



CLI コマンド

この章では、WAAS ソフトウェアの次のタイプの CLI コマンドについて詳しく説明します。

- WAAS デバイスにログイン後に入力可能な EXEC モード コマンド。コマンドの詳細なリストについては、「[EXEC モード コマンド](#)」セクションを参照してください。
- WAAS デバイスにログインし、グローバル コンフィギュレーション モードにアクセスしたあとに入力可能なグローバル コンフィギュレーション モード コマンド。コマンドの詳細なリストについては、「[コンフィギュレーション モード コマンド](#)」セクションを参照してください。
- グローバル コンフィギュレーション モードにアクセスしたあとに入力可能なインターフェイス コンフィギュレーション モード コマンド。コマンドの詳細なリストについては、「[インターフェイス コンフィギュレーション モード コマンド](#)」セクションを参照してください。
- グローバル コンフィギュレーション モードにアクセスしたあとに入力可能な標準および拡張 ACL コンフィギュレーション モード コマンド。コマンドの詳細なリストについては、「[\(config\) ip access-list](#)」および「[\(config\) ip access-list](#)」セクションを参照してください。

コマンドごとに次について説明します。

- コマンドの構文、デフォルト値、コマンドモード、使用上のガイドライン、および例
- 関連コマンド（適用可能な場合）

CLI の使用方法と CLI コマンドモードの詳細については、[第 1 章「WAAS コマンドライン インターフェイスの使用法](#)」を参照してください。

EXEC モードコマンド

EXEC モードは、システム動作の設定、表示、テスト用に使用します。通常、ユーザ EXEC コマンドにより、リモートデバイスへの接続、一時的な端末回線設定の変更、基本的なテストの実行、システム情報の表示ができます。

EXEC モードは、ユーザ レベルと特権レベルの2つのアクセス レベルに分かれています。

ユーザ EXEC モードはローカルおよび一般的なシステム管理者が使用し、特権 EXEC モードはルート管理者が使用します。2つのモード間での切り替えには、**enable** および **disable** コマンドを使用します。ユーザレベル EXEC コマンドラインのアクセスには有効なパスワードが必要です。

ユーザレベル EXEC コマンドは、特権レベル EXEC コマンドのサブセットです。ユーザレベル EXEC プロンプトはホスト名のあとにかぎカッコ (>) が続きます。特権レベル EXEC コマンドラインのプロンプトは、ポンド記号 (#) です。EXEC コマンドを実行するには、EXEC システム プロンプトでコマンドを入力してから **Enter** キーを押します。



(注)

ホスト名は、**hostname** グローバル コンフィギュレーション コマンドを使用して変更できます。

次の例では、ユーザ レベルから特権レベル EXEC コマンドラインにアクセスします。

```
WAE> enable
WAE#
```

EXEC モードを終了するには、システム プロンプトで **exit** コマンドを使用します。

```
WAE# exit
WAE>
```

cd

WAAS ソフトウェア内で、あるディレクトリから別のディレクトリに変更するには、**cd EXEC** コマンドを使用します。

```
cd directoryname
```

シンタックスの説明

<i>directoryname</i>	ディレクトリ名
----------------------	---------

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

ディレクトリ間のナビゲートやファイル管理に、このコマンドを使用します。ディレクトリ名は、すべての相対パスに対するデフォルトのプレフィクスとなります。相対パスはスラッシュ (/) で始まりません。絶対パスはスラッシュ (/) で始まります。

例

次の例は、相対パスを使用してディレクトリを変更する方法を示します。

```
WAE(config)# cd local1
```

次の例は、絶対パスを使用してディレクトリを変更する方法を示します。

```
WAE(config)# cd /local1
```

関連コマンド

[deltree](#)

[dir](#)

[lls](#)

[ls](#)

[mkdir](#)

[pwd](#)

cifs

CIFS アダプタ操作および実行コンフィギュレーションを制御するには、**cifs EXEC** コマンドを使用します。

```
cifs {auto-discovery {disable | enable | reset-log} | mss value | restart [core | edge] | reverse-dns
{active | disable | enable} | session disconnect [client-ip ipaddress | server-ip ipaddress]}
```

シンタックスの説明

auto-discovery	CIFS 自動ディスカバリの設定およびデバッグを制御します。
disable	CIFS サーバの自動ディスカバリをディセーブルにします。
enable	CIFS サーバの自動ディスカバリをイネーブルにします。
reset-log	ログメモリをリセットします。
mss	CIFS アダプタに TCP Maximum Segment Size (MSS; 最大セグメントサイズ) を設定します。
<i>value</i>	MSS。この値は 512 ~ 1460 の範囲の整数である必要があります。
restart	CIFS アプリケーションを再起動します。
core	Core WAE 上で CIFS アプリケーションを再起動します。
edge	Edge WAE 上で CIFS アプリケーションを再起動します。
reverse-dns	Core WAE 上でサーバ名を解決するには、リバース DNS を使用します。
active	リバース DNS がアクティブであるか確認します。
disable	Core WAE 上でリバース DNS を無効にします。
enable	Core WAE 上でリバース DNS をアクティブにします。
session	アクティブな CIFS セッションに操作を設定します。
disconnect	CIFS セッションを接続解除します。
client-ip	クライアントの IP アドレスまたはアドレスセットを設定します。
<i>ipaddress</i>	IP アドレス
server-ip	サーバの IP アドレスまたはアドレスセットを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

WAE をリブートしないで設定を変更するため WAFS サービスを再開するには、**cifs restart** コマンドを使用します。

関連コマンド

[show cifs](#)

[show statistics cifs](#)

clear

ハードウェア インターフェイス、統計情報、およびその他の設定をクリアするには、**clear EXEC** コマンドを使用します。

```
clear arp-cache [ipaddress | interface {GigabitEthernet 1-2/port | PortChannel 1-2 | Standby 1-4}]
```

```
clear cache dre
```

```
clear cdp {counters | table}
```

```
clear ip access-list counters [acl-num | acl-name]
```

```
clear logging
```

```
clear statistics {all | authentication | epm | flow monitor tcpstat-v1 | history | icmp | inline | ip | radius |  
running | tacacs | tcp | udp | windows-domain}
```

```
clear statistics dre [connection | global | nack | peer]
```

```
clear statistics tfo {all | auto-discovery | blacklist | filtering | peer | policy-engine | synq}
```

```
clear windows-domain-log
```

シンタックスの説明

arp-cache	ARP キャッシュをクリアします。
<i>ipaddress</i>	IP アドレスの ARP エントリをすべてクリアします。
interface	インターフェイス上の ARP エントリをすべてクリアします。
GigabitEthernet	ギガビット イーサネット インターフェイス
<i>1-2/port</i>	ギガビット イーサネット スロット / ポート
PortChannel	PortChannel インターフェイス
<i>1-2</i>	PortChannel 番号。値は 1 または 2 です。
Standby	スタンバイ インターフェイス
<i>1-4</i>	スタンバイ インターフェイス番号 1、2、3、または 4
cache	キャッシュ オブジェクトをクリアします。
dre	DRE キャッシュをクリアします。
cdp	Cisco Discovery Protocol (CDP; シスコ検出プロトコル) 統計データをリセットします。
counters	CDP カウンタをクリアします。
table	CDP テーブルをクリアします。
ip access-list	IP アクセス リスト統計情報をクリアします。
counters	IP アクセス リスト カウンタをクリアします。
<i>acl-num</i>	(オプション) 数値の識別情報 (標準アクセス リストの場合は 1 ~ 99、拡張アクセス リストの場合は 100 ~ 199) により識別される、指定のアクセス リストのカウンタをクリアします。
<i>acl-name</i>	(オプション) 文字で始まる最大 30 文字の英数字の識別情報で識別される、指定されたアクセス リストのカウンタをクリアします。
logging	ディスク ファイルに保存されている Syslog メッセージをクリアします。
statistics	指定されたとおりに統計情報をクリアします。
all	すべての統計情報をクリアします。
authentication	認証統計情報をクリアします。
dre	Data Redundancy Elimination (DRE) 統計情報をクリアします。

connection	(オプション) すべての DRE 接続の統計情報をクリアします。
global	(オプション) グローバル DRE 統計情報をクリアします。
nack	(オプション) すべての DRE NACK 統計情報をクリアします。
peer	(オプション) すべての DRE ピアの統計情報をクリアします。
epm	DCE-RPC EPM 統計情報をクリアします。
flow	ネットワーク トラフィック フローの統計情報をクリアします。
monitor	モニタ フロー パフォーマンスの統計情報をクリアします。
tcpstat-v1	tcpstat-v1 コレクタの統計情報をクリアします。
history	統計情報の履歴をクリアします。
icmp	ICMP 統計情報をクリアします。
inline	インライン インターセプト統計情報をクリアします。
ip	IP 統計情報をクリアします。
radius	RADIUS 統計情報をクリアします。
running	実行中の統計情報をクリアします。
tacacs	TACACS+ 統計情報をクリアします。
tcp	TCP 統計情報をクリアします。
udp	UDP 統計情報をクリアします。
windows-domain	Windows ドメイン統計情報をクリアします。
tfo	TCP Flow Optimization (TFO) 統計情報をクリアします。
all	TFO 統計情報をすべてクリアします。
auto-discovery	TFO auto-discovery 統計情報をクリアします。
blacklist	TFO blacklist 統計情報をクリアします。
filtering	TFO フィルタ テーブル統計情報をクリアします。
peer	TFO peer 統計情報をクリアします。
policy-engine	TFO アプリケーションおよびパススルー統計情報をクリアします。
synq	TFO SynQ モジュール統計情報をクリアします。
windows-domain-log	Samba、Kerberos および Winbind ログ ファイルをクリアします。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン **clear cache dre** コマンドを使用したあと、最初の 1 MB のデータは最適化されません。Cisco WAAS は tcpproxy サービスの再開後、最初の 1 MB のデータを最適化しません。最初の 1 MB のデータのあとに送信されたデータは、設定したポリシーに従って最適化されます。

clear logging コマンドは、*syslog.txt* ファイルから現在のエントリをすべて削除しますが、ファイルのアーカイブは作成しません。次の例のように *syslog.txt* ファイルに「Syslog cleared」というメッセージを入れて、Syslog がクリアされたことを示します。

```
Feb 14 12:17:18 WAE# exec_clear_logging:Syslog cleared
```

clear statistics コマンドは、指定されたパラメータに該当するすべての統計カウンタをクリアします。このコマンドを使用して、キャッシュ オブジェクトや設定を失うことなく、一部またはすべての機能に対する最新の統計データを監視します。

clear windows-domain-log コマンドは、Windows ドメイン ログ ファイルから現在のエントリをすべて削除します。

例

次の例では、WAAS デバイス上の *syslog.txt* ファイルのすべてのエントリがクリアされます。

```
WAE# clear logging
```

次の例では、WAAS デバイス上の認証、RADIUS、および TACACS+ 情報がすべてクリアされます。

```
WAE# clear statistics radius
WAE# clear statistics tacacs
WAE# clear statistics authentication
```

次の例では、WAAS デバイス上の Windows ドメイン ログ ファイルのすべてのエントリがクリアされます。

```
WAE# clear windows-domain-log
```

関連コマンド

[show interface](#)

[show wccp](#)

clear users

ユーザ接続をクリアする、またはロックアウトされているユーザをロック解除するには、**clear users EXEC** コマンドを使用します。

```
clear users [administrative | locked-out {all | username username}]
```

シンタックスの説明

users	認証されたユーザの接続（ログイン）をクリアします。
administrative	リモート ログイン サービスを介して認証された管理ユーザの接続（ログイン）をクリアします。
locked-out all	ロックアウトされているすべてのユーザ アカウントをロック解除します。
locked-out username	ロックアウトされている指定のユーザ アカウントをロック解除します。
<i>username</i>	ロック解除されるアカウントのユーザ名

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

clear users administrative コマンドは、TACACS などのリモート ログイン サービスを介して認証された全管理ユーザの接続をクリアします。ローカル データベースを介して認証された管理ユーザは、このコマンドの影響を受けません。

clear users locked-out コマンドは、ロックアウトされているユーザ アカウントをロック解除します。強度の強いパスワード ポリシーがイネーブルの場合に（[\(config\) authentication strict-password-policy](#) を参照）、ユーザが 3 回連続してログイン試行に失敗すると、ユーザ アカウントはロックアウトされます（これは、[admin] アカウントには適用されません）。

例

次の例では、認証されたすべてのユーザがクリアされます。

```
WAE(config)# clear users
```

次の例では、リモート ログイン サービスを介して認証されたすべての管理ユーザがクリアされます（ローカル データベースを介して認証された管理ユーザは、このコマンドの影響を受けません）。

```
WAE(config)# clear users administrative
```

次の例では、ロックアウトされたすべてのユーザ アカウントがロック解除されます。

```
WAE(config)# clear users locked-out all
```

次の例では、ユーザ名のダルシーをロック解除します。

```
WAE(config)# clear users locked-out username darcy
```


関連コマンド

clear

(config) authentication strict-password-policy

clock

クロック機能を設定するか、カレンダーをアップデートするには、**clock EXEC** コマンドを使用します。クロック機能とカレンダーをクリアするには、このコマンドの **no** 形式を使用します。

clock {read-calendar | set time day month year | update-calendar}

シンタックスの説明

read-calendar	カレンダーを読み込んでシステムクロックをアップデートします。
set	時刻と日付を設定します。
<i>time</i>	時刻を hh : mm : ss 形式 (hh : 00 ~ 23、mm : 00 ~ 59、ss : 00 ~ 59) で設定します。
<i>day</i>	日 (1 ~ 31)
<i>month</i>	月 (January、February、March、April、May、June、July、August、September、October、November、December)
<i>year</i>	年 (1993 ~ 2035)
update-calendar	システムクロックとともにカレンダーをアップデートします。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

時刻サービス (NTP サーバなど) を提供する外部ソースがネットワークにある場合は、手動でシステムクロックを設定する必要はありません。クロックを設定する場合は、現地時間を入力します。WAAS デバイスでは、**clock timezone** グローバル コンフィギュレーション コマンドによって設定された時間帯に基づいて UTC を算出します。

システムには、ソフトウェアクロックとハードウェアクロックの2つのクロックが存在します。ソフトウェアは、ソフトウェアクロックを使用します。ハードウェアクロックが使用されるのは、起動時にソフトウェアクロックを初期化する場合だけです。

ソフトウェアクロックは、**set** キーワードで設定します。

例

次の例では、WAAS デバイスでソフトウェアクロックを設定します。

```
WAE# clock set 13:32:00 01 February 2005
```

関連コマンド

show clock

cms

WAAS の Centralized Management System (CMS; 中央集中型管理システム) 組み込みデータベースのパラメータを設定するには、**cms EXEC** コマンドを使用します。

```
cms {config-sync | database {backup | create | delete | downgrade [script filename] |
  lcm {enable | disable} | maintenance {full | regular} | restore filename | validate} | deregister
  [force] | recover {identity word}}
```

シンタックスの説明

config-sync	設定を WAAS Cenral Manager と同期化するためのノードを設定します。
database	CMS 組み込みデータベース管理テーブルまたはファイルを作成、バックアップ、削除、元に戻したり、または妥当性を検証します。
backup	データベース管理テーブルをバックアップします。
create	組み込みデータベース管理テーブルを作成します。
delete	組み込みデータベース ファイルを削除します。
downgrade	CMS データベースをダウングレードします。
script	(オプション) ダウングレードスクリプトを適用して CMS データベースをダウングレードします。
<i>filename</i>	ダウングレードされたスクリプト ファイル名
lcm	WAAS Central Manager に登録されている WAAS デバイスでローカル / 中央管理を設定します。
enable	デバイスの WAAS ネットワーク設定のローカル CLI 設定との同期化をイネーブルにします。
disable	デバイスの WAAS ネットワーク設定のローカル CLI 設定との同期化をディセーブルにします。
maintenance	組み込みデータベース テーブルをクリーンし、再度インデックスを付けます。
full	組み込みデータベース テーブルのフル メンテナンスルーチンを指定します。
regular	組み込みデータベース テーブルの定期メンテナンス ルーチンを指定します。
restore	バックアップ ローカル ファイル名を使用してデータベース管理テーブルを元に戻します。
<i>filename</i>	データベースのローカルバックアップ ファイル名
validate	データベース ファイルを検証します。
deregister	CMS プロトデバイスの登録を削除します。
force	(オプション) ノード登録を強制削除します。
recover	WAAS デバイスの ID を回復します。
identity	回復したデバイスの ID を指定します。
<i>word</i>	回復したデバイスの ID

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

WAAS ネットワークは WAAS デバイスと WAAS Central Manager ノードの集まりです。1つのプライマリ WAAS Central Manager が WAAS ネットワーク設定を保持し、他の WAAS ネットワーク ノードにアップデートを提供します。ノード間の通信は Secure Shell Layer (SSL) プロトコルを使用してセキュア チャネルで行われ、WAAS ネットワーク上の各ノードは Rivest, Shamir, Adelman (RSA) 認証キー ペアを使用して他のノードと通信します。

cms config-sync コマンドを使用して、登録された WAAS デバイスとスタンバイ WAAS Central Manager が 5 分 (デフォルト) のポーリング間隔の前にプライマリ WAAS Central Manager とただちに通信して **getUpdate** (コンフィギュレーション ポールの取得) 要求を出せるようにします。たとえば、あるノードがプライマリ WAAS Central Manager に登録され起動されている場合、**getUpdate** 要求を送信するまで WAAS Central Manager GUI には Pending と示されます。**cms config-sync** コマンドにより、登録されたノードはすぐに **getUpdate** を送信し、ノードのステータスは Online に変わります。

CMS データベースの初期化には **cms database create** コマンドを使用します。ノードは WAAS ネットワーク加入前にまず登録して、そのあと起動する必要があります。**cms enable** グローバル コンフィギュレーション コマンドは自動的にノードをデータベース管理テーブルに登録し、CMS をイネーブルにします。ノードはアトリビュート情報を SSL プロトコルを介して WAAS Central Manager に送信し、新しいノード情報を保存します。WAAS Central Manager はアドミッション コントロールなしでこれらのノード登録要求を受け付け、登録確認とアップデート取得に必要な他の関連セキュリティ情報で応答します。ノードは WAAS Central Manager GUI を使用して起動します。

ノードは起動したあと、WAAS Central Manager から自動的にコンフィギュレーション アップデートおよび必要なセキュリティ RSA 認証キーペアを受信します。このセキュリティキーによりノードは WAAS ネットワーク内の他のノードと通信できます。**cms deregister** コマンドは登録情報とデータベース テーブルを削除して WAAS ネットワークからノードを削除します。

WAAS Central Manager の現在の管理データベースをバックアップするには、**cms database backup** コマンドを使用します。データベースのバックアップでは次の項目を指定します。

- 位置、パスワードおよびユーザ ID
- PostgreSQL プレーンテキスト構文でのダンプ フォーマット

バックアップ ファイルのネーミング規則にはタイム スタンプが含まれます。

**(注)**

WAAS Cental Manager で CMS データベースをバックアップするおよび元に戻す手順の詳細は、『*Cisco Wide Area Application Services Configuration Guide*』を参照してください。

