホスト 2、および syslog ホスト 3 に割り当てます)。

リモート ホストへのシステム ログイングを設定し、ホストに送信する必要があるさまざまなレベルのメッセージを指定するには、`logging host` グローバル コンフィギュレーション コマンドを使用します。デフォルトのプライオリティ レベルは警告です。

```
logging host hostname [priority priority-code | port port |rate-limit limit]
```

システム ログイングをリモート ホストに設定する場合は、ファシリティも指定できます。ファシリティ オプションを、リモート syslog サーバと組み合わせて使用し、リモート サーバの着信 WAE syslog メッセージを分類 (サービス タイプ別) できます。表 11-8 に、ファシリティ オプションを示しています。

表 11-8 システム ログイングのファシリティ オプション

ファシリティ名	説明	ファシリティ名	説明
auth	認証システム	local5	ローカルで使用
daemon	システム デーモン	local6	ローカルで使用
kernel	カーネル	local7	ローカルで使用
local0	ローカルで使用	mail	メール システム
local1	ローカルで使用	news	USENET ニュース
local2	ローカルで使用	syslog	syslog 自身
local3	ローカルで使用	user	ユーザ プロセス
local4	ローカルで使用	uucp	UUCP システム

次の例では、192.168.34.1 にある syslog ホストが、7,000 メッセージ / 秒の速度で、クリティカルレベルのメッセージをデフォルト ポートで受信するように設定します。

```
WAE(config)# logging host 192.168.34.1 priority critical rate-limit 7000
WAE(config)# logging facility syslog
```

次の例では、このホストに設定されているレートリミットを削除します。

```
WAE(config)# logging host 192.168.34.1 rate-limit 0
```

次の例では、192.168.75.36 にバックアップシステム ログ ホストを作成します。

```
WAE(config)# logging host 192.168.75.36 priority critical rate-limit 7000
```

次の例では、メール ホストの mailhost1 が、100 メッセージ / 秒の速度で警告レベルのメッセージを受信するように設定します。

```
WAE(config)# logging host mailhost1 rate-limit 100
WAE(config)# logging facility mail
```

WAFS アラームの設定

着信アラーム レートが最高水準点 (HWM) を超えると、WAE はアラーム過負荷状態になります。このレートがいつ HWM を超えたかを検出できるアラームは、ユーザが設定可能な WAFS アラームだけです。

アラーム過負荷状態を検出する手順は、次のとおりです。

-
- ステップ 1** WAE は過負荷アラームをトリガーする必要があるレートとして、10 アラーム / 秒 ~ 1000 アラーム / 秒までのレートをアラームに設定します。

```
WAE(config)# alarm overload-detect raise 750
```

- ステップ 2** WAE が過負荷アラームをクリアする必要があるレートとして、1 アラーム / 秒 ~ 999 アラーム / 秒までのレートをアラームに設定します。

```
WAE(config)# alarm overload-detect clear 250
```

- ステップ 3** アラーム過負荷をイネーブルにします。

```
WAE(config)# alarm overload-detect enable
```

アラーム過負荷検出をディセーブルにするには、このコマンドの **no** 形式である、**no alarm overload-detect enable** コマンドを使用します。

システム ログの現在の設定の表示

WAE の現在の syslog ホスト設定を表示するには、**show logging EXEC** コマンドを入力します。

```
WAE# show logging
Syslog to host is enabled.
Priority for host logging to 1.2.1.1:514 is set to: warning
Syslog to console is disabled
Priority for console logging is set to: warning
Syslog to disk is enabled
Priority for disk logging is set to: notice
Filename for disk logging is set to: /local1/syslog.txt
Syslog facility is set to syslog
Syslog disk file recycle size is set to 10000000
```

CiscoWorks2000 の使用方法

CiscoWorks2000 (CW2K) は、大半のシスコ製デバイスの管理に使用される一連の管理アプリケーションを提供するシスコ製品です。WAE は、変更を加えることなく、次の方法で CiscoWorks2000 と相互運用できます。

- CW2K は、「Generic SNMP」デバイス配下の WAE を一覧にできます。
- CW2K インベントリ モジュールが、WAE と、そのデバイス名、システム名、説明 (ソフトウェアバージョンを含む)、アップタイム、およびネットワーク インターフェイス情報を一覧にします。
- CW2K syslog モジュールは、WAE syslog を解釈できます。
- CW2K アベイラビリティ モジュールは、WAE を追跡できます。

WAFS Manager GUI または CLI のどちらかを使用して、CiscoWorks2000 互換の形式での syslog メッセージの生成をイネーブルまたはディセーブルにすることができます。たとえば、CLI を使用して CW2K をリモート syslog ホストとして設定するには、[11-24 ページの「リモート ホストへのシステム ログの設定」](#)に説明するとおり、**logging host hostname** グローバル コンフィギュレーション コマンドを使用します。