損失した登録情報の回復時、または故障したノードを同じ登録情報を持つ新しいノードと交換する際に **cms recover identity word** コマンドを使用する場合は、WAAS Central Manager GUI の System.device.recovery.key ウィンドウの Modifying Config Property で設定したデバイス回復キーを指定する必要があります。

lcm コマンドを使用して WAE の Local/Central Management (LCM) を設定します。LCM 機能を利用して、デバイス CLI または GUI を使用して設定される設定を WAAS ネットワーク全体の設定データ (イネーブルまたはディセーブル) の一部として保存できます。

cms lcm enable コマンドを入力すると、WAE とスタンバイ WAAS Central Manager で動作している CMS プロセスが CLI を使用してこれらのデバイスで行われた設定変更を検出し、その変更をプライマリ WAAS Central Manager に送信します。

cms lcm disable コマンドを入力すると、WAE とスタンバイ WAAS Central Manager で動作している CMS プロセスは CLI 変更をプライマリ WAAS Central Manager に送信しません。デバイス CLI を使用した設定では、プライマリ WAAS Central Manager へ送信されません。

LCM がディセーブルである場合、WAAS Central Manager GUI からの設定では WAE からの設定を上書きしますが、この規則は、ローカルデバイス設定時に WAAS Central Manager が上書きしたローカル デバイス設定だけに適用されます。特定の設定が WAAS Central Manager により上書きされたあと、ローカルデバイス設定を (ローカル CLI ユーザとして) 変更した場合、WAAS Central Manager が WAE からフル デバイス 統計情報アップデートを要求するまで (WAAS Central Manager GUI から **Force full database update** ボタンをクリックしてフル アップデートを開始する)、ローカルデバイス設定が適用されます。WAAS Central Manager がデバイスからフル アップデートを要求した場合、WAAS Central Manager の設定はローカル デバイス設定を上書きします。

例 次の例は、WAAS Central Manager、waas-cm 上の cms 管理テーブルをバックアップします。

```
waas-cm# cms database backup
creating backup file with label `backup'
backup file local1/acns-db-9-22-2002-17-36.dump is ready. use `copy' commands to move
the backup file to a remote host.
```

次の例は、WAAS Central Manager、waas-cm 上の cms データベース管理テーブルを検証します。

```
waas-cm# cms database validate
Management tables are valid
```

関連コマンド

[\(config\) cms](#)

[show cms](#)

cms secure-store

セキュア ストア暗号化を設定するには、**cms secure-store** コマンドを使用します。

```
cms secure-store {init | open | change | clear}
```

シンタックスの説明

init	<p>WAAS デバイス上でセキュア ストア暗号化を初期化します。セキュア ストア暗号化は、続いて cms secure-store open コマンドを実行しない限り、非アクティブのままです。</p> <p>Central Manager 上では、このコマンドによりセキュア ストア暗号化のパスワードの入力が要求されます。</p>
open	<p>セキュア ストア暗号化をアクティブにします (WAAS はセキュア ストア暗号化を使用して、ストアされたデータを暗号化します)。セキュア ストア暗号化は、cms secure-store init コマンドを使用して初期化済みである必要があります。</p> <p>Central Manager 上では、このコマンドによりセキュア ストア暗号化パスワードの入力が要求されます。</p>
change	<p>セキュア ストア暗号化パスワードおよび暗号化キーを変更します。Central Manager 上では、このコマンドにより新しいパスワードの入力および確認が要求されます。WAAS デバイスはパスワードを使用して、セキュア ディスク暗号化の暗号化キーを生成します。</p>
clear	<p>セキュア ストア暗号化をディセーブルにします。</p>

デフォルト

標準暗号化およびキー管理はデフォルトです。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

セキュア ストレージ暗号化により、WAAS システムにより強固な暗号化とキー管理が提供されます。WAAS Central Manager および WAE デバイスは、セキュア ストレージ暗号化を使用して、パスワード処理、暗号化キーの管理、およびデータの暗号化を行います。

cms secure-store EXEC コマンドを使用して Central Manager または WAE デバイス上でセキュア ストアをイネーブルにすると、WAAS システムは強固な暗号化アルゴリズムおよびキー管理ポリシーを使用して、システム上の特定のデータを保護します。このデータには、WAAS システム内のアプリケーションで使用される暗号化キー、CIFS パスワード、およびユーザのログイン パスワードが含まれます。

Central Manager でセキュア ストアがイネーブルである場合、SHA-1 ハッシュおよび AES 256-ビット アルゴリズムにより入力するパスワードから生成される暗号化キーを使用して、データを暗号化します。WAE デバイスでセキュア ストアがイネーブルである場合、SecureRandom により生成される 256-ビットの暗号化キー (暗号的に強固な擬似ランダム番号) を使用して、データを暗号化

します。セキュアストアをイネーブルにするには、パスワードを入力する必要があります。Central Manager をリブートするたびに、コンソール端末を介してこのパスワードを入力する必要があります。

WAE 上でセキュアストアをイネーブルにすると、WAE は Central Manager からの新しい暗号化キーを初期化し、取得します。WAE はこのキーを使用して、WAE 上にストアされている WAFS パスワード認定書を暗号化し、ディスク暗号化もイネーブルである場合は、ディスクを暗号化します。セキュアストアをイネーブルにしたあとに WAE をリブートすると、WAE は Central Manager からキーを自動的に取得し、WAAS 永久ストレージにストアされているデータに通常どおりアクセスできるようにします。

例 次に、WAAS Central Manager 上でセキュアストア暗号化を初期化し、アクティブ化する例を示します。

```

waas-cm# cms secure-store init
enter pass-phrase(case-sensitive, no less than 8 characters)*****
re-enter pass-phrase*****
successfully initialized secure-store.

waas-cm#cms secure-store open
stopping cms..stopped
stopping keymgr..stopped.
enter pass-phrase: <pass phrase>
successfully updated cifs password in database.
successfully opened secure-store.
starting cms..started.
starting keymgr..started.
waas-cm#

```

次に、セキュアストア暗号化を無効にする例を示します。

```

waas-cm#cms secure-store clear
stopping cms..stopped
stopping keymgr..stopped.
successfully updated cifs password in database.
secure-store clear
starting cms..started.
starting keymgr..started.
waas-cm#

```

関連コマンド [show cms secure-store](#)

configure

グローバル コンフィギュレーション モードを開始するには、**configure EXEC** コマンドを使用します。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には、グローバル コンフィギュレーション モードを開始しておく必要があります。

configure

グローバル コンフィギュレーション モードを終了するには、**end** または **exit** コマンドを使用します。**Ctrl-Z** を押して、グローバル コンフィギュレーション モードを終了することもできます。

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン このコマンドを使用してグローバル コンフィギュレーション モードを開始します。

例 次の例は、WAAS デバイスでグローバル コンフィギュレーション モードをイネーブルにする方法を示します。

```
WAE# configure
WAE(config)#
```

関連コマンド [\(config\) end](#)
[\(config\) exit](#)
[show running-config](#)
[show startup-config](#)

copy cdrom

CD-ROM からソフトウェア リリース ファイルをコピーするには、**copy cdrom EXEC** コマンドを使用します。

```
copy cdrom install filedir filename
```

シンタックスの説明

cdrom	CD-ROM からファイルをコピーします。
install	ソフトウェア リリース ファイルをインストールします。
<i>filedir</i>	ソフトウェア リリース ファイルのディレクトリ位置
<i>filename</i>	ソフトウェア リリース ファイルのファイル名

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

関連コマンド

[install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy compactflash

CompactFlash カード からソフトウェア リリース ファイルをコピーするには、**copy compactflash EXEC** コマンドを使用します。

```
copy compactflash install filename
```

シンタックスの説明	
compactflash	CompactFlash カードからファイルをコピーします。
install	ソフトウェア リリース ファイルをインストールします。
<i>filename</i>	イメージファイル名

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

関連コマンド [install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy disk

FTP を使用してディスクからリモート位置または `startup config` に、設定またはイメージデータをコピーするには、**copy disk EXEC** コマンドを使用します。

```
copy disk {ftp {hostname | ip-address} remotefiledir remotefilename localfilename | startup-config filename}
```

シンタックスの説明

disk	ローカルディスクのファイルをコピーします。
ftp	FTP サーバにファイルをコピーします。
<i>hostname</i>	FTP サーバのホスト名
<i>ip-address</i>	FTP サーバの IP アドレス
<i>remotefiledir</i>	ローカルファイルのコピー先の FTP サーバ上のディレクトリ
<i>remotefilename</i>	すでに FTP サーバにコピーされているローカルファイルの名前
<i>localfilename</i>	コピーするローカルファイルの名前
startup-config	ディスクから <code>startup-config</code> (NVRAM) に、設定ファイルをコピーします。
<i>filename</i>	既存の設定ファイルの名前

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

SYSFS パーティションから FTP サーバにファイルをコピーするには、**copy disk ftp EXEC** コマンドを使用します。`startup config` ファイルを NVRAM にコピーするには、**copy disk startup-config EXEC** コマンドを使用します。

関連コマンド

[install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy ftp

FTP サーバからソフトウェア設定またはイメージデータをコピーするには、**copy ftp** EXEC コマンドを使用します。

```
copy ftp {central {hostname | ip-address} remotefiledir remotefilename slotnumber [username
username password | proxy {hostname | ip-address} proxy_portnum [username username
password] | port port-num | md5 md5sum] | disk {hostname | ip-address} remotefiledir
remotefilename localfilename | install {hostname | ip-address} remotefiledir remotefilename}
```

シンタックスの説明

ftp	FTP サーバからファイルをコピーします。
central	ソフトウェア アップグレード イメージ リポジトリにファイルをコピーします。
<i>hostname</i>	FTP サーバのホスト名
<i>ip-address</i>	FTP サーバの IP アドレス
<i>remotefiledir</i>	コピーするイメージファイルがある FTP サーバ上のディレクトリ
<i>remotefilename</i>	イメージ リポジトリにコピーするファイルの名前
<i>slotnumber</i>	アップグレード イメージのコピー先のスロット位置 (1 ~ 5)
username	(オプション) FTP 認証を指定します。
<i>username</i>	(オプション) クリア テキストでのユーザ名
<i>password</i>	(オプション) FTP 認証用のパスワード
proxy	(オプション) プロキシアドレスを指定します。
<i>hostname</i>	(オプション) プロキシサーバのホスト名
<i>ip-address</i>	(オプション) プロキシサーバの IP アドレス
<i>proxy_portnum</i>	(オプション) プロキシサーバのポート番号
username	(オプション) プロキシサーバの認証ユーザ名を指定します。
<i>username</i>	(オプション) クリア テキストでのユーザ名
<i>password</i>	(オプション) プロキシサーバ認証用のパスワード
port	(オプション) FTP サーバに接続するポートを指定します。
<i>port-num</i>	(オプション) FTP サーバのポート番号
md5	(オプション) コピー元のファイルの MD5 シグニチャを指定します。
<i>md5sum</i>	(オプション) MD5 シグニチャ
disk	ローカル ディスクにファイルをコピーします。
<i>hostname</i>	FTP サーバのホスト名
<i>ip-address</i>	FTP サーバの IP アドレス
<i>remotefiledir</i>	コピーするファイルがある FTP サーバ上のディレクトリ
<i>remotefilename</i>	(オプション) ローカル ディスクにコピーするファイルの名前
<i>localfilename</i>	(オプション) コピーされたファイルがローカル ディスクに表示されるときの名前
install	(オプション) FTP サーバからファイルをコピーして、ローカル デバイスにソフトウェア リリース ファイルをインストールします。
<i>hostname</i>	(オプション) FTP サーバの名前
<i>ip-address</i>	(オプション) FTP サーバの IP アドレス
<i>remotefiledir</i>	リモート ファイルのディレクトリ
<i>remotefilename</i>	リモート ファイル名

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン FTP サーバから WAAS デバイスの SYSFS パーティションにファイルをコピーするには、**copy ftp disk EXEC** コマンドを使用します。

FTP サーバからイメージ ファイルを WAAS デバイスにインストールするには、**copy ftp install EXEC** コマンドを使用します。イメージの内、一部はディスクに、一部はフラッシュ メモリにインストールされます。FTP サーバからリポジトリにソフトウェア イメージをダウンロードするには、**copy ftp central EXEC** コマンドを使用します。

copy ftp install EXEC コマンドを使用して、転送を別の場所にリダイレクトすることもできます。ユーザ名とパスワードは、WAAS デバイスへのソフトウェア リリース ファイルの転送が許可される前に、プライマリ ドメイン コントローラ (PDC) で認証を受けておく必要があります。

BIOS のアップグレード

WAE-511、WAE-512、WAE-611、WAE-612、WAE-7326 の BIOS はリモートでアップグレードできます。すべてのコンピュータ ハードウェアは、インターフェイスを介してソフトウェアと連動する必要があります。BIOS は、そのようなインターフェイスを提供します。コンピュータに組み込まれたスタータ キットは、ハードディスク ドライブから他のソフトウェアを実行します。BIOS は、基本命令セットを提供してコンピュータをブートする役割があります。電源投入時自己テスト (POST) 動作やハードディスク ドライブからのオペレーティング システムのブーティングなど、起動時に実行する必要があるタスクをすべて実行します。さらに、割り込みハンドラのライブラリの形式で、ハードウェアとオペレーティング システム間のインターフェイスを提供します。たとえば、キーが押されるたびに CPU は割り込みを実行してそのキーを読み取ります。これは、シリアルおよびパラレル ポート、ビデオカード、サウンドカード、ハードディスク コントローラなどの他の入出力デバイスでも同様です。一部の旧式の PC では、最新のハードウェアとの相互運用を行えません。BIOS がハードウェアをサポートしておらず、オペレーティング システムが BIOS ルーチンを使用するためにコールできないためです。この問題は、新しいハードウェアをサポートする BIOS に交換するか、そのハードウェアに対応したデバイス ドライバをインストールすれば解決できます。

特定のハードウェア モデルの BIOS アップデートに必要なすべての BIOS ファイルは、1 つの *.bin* パッケージ ファイルとして Cisco.com で入手できます。このファイルは専用の *<WAAS-installable>.bin* ファイルで、通常のソフトウェア アップデート手順でインストールできます。

BIOS のバージョンアップデートをサポートする WAAS デバイスの BIOS バージョンをアップデートするには、次のものがが必要です。

- ソフトウェア ファイルのある FTP サーバ
- アップデートするデバイスとアップデート ファイルを格納するサーバ間のネットワーク接続
- 当該の *.bin* BIOS アップデート ファイル
 - 511_bios.bin

- 611_bios.bin
- 7326_bios.bin

**注意**

フラッシュ BIOS をアップグレードする際は、特に注意してください。BIOS アップグレードパッチが完全に正しいものであることをしっかりと確認してください。適用したパッチが間違っていた場合、システムはブート不能になり、正しいパッチを適用し直しても回復不能になる可能性があります。

**注意**

フラッシュ BIOS アップデートの失敗で非常に深刻な結果がもたらされる可能性があるため、フラッシュ BIOS は必ず、最初にシステムを Uninterruptible Power Supply (UPS; 無停電電源装置) に接続してからアップデートしてください。

BIOS アップデート ファイルをリモートでインストールするには、次のように **copy ftp install EXEC** コマンドを使用します。

```
WAE# copy ftp install ftp-server remote_file_dir 7326_bios.bin
```

BIOS アップデート ファイルをシステムにコピーしたら、次のように **reload EXEC** コマンドを使用してリブートします。

```
WAE# reload
```

新しい BIOS は、システムをリブートしたあと、有効になります。

例

次の例は、FTP サーバからイメージ ファイルをコピーして、そのファイルをローカル デバイスにインストールする方法を示します。

```
WAE# copy ftp install 10.1.1.1 //ftp-sj.cisco.com/cisco/waas/4.0 WAAS-4.0.0-k9.bin
Enter username for remote ftp server:biff
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER biff
10.1.1.1 FTP server (Version) Mon Feb 28 10:30:36 EST
2000) ready.
Password required for biff.
Sending:PASS *****
User biff logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:CWD //ftp-sj.cisco.com/cisco/waas/4.0
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:RETR WAAS-4.0.0-k9.bin
Opening BINARY mode data connection for ruby.bin (87376881 bytes).
#####
writing flash component:
.....
The new software will run after you reload.
```

次の例は、BIOS をアップグレードする方法を示します。すべての出力は、追跡できるように別のファイル (`/local1/bios_upgrade.txt`) に書き込まれます。BIOS アップグレードのため Cisco.com からダウンロードされたハードウェア依存ファイルは、BIOS アップグレード手順の完了後、自動的に WAAS デバイスから削除されます。

```

WAE-7326# copy ftp install upgradeserver /bios/update53/derived/ 7326_bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER myusername
upgradeserver.cisco.com FTP server (Version wu-2.6.1-18) ready.
Password required for myusername.
Sending:PASS *****
Please read the file README_dotfiles
  it was last modified on Wed Feb 19 16:10:26 2005- 94 days ago
Please read the file README_first
  it was last modified on Wed Feb 19 16:05:29 2005- 94 days ago
User myusername logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,240,57,37)
Sending:CWD /bios/update53/derived/
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,240,146,117)
Sending:RETR 7326_bios.bin
Opening BINARY mode data connection for 7326_bios.bin (834689 bytes).
Fri Jan 7 15:29:07 UTC 2005
BIOS installer running!
Do not turnoff the system till BIOS installation is complete.
Flash chipset:Macronix 29LV320B
0055000.FLS:280000 [80000]
Erasing block 2f:280000 - 28ffff
Erasing block 30:290000 - 29ffff
Erasing block 31:2a0000 - 2afffff
Erasing block 32:2b0000 - 2bffff
Erasing block 33:2c0000 - 2cffff
Erasing block 34:2d0000 - 2dffff
Erasing block 35:2e0000 - 2efffff
Erasing block 36:2f0000 - 2fffff
Programming block 2f:280000 - 28ffff
Programming block 30:290000 - 29ffff
Programming block 31:2a0000 - 2afffff
Programming block 32:2b0000 - 2bffff
Programming block 33:2c0000 - 2cffff
Programming block 34:2d0000 - 2dffff
Programming block 35:2e0000 - 2efffff
Programming block 36:2f0000 - 2fffff
SCSIROM.BIN:260000 [20000]
Erasing block 2d:260000 - 26ffff
Erasing block 2e:270000 - 27ffff
Programming block 2d:260000 - 26ffff
Programming block 2e:270000 - 27ffff
PXEROM.BIN:250000 [10000]
Erasing block 2c:250000 - 25ffff
Programming block 2c:250000 - 25ffff
Primary BIOS flashed successfully
Cleanup BIOS related files that were downloaded....
The new software will run after you reload.
WAE-7326#

```

関連コマンド

[install](#)

[reload](#)

[show running-config](#)[show startup-config](#)[wafs](#)[write](#)

copy http

HTTP サーバから WAAS デバイスに設定またはイメージ ファイルをコピーするには、**copy http EXEC** コマンドを使用します。

```
copy http install {hostname | ip-address}remotefiledir remotefilename [port portnum] [proxy proxy_portnum] [username username password]
```

シンタックスの説明

http	HTTP サーバからファイルをコピーします。
install	HTTP サーバからファイルをコピーして、ローカル デバイスにソフトウェア リリース ファイルをインストールします。
<i>hostname</i>	HTTP サーバの名前
<i>ip-address</i>	HTTP サーバの IP アドレス
<i>remotefiledir</i>	リモート ファイルのディレクトリ
<i>remotefilename</i>	リモート ファイル名
port	(オプション) HTTP サーバに接続するポート (デフォルトは 80)
<i>portnum</i>	HTTP サーバのポート番号 (1 ~ 65535)
proxy	(オプション) HTTP プロキシ サーバに要求をリダイレクトできるようにします。
<i>proxy_portnum</i>	HTTP プロキシ サーバのポート番号 (1 ~ 65535)
username	(オプション) HTTP プロキシ サーバにアクセスするためのユーザ名
<i>username</i>	ユーザのログイン名
<i>password</i>	パスワード認証を確立します。

デフォルト

HTTP サーバ ポート : 80

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

HTTP サーバからイメージ ファイルをインストールして、それを WAAS デバイスにインストールするには、**copy http install EXEC** コマンドを使用します。転送プロトコルとして HTTP を使用して HTTP サーバから WASS デバイスにイメージを転送し、デバイスにソフトウェアをインストールし

ます。イメージの内、一部はディスクに、一部はフラッシュメモリにインストールされます。HTTP サーバからリポジトリにソフトウェアイメージをダウンロードするには、**copy http central EXEC** コマンドを使用します。

proxy hostname | ip-address オプションを指定することで、**copy http install EXEC** コマンドを使用して、転送を別の場所または HTTP プロキシサーバにリダイレクトすることもできます。ユーザ名とパスワードは、WAAS デバイスへのソフトウェアリリースファイルの転送が許可される前に、PDC で認証を受けておく必要があります。

BIOS のアップグレード

WAE-511、WAE-512、WAE-611、WAE-612、WAE-7326 の BIOS はリモートでアップグレードできます。すべてのコンピュータハードウェアは、インターフェイスを介してソフトウェアと連動する必要があります。BIOS は、そのようなインターフェイスを提供します。コンピュータに組み込まれたスタータキットは、ハードディスクドライブから他のソフトウェアを実行します。BIOS は、基本命令セットを提供してコンピュータをブートする役割があります。POST 動作やハードディスクドライブからのオペレーティングシステムのブーティングなど、起動時に実行する必要があるタスクをすべて実行します。さらに、割り込みハンドラのライブラリの形式で、ハードウェアとオペレーティングシステム間のインターフェイスを提供します。たとえば、キーが押されるたびに CPU は割り込みを実行してそのキーを読み取ります。これは、シリアルおよびパラレルポート、ビデオカード、サウンドカード、ハードディスクコントローラなどの他の入出力デバイスでも同様です。一部の旧式の PC では、最新のハードウェアとの相互運用を行えません。BIOS がハードウェアをサポートしておらず、オペレーティングシステムが BIOS ルーチンを使用するためにコールできないためです。この問題は、新しいハードウェアをサポートする BIOS に交換するか、そのハードウェアに対応したデバイスドライバをインストールすれば解決できます。

特定のハードウェアモデルの BIOS アップデートに必要なすべての BIOS ファイルは、1 つの *.bin* パッケージファイルとして Cisco.com で入手できます。このファイルは専用の *<WAAS-installable>.bin* ファイルで、通常のソフトウェアアップデート手順でインストールできます。

BIOS のバージョンアップデートをサポートする WAAS デバイスの BIOS バージョンをアップデートするには、次のものがが必要です。

- ソフトウェアファイルのある HTTP サーバ
- アップデートするデバイスとアップデートファイルを格納するサーバ間のネットワーク接続
- 当該の *.bin* BIOS アップデートファイル
 - 511_bios.bin
 - 611_bios.bin
 - 7326_bios.bin



注意

フラッシュ BIOS をアップグレードする際は、特に注意してください。BIOS アップグレードパッチが完全に正しいものであることをしっかりと確認してください。適用したパッチが間違っていた場合、システムはブート不能になり、正しいパッチを適用し直しても回復不能になる可能性があります。



注意

フラッシュ BIOS アップデートの失敗で非常に深刻な結果がもたらされる可能性があるため、フラッシュ BIOS は必ず、最初にシステムを UPS に接続してからアップデートしてください。

BIOS アップデート ファイルを WAAS デバイスにインストールするには、次のように **copy http install EXEC** コマンドを使用します。

```
WAE# copy http install http-server remote_file_dir 7326_bios.bin
[portnumber]
```

BIOS アップデート ファイルをシステムにコピーしたら、次のように **reload EXEC** コマンドを使用して WAAS デバイスをリブートします。

```
WAE# reload
```

新しい BIOS は、システムをリブートしたあと、有効になります。

例

次の例は、HTTP サーバからイメージ ファイルをコピーして、そのファイルを WAAS デバイスにインストールする方法を示します。

```
WAE# copy http install 10.1.1.1 //ftp-sj.cisco.com/cisco/waas/4.0 WAAS-4.0.0-k9.bin
Enter username for remote ftp server:biff
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER biff
10.1.1.1 FTP server (Version) Mon Feb 28 10:30:36 EST
2000) ready.
Password required for biff.
Sending:PASS *****
User biff logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:CWD //ftp-sj.cisco.com/cisco/waas/4.0
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,244,55,156)
Sending:RETR WAAS-4.0.0-k9.bin
Opening BINARY mode data connection for ruby.bin (87376881 bytes).
#####
writing flash component:
.....
The new software will run after you reload.
```

次の例は、BIOS をアップグレードする方法を示します。すべての出力は、追跡できるように別のファイル (`/local/bios_upgrade.txt`) に書き込まれます。BIOS アップグレードのため Cisco.com からダウンロードされたハードウェア依存ファイルは、BIOS アップグレード手順の完了後、自動的に WAAS デバイスから削除されます。

```

WAE-7326# copy ftp install upgradeserver /bios/update53/derived/ 7326_bios.bin
Enter username for remote ftp server:myusername
Enter password for remote ftp server:*****
Initiating FTP download...
printing one # per 1MB downloaded
Sending:USER myusername
upgradeserver.cisco.com FTP server (Version wu-2.6.1-18) ready.
Password required for myusername.
Sending:PASS *****
Please read the file README_dotfiles
  it was last modified on Wed Feb 19 16:10:26 2005- 94 days ago
Please read the file README_first
  it was last modified on Wed Feb 19 16:05:29 2005- 94 days ago
User myusername logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (128,107,193,240,57,37)
Sending:CWD /bios/update53/derived/
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,240,146,117)
Sending:RETR 7326_bios.bin
Opening BINARY mode data connection for 7326_bios.bin (834689 bytes).
Fri Jan  7 15:29:07 UTC 2005
BIOS installer running!
Do not turnoff the system till BIOS installation is complete.
Flash chipset:Macronix 29LV320B
0055000.FLS:280000 [80000]
Erasing block 2f:280000 - 28ffff
Erasing block 30:290000 - 29ffff
Erasing block 31:2a0000 - 2affff
Erasing block 32:2b0000 - 2bffff
Erasing block 33:2c0000 - 2cffff
Erasing block 34:2d0000 - 2dffff
Erasing block 35:2e0000 - 2effff
Erasing block 36:2f0000 - 2fffff
Programming block 2f:280000 - 28ffff
Programming block 30:290000 - 29ffff
Programming block 31:2a0000 - 2affff
Programming block 32:2b0000 - 2bffff
Programming block 33:2c0000 - 2cffff
Programming block 34:2d0000 - 2dffff
Programming block 35:2e0000 - 2effff
Programming block 36:2f0000 - 2fffff
SCSIROM.BIN:260000 [20000]
Erasing block 2d:260000 - 26ffff
Erasing block 2e:270000 - 27ffff
Programming block 2d:260000 - 26ffff
Programming block 2e:270000 - 27ffff
PXEROM.BIN:250000 [10000]
Erasing block 2c:250000 - 25ffff
Programming block 2c:250000 - 25ffff
Primary BIOS flashed successfully
Cleanup BIOS related files that were downloaded....
The new software will run after you reload.

```

関連コマンド

[install](#)

[reload](#)

[show running-config](#)

[show startup-config](#)[wafs](#)[write](#)

copy running-config

現在の設定から設定データまたはイメージデータをコピーするには、**copy running-config EXEC** コマンドを使用します。

```
copy running-config {disk filename | startup-config | tftp {hostname | ip-address} remotefilename}
```

シンタックスの説明

running-config	現在のシステム設定をコピーします。
disk	ディスク ファイルに現在のシステム設定をコピーします。
<i>filename</i>	ディスク上に作成するファイルの名前
startup-config	startup-config (NVRAM) に、実行コンフィギュレーションをコピーします。
tftp	TFTP サーバ上のファイルに実行コンフィギュレーションをコピーします。
<i>hostname</i>	TFTP サーバのホスト名
<i>ip-address</i>	TFTP サーバの IP アドレス
<i>remotefilename</i>	TFTP サーバ上に作成される設定ファイルのリモート ファイル名。完全パス名を使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

WAAS デバイスの実行システム コンフィギュレーションを SYSFS パーティション、フラッシュ メモリ、または TFTP サーバにコピーするには、**copy running-config EXEC** コマンドを使用します。**copy running-config startup-config EXEC** コマンドは、**write memory** コマンドと同等です。

関連コマンド

[install](#)[reload](#)[show running-config](#)[show startup-config](#)[wafs](#)[write](#)

copy startup-config

startup-config から設定データまたはイメージ データをコピーするには、**copy startup-config EXEC** コマンドを使用します。

```
copy startup-config {disk filename | running-config | tftp {hostname | ip-address} remotefilename}
```

シンタックスの説明

startup-config	startup-config をコピーします。
disk	ディスク ファイルに startup-config をコピーします。
<i>filename</i>	ローカル ディスクにコピーする startup-config ファイルの名前
running-config	startup-config を実行コンフィギュレーションにコピーします。
tftp	TFTP サーバ上のファイルに startup-config をコピーします。
<i>hostname</i>	TFTP サーバのホスト名
<i>ip-address</i>	TFTP サーバの IP アドレス
<i>remotefilename</i>	TFTP サーバ上に作成される startup-config ファイルのリモート ファイル名。 完全パス名を使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

TFTP サーバまたは SYSFS パーティションに startup-config ファイルをコピーするには、**copy startup-config EXEC** コマンドを使用します。

関連コマンド

[install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy sysreport

デバイスからシステムトラブルシューティング情報をコピーするには、**copy sysreport EXEC** コマンドを使用します。

```
copy sysreport {disk filename | ftp {hostname | ip-address} remotedirectory remotefilename | tftp
                {hostname | ip-address} remotefilename} [start-date {day month | month day} year [end-date {day
                month | month day} year]]
```

シンタックスの説明

sysreport	WAAS システム情報が含まれるレポートを作成し、ファイルに保存します。
disk	ディスク ファイルにシステム情報をコピーします。
<i>filename</i>	ディスク上に作成するファイルの名前なお、.tar.gz が指定したファイル名に付け加えられます。
ftp	FTP サーバにシステム情報をコピーします。
<i>hostname</i>	FTP サーバのホスト名
<i>ip-address</i>	FTP サーバの IP アドレス
<i>remotedirectory</i>	システム情報ファイルが作成される FTP サーバ上のリモートディレクトリ
<i>remotefilename</i>	FTP サーバ上に作成されるシステム情報ファイルのリモート ファイル名
tftp	TFTP サーバにシステム情報をコピーします。
<i>hostname</i>	TFTP サーバのホスト名
<i>ip-address</i>	TFTP サーバの IP アドレス
<i>remotefilename</i>	TFTP サーバ上に作成されるシステム情報ファイルのリモート ファイル名完全パス名を使用します。
start-date	(オプション) 作成されたシステム レポート内の情報の開始日
<i>day month</i>	開始の日付 (1 ~ 31) および月 (January, February, March, April, May, June, July, August, September, October, November, December)。先に月、そのあとに日を指定することもできます。
<i>year</i>	開始日の年 (1993 ~ 2035)
end-date	(オプション) 作成されたシステム レポート内の情報の終了日。省略した場合、この日付はデフォルトにより本日の日付になります。レポートにはこの日の終わりまでのファイルが含まれます。
<i>day month</i>	終了日 (1 ~ 31) および月 (January, February, March, April, May, June, July, August, September, October, November, December)。先に月、そのあとに日を指定することもできます。
<i>year</i>	終了日の年 (1993 ~ 2035)

デフォルト

終了日を指定しないと、本日の日付が使用されます。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

copy sysreport コマンドはかなりの多くの CPU とディスク リソースを消費するので、実行中、システム パフォーマンスが低下する可能性があります。

例

次の例では、ローカル WAAS デバイスのファイル `mysysinfo` にシステム情報をコピーする方法を示します。

```
WAE# copy sysreport disk mysysinfo start-date 1 April 2006 end-date April 30 2006
```

次の例は、FTP サーバ `myserver` のルート ディレクトリにあるファイル `foo` に FTP によりシステム情報をコピーする方法を示します。

```
WAE# copy sysreport ftp myserver / foo start-date 1 April 2006 end-date April 30 2006
```

関連コマンド

[show running-config](#)

[show startup-config](#)

[wafs](#)

copy system-status

デバック目的でシステムからステータス情報をコピーするには、**copy system-status EXEC** コマンドを使用します。

copy system-status disk filename

シンタックスの説明

system-status disk	ディスク ファイルにシステム ステータスをコピーします。
<i>filename</i>	ディスク上に作成するファイルの名前

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

ハードウェアおよびソフトウェア ステータス情報を格納する SYSFS パーティションにファイルを作成するには、**copy system-status EXEC** コマンドを使用します。

関連コマンド

[install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy tech-support

Cisco TAC への問い合わせに利用するためシステムから設定またはイメージデータをコピーするには、**copy tech-support EXEC** コマンドを使用します。

```
copy tech-support {disk filename | tftp {hostname | ip-address} remotefilename}
```

シンタックスの説明

tech-support	テクニカル サポート用にシステム情報をコピーします。
disk	テクニカル サポート用にシステム情報をディスク ファイルにコピーします。
<i>filename</i>	ディスク上に作成するファイルの名前
tftp	テクニカル サポート用にシステム情報を TFTP サーバにコピーします。
<i>hostname</i>	TFTP サーバのホスト名
<i>ip-address</i>	TFTP サーバの IP アドレス
<i>remotefilename</i>	TFTP サーバ上に作成されるシステム情報ファイルのリモート ファイル名完全パス名を使用します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

TFTP サーバまたは SYSFS パーティションにテクニカル サポート情報をコピーするには、**copy tech-support tftp EXEC** コマンドを使用します。

関連コマンド

[install](#)
[reload](#)
[show running-config](#)
[show startup-config](#)
[wafs](#)
[write](#)

copy tftp

TFTP サーバから設定またはイメージデータをコピーするには、**copy tftp** EXEC コマンドを使用します。

```
copy tftp {disk {hostname | ip-address} remotefilename localfilename | running-config
          {hostname | ip-address} remotefilename | startup-config {hostname | ip-address} remotefilename}
```

シンタックスの説明

tftp	TFTP サーバからのイメージをコピーします。
disk	ディスク ファイルに TFTP サーバからのイメージをコピーします。
<i>hostname</i>	TFTP サーバのホスト名
<i>ip-address</i>	TFTP サーバの IP アドレス
<i>remotefilename</i>	TFTP サーバからコピーするリモート イメージ ファイルの名前。完全パス名を使用します。
<i>localfilename</i>	ローカル ディスク上に作成するイメージ ファイルの名前
running-config	実行コンフィギュレーションに TFTP サーバからイメージをコピーします。
<i>hostname</i>	TFTP サーバのホスト名
<i>ip-address</i>	TFTP サーバの IP アドレス
<i>remotefilename</i>	TFTP サーバからコピーするリモート イメージ ファイルの名前。完全パス名を使用します。
startup-config	スタートアップ コンフィギュレーションに TFTP サーバからイメージをコピーします。
<i>hostname</i>	TFTP サーバのホスト名
<i>ip-address</i>	TFTP サーバの IP アドレス
<i>remotefilename</i>	TFTP サーバからコピーするリモート イメージ ファイルの名前。完全パス名を使用します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

TFTP サーバからディスクにファイルをコピーするには、**copy tftp disk** EXEC コマンドを使用します。

関連コマンド

install
reload
show running-config
show startup-config
wafs
write

cpfile

ファイルのコピーを作成するには、**cpfile EXEC** コマンドを使用します。

```
cpfile oldfilename newfilename
```

シンタックスの説明

<i>oldfilename</i>	コピーするファイルの名前
<i>newfilename</i>	作成されるファイルの名前

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドを使用してファイルのコピーを作成します。SYSFS ファイルだけがコピーできます。

例

次の例は、ファイルのコピーを作成する方法を示します。

```
WAE# cpfile fe511-194616.bin fd511-194618.bin
```

関連コマンド

[deltree](#)
[dir](#)
[lls](#)
[ls](#)
[mkdir](#)
[pwd](#)
[rename](#)

debug

WAAS アプリケーション アクセラレーションおよびセントラル マネージャ機能を監視および記録するには、**debug EXEC** コマンドを使用します。デバッグング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 (**undebug** コマンドも参照)。

application-accelerator デバイス モードでは、**debug** コマンドは次のとおりです。

```

debug authentication {content-request | user | windows-domain}
debug buf {all | dmbuf | dmsg}
debug cdp {adjacency | events | ip | packets}
debug cli {all | bin | parser}
debug cms
debug dataserver {all | clientlib | server}
debug dhcp
debug dre {aggregation | all | cache | connection {aggregation [acl] | cache [acl] | core [acl] | message
[acl] | misc [acl] | acl} | core | lz | message | misc}
debug epm
debug flow monitor tcpstat-v1
debug logging all
debug ntp
debug print-spooler {all | brief | errors | warnings}
debug rbc
debug snmp {all | cli | main | mib | traps}
debug stats {all | collections | computation | history}
debug tfo {buffer-mgr | connection [auto-discovery [acl] | comp-mgr [acl] | conn-mgr [acl] |
egress-method [acl] | filtering [acl] | netio-engine [acl] | policy-engine [acl] | synq [acl] | acl] |
stat-mgr | translog}
debug translog export
debug wafs {{all | core-fe | edge-fe | manager | utilities} {debug | error | info | warn}}
debug wccp {all | detail | error | events | keepalive | packets | slowstart}

```



(注)

dre、*epm*、*flow monitor*、*print-spooler*、*rbc*、*tfo*、*translog*、*wafs*、および *wccp* コマンド オプションは application-accelerator デバイス モードのみでサポートされます。

central manager デバイス モードでは、**debug** コマンドは次のとおりです。

```

debug aaa accounting
debug all
debug authentication {content-request | user | windows-domain}
debug buf {all | dmbuf | dmsg}
debug cdp {adjacency | events | ip | packets}

```

```

debug cli {all | bin | parser}
debug cms
debug dataserver {all | clientlib | server}
debug dhcp
debug emdb [level [levelnum]]
debug key-manager
debug logging all
debug ntp
debug rpc {detail | trace}
debug snmp {all | cli | main | mib | traps}
debug stats {all | collections | computation | history}

```



(注)

emdb および *rpc* コマンド オプションは、central manager デバイス モードでのみサポートされます。

シンタックスの説明

aaa accounting	(オプション) AAA アカウンティング アクションをイネーブルにします。
all	(オプション) すべてのデバッグ オプションをイネーブルにします。
authentication	(オプション) 認証デバッグをイネーブルにします。
content-request	コンテンツ要求認証のデバッグをイネーブルにします。
user	システム認証に対するユーザ ログインのデバッグをイネーブルにします。
windows-domain	Windows ドメイン認証のデバッグをイネーブルにします。
buf	(オプション) バッファ マネージャのデバッグをイネーブルにします。
all	すべてのバッファ マネージャのデバッグをイネーブルにします。
dmbuf	dmbuf デバッグのみをイネーブルにします。
dmsg	dmsg デバッグだけをイネーブルにします。
cdp	(オプション) CDP デバッグをイネーブルにします。
adjacency	CDP ネイバー情報のデバッグをイネーブルにします。
events	CDP イベントのデバッグをイネーブルにします。
ip	CDP IP のデバッグをイネーブルにします。
packets	パケット関連 CDP のデバッグをイネーブルにします。
cli	(オプション) CLI デバッグをイネーブルにします。
all	すべての CLI のデバッグをイネーブルにします。
bin	CLI コマンド バイナリ プログラムのデバッグをイネーブルにします。
parser	CLI コマンド パーサーのデバッグをイネーブルにします。
cms	(オプション) CMS デバッグをイネーブルにします。
dataserver	(オプション) データ サーバのデバッグをイネーブルにします。
all	すべてのデータ サーバのデバッグをイネーブルにします。
clientlib	データ サーバ クライアント ライブラリ モジュールのデバッグをイネーブルにします。
server	データ サーバ モジュールのデバッグをイネーブルにします。

dhcp	(オプション) DHCP デバッグをイネーブルにします。
dre	(オプション) DRE デバッグをイネーブルにします。
aggregation	DRE チャンク集約のデバッグをイネーブルにします。
all	すべての DRE コマンドのデバッグをイネーブルにします。
cache	DRE キャッシュのデバッグをイネーブルにします。
connection	DRE 接続のデバッグをイネーブルにします。
aggregation [acl]	指定された接続の DRE チャンク集約のデバッグをイネーブルにします。
cache [acl]	指定された接続の DRE キャッシュのデバッグをイネーブルにします。
core [acl]	指定された接続の DRE コアのデバッグをイネーブルにします。
message [acl]	指定された接続の DRE メッセージのデバッグをイネーブルにします。
misc [acl]	指定された接続のその他の DRE デバッグをイネーブルにします。
acl	トレースされた接続を制限する ACL
core	DRE コアのデバッグをイネーブルにします。
message	DRE メッセージのデバッグをイネーブルにします。
misc	その他の DRE デバッグをイネーブルにします。
epm	(オプション) DCE-RPC EPM デバッグをイネーブルにします。
flow	(オプション) ネットワーク トラフィック フローのデバッグをイネーブルにします。
monitor	モニタ フロー パフォーマンスのデバッグ コマンドをイネーブルにします。
tcpstat-v1	tcpstat-v1 のデバッグをイネーブルにします。
logging	(オプション) ロギングのデバッグをイネーブルにします。
all	すべてのロギングのデバッグをイネーブルにします。
ntp	(オプション) NTP デバッグをイネーブルにします。
print-spooler	(オプション) プリント スプーラのデバッグをイネーブルにします。
all	すべてのデバッグ機能を使用して、プリント スプーラのデバッグをイネーブルにします。
brief	簡潔なデバッグ メッセージのみを使用して、プリント スプーラのデバッグをイネーブルにします。
errors	エラー条件のみを使用して、プリント スプーラのデバッグをイネーブルにします。
warnings	警告条件のみを使用して、プリント スプーラのデバッグをイネーブルにします。
rbcp	(オプション) RBCP デバッグをイネーブルにします。
snmp	(オプション) SNMP デバッグ コマンドをイネーブルにします。
all	すべての SNMP デバッグ コマンドをイネーブルにします。
cli	すべての SNMP CLI のデバッグをイネーブルにします。
main	SNMP のメイン デバッグをイネーブルにします。
mib	SNMP MIB のデバッグをイネーブルにします。
traps	SNMP トラップのデバッグをイネーブルにします。
stats	(オプション) 統計情報のデバッグをイネーブルにします。
all	すべての statistics デバッグ コマンドをイネーブルにします。
collection	統計情報収集のデバッグをイネーブルにします。
computation	統計情報計算のデバッグをイネーブルにします。

history	統計情報履歴のデバッグをイネーブルにします。
tfo	(オプション) TFO デバッグをイネーブルにします。
buffer-mgr	TFO バッファ マネージャのデバッグをイネーブルにします。
connection	TFO 接続のデバッグをイネーブルにします。
auto-discovery [acl]	自動ディスカバリ モジュールの TFO 接続のデバッグをイネーブルにします。
comp-mgr [acl]	圧縮モジュールの TFO 接続のデバッグをイネーブルにします。
conn-mgr [acl]	Connection Manager の TFO 接続のデバッグをイネーブルにします。
egress-method [acl]	接続出力方式の TFO 接続のデバッグをイネーブルにします。
filtering [acl]	フィルタリング モジュールの TFO 接続のデバッグをイネーブルにします。
netio-engine [acl]	ネットワーク入出力モジュールの TFO 接続のデバッグをイネーブルにします。
policy-engine [acl]	アプリケーション ポリシーの TFO 接続のデバッグをイネーブルにします。
synq [acl]	SynQ モジュールの TFO 接続のデバッグをイネーブルにします。
acl	TFO 接続を制限する ACL
stat-mgr	TFO Statistics Manager のデバッグをイネーブルにします。
translog	TFO トランザクション ログのデバッグをイネーブルにします。
translog	(オプション) transaction logging デバッグ コマンドをイネーブルにします。
export	トランザクション ログ FTP エクスポートのデバッグをイネーブルにします。
wafs	(オプション) WASS ソフトウェア コンポーネントとユーティリティからのメッセージがロギングされる通知レベル (debug、info、warn、error) をアンセットします。
all	すべてのソフトウェア コンポーネントとユーティリティのロギング レベルを同時にアンセットします。
core-fe	Core File Engine として機能する WAE のロギング レベルをアンセットします。
edge-fe	Edge File Engine として機能する WAE のロギング レベルをアンセットします。
manager	Device Manager のロギング レベルをアンセットします。
utilities	WAAS ユーティリティのロギング レベルをアンセットします。
wccp	(オプション) WCCP 情報のデバッグをイネーブルにします。
all	すべての WCCP デバッグ機能をイネーブルにします。
detail	WCCP の詳細なデバッグをイネーブルにします。
error	WCCP エラーのデバッグをイネーブルにします。
events	WCCP イベントのデバッグをイネーブルにします。
keepalive	アプリケーションに送信される WCCP キープアライブのデバッグをイネーブルにします。
packets	WCCP パケット関連情報のデバッグをイネーブルにします。
slowstart	WCCP スロースタートのデバッグをイネーブルにします。

次の構文表では、**central manager** デバイス モードで使用するオプションについて説明します。

emdb	(オプション) 組み込みデータベースのデバッグをイネーブルにします。
level	(オプション) EMDB サービスの指定されたデバッグ レベルをイネーブルにします。
levelnum	(オプション) ディセーブルにするデバッグ レベル (レベル 0 はデバッグをディセーブルにします)
key-manager	(オプション) Central Manager のキー マネージャのデバッグをイネーブルにします。
rpc	(オプション) Remote Procedure Call (RPC; リモート プロシージャ コール) ログをイネーブルにします。
detail	プライオリティ レベルが「detail」以上の RPC ログをイネーブルにします。
trace	プライオリティ レベルが「trace」以上の RPC ログをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

debug コマンドを使用すると WAAS デバイスのパフォーマンスが低下するので、このコマンドは TAC から指示があった場合にだけ使用することを推奨します。詳細については、「[マニュアルの入手方法および Service Request ツールの使用方法](#)」(p.xv) を参照してください。

Watchdog ユーティリティが動作していないと、「WAAS is not running」メッセージが出力されます。

イネーブル化された **debug** オプションを表示するには、**show debugging** コマンドを使用します。

例

次の例は、ユーザ認証のデバッグ モニタリングをイネーブルにし、イネーブルになっているか確認し、続いてデバッグ モニタリングをディセーブルにする方法を示します。

```
WAE# debug authentication user
WAE# show debugging
Debug authentication (user) is ON
WAE# no debug authentication user
```

次の例は、システム内の Core WAE のデバッグするためのロギング レベルを設定し、その後ロギング レベルをデフォルト (info) に戻す方法を示します。

```
WAE# debug wafs ?
  all          log level for all components
  core-fe      log level for Core FE
  edge-fe      log level for Edge FE
  manager      log level for Manager
  utilities    log level for Utilities
WAE# debug wafs core-fe ?
  debug set log level to DEBUG
  error  set log level to ERROR
  info   set log level to INFO (default)
  warn   set log level to WARN
WAE# debug wafs core-fe debug
corefe log level set to DEBUG
```

関連コマンド

[show debugging](#)

[undebug](#)

delfile

現在のディレクトリからファイルを削除するには、**delfile EXEC** コマンドを使用します。

delfile *filename*

シンタックスの説明

<i>filename</i>	削除するファイルの名前
-----------------	-------------

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

この EXEC コマンドを使用して、WAAS デバイスのディスク ドライブの SYSFS パーティションからファイルを削除します。

例

次の例は、絶対パスを使用して */local1* ディレクトリから一時ファイルを削除する方法を示します。

```
WAE# delfile /local1/tempfile
```

関連コマンド

[cpfile](#)

[dir](#)

[lls](#)

[ls](#)

[mkdir](#)

[pwd](#)

[rename](#)

deltree

ディレクトリを、そのすべてのサブディレクトリおよびファイルとともに削除するには、**deltree** EXEC コマンドを使用します。

deltree *directory*

シンタックスの説明

directory 削除するディレクトリ ツリーの名前

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

この EXEC コマンドを使用してディレクトリとそのディレクトリ内のすべてのファイルを、WAAS SYSFS ファイル システムから削除します。サブディレクトリおよびファイルを削除しているという警告は表示されません。



(注)

WAAS が正常に機能するのに必要なファイルやディレクトリは、決して削除しないでください。

例

次の例は、*/local1* ディレクトリから *testdir* ディレクトリを削除する方法を示します。

```
WAE# deltree /local1/testdir
```

関連コマンド

[cpfile](#)

[dir](#)

[lls](#)

[ls](#)

[mkdir](#)

[pwd](#)

[rename](#)

dir

ディレクトリの1つのファイルまたはすべてのファイルの詳細を表示するには、**dir** EXEC コマンドを使用します。

dir [directory]

シンタックスの説明

directory (オプション) リストするディレクトリの名前

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドを使用して、名前、サイズ、作成時間など、作業ディレクトリ内部に含まれているファイルの詳細リストを表示します。**lls** EXEC コマンドも同じ出力を生成します。

例

次の例は、現在のディレクトリのすべてのファイルの詳細リストを示します。

```
WAB# dir
size          time of last change          name
-----
    4096  Fri Feb 24 14:40:00 2006  <DIR>  actona
    4096  Tue Mar 28 14:42:44 2006  <DIR>  core_dir
    4096  Wed Apr 12 20:23:10 2006  <DIR>  crash
    4506  Tue Apr 11 13:52:45 2006          dbupgrade.log
    4096  Tue Apr  4 22:50:11 2006  <DIR>  downgrade
    4096  Sun Apr 16 09:01:56 2006  <DIR>  errorlog
    4096  Wed Apr 12 20:23:41 2006  <DIR>  logs
   16384  Thu Feb 16 12:25:29 2006  <DIR>  lost+found
    4096  Wed Apr 12 03:26:02 2006  <DIR>  sa
   24576  Sun Apr 16 23:38:21 2006  <DIR>  service_logs
    4096  Thu Feb 16 12:26:09 2006  <DIR>  spool
  9945390  Sun Apr 16 23:38:20 2006          syslog.txt
 10026298  Thu Apr  6 12:25:00 2006          syslog.txt.1
 10013564  Thu Apr  6 12:25:00 2006          syslog.txt.2
 10055850  Thu Apr  6 12:25:00 2006          syslog.txt.3
 10049181  Thu Apr  6 12:25:00 2006          syslog.txt.4
    4096  Thu Feb 16 12:29:30 2006  <DIR>  var
    508   Sat Feb 25 13:18:35 2006          wdd.sh.signed
```

次の例では、*logs* ディレクトリの詳細情報のみを示します。

```
WAE# dir logs
size          time of last change          name
-----
4096 Thu Apr  6 12:13:50 2006 <DIR> actona
4096 Mon Mar  6 14:14:41 2006 <DIR> apache
4096 Sun Apr 16 23:36:40 2006 <DIR> emdb
4096 Thu Feb 16 11:51:51 2006 <DIR> export
  92 Wed Apr 12 20:23:20 2006 ftp_export.status
4096 Wed Apr 12 20:23:43 2006 <DIR> rpc_httpd
  0 Wed Apr 12 20:23:41 2006 snmpd.log
4096 Sun Mar 19 18:47:29 2006 <DIR> tfo
```

関連コマンド

[lls](#)

[ls](#)

disable

特権 EXEC コマンドを無効にするには、**disable EXEC** コマンドを使用します。

disable

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン WAAS ソフトウェアの CLI EXEC モードは、システム動作の設定、表示、テスト用に使用します。このコマンドモードは、ユーザと特権の2つのアクセスレベルに分けられます。特権レベル EXEC モードにアクセスするには、ユーザアクセスレベルのプロンプトで **enable EXEC** コマンドを入力し、パスワードの入力のプロンプトが表示されたら特権 EXEC パスワード（スーパーユーザまたは管理者相当のパスワード）を指定します。

```
WAE> enable
```

パスワード:

disable コマンドにより、ユーザレベルの EXEC シェルに入ります（プロンプトが変わります）。

例 次の例では、特権 EXEC モードからユーザレベル EXEC モードに入ります。

```
WAE# disable  
WAE>
```

関連コマンド [enable](#)

disk

WAAS デバイスでディスクを設定するには、**disk EXEC** コマンドを使用します。

disk delete-partitions *diskname*

disk disk-name *diskxx* **replace**

disk insert *diskname*

disk recreate-raid

disk reformat *diskname*

disk scan-errors *diskname*

delete-partitions	指定された論理ディスク ドライブのデータを削除します。このコマンドの実行後は、指定されたディスク ドライブは WAAS ソフトウェアによってブランクとして取り扱われます。そのドライブの以前のデータは、すべてアクセス不能です。
<i>diskname</i>	パーティションを削除するディスクの名前 (disk00、disk01)。 RAID-5 システムの場合、1つの論理ドライブのみがアクティブなので、このオプションは利用できません。
disk-name <i>diskxx</i> replace	RAID-5 アレイで交換できるように、 <i>diskxx</i> という名前の物理ディスク (disk00、disk01 など) をシャットダウンします。
	 (注) このオプションは RAID-5 システムでのみ利用できます。
insert	新しく挿入されたディスクを検出およびマウントするために、SCSI ホストにバスを再スキャンさせます。
	 (注) このオプションは、WAE-612 および WAE-7326 モデルでのみ利用できます。
<i>diskname</i>	挿入するディスクの名前 (disk00、disk01)
recreate-raid	RAID-5 アレイを再構築します。
	 (注) このオプションは RAID-5 システムでのみ利用できます。
reformat	SCSI ディスク ドライブのローレベル再フォーマットを行い、不良セクタをリマップします。
	 注意 このコマンドはデータを損失しないよう十分に注意して使用してください。
	 (注) このオプションは RAID-5 システムでは利用できません。
<i>diskname</i>	再フォーマットするディスクの名前 (disk00、disk01)

scan-errors	エラーがないか SCSI または IDE ディスクをスキャンし、未使用の場合は不良セクターをリマップします。 RAID-5 システムの場合、このコマンドは論理 RAID デバイスにエラーがないかスキャンします。これらのシステムでは、 <i>diskname</i> オプションはありません。
<i>diskname</i>	再フォーマットするディスクの名前 (disk00、disk01)

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン RAID-5 による論理ディスク処理

Redundant Array of Independent Disks-5 (RAID-5; 冗長ディスク アレイ 5) を処理する論理ディスクは、ハードウェア機能として WAAS に実装されています。RAID-5 デバイスは、論理ディスクの容量を増やすため最大 6 つの物理ハードディスク ドライブを備えた単一の論理ディスク ドライブを作成できます (WAE-7341 は 4 つのディスクをサポートし、WAE-7371 は 6 つのディスクをサポートします)。

物理ドライブの 1 つに障害が発生しても (RAID-5 によりドライブが Defunct ステートに移行)、RAID-5 を備えたシステムは操作を継続します。障害が発生したドライブを適切にシャットダウンしたあと、RAID-5 はディスク ハードウェアのホットスワップも可能にします (RAID-5 システムのディスクの取り外しおよび交換手順については、『Cisco Wide Area Application Services Configuration Guide』の Chapter 14 を参照してください)。

RAID-1 による論理ディスク処理

RAID-1 はソフトウェア機能として WAAS に実装されています。RAID-1 WAAS デバイスは信頼性の向上のため 2 つのディスク ドライブを使用できます。RAID-1 はディスク ミラーリングを提供します (データは 2 つ以上のドライブに重複して書き込まれます)。冗長性による信頼性の向上が目的です。RAID-1 の場合、1 つのディスク書き込みを 2 つのディスク ドライブに対して行う必要があるため、ファイル システムの書き込みパフォーマンスに影響を与えます。RAID-1 (ミラーリング) は RAID-1 デバイス上のすべてのファイル システムに使用されます。この設定により、いかなる場合にも信頼性のあるソフトウェアの実行が保証されます。



(注) WAAS ソフトウェアは、Wide Area File Services (WAFS) ファイル システムおよび、Data Redundancy Elimination (DRE) キャッシュの両方に CONTENT ファイル システムを使用します。

WAE-612、WAE-7326、WAE-7341、および WAE-7371 ディスク ドライブのホットスワップ

このリリースの WAAS では、障害のあるディスクの交換およびスケジューリングされたディスク メンテナンスのためにホットスワップ機能がサポートされています。WAE-612 および WAE-7326 では、**disk disk-name diskxx shutdown** 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、スケジューリングされたディスク メンテナンスを行うディスクをシャットダウンします。WAE-7341 お

および WAE-7371 では、**disk disk-name diskxx replace EXEC** コマンドを使用して、ディスクをシャットダウンします (スケジューリングされたディスク メンテナンス手順については、『Cisco Wide Area Application Services Configuration Guide』の Chapter 14 を参照してください)。

ディスクが完全にシャットダウンされるまで待ってから、ディスクを WAE から物理的に取り外してください。RAID の取り外し処理が終了すると、WAAS はディスク障害アラームおよびトラップを生成します。さらに、syslog ERROR メッセージがログに記録されます。

RAID 再構築プロセス中に障害のあるディスクがソフトウェアで削除された場合は、RAID 再構築エラーのアラームが生成されます。RAID 再構築プロセス中にディスクを管理上のシャットダウンにした場合は、代わりに RAID 再構築の中断アラームが生成されます。

RAID の再構築処理中に削除イベントが発生した場合は、RAID 削除処理の正常終了に 1 分ほどかかる場合があります。この処理にかかる実際の時間は、ディスクのサイズによって異なります。

障害の発生したディスクの自動処理

クリティカル ディスク アラームがシステムで 1 つ検出されると、障害ディスクはディスクのホットスワップ機能により自動的に無効にされます。**disk error-handling** が設定されているかどうかに関係なく、障害の発生したディスクは自動的に削除されます。

障害ディスクの交換

WAE-7341 および WAE-7371 モデルでは、ソフトウェアによって自動的にディセーブルされた障害のあるディスクを交換すると、ディスクは自動的にサービス状態に戻ります。WAE-612 および WAE-7326 モデルでは、ソフトウェアによって自動的にディセーブルされた障害のあるディスクを交換する場合、EXEC モードの **disk insert** コマンドを使用するとディスクをサービス状態に戻します。その他のモデルについては、「(config) **disk disk-name command**」を参照してください。

RAID-5 ディスク アレイの再構築

RAID-5 システムの論理ディスク アレイを再構築するには、一連の設定で示すように、EXEC モードの **disk recreate-raid** コマンドを使用します。

```
WAE-7341(config)# disk logical shutdown
WAE-7341# reload
WAE-7341# copy running-config startup-config
```

システムがブートアップするのを待ちます。

```
WAE-7341# disk recreate-raid
WAE-7341(config)# no disk logical shutdown
WAE-7341# reload
WAE-7341# copy running-config startup-config
```

システムがブートしたら、すべてのファイルシステムを再構築するまで約 30 分間待ちます。



注意

RAID-5 ディスク アレイを再構築すると、ドライブ上のすべてのデータが失われます。

EXEC モードで **copy ftp install** を入力してソフトウェアを再インストールします。

300 GB SAS ドライブの場合、RAID アレイを再構築し同期化するのに最大で 5 時間かかります。RAID-5 の同期化がバックグラウンドで実行されている間、システムは完全に機能していますが、パフォーマンスはバックグラウンド操作によって影響を受けます。

ディスク情報

障害ディスクまたは不良ディスクとされているディスクを識別するには、**show disks failed-disk-id EXEC** コマンドを使用します。このリストに示されたシリアル番号を持つディスクを再度挿入しないでください。

**(注)**

このコマンドは、WAE-7341 および WAE-7371 モデルでは利用できません。

SCSI ディスク ドライブの再フォーマット

WAAS デバイスの SCSI ディスク ドライブを再フォーマットするには、**disk reformat EXEC** コマンドを使用します。このコマンドを実行するとき、SCSI ドライブは使用できません。

**注意**

データの損失を防止するため、このコマンドは十分に注意して使用してください。

**(注)**

このコマンドは、SCSI ドライブを装備したシステム (WAE-612) でのみ有効です。このコマンドは、WAAS 4.0.13 の WAE-611 および WAE-7326 システムでは削除されています。

SCSI ドライブを再フォーマットする方法を、次のシナリオで説明します。

1. ファイルシステムをアンマウントし、グローバル コンフィギュレーション モードで **disk disk-name diskxx shutdown** コマンドを使用して RAID-1 アレイからディスクを削除します。

```
WAB611(config)# disk disk-name disk01 shutdown
```

2. ディスクを再フォーマットします。このコマンドが完了すると、ドライブはブランクになります。

```
WAB611# disk reformat disk01
```

3. グローバル コンフィギュレーション モードで **no disk disk-name diskxx shutdown** コマンドを使用してディスクをサービス状態に戻します。

```
WAB611(config)# no disk disk-name disk01 shutdown
```

disk scan errors コマンドを使用するには、**disk reformat** コマンドと同じ手順に従います。

1 つのディスク ドライブのすべてのディスク パーティションの削除および RAID-5 システムの論理ドライブのディスク パーティションの削除

WAAS デバイス上の 1 つのディスク ドライブのすべてのディスク パーティションを削除する、または RAID-5 システムの論理ドライブのディスク パーティションを削除するには、**disk delete-partitions EXEC** コマンドを使用します。

**注意**

disk delete-partitions EXEC コマンドの実行後は、指定されたディスク ドライブは WAAS ソフトウェアによってブランクとして取り扱われます。そのドライブの以前のデータは、すべてアクセス不能です。

このコマンドは、新しいディスク ドライブを追加する場合に、そのドライブが以前に別のオペレーティング システム（たとえば、Microsoft Windows や Linux オペレーティング システム）で使用されていたときに使用します。ディスク上のすべてを消去するか尋ねられたら、次のように「yes」を指定して続けます。

```
WAE# disk delete-partitions disk01
This will erase everything on disk. Are you sure? [no] yes
```



(注)

WAE-7341 または WAE-7371 モデルで **disk delete-partitions EXEC** コマンドを使用する場合、コマンドは論理容量全体を削除します。個々のディスク名オプションは、これらのプラットフォームでは利用できません。

関連コマンド

[\(config\) disk disk-name](#)

[\(config\) disk error-handling](#)

[\(config\) disk logical shutdown](#)

[show disks](#)

dnslookup

ホスト名またはドメイン名を IP アドレスに解決するには、**dnslookup** EXEC コマンドを使用します。

```
dnslookup {hostname | domainname}
```

シンタックスの説明

<i>hostname</i>	ネットワーク上の DNS サーバの名前
<i>domainname</i>	ドメインの名前

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
replication-accelerator
central-manager

例

次の3つの例では、**dnslookup** コマンドを使用して、ホスト名 *myhost* を IP アドレス 172.31.69.11 に解決し、*abd.com* を IP アドレス 192.168.219.25 に解決し、ホスト名として使用されている IP アドレスを 10.0.11.0 に解決する方法を示します。

```
WAE# dnslookup myhost  
official hostname: myhost.abc.com  
address: 172.31.69.11
```

```
WAE# dnslookup abc.com  
official hostname: abc.com  
address: 192.168.219.25
```

```
WAE# dnslookup 10.0.11.0  
official hostname: 10.0.11.0  
address: 10.0.11.0
```

enable

特権 EXEC コマンドにアクセスするには、**enable** EXEC コマンドを使用します。

enable

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン WAAS ソフトウェアの CLI EXEC モードは、システム動作の設定、表示、テスト用に使用します。このコマンドモードは、ユーザレベルと特権レベルの2つのアクセスレベルに分かれています。特権レベル EXEC モードにアクセスするには、ユーザアクセスレベルのプロンプトで **enable** EXEC コマンドを入力し、パスワードの入力のプロンプトが表示されたら特権 EXEC パスワード（スーパーユーザまたは管理者相当のパスワード）を指定します。

TACACS+ にはイネーブルパスワード機能があり、これにより管理者は、管理レベルユーザごとに異なるイネーブルパスワードを定義できます。管理レベルユーザが、管理者または管理者相当のユーザアカウント（特権レベル 15）ではなく、標準レベルのユーザアカウント（特権レベル 0）で WAAS デバイスにログインした場合、特権レベル EXEC モードにアクセスするには、管理者パスワードを入力する必要があります。

WAE> **enable**

パスワード:



(注)

この警告は、WAAS ユーザがログイン認証に TACACS+ を使用している場合でも当てはまります。

disable コマンドで、特権 EXEC モードからユーザ EXEC モードに移行します。

例 次の例は、特権 EXEC モードにアクセスする方法を示します。

WAE> **enable**

WAE#

関連コマンド [disable](#)

[exit](#)

exit

特権レベル EXEC モードを終了させてユーザレベル EXEC モードに戻るには、**exit** コマンドを使用します。

exit

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード すべてのモード

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン このコマンドは、**Ctrl-Z** または **end** コマンドと同じです。ユーザレベル EXEC シェルで発行された **exit** コマンドは、コンソールまたは Telnet セッションを終了します。

例 次の例では、特権レベル EXEC モードを終了してユーザレベル EXEC モードに戻る方法を示します。

```
WAE# exit  
WAE>
```

find-pattern

ファイル内の特定のパターンを検索するには、EXEC モードで **find-pattern** コマンドを使用します。

```
find-pattern {binary reg-express filename | case {binary reg-express filename | count reg-express filename | lineno reg-express filename | match reg-express filename | nomatch reg-express filename | recursive reg-express filename} | count reg-express filename | lineno reg-express filename | match reg-express filename | nomatch reg-express filename | recursive reg-express filename}
```

シンタックスの説明

binary	バイナリ出力を抑制しません。
<i>reg-express</i>	照合する正規表現
<i>filename</i>	ファイル名
case	大文字小文字を区別するパターンを照合します。
count	一致する行数を印刷します。
lineno	出力とともに行番号を印刷します。
match	一致する行を表示します。
nomatch	一致しない行を表示します。
recursive	ディレクトリを反復して検索します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

この EXEC コマンドを使用して、ファイル内の特定の正規表現パターンを検索します。

例

次の例は、大文字と小文字を区別するパターンについてファイルを反復して検索する方法を示します。

```
WAE# find-pattern case recursive admin removed_core
-rw----- 1 admin root 95600640 Oct 12 10:27 /local/local1/core_dir/
core.3.0.0.b5.eh.2796
-rw----- 1 admin root 97054720 Jan 11 11:31 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14086
-rw----- 1 admin root 96845824 Jan 11 11:32 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.14823
-rw----- 1 admin root 101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.15134
-rw----- 1 admin root 96759808 Jan 11 12:59 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.20016
-rw----- 1 admin root 97124352 Jan 11 13:26 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.8095
```

次の例では、あるパターンについてファイルを検索し、一致する行を印刷する方法を示します。

```
WAE# find-pattern match 10 removed_core
Tue Oct 12 10:30:03 UTC 2004
-rw----- 1 admin root 95600640 Oct 12 10:27 /local/local1/core_dir/
core.3.0.0.b5.eh.2796
-rw----- 1 admin root 101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.3.0.0.b131.cnbuild.15134
```

次の例では、あるパターンについてファイルを検索し、一致する行数を印刷する方法を示します。

```
WAE# find-pattern count 10 removed_core
3
```

関連コマンド

[cd](#)

[dir](#)

[lls](#)

[ls](#)

help

command-line interface (CLI; コマンドライン インターフェイス) のオンライン ヘルプを取得するには、**help EXEC** コマンドを使用します。

help

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC およびグローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン コマンド内のどの位置でも疑問符 (?) を入力すればヘルプが得られます。一致するものがない場合、ヘルプ リストは空なので、利用できるオプションが表示されるまで、? の位置を前にずらして入力する必要があります。

次の2つのヘルプ スタイルが用意されています。

- コマンド引数を入力する準備ができている場合、完全ヘルプを使って (たとえば **show ?**)、可能な引数を表示させることができます。
- コマンドを簡略化して入力し、どんな引数が入力に一致するか知りたい場合 (たとえば、**show stat?**)、部分ヘルプを使用します。

例 次の例は、**help EXEC** コマンドの出力を示します。

```
WAE# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.
```

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered.

install

新しいソフトウェア イメージ (WAAS ソフトウェアなど) を WAAS デバイス上のフラッシュにインストールするには、**install EXEC** コマンドを使用します。

```
install imagefilename
```

シンタックスの説明

<i>imagefilename</i>	インストールする <i>.bin</i> ファイルの名前
----------------------	------------------------------

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

install コマンドは、システム イメージをフラッシュ メモリにロードし、オプションのソフトウェアのコンポーネントをソフトウェア ファイル システム (swfs) パーティションにコピーします。



(注)

オプションのソフトウェアを格納するシステム イメージをインストールする場合は、SWFS パーティションが `disk00` にマウントされていることを確認してください。

システム イメージをインストールするには、イメージ ファイルを `SYSFS` ディレクトリ `local1` または `local2` にコピーします。**install** コマンドを実行する前に、現在の作業ディレクトリをシステム イメージのあるディレクトリに変更します。**install** コマンドを実行すると、イメージ ファイルは拡張されます。拡張されたファイルは、WAAS デバイス上の既存のファイルを上書きします。システム イメージをリロードすると、新たにインストールされたバージョンが適用されます。



(注)

install コマンドは `.pax` ファイルを受け付けません。ファイルのタイプは `.bin` (たとえば、`cache-sw.bin`) である必要があります。また、インストールするリリースが新しいシステム イメージを必要としない場合は、フラッシュ メモリに書き込む必要がないこともあります。新しいバージョンに変更が加えられており、そのために、新しいシステム イメージをインストールする必要がある場合は、**install** コマンドによって、フラッシュ メモリへの書き込みが実行される場合があります。

例

次の例は、`wae511-cache-300.bin` ファイルに格納されたシステム イメージをロードします。

```
WAE# install wae511-cache-300.bin
```

関連コマンド

[copy disk](#)

[reload](#)

less

LESS アプリケーションを使用するファイルを表示するには、**less EXEC** コマンドを使用します。

```
less file_name
```

シンタックスの説明

<i>file_name</i>	表示するファイルの名前
------------------	-------------

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

LESS は、テキスト ファイルを一度に 1 ページずつ表示するアプリケーションです。LESS を使用してファイルのコンテンツを表示できます。ただし、編集はできません。LESS は、**type** などの従来のテキスト ファイル ビューア アプリケーションと比較した場合、追加機能を備えています。追加機能は次のとおりです。

- 後方移動 — 表示されたテキストの後方に移動できます。後方移動には、**k**、**Ctrl-k**、**y**、**Ctrl-y** を使用します。詳細は LESS コマンドの要約を参照してください。要約を表示するには、LESS でファイルを表示中に **h** または **H** を押します。
- 検索および強調表示 — 表示しているファイル内のテキストを検索できます。前方と後方に検索ができます。LESS では検索に一致するテキストを強調表示して、一致している位置を見つけやすくします。
- 複数ファイルのサポート — LESS では、異なるファイル間で切り替えができ、各ファイルでの位置を記憶しています。処理している全ファイルにまたがって検索を行うこともできます。

例

次の例は、LESS アプリケーションを使用して、*syslog.txt* ファイルのコンテンツを表示する方法を示しています。

```
WAE# less syslog.txt
```

lls

ディレクトリ名の長いリストを表示するには、**lls EXEC** コマンドを使用します。

```
lls [directory]
```

シンタックスの説明

directory (オプション) 長いファイルリストを表示するディレクトリの名前

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

このコマンドは、現在の作業ディレクトリにストアされているファイルとサブディレクトリに関する詳細な情報（サイズ、作成の日付時刻、SYSFS 名、ファイルのロング ネームなど）を提供します。この情報は、**dir** コマンドでも表示できます。

例

次の例は、現在のディレクトリ内のすべてのファイルの詳細リストを提供します。

```
WAB# lls
size          time of last change          name
-----
    4096  Fri Feb 24 14:40:00 2006 <DIR>  actona
    4096  Tue Mar 28 14:42:44 2006 <DIR>  core_dir
    4096  Wed Apr 12 20:23:10 2006 <DIR>  crash
    4506  Tue Apr 11 13:52:45 2006          dbupgrade.log
    4096  Tue Apr  4 22:50:11 2006 <DIR>  downgrade
    4096  Sun Apr 16 09:01:56 2006 <DIR>  errorlog
    4096  Wed Apr 12 20:23:41 2006 <DIR>  logs
   16384  Thu Feb 16 12:25:29 2006 <DIR>  lost+found
    4096  Wed Apr 12 03:26:02 2006 <DIR>  sa
   24576  Sun Apr 16 23:54:30 2006 <DIR>  service_logs
    4096  Thu Feb 16 12:26:09 2006 <DIR>  spool
   9951236  Sun Apr 16 23:54:20 2006          syslog.txt
  10026298  Thu Apr  6 12:25:00 2006          syslog.txt.1
  10013564  Thu Apr  6 12:25:00 2006          syslog.txt.2
  10055850  Thu Apr  6 12:25:00 2006          syslog.txt.3
  10049181  Thu Apr  6 12:25:00 2006          syslog.txt.4
    4096  Thu Feb 16 12:29:30 2006 <DIR>  var
    508   Sat Feb 25 13:18:35 2006          wdd.sh.signed
```

関連コマンド

[dir](#)
[lls](#)
[ls](#)

ls

ディレクトリ内のファイル名やサブディレクトリ名のリストを表示するには、**ls** EXEC コマンドを使用します。

```
ls [directory]
```

シンタックスの説明

<i>directory</i>	(オプション) ファイルリストを表示するディレクトリの名前
------------------	-------------------------------

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

特定のディレクトリ内のファイル名やサブディレクトリをリストするには、**ls *directory*** コマンドを使用します。

現在の作業ディレクトリのファイル名やサブディレクトリをリストするには、**ls** コマンドを使用します。

現在の作業ディレクトリを表示するには、**pwd** コマンドを使用します。

例

次の例は、ルートディレクトリ内でリストされたファイルとサブディレクトリを示します。

```
WAE# ls
actona
core_dir
crash
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
syslog.txt.2
syslog.txt.3
syslog.txt.4
var
wdd.sh.signed
```

関連コマンド

[dir](#)
[lls](#)
[pwd](#)

mkdir

ディレクトリを作成するには、**mkdir** EXEC コマンドを使用します。

```
mkdir directory
```

シンタックスの説明

<i>directory</i>	作成するディレクトリの名前
------------------	---------------

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

この EXEC コマンドを使用して、WAAS ファイル システムに新しいディレクトリまたはサブディレクトリを作成します。

例

次の例では、新しいディレクトリ *oldpaxfiles* を作成する方法を示します。

```
WAE# mkdir /oldpaxfiles
```

関連コマンド

[cpfile](#)

[dir](#)

[lls](#)

[ls](#)

[pwd](#)

[rename](#)

[rmdir](#)

mkfile

新しいファイルを作成するには、**mkfile** EXEC コマンドを使用します。

mkfile *filename*

シンタックスの説明

<i>filename</i>	作成するファイルの名前
-----------------	-------------

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドを使用して、WAAS デバイスの任意のディレクトリに新しいファイルを作成します。

例

次の例では、ルート ディレクトリに新しいファイル *traceinfo* を作成する方法を示します。

```
WAE# mkfile traceinfo
```

関連コマンド

[cpfile](#)
[dir](#)
[lls](#)
[ls](#)
[mkdir](#)
[pwd](#)
[rename](#)

ntpdate

NTP サーバを使用して WAAS デバイスのソフトウェア クロック（日付時刻）を設定するには、**ntpdate** EXEC コマンドを使用します。

```
ntpdate {hostname | ip-address} [key {authentication-key}]
```

シンタックスの説明

<i>hostname</i>	NTP ホスト名
<i>ip-address</i>	NTP サーバ IP アドレス
key	NTP サーバによる認証を使用するには、この引数を追加します。
<i>authentication-key</i>	NTP サーバ認証と併せて使用する認証キー ストリング値は、0 ~ 4294967295 の範囲で設定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

NTP を使用して現在の時刻を検出し、WAAS デバイスの現在時刻を一致するように設定します。時刻は、リロード後元に戻す予定の場合は、**clock save** コマンドを使用してハードウェア クロックに保存する必要があります。

例

次の例では、NTP サーバを使用して WAAS デバイスのソフトウェア クロックを設定する方法を示します。

```
WAE# ntpdate 10.11.23.40
```

関連コマンド

clock
(config) clock
(config) ntp
show clock
show ntp

ping

ネットワーク上の基本ネットワーク接続を診断する目的でエコー パケットを送信するには、**ping** EXEC コマンドを使用します。

```
ping {hostname | ip-address}
```

シンタックスの説明

<i>hostname</i>	PING を実行するシステムのホスト名
<i>ip-address</i>	PING を実行するシステムの IP アドレス

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

引数 *hostname* を指定してこのコマンドを使用するには、WAAS デバイスに DNS 機能が設定されていることを確認してください。応答のないホストを強制的にタイムアウトする場合、またはループサイクルを解除する場合は、**Ctrl-C** を押します。

例

次の例は、アドレスが 172.19.131.189 のマシンにエコー パケットを送信して、ネットワーク上でのそのアベイラビリティを確認する方法を示します。

```
WAE# ping 172.19.131.189
PING 172.19.131.189 (172.19.131.189) from 10.1.1.21 : 56(84) bytes of
data.
64 bytes from 172.19.131.189: icmp_seq=0 ttl=249 time=613 usec
64 bytes from 172.19.131.189: icmp_seq=1 ttl=249 time=485 usec
64 bytes from 172.19.131.189: icmp_seq=2 ttl=249 time=494 usec
64 bytes from 172.19.131.189: icmp_seq=3 ttl=249 time=510 usec
64 bytes from 172.19.131.189: icmp_seq=4 ttl=249 time=493 usec

--- 172.19.131.189 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.485/0.519/0.613/0.047 ms
WAE#
```


pwd

WAAS デバイスの現在の作業ディレクトリを表示するには、**pwd** EXEC コマンドを使用します。

pwd

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン このコマンドを使用して、WAAS デバイスの現在の作業ディレクトリを表示させます。

例 次の例は、現在の作業ディレクトリを表示する方法を示します。

```
WAE# pwd  
/local1
```

関連コマンド [cd](#)
[dir](#)
[lls](#)
[ls](#)

reload

WAAS デバイスを停止してコールドリスタートを実行するには、**reload EXEC** コマンドを使用します。

```
reload [force]
```

シンタックスの説明

force (オプション) 追加要求なしでリブートを強制実行させます。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

WAAS デバイスをリブートするには、**reload** コマンドを使用します。フラッシュメモリに設定が保存されていない場合は、再起動時に設定パラメータの入力を要求されます。開いている接続がある場合は、このコマンドを発行するとドロップされ、ファイルシステムは再起動時に再フォーマットされます。

例

次の例は、WAAS デバイスの動作を停止させ、フラッシュメモリに保存されている設定でリブートする方法を示します。プロセス中に確認のプロンプトは出ません。

```
WAE# reload force
```

関連コマンド

[write](#)

rename

WAAS デバイスのファイルの名前を変更するには、**rename EXEC** コマンドを使用します。

```
rename oldfilename newfilename
```

シンタックスの説明

<i>oldfilename</i>	元のファイル名
<i>newfilename</i>	新しいファイル名

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

このコマンドを使用して、ファイルのコピーを作成しないで **SYSFS** ファイルの名前を変更します。

例

次の例では、ファイル名を *errlog.txt* から *old_errlog.txt* に変更する方法を示します。

```
WAE# rename errlog.txt old_errlog.txt
```

関連コマンド

[cpfile](#)

restore

デバイスを工場出荷時のデフォルト状態に戻し、ディスクとフラッシュ メモリからユーザ データを削除するには、**restore EXEC** コマンドを使用します。

```
restore {factory-default [preserve basic-config] | rollback}
```

シンタックスの説明

factory-default	デバイス コンフィギュレーションおよびデータを工場出荷時のデフォルト状態にリセットします。
preserve	(オプション) デバイスの設定とデータの一部を保存します。
basic-config	(オプション) 基本ネットワーク コンフィギュレーションを選択します。
rollback	直前に機能していたソフトウェアおよびデバイス コンフィギュレーションに設定をロールバックします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドを使用して、特定のタイムスタンプ評価データを保存しながら、ディスク上およびフラッシュ メモリ内のデータを工場出荷時のデフォルトに戻したり、直前に機能していたデータおよびデバイス コンフィギュレーションに設定をロールバックします。

このコマンドは、デバイス上にある既存のコンテンツをすべて消去します。ただし、ネットワーク コンフィギュレーションは保存されており、リブート後、Telnet および Secure Shell (SSH; セキュア シェル) セッションを介してアクセス可能です。

Central Manager データベースのバックアップ

プライマリ WAAS Central Manager で **restore factory-default** コマンドを使用する、またはプライマリからスタンバイ WAAS Central Manager に切り替える前に必ず、WAAS Central Manager データベースをバックアップし、バックアップ ファイルを WAAS Central Manager から離れた安全な場所にコピーしてください。WAAS Central Manager の動作を停止してから、バックアップおよび復元コマンドを始める必要があります。



注意

このコマンドは、フラッシュ イメージに保存されているユーザ指定の設定を消去し、ディスクやユーザ定義のディスク パーティション上のデータ、および Central Manager データベース全体を削除します。削除されるユーザ定義のディスク パーティションには、SYSFS、WAAS、および PRINTSPOOLFS パーティションが含まれます。削除される設定には、デバイスの起動設定が含まれます。

WAAS Central Manager データベースを削除することによって、WAAS ネットワーク全体のすべての設定記録が削除されます。有効なバックアップ ファイルまたはスタンバイ WAAS Central Manager がない場合、以前に設定したデータはすべて失われるので、すべての WAE を WAAS Central Manager に登録する必要があります。

プライマリ Central Manager を再設定しながらスタンバイ WAAS Central Manager を使用してデータベースを保存した場合は、以前のプライマリを新しいスタンバイ WAAS Central Manager として登録するだけで済みます。

プライマリ WAAS Central Manager を設定しながらバックアップ ファイルを作成している場合は、バックアップ ファイルをこの新たに再設定された WAAS Central Manager にコピーできます。

設定のロールバック

restore rollback コマンドを使用して、WAAS デバイスのソフトウェアと設定を以前のバージョンにロールバックできます。ソフトウェアのロールバックは、通常、新たにインストールしたバージョンの WAAS ソフトウェアが正常に機能しない場合だけです。

restore rollback コマンドは最後に保存された WAAS.bin イメージをシステム ディスクにインストールします。ソフトウェア インストール中に WAAS.bin イメージが作成され、システム ディスクに保存されます。WAAS デバイスに保存されたバージョンがない場合は、ソフトウェアはロールバックされません。



(注)

WAFS から WAAS への移行はサポートされていますが、WAAS から WAFS へのロールバックはサポートされていません。

例

次の 2 つの例は、**restore factory-default** および **restore factory-default preserve basic-config** コマンドを使用する方法を示します。設定パラメータとデータが失われるため、元に戻す操作の前にプロンプトが示され、処理を進めて良いか確認を取ります。

```
WAE# restore factory-default
This command will wipe out all of data on the disks
and wipe out WAAS CLI configurations you have ever made.
If the box is in evaluation period of certain product,
the evaluation process will not be affected though.
```

```
It is highly recommended that you stop all active services
before this command is run.
```

```
Are you sure you want to go ahead?[yes/no]
```

```
WAE# restore factory-default preserve basic-config
This command will wipe out all of data on the disks
and all of WAAS CLI configurations except basic network
configurations for keeping the device online.
The to-be-preserved configurations are network interfaces,
default gateway, domain name, name server and hostname.
If the box is in evaluation period of certain product,
the evaluation process will not be affected.
```

```
It is highly recommended that you stop all active services
before this command is run.
```

```
Are you sure you want to go ahead?[yes/no]
```



(注)

この時点、またはあとで **command-line interface (CLI)** (コマンドライン インターフェイス) の入力を通じて、基本の設定パラメータ (IP アドレス、ホスト名、ネーム サーバなど) を入力できます。

次の例では、**restore** コマンドの使用後 **show disks details** コマンドを入力し、**restore** コマンドによって、データがパーティション化されたファイルシステム、SYSFS、WAAS、および PRINTSPOOLFS から削除されたことを確認します。

```
WAE# show disks details
```

```
Physical disk information:
```

```
disk00: Normal                (h00 c00 i00 100 - DAS)    140011MB (136.7GB)
disk01: Normal                (h00 c00 i01 100 - DAS)    140011MB (136.7GB)
```

```
Mounted filesystems:
```

MOUNT POINT	TYPE	DEVICE	SIZE	INUSE	FREE	USE%
/	root	/dev/root	35MB	30MB	5MB	85%
/swstore	internal	/dev/md1	991MB	333MB	658MB	33%
/state	internal	/dev/md2	3967MB	83MB	3884MB	2%
/disk00-04	CONTENT	/dev/md4	122764MB	33MB	122731MB	0%
/local/local1	SYSFS	/dev/md5	3967MB	271MB	3696MB	6%
.../local1/spool	PRINTSPOOL	/dev/md6	991MB	16MB	975MB	1%
/sw	internal	/dev/md0	991MB	424MB	567MB	42%

```
Software RAID devices:
```

DEVICE NAME	TYPE	STATUS	PHYSICAL DEVICES AND STATUS
/dev/md0	RAID-1	NORMAL OPERATION	disk00/00 [GOOD] disk01/00 [GOOD]
/dev/md1	RAID-1	NORMAL OPERATION	disk00/01 [GOOD] disk01/01 [GOOD]
/dev/md2	RAID-1	NORMAL OPERATION	disk00/02 [GOOD] disk01/02 [GOOD]
/dev/md3	RAID-1	NORMAL OPERATION	disk00/03 [GOOD] disk01/03 [GOOD]
/dev/md4	RAID-1	NORMAL OPERATION	disk00/04 [GOOD] disk01/04 [GOOD]
/dev/md5	RAID-1	NORMAL OPERATION	disk00/05 [GOOD] disk01/05 [GOOD]
/dev/md6	RAID-1	NORMAL OPERATION	disk00/06 [GOOD] disk01/06 [GOOD]

```
Currently content-fileSYSTEMS RAID level is not configured to change.
```

次の例では、WAAS ソフトウェアをアップグレードまたは古いバージョンに戻す方法を示します。最初の例では、バージョン Y のソフトウェアがインストールされています (**copy** コマンドを使用) が、管理者がまだ切り替えていないので、現在のバージョンはまだ X のままです。このあと、システムはリロードされ (**reload** コマンドを使用)、バージョン Y が現在稼働するバージョンであることを確認します。

次の例では、ソフトウェアがバージョン X にロールバックされ (**restore rollback** コマンドを使用)、ソフトウェアが再度リロードされます。

```
WAE# copy ftp install server path waas.versionY.bin
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.0.0 (build b340 Mar 25 2
006)
Version: fe611-4.0.0.340

Compiled 17:26:17 Mar 25 2006 by cnbuild

System was restarted on Mon Mar 27 15:25:02 2006.
The system has been up for 3 days, 21 hours, 9 minutes, 17 seconds.

WAE# show version last
  Nothing is displayed.
WAE# show version pending
WAAS 4.0.1 Version Y
WAE# reload
..... reloading .....
WAE# show version
Cisco Wide Area Application Services Software (WAAS)
...
WAE# restore rollback
WAE# reload
..... reloading .....
```

フラッシュ メモリの設定は **restore** コマンドの実行後失われているため、**show startup-config** コマンドでは、フラッシュ メモリのデータは何も返されません。**show running-config** コマンドは、デフォルトの実行コンフィギュレーションを返します。

関連コマンド

[reload](#)

[show disks](#)

[show running-config](#)

[show startup-config](#)

[show version](#)

rmdir

WAAS デバイスのディレクトリを削除するには、**rmdir** EXEC コマンドを使用します。

rmdir *directory*

シンタックスの説明

<i>directory</i>	削除するディレクトリの名前
------------------	---------------

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドを使用して WAAS ファイルシステムからディレクトリを削除します。**rmdir** コマンドは空のディレクトリしか削除できません。

例

次の例は、*local1* ディレクトリから *oldfiles* ディレクトリを削除する方法を示します。

```
WAE# rmdir /local1/oldfiles
```

関連コマンド

[cpfile](#)
[dir](#)
[lls](#)
[ls](#)
[mkdir](#)
[pwd](#)
[rename](#)

scp

ネットワーク ホスト間でファイルをコピーするには、**scp** コマンドを使用します。

```
scp [1][2][4][6][B][C][p][q][r][v] [c cipher] [F config-file] [i id-file] [l limit]
[o ssh_option] [P port] [S program] [[user@] host : file] [...] [[user-n@] host-n : file-n]
```

シンタックスの説明

1	(オプション) このコマンドでプロトコル 1 を強制的に使用します。
2	(オプション) このコマンドでプロトコル 2 を強制的に使用します。
4	(オプション) このコマンドで IPv4 アドレスのみを強制的に使用します。
6	(オプション) このコマンドで IPv6 アドレスのみを強制的に使用します。
B	(オプション) バッチ モードを指定します。このモードでは、 scp コマンドはパスワードまたはパスフレーズの入力を要求しません。
C	(オプション) 圧縮をイネーブルにします。 scp コマンドはこのオプションを ssh コマンドに渡し、圧縮をイネーブルにします。
p	(オプション) ソース ファイルから、修正時刻、アクセス時刻、およびモードを保存します。
q	(オプション) 進捗情報の表示をディセーブルにします。
r	(オプション) ディレクトリとそのコンテンツを繰り返しコピーします。
v	(オプション) 詳細なモードを指定します。 scp コマンドと ssh コマンドにその進行についてのデバッグ メッセージをプリントさせます。このオプションは、接続、認証、設定問題のトラブルシューティングに役立ちます。
c	(オプション) コピー元のデータの暗号化に使用する暗号を指定します。 scp コマンドはこのオプションを ssh コマンドにそのまま渡します。
<i>cipher</i>	コピー元のデータの暗号化に使用する暗号
F	(オプション) SSH の別のユーザごとの設定ファイルを指定します。 scp コマンドはこのオプションを ssh コマンドにそのまま渡します。
<i>config-file</i>	設定ファイルの名前
i	(オプション) RSA 認証の秘密鍵が格納されているファイルを指定します。 scp コマンドはこの情報を ssh コマンドにそのまま渡します。
<i>id-file</i>	RSA 認証の秘密鍵が格納されているファイルの名前
l	(オプション) 帯域幅の使用を制限します。
<i>limit</i>	ファイルのコピーに使用する帯域幅 (kbps)
o	(オプション) オプションを ssh_config5 で使用されるフォーマットで ssh コマンドに渡します。
<i>ssh_option</i>	利用できるオプションの詳細は、 ssh コマンドを参照してください。
P	(オプション) リモート ホスト上の接続先ポートを指定します。
<i>port</i>	リモート ホスト上の接続先ポート
S	(オプション) 暗号化接続に使用するプログラムを指定します。
<i>program</i>	暗号化接続に使用するプログラムの名前
<i>user</i>	(オプション) ユーザ名
<i>host</i>	(オプション) ホスト名
<i>file</i>	(オプション) コピーするファイルの名前

コマンドモード

EXEC

■ scp

デバイス モード

- application-accelerator
- replication-accelerator
- central-manager

使用上のガイドライン **scp** コマンドはホスト間のデータ転送に SSH を使用します。
このコマンドは、認証に必要な場合、パスワードまたはパスフレーズの入力を要求します。

関連コマンド [ssh](#)

script

シスコが提供するスクリプトを実行するか、エラーがないかスクリプトを確認するには、**script EXEC** コマンドを使用します。

```
script {check | execute} file_name
```

シンタックスの説明

check	スクリプトの有効性をチェックします。
execute	スクリプトを実行します。スクリプト ファイルは、現在のディレクトリの SYSFS ファイルである必要があります。
<i>file_name</i>	スクリプト ファイルの名前

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

script EXEC コマンドはスクリプト ユーティリティを開き、これにより、シスコが提供するスクリプトを実行するか、このスクリプト内のエラーを確認できます。スクリプト ユーティリティは、実行するスクリプトがユーザからの入力が必要とする場合は、ユーザからの標準端末入力を読み込みます。



(注) スクリプト ユーティリティは、シスコが提供するスクリプトだけを実行するように設計されています。シスコのシングルチャージがないスクリプト ファイルや、破損または変更されたスクリプト ファイルは実行できません。

例

次の例は、スクリプト ファイル *test_script.pl* にエラーがないかチェックする方法を示します。

```
WAE# script check test_script.pl
```

setup

WAAS デバイスの基本構成設定（一般設定、デバイス ネットワーク コンフィギュレーション、およびディスク コンフィギュレーション）を設定する、または WAAS ソフトウェアへのアップグレード後に基本設定を完了するには、**setup EXEC** コマンドを使用します。

setup

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン **setup** コマンドの使用方法は、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。

例 次の例は、WAAS ソフトウェアを実行している WAAS デバイスで、**setup EXEC** コマンドを実行したときの、ウィザードの最初の画面を示します。

```
WAE# setup
Please choose an interface to configure from the following list:
1: GigabitEthernet 1/0
2: GigabitEthernet 2/0

Enter choice:
.
.
.
Press the ESC key at any time to quit this session
```

show aaa accounting

WAAS デバイスの Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントティング) アカウントティング設定情報を表示するには、**show aaa accounting** EXEC コマンドを使用します。

show aaa accounting

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン この EXEC コマンドを使用し、次の AAA アカウントティング タイプの設定情報を表示します。

- Exec シェル
- コマンド (標準ユーザおよびスーパーユーザ)
- システム

例 表 3-1 では、**show aaa accounting** 出力のフィールドについて説明します。

表 3-1 show aaa accounting コマンドのフィールドの説明

フィールド	説明
Accounting Type	次のユーザ アカウント タイプの AAA アカウントティング設定を表示します。 Exec コマンド レベル 0 コマンド レベル 15 システム
Record Event(s)	アカウントティング サーバに送信される AAA アカウントティング通知の設定を表示します。
stop-only	WAAS デバイスは、指定されたアクティビティまたはイベントの終了時に、停止レコード アカウントティング通知を TACACS+ アカウントティング サーバへ送信します。
start-stop	WAAS デバイスは、イベントの開始時に開始レコード アカウントティング通知を、イベントの終了時に停止レコード アカウントティング通知を TACACS+ アカウントティング サーバへ送信します。 アカウントティング開始記録はバックグラウンドで送信されます。TACACS+ アカウントティング サーバがアカウントティング開始レコードを確認応答したかどうかに関係なく、要求されたユーザ サービスが開始されます。

表 3-1 show aaa accounting コマンドのフィールドの説明 (続き)

フィールド	説明
wait-start	WAAS デバイスは、開始および停止のアカウントティング レコード両方を TACACS+ アカウントティング サーバに送信します。ただし、要求されたユーザ サービスは、アカウントティング開始レコードが確認応答されるまで開始されません。アカウントティング停止レコードも送信されます。
disabled	指定されたイベントでは、アカウントティングはディセーブルです。
Protocol	設定されたアカウントティング プロトコルを表示します。

関連コマンド[cd](#)

show adapter

EndPoint Mapper (EPM) アダプタのステータスと設定を表示するには、**show adapter EXEC** コマンドを使用します。

show adapter epm

シンタックスの説明

epm Microsoft PortMapper アダプタを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

このコマンドは、WAE application-accelerator アプライアンスで有効です。Central Manager (CM) アプライアンスでは有効ではありません。

例

表 3-2 では、**show adapter epm** 出力のフィールドについて説明します。

表 3-2 show adapter epm コマンドのフィールドの説明

フィールド	説明
EPM (MS-PortMapper) adapter is enabled.	EPM アダプタの設定ステータス
EPM (MS-PortMapper) adapter is disabled.	

関連コマンド

[\(config\) adapter](#)

[show statistics epm](#)

show alarms

WAAS デバイスで各種のアラーム、そのステータス、および履歴を表示するには、**show alarms EXEC** コマンドを使用します。

```
show alarms [critical [detail [support]] | detail [support] | history [start_num [end_num [detail
[support]]] | critical [start_num [end_num [detail [support]]]] | detail [support] | major [start_num
[end_num [detail [support]]]] | minor [start_num [end_num [detail [support]]]] | detail [support]
| major [detail [support]] | minor [detail [support]] | status]
```

シンタックスの説明

critical	(オプション) クリティカルアラーム情報を表示します。
detail	(オプション) 各アラームの詳細情報を表示します。
support	(オプション) 各アラームの追加情報を表示します。
history	(オプション) さまざまなアラームの履歴に関する情報を表示します。
start_num	(オプション) アラーム履歴の最初に出現するアラーム番号
end_num	(オプション) アラーム履歴の最後に出現するアラーム番号
major	(オプション) メジャーアラームに関する情報を表示します。
minor	(オプション) マイナーアラームに関する情報を表示します。
status	(オプション) さまざまなアラームのステータスとアラーム オーバーロード設定を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

WAAS ソフトウェアの Node Health Manager により、WAAS アプリケーションはアラームを発生させ、エラーまたは注意を要する状態であることを教えます。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、WAAS デバイスで監視されるアプリケーション、サービスおよびリソース (ディスク ドライブなど) のヘルスおよびアラーム情報を集約します。たとえば、この機能により、WAE が大量のアラームを受信しているかどうかを判別するメカニズムが提供されます。このようなアラームは「WAAS ソフトウェア アラーム」と呼ばれます。

WAAS ソフトウェアは、SNMP トラップを生成することにより、SNMP を使ってエラー状態を通知します。次の WAAS アプリケーションは、WAAS 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)
- System Monitor (sysmon) (ディスク障害用)

WAAS ソフトウェアには次の 3 つのアラーム レベルがあります。

- クリティカル — WAE を介して既存のトラフィックに影響を与えるアラームで、致命的とみなされる (WAE は回復して、トラフィックを処理し続けることができません)。

- メジャー — 主要なサービス（たとえば、キャッシュ サービス）が損傷したか失われたことを示すアラーム。このサービスを元に戻すには緊急の対策が必要です。ただし、他のノードコンポーネントは完全に機能するため、既存のサービスに対する影響は最小限です。
- マイナー — サービスに影響を与えない状況が発生しているが、重大な障害が発生しないように処置が必要なことを示すアラーム。

snmp-server enable traps alarms 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、アラームを設定できます。

show alarms critical EXEC コマンドを使用すると、WAAS ソフトウェア アプリケーションによって生成されている現在のクリティカル アラームを表示できます。**show alarms critical detail EXEC** コマンドを使用すると、生成されている各クリティカル アラームの追加の詳細情報を表示できます。アラームが発生した状況に関する説明と問題の原因を検出する方法は、**show alarms critical detail support EXEC** コマンドを使用すると、表示されます。同様に、メジャーおよびマイナー アラームの詳細情報も、**show alarms major** および **show alarms minor EXEC** コマンドを使用して表示できます。

ソフトウェアが最後にリロードされてから WAAS デバイス上で WAAS ソフトウェアによって生成され、クリアされた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。WAAS ソフトウェアは、直近の 100 個のアラーム生成およびクリア イベントだけを保持できます。

現在のアラームのステータス、WAAS デバイスのアラーム過負荷状態およびアラーム過負荷設定を表示するには、**show alarms status EXEC** コマンドを使用します。

例

表 3-3 では、**show alarms history** 出力のフィールドについて説明します。

表 3-3 show alarms history コマンドのフィールドの説明

フィールド	説明
Op	アラームの動作ステータス。値は、R-Raised または C-Cleared です。
Sev	アラームの重大度。値は、Cr-Critical、Ma-Major、または Mi-Minor です。
Alarm ID	アラームの原因となるイベント タイプ。たとえば、wafs_edge_down、wafs_core_down です。
Module/Submodule	影響を受けたソフトウェア モジュール。たとえば、wafs
Instance	このアラームが関連付けられたオブジェクト。たとえば、Alarm ID disk_failed のあるアラーム イベントの場合、インスタンスは障害の発生したディスクの名前になります。Instance フィールドでは値を事前に定義しません。これはアプリケーション固有です。

表 3-4 では、**show alarms status** 出力のフィールドについて説明します。

表 3-4 show alarms status コマンドのフィールドの説明

フィールド	説明
Critical Alarms	クリティカル アラーム数
Major Alarms	メジャー アラーム数
Minor Alarms	マイナー アラーム数
Overall Alarm Status	アラーム ステータスを集約します。
Device is NOT in alarm overload state.	デバイス アラーム過負荷状態のステータス

表 3-4 show alarms status コマンドのフィールドの説明 (続き)

フィールド	説明
Device enters alarm overload state @ 999 alarms/sec.	デバイスがアラーム過負荷状態になる場合の秒単位のアラーム数のしきい値
Device exits alarm overload state @ 99 alarms/sec.	デバイスがアラーム過負荷状態を終了する場合の秒単位のアラーム数のしきい値
Overload detection is ENABLED.	デバイス上で過負荷状態の検出がイネーブルであるかどうかのステータス

関連コマンド

(config) alarm overload-detect

(config) snmp-server enable traps

show arp

WAAS デバイスの ARP テーブルを表示するには、**show arp EXEC** コマンドを使用します。

show arp

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン Address Resolution Protocol (ARP; アドレス解決プロトコル) のインターネットからイーサネットへのアドレス変換テーブルを表示するには、**show arp** コマンドを使用します。フラグがない場合は、ホスト名の現在の ARP エントリが表示されます。

例 表 3-5 では、**show arp** 出力のフィールドについて説明します。

表 3-5 show arp コマンドのフィールドの説明

フィールド	説明
Protocol	プロトコルのタイプ
Address	ホスト名の IP アドレス
Flags	現在の ARP フラグ ステータス
Hardware Addr	コロンの区切られた 6 個の 16 進バイトで示されるハードウェア IP アドレス
Type	ワイドエリア ネットワークのタイプ
Interface	インターフェイスの名前およびスロット / ポート情報

show authentication

WAAS デバイスの認証設定を表示するには、**show authentication EXEC** コマンドを使用します。

```
show authentication {user | content-request}
```

シンタックスの説明

user	システムにログインするユーザの認証設定を表示します。
content-request	切断モードでのコンテンツ要求認証の設定情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

WAAS デバイスが、NTLM、LDAP、TACACS+、RADIUS、または Windows ドメイン サーバを介してユーザを認証すると、認証の記録がローカルに保存されます。そのエントリが保存されている限り、同一ユーザによる制限されたインターネット コンテンツへのその後のアクセスで、再度サーバをルックアップする必要はありません。ユーザ ログインに対するローカルおよびリモートの認証設定を表示するには、**show authentication user EXEC** コマンドを使用します。

切断モードでコンテンツ要求認証の設定情報を表示するには、**show authentication content-request EXEC** コマンドを使用します。

例

表 3-6 では、**show authentication user** 出力のフィールドについて説明します。

表 3-6 show authentication user コマンドのフィールドの説明

フィールド	説明
Login Authentication: Console/Telnet/Ftp/SSH Session	ログイン認証に対してイネーブルになる認証サービスとサービスの設定ステータスを表示します。
Windows domain	認証サービスの動作ステータス。値は enabled または disabled です。
RADIUS	
TACACS+	各認証サービスのプライオリティ ステータス。値は、 primary 、 secondary 、または tertiary です。
Local	
Configuration Authentication: Console/Telnet/Ftp/SSH Session	設定認証に対してイネーブルになる認証サービスとサービスの設定ステータスを表示します。
Windows domain	認証サービスの動作ステータス。値は enabled または disabled です。
RADIUS	
TACACS+	各認証サービスのプライオリティ ステータス。値は、 primary 、 secondary 、または tertiary です。
Local	

表 3-7 では、**show authentication content-request** 出力のフィールドについて説明します。

表 3-7 show authentication content-request コマンドのフィールドの説明

フィールド	説明
The content request authentication in disconnected mode is XXX.	切断モードでのコンテンツ要求認証の動作ステータス。値は enabled または disabled です。

関連コマンド

[\(config\) authentication](#)

[clear](#)

[show statistics authentication](#)

show auto-register

WAE の自動登録機能のステータスを表示するには、**show auto-register EXEC** コマンドを使用します。

show auto-register

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator

例 表 3-8 に、**show auto-register** 表示の出力について説明します。

表 3-8 show auto-register コマンドのフィールドの説明

フィールド	説明
Auto registration is enabled.	自動登録機能の設定ステータス
Auto registration is disabled.	

関連コマンド [\(config\) auto-register](#)

show banner

Message of the Day (MOTD)、ログイン、EXEC バナーの設定を表示するには、**show banner EXEC** コマンドを使用します。

show banner

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-9 では、**show banner** 出力のフィールドについて説明します。

表 3-9 show banner コマンドのフィールドの説明

フィールド	説明
Banner is enabled.	バナー機能の設定ステータス
MOTD banner is:abc	(日付メッセージ) その日に設定されたメッセージを表示します。
Login banner is:acb	設定されたログイン バナーを表示します。
Exec banner is:abc	設定された EXEC バナーを表示します。

関連コマンド [\(config\) auto-register](#)

show bypass

WAE の静的バイパス設定情報を表示するには、**show bypass EXEC** コマンドを使用します。

show bypass list

シンタックスの説明

list バイパス リスト エントリを表示します。最大 50 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

使用上のガイドライン

静的バイパス エントリの最大数は 50 です。

例

表 3-10 では、**show bypass list** 出力のフィールドについて説明します。

表 3-10 show bypass list コマンドのフィールドの説明

フィールド	説明
Client	クライアントの IP アドレスおよびポート。この IP アドレスのあるクライアントの場合、WAE はパケットを処理しませんが、パケットをバイパスしてルータに送信します。
Server	サーバの IP アドレスおよびポート
Entry type	バイパス リスト エントリのタイプ。Entry type には、static-config、auth-traffic、server-error、または accept のいずれかの値が含まれます。 static-config エントリは、ユーザ設定であるバイパス リスト エントリです。auth-traffic エントリは、サーバが認証を要求したときに内部ソフトウェアが自動的に追加するダイナミック エントリのタイプです。

関連コマンド

(config) bypass

show cdp

CDP 設定情報を表示するには、**show cdp EXEC** コマンドを使用します。

```
show cdp [entry neighbor [protocol | version [protocol]] | holdtime | interface [FastEthernet slot/port
| GigabitEthernet slot/port] | neighbors [detail | FastEthernet slot/port [detail] | GigabitEthernet
slot/port [detail]] | run | timer | traffic]
```

シンタックスの説明

entry	(オプション) 特定のネイバー エントリの情報を表示します。
neighbor	CDP ネイバー エントリの名前
protocol	(オプション) CDP プロトコル情報を表示します。
version	(オプション) CDP のバージョンを表示します。
holdtime	(オプション) CDP 情報がネイバーによって保持される時間の長さを表示します。
interface	(オプション) インターフェイスのステータスと設定を表示します。
FastEthernet	(オプション) ファスト イーサネット設定を表示します。
slot/port	ファスト イーサネット スロット (0 ~ 3) およびポート番号
GigabitEthernet	(オプション) ギガビット イーサネット設定を表示します。
slot/port	ギガビット イーサネット スロット (1 ~ 2) およびポート番号
neighbors	(オプション) CDP ネイバー エントリを表示します。
detail	(オプション) 詳細なネイバー エントリ情報を表示します。
FastEthernet	(オプション) ネイバー ファスト イーサネット情報を表示します。
slot/port	ネイバー ファスト イーサネット スロット (0 ~ 3) およびポート番号
detail	詳細なネイバー ファスト イーサネット ネットワーク情報を表示します。
GigabitEthernet	(オプション) ネイバー ギガビット イーサネット情報を表示します。
slot/port	ネイバー ギガビット イーサネット スロット (1 ~ 2) およびポート番号
detail	(オプション) 詳細なギガビット イーサネット ネイバー ネットワーク情報を表示します。
run	(オプション) CDP プロセスのステータスを表示します。
timer	(オプション) CDP 情報がネイバーに再送信される時間を表示します。
traffic	(オプション) CDP 統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

show cdp コマンドは、CDP パケットがネイバーに再送信される頻度、ネイバーによって CDP パケットが保持される時間、CDP バージョン 2 マルチキャスト アドバタイズのディセーブル化したステータス、CDP イーサネット インターフェイス ポート、CDP トラフィックの概要などの情報を表示します。

例

表 3-11 では、**show cdp** 出力のフィールドについて説明します。

表 3-11 show cdp コマンドのフィールドの説明

フィールド	説明
Sending CDP packets every XX seconds	CDP アドバタイズメントの送信間隔 (秒)。このフィールドは、 cdp timer コマンドによって制御されます。
Sending a holdtime value of XX seconds	デバイスがネイバーに対し、CDP アドバタイズメントを廃棄するまで保持するよう指示する時間 (秒)。このフィールドは、 cdp holdtime コマンドによって制御されます。
Sending CDPv2 advertisements is XX	CDP Version-2 タイプ アドバタイズメントを送信するための送信ステータス。可能な値は enabled または disabled です。

表 3-12 では、**show cdp entry neighbor** 出力のフィールドについて説明します。

表 3-12 show cdp entry コマンドのフィールドの説明

フィールド	説明
Device ID	近接デバイスの名前と、このデバイスの Media Access Control (MAC; メディア アクセス制御) アドレスまたはシリアル番号
Entry address (es)	
IP address	近接デバイスの IP アドレス
CLNS address	非 IP ネットワーク アドレス。ネイバー タイプによって異なります。
DECnet address	非 IP ネットワーク アドレス。ネイバー タイプによって異なります。
Platform	近接デバイスの製品名および製品番号
Interface	接続メディアが使用するプロトコル
Port ID (outgoing port)	近接デバイス上のポートのポート番号
Capabilities	近接デバイス上で検出された機能コード。これは、CDP Neighbors テーブルで示すデバイスのタイプです。可能な値は次のとおりです。 R — ルータ T — 透過的なブリッジ B — 送信元ルーティングブリッジ S — スイッチ H — ホスト I — IGMP デバイス R — リピータ

表 3-12 show cdp entry コマンドのフィールドの説明 (続き)

フィールド	説明
Holdtime	現在のデバイスが、送信ルータからの CDP アドバタイズメントを廃棄するまで保持する時間 (秒)
Version	近接デバイス上で動作するソフトウェアのバージョン

表 3-13 では、`show cdp entry neighbor protocol` 出力のフィールドについて説明します。

表 3-13 show cdp entry protocol コマンドのフィールドの説明

フィールド	説明
Protocol information for XX	近接デバイスの名前または識別情報
IP address	近接デバイスの IP アドレス
CLNS address	非 IP ネットワーク アドレス。ネイバータイプによって異なります。
DECnet address	非 IP ネットワーク アドレス。ネイバータイプによって異なります。

表 3-14 では、`show cdp entry neighbor version` 出力のフィールドについて説明します。

表 3-14 show cdp entry version コマンドのフィールドの説明

フィールド	説明
Version information for XX	近接デバイスの名前または識別情報
Software, Version	近接デバイス上で動作するソフトウェアのバージョン
Copyright	近接デバイスの著作権情報

表 3-15 では、`show cdp holdtime` 出力のフィールドについて説明します。

表 3-15 show cdp holdtime コマンドのフィールドの説明

フィールド	説明
XX seconds	現在のデバイスが、送信ルータからの CDP アドバタイズメントを廃棄するまで保持する時間 (秒)

表 3-16 では、`show cdp interface` 出力のフィールドについて説明します。

表 3-16 show cdp interface コマンドのフィールドの説明

フィールド	説明
Interface_slot/port is XX	CDP インターフェイスの動作ステータス。値は up または down です。
CDP protocol is XX	接続メディアが使用するプロトコル

表 3-17 では、`show cdp neighbors` 出力のフィールドについて説明します。

表 3-17 show cdp neighbors コマンドのフィールドの説明

フィールド	説明
Device ID	近接デバイスの設定された ID (名前)、MAC アドレス、またはシリアル番号
Local Intrfce	(ローカルインターフェイス) 接続メディアが使用するプロトコル
Holdtime	現在のデバイスが、送信ルータからの CDP アドバタイズメントを廃棄するまで保持する時間 (秒)
Capability	デバイス上で検出された機能コード。これは、CDP Neighbors テーブルで示すデバイスのタイプです。可能な値は次のとおりです。 R — ルータ T — 透過的なブリッジ B — 送信元ルーティングブリッジ S — スイッチ H — ホスト I — IGMP デバイス R — リピータ
Platform	デバイスの製品番号
Port ID (outgoing port)	デバイスのポート番号

表 3-18 では、`show cdp neighbors detail` 出力のフィールドについて説明します。

表 3-18 show cdp neighbors detail コマンドのフィールドの説明

フィールド	説明
Device ID	近接デバイスの設定された ID (名前)、MAC アドレス、またはシリアル番号
Entry address (es)	近接デバイスのネットワーク アドレス リスト
Platform	近接デバイスの製品名および製品番号
Capabilities	ネイバーのデバイス タイプ。このデバイスは、ルータ、ブリッジ、透過的なブリッジ、送信元ルーティングブリッジ、スイッチ、ホスト、IGMP デバイス、またはリピータになることができます。
Interface	接続メディアが使用するプロトコル
Port ID (outgoing port)	近接デバイス上のポートのポート番号
Holdtime	現在のデバイスが、送信ルータからの CDP アドバタイズメントを廃棄するまで保持する時間 (秒)
Version	近接デバイス上で動作するソフトウェアのバージョン
Copyright	近接デバイスの著作権情報
advertisement version	CDP アドバタイズメントに使用する CDP のバージョン
VTP Management Domain	VLAN Trunk Protocol 管理ドメイン。VLAN 情報は、同じドメインの一部であるすべてのスイッチに配信されます。
Native VLAN	ネイバー インターフェイスが所属する VLAN

表 3-19 では、`show cdp run` 出力のフィールドについて説明します。

表 3-19 show cdp run コマンドのフィールドの説明

フィールド	説明
CDP is XX.	CDP がイネーブルかディセーブルかを示します。

表 3-20 では、`show cdp timer` 出力のフィールドについて説明します。

表 3-20 show cdp timer コマンドのフィールドの説明

フィールド	説明
cdp timer XX	CDP 情報をネイバーに再送信する時間

表 3-21 では、`show cdp traffic` 出力のフィールドについて説明します。

表 3-21 show cdp traffic コマンドのフィールドの説明

フィールド	説明
Total packets Output	(送信されたパケットの総数) ローカル デバイスによって送信された CDP アドバタイズメントの数。この値は、CDP Version 1 advertisements output フィールドと CDP Version 2 advertisements output フィールドの合計であることに注意してください。
Input	(受信したパケットの総数) ローカル デバイスによって受信された CDP アドバタイズメントの数。この値は、CDP Version 1 advertisements input フィールドと CDP Version 2 advertisements input フィールドの合計であることに注意してください。
Hdr syntax	(ヘッダー構文) ローカル デバイスによって受信された、不良ヘッダーのある CDP アドバタイズメントの数
Chksum error	(チェックサムエラー) チェックサム (確認) 動作が着信 CDP アドバタイズメント上で失敗した回数
Encaps failed	(カプセル化の失敗) ローカル デバイスのブリッジ ポートが引き起こした障害によって、CDP がインターフェイス上でアドバタイズメントの送信に失敗した回数
No memory	ローカル デバイスが送信用のアドバタイズメント パケットを組み立てようとしたとき、およびこのパケットの受信時にその解析を試みたときに、ローカル デバイスで、アドバタイズメント キャッシュ テーブルに CDP アドバタイズメントをストアできるだけのメモリがなかった回数
Invalid packet	ローカル デバイスによって送受信された無効な CDP アドバタイズメントの数
Fragmented	完全なアドバタイズメントではなく、1つの CDP アドバタイズメントのフラグメントまたは部分がローカル デバイスによって受信された回数
CDP version 1 advertisements Output	ローカル デバイスによって送信された CDP バージョン 1 アドバタイズメントの数
Input	ローカル デバイスによって受信された CDP バージョン 1 アドバタイズメントの数

表 3-21 show cdp traffic コマンドのフィールドの説明 (続き)

フィールド	説明
CDP version 2 advertisements Output	ローカル デバイスによって送信された CDP バージョン 2 アドバタイズメントの数
Input	ローカル デバイスによって受信された CDP バージョン 2 アドバタイズメントの数

関連コマンド[\(config\) cdp](#)[\(config-if\) cdp](#)[clear](#)

show cifs

CIFS 実行時情報を表示するには、**show cifs EXEC** コマンドを使用します。

```
show cifs {auto-discovery [enabled | host-db | last] | cache {disk-use | entry-count} | connectivity
peers | mss | requests {count | waiting} | sessions {count | list}}
```

シンタックスの説明

auto-discovery	CIFS 自動ディスカバリ ステータスおよび実行時データ
enabled (有効)	CIFS 自動ディスカバリの現在のステートを表示します。
host-db	現在、わかっているホストを表示します。
last	最後の自動ディスカバリ エントリを表示します。
cache	CIFS キャッシュ情報を表示します。
disk-use	CIFS キャッシュ用のディスクの総使用量を表示します。
entry-count	キャッシュされたファイルおよびディレクトリ エントリのカウント
connectivity	Edge-Core 接続に関する実行時情報を表示します。
peers	接続されたコアのリストを表示します。
mss	CIFS アダプタの TCP Maximum Segment Size (MSS; 最大セグメント サイズ) を表示します。セグメント サイズの範囲は 512 ~ 1460 です。
requests	アクティブな CIFS 要求に関する実行時情報を表示します。
count	保留中の CIFS 要求の数
waiting	待機中の CIFS 要求の数
sessions	アクティブな CIFS セッションに関する実行時情報を表示します。
count	接続されたセッション カウント
list	接続された CIFS セッションのリスト

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

キャッシング効率に関する情報を表示するには、**show cifs cache** コマンドを使用します。このコマンドを使用して、キャッシュに十分なスペースがあるか、またはより多くのスペースが必要であるか判断できます。パフォーマンスに問題がある場合、このコマンドを使用してキャッシュがフルであるかどうか判断できます。

WAN リンク ステートと、Edge と Core の接続性を検証するには、**show cifs connectivity peers** コマンドを使用します。このコマンドは、一般的なモニタリングとデバッグに利用できます。

CIFS トラフィックの負荷を監視するには、**show cifs requests count** または **show cifs requests waiting** コマンドを使用します。処理されない要求を隔離するため、デバッグ目的でこのコマンドを使用することもできます。

セッション情報を表示するには、**show cifs sessions count** または **show cifs sessions list** コマンドを使用します。ピーク時とオフピーク時に接続されたユーザを監視するために、このコマンドを使用できます。

関連コマンド **cifs**

show clock

WAAS デバイスのシステム クロックに関する情報を表示するには、**show clock EXEC** コマンドを使用します。

```
show clock [detail | standard-timezones {all | details timezone | regions | zones region-name}]
```

シンタックスの説明

detail	(オプション) 詳細情報を表示します。クロック ソース (NTP) と現在のサマータイム設定 (ある場合) を示します。
standard-timezones	(オプション) 標準時間帯に関する情報を表示します。
all	すべての標準時間帯 (約 1500 の時間帯) を表示します。各時間帯を個別の行でリストします。
details	特定の時間帯の詳細情報を表示します。
<i>timezone</i>	時間帯の名前
regions	すべての標準時間帯の地域名を表示します。1500 の時間帯すべてが地域別にディレクトリに編成されています。
zones	指定された地域内のすべての時間帯の名前を表示します。
<i>region-name</i>	地域の名前

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

WAAS デバイスには、事前に定義されたいくつかの「標準」時間帯があります。サマータイム情報が組み込まれている時間帯もあれば、そうでない時間帯もあります。たとえば、アメリカ合衆国 (US) の東部地域にいる場合、サマータイム情報を含んだ US/Eastern 時間帯を使用して、システムクロックが毎 4 月および 10 月に自動的に調整されるようにする必要があります。約 1500 の「標準」時間帯名があります。

標準時間帯が設定されている場合、厳密なチェックにより **clock summertime** コマンドはディセーブルになります。サマータイムは、時間帯が標準時間帯でない (つまり、時間帯が「カスタマイズ」時間帯である) 場合にしか設定できません。

show clock standard-timezones all EXEC コマンドにより、すべての標準時間帯を参照し、事前に定義されたこれらの時間帯から選択できます。これにより、標準時間帯の事前に定義された名前と競合しないカスタマイズ名を選択できます。大部分の標準時間帯の事前に定義された名前には、地域

名とゾーン名の2つの要素があります。時間帯は、地域やゾーンなどいくつかの条件でリストできます。地域別のディレクトリに編成された第1レベルの時間帯名をすべて表示するには、**show clock standard-timezones region EXEC** コマンドを使用します。

show clock コマンドは現地の日付時刻情報を示し、**show clock detail** コマンドはオプションの詳細な日付時刻情報を示します。

例

表 3-22 では、**show clock** 出力のフィールドについて説明します。

表 3-22 show clock コマンドのフィールドの説明

フィールド	説明
Local time	UTC オフセットを基準にした現地時間の曜日、月、日付、時刻 (hh : mm : ss)、および年

表 3-23 では、**show clock detail** 出力のフィールドについて説明します。

表 3-23 show clock detail コマンドのフィールドの説明

フィールド	説明
Local time	UTC を基準にした現地時間
UTC time	世界標準時の日付および時間
Epoch	1970 年 1 月 1 日以降の秒数
UTC offset	秒、分、時間単位の UTC オフセット

関連コマンド

[clock](#)

[\(config\) clock](#)

show cms

WAAS デバイスの Centralized Management System (CMS; 中央集中型管理システム) 組み込みデータベースのコンテンツとメンテナンス ステータス、およびその他の情報を表示するには、**show cms EXEC** コマンドを使用します。

```
show cms {database content {dump filename | text | xml} | info | processes}
```

シンタックスの説明

database	組み込みデータベースのメンテナンス情報を表示します。
content	ファイルにデータベースのコンテンツを書き込みます。
dump	テキスト ファイルにすべてのデータベース コンテンツをダンプします。
filename	local1 ディレクトリに保存するファイルの名前
text	テキスト フォーマットのファイルにデータベース コンテンツを書き込みます。
xml	XML フォーマットのファイルにデータベース コンテンツを書き込みます。
info	CMS アプリケーション情報を表示します。
processes	CMS アプリケーション プロセスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

例

表 3-24 では、WAAS アプリケーション エンジンの **show cms info** 出力のフィールドについて説明します。

表 3-24 WAAS アプリケーション エンジンの show cms info コマンドのフィールドの説明

フィールド	説明
デバイス登録情報	
Device Id	登録時に Central Manager によってデバイスに与えられた一意な識別情報。デバイスの管理に使用します。
Device registered as	登録時に使用するデバイス タイプ。WAAS Application Engine または WAAS Central Manager
Current WAAS Central Manager	central-manager address グローバル コンフィギュレーション コマンドで現在設定された Central Manager のアドレス。デバイスが登録されているプライマリ Central Manager の代わりにスタンバイ Central Manager がデバイスを管理する場合、このアドレスは登録したアドレスとは異なります。
Registered with WAAS Central Manager	デバイスが登録されている Central Manager のアドレス

表 3-24 WAAS アプリケーション エンジンの show cms info コマンドのフィールドの説明 (続き)

フィールド	説明
Status	デバイスと Central Manager の接続ステータス。このフィールドには、online、offline、または pending の値のいずれかが含まれます。
Time of last config-sync	アップデートのため、デバイス マネジメント サービスが最後に Central Manager に接続した時間
CMS サービス情報	
Service cms_ce is running	WAE デバイス マネジメント サービスのステータス (動作中または動作していない)。このフィールドは、WAE のみに固有です。

表 3-25 では、WAAS Central Manager の show cms info 出力のフィールドについて説明します。

表 3-25 WAAS Central Manager の show cms info コマンドのフィールドの説明


フィールド	説明
デバイス登録情報	
Device Id	登録時に Central Manager によってデバイスに与えられた一意な識別情報。デバイスの管理に使用します。
Device registered as	登録時に使用するデバイス タイプ。WAAS Application Engine または WAAS Central Manager
Current WAAS Central Manager role	現在の Central Manager の役割。プライマリまたはスタンバイです。  (注) プライマリおよびスタンバイ Central Manager デバイスの出力は異なります。スタンバイでは、出力に Current WAAS Central Manager と Registered with WAAS Central Manager に関する追加情報が含まれます。
Current WAAS Central Manager	central-manager address グローバル コンフィギュレーション コマンドで現在設定されたスタンバイ Central Manager のアドレス
Registered with WAAS Central Manager	デバイスが登録されているスタンバイ Central Manager のアドレス
CMS サービス情報	
Service cms_httpd is running	マネジメント サービスのステータス (動作中または動作していない)。このフィールドは、Central Manager のみに固有です。
Service cms_cdm is running	マネジメント サービスのステータス (動作中または動作していない)。このフィールドは、Central Manager のみに固有です。

表 3-26 では、**show cms database content text** 出力のフィールドについて説明します。

表 3-26 show cms database content text コマンドのフィールドの説明

フィールド	説明
Database content can be found in /local1/cms-db-12-12-2002-17:06:08:070.txt.	データベース コンテンツ テキスト ファイルの名前と場所。このコマンドは、現在の設定を自動的に生成されたファイルにテキストフォーマットで書き込むようマネジメント サービスに要求します。

表 3-27 では、**show cms database content xml** 出力のフィールドについて説明します。

表 3-27 show cms database content xml コマンドのフィールドの説明

フィールド	説明
Database content can be found in /local1/cms-db-12-12-2002-17:07:11:629.xml.	データベース コンテンツ XML ファイルの名前と場所。このコマンドは、現在の設定を自動的に生成されたファイルに XML フォーマットで書き込むようマネジメント サービスに要求します。

関連コマンド

[cms](#)

[\(config\) cms](#)

show cms secure-store

セキュア ディスクの暗号化ステータスを表示するには、**show cms secure-store** EXEC コマンドを使用します。

show cms secure-store

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 次の例では、セキュア ディスクの暗号化が完全に動作している（初期化済みで、オープンである）ことを示します

```
WAE# show cms secure-store
secure-store initialized and open
```

コマンドにより、次のステータス メッセージのいずれかが表示されます。

secure-store not initialized	セキュア ディスクの暗号化が初期化されていません。
secure-store initialized. use secure-store open command to open	セキュア ディスクの暗号化は初期化されていますが、オープンではありません。
secure-store initialized and open	セキュア ディスクの暗号化は初期化されていて、オープンです。

関連コマンド [cms secure-store](#)

show debugging

WAAS デバイスで以前にイネーブル化された各デバッグ オプションの状態を表示するには、**show debugging EXEC** コマンドを使用します。

show debugging

シンタックスの説明 このコマンドには引数やキーワードがありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン このコマンドは、イネーブル化またはディセーブル化されたデバッグ オプションを表示します。デバッグ オプションが設定されていない場合、このコマンドは出力を表示しません。

dre、*epm*、*flow*、*print-spooler*、*rbcp*、*tfo*、*translog*、*wafs*、および *wccp* コマンド オプションは application-accelerator デバイス モードのみでサポートされます。*emdb* および *rpc* コマンド オプションは、central manager デバイス モードでのみサポートされます。

このコマンドが表示するのはイネーブル化されたデバッグ タイプだけで、特定のコマンドのサブセットは表示しません。

例 次の例では、**debug tfo buffer-mgr** および **debug tfo connection** コマンドと組み合わせた **show debugging** コマンドが、**tfo buffer-mgr** および **tfo connection** デバッグ オプションの状態を示します。

```
WAE# debug tfo buffer-mgr
WAE# debug tfo connection
WAE# show debugging
tfo bufmgr debugging is on
tfo compmgr debugging is on
tfo connmgr debugging is on
tfo netio debugging is on
tfo statmgr debugging is on
tfo translog debugging is on
```

関連コマンド [debug](#)
[undebug](#)

show device-mode

WAAS デバイスの設定された、または現在のデバイス モードを表示するには、**show device-mode EXEC** コマンドを使用します。

```
show device-mode {configured | current}
```

シンタックスの説明

configured	設定されたデバイス モードを表示します。ただし、まだ有効になっていません。
current	現在のデバイス モードを表示します。

コマンドモード

EXEC

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

WAAS Central Manager は専用アプライアンスで展開する必要があります。デバイス モード機能により、WAAS デバイスは WAAS Central Manger または WAE のどちらかで導入できます。WAAS Central Manager は専用アプライアンスで導入する必要があるため、WAAS デバイスは central-manager モードまたは application-accelerator モードのどちらか1つのデバイス モードで動作できるだけです。

設定されたデバイス モードと現在のモードが異なる場合、設定されたデバイス モードを有効にするにはリロードが必要です。

WAAS デバイスの現在のデバイス モードを表示するには、**show device mode EXEC** コマンドを入力します。

```
WAE# show device-mode
```

WAAS デバイスが動作している現在のモードを表示するには、**show device-mode current EXEC** コマンドを入力します。

```
WAE# show device-mode current  
Current device mode: application-accelerator
```

まだ有効になっていない設定されたデバイス モードを表示するには、**show device-mode configured EXEC** コマンドを入力します。たとえば、WAAS デバイスで **device mode central-manager** 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デバイス モードを central manager に変更したあと、**copy run start EXEC** コマンドを入力してデバイスの実行コンフィギュレーションをまだ保存していない場合、WAAS デバイスで **show device-mode configured** コマンドを入力すると、コマンド出力は設定されたデバイス モードが central-manager であることを示します。

```
WAE# show device-mode configured  
Configured device mode: central-manager
```

例

表 3-28 では、**show device-mode current** 出力のフィールドについて説明します。

表 3-28 show device-mode current コマンドのフィールドの説明

フィールド	説明
Current device mode	WAAS デバイスが動作する現在のモード

表 3-29 では、**show device-mode configured** 出力のフィールドについて説明します。

表 3-29 show device-mode configured コマンドのフィールドの説明

フィールド	説明
Configured device mode	設定されていますが、まだ有効になっていないデバイス モード

関連コマンド


[\(config\) device mode](#)

show disks

WAAS デバイスのディスクに関する情報を表示するには、**show disks** EXEC コマンドを使用します。

```
show disks {details | failed-disk-id | failed-sectors [disk_name] | tech-support [details]}
```

シンタックスの説明

details	現在有効な設定を詳細情報とともに表示します。
failed-disk-id	障害があるとして識別されたディスクのシリアル番号のリストを表示します。
	 <p>(注) このオプションは、WAE-7341 および WAE-7371 モデルでは利用できません。</p>
failed-sectors	すべてのディスクの障害のあるセクターのリストを表示します。
disk_name	(オプション) 障害のあるセクターが表示されているディスクの名前 (disk00 または disk01)
tech-support	ハードドライブ診断情報および近い将来のディスク障害に関する情報を表示します。 ディスク ステータス (論理または物理)、ディスク ベンダー ID、シリアル番号を含めた、RAID コントローラから利用できる情報をすべて表示します。 このコマンドは show disk smart-info EXEC コマンドに代わるものです。
details	(オプション) 詳細な SMART ディスク モニタリング情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

show disks details EXEC コマンドは、リブート後、各ファイルシステムに割り当てられたディスクスペースの割合や量、ディスク ドライブの動作ステータスを表示します。

WAAS ソフトウェアは、IDE、SCSI、および SATA ディスクの単一障害セクションに対する、複数の Syslog メッセージのフィルタリングをサポートします。全ディスク ドライブにおける障害のあるセクターのリストを表示するには、**show disks failed-sectors** EXEC コマンドを入力します。

```
WAE# show disks failed-sectors
disk00
=====
89923
9232112

disk01
=====
(None)
```

特定のディスク ドライブのみにおける障害のあるセクターのリストを表示するには、**show disks failed-sectors** コマンドの入力時に、ディスクの名前を指定します。次の例は、disk01 における障害のあるセクターのリストを表示する方法を示します。

```
WAE# show disks failed-sectors disk01
disk01
=====
(None)
```

ディスク障害がある場合は、メッセージが表示され、ログイン時にこの状況について通知します。

SMART によるディスク ヘルスの予防的モニタリング

SMART を使用すると、ディスク ヘルスの予防的モニタリング機能が利用できます。SMART は、ハードドライブ診断情報および近い将来の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 ヘルス进行を判断する標準的な方法です。SMART のアトリビュートにはいくつかの読み取り専用アトリビュートがあり（たとえば、稼動時間属性や、ロードおよびアンロード カウント属性）、これにより WAAS ソフトウェアに、近い将来のディスク障害を示唆する動作および環境状態に関する情報を提供します。

SMART のサポートは、ベンダーおよびドライブ テクノロジー（IDE または SCSI ディスク ドライブ）依存です。各ディスク ベンダーで、サポートしている SMART アトリビュートセットは異なります。

SMART アトリビュートはベンダーに依存しますが、ほとんどの SMART アトリビュートを解釈する一般的な方法があります。各 SMART アトリビュートには、正規化された現在値としきい値があります。現在値がしきい値を超えると、ディスクは「障害が発生した」とみなされます。WAAS ソフトウェアは SMART アトリビュートを監視し、Syslog メッセージ、SNMP トラップ、およびアラームを介して、将来の障害を通知します。

SMART 情報を表示するには、**show disks tech-support EXEC** コマンドを使用します。詳細な SMART 情報を表示するには、**show disks tech-support details EXEC** コマンドを入力します。**show tech-support EXEC** コマンドの出力には、SMART 情報も含まれます。

例

表 3-30 では、**show disks failed-disk-id** 出力のフィールドについて説明します。

表 3-30 show disks failed-disk-id コマンドのフィールドの説明

フィールド	説明
Diskxx	物理ディスクの番号と場所
Alpha-numeric string	ディスクのシリアル番号

表 3-31 では、**show disks details** 出力のフィールドについて説明します。

表 3-31 show disks details コマンドのフィールドの説明

フィールド	説明
Physical disk information	番号別にディスクをリストします。WAE 7300 シリーズ アプライアンスは 6 つのディスク ドライブの情報を示し、WAE 500 および 600 シリーズ アプライアンスは 2 つのディスク ドライブの情報を示します。
disk00	ディスクのアベイラビリティ (Present、Not present or Not responding、または Not used [*])。 ディスク ID 番号およびタイプ (たとえば、h00 c00i00 100 - DAS)。 メガバイトまたはギガバイト単位のディスク サイズ (たとえば、140011MB [136.7GB])。
disk01	同じタイプの情報がディスクごとに表示されます。
Mounted filesystems	次のカラム ヘッドを含んだ表
Mount point	ファイル システムのマウント ポイント。たとえば、SYSFS のマウント ポイントは /local/local1 です。
Type	ファイル システムのタイプ。値には、root、internal、CONTENT、SYSFS、および PRINTSPOOL が含まれます。
Device	ディスク上のパーティションへのパス
Size	ファイル システムの総サイズ (メガバイト単位)
Inuse	ファイル システムが使用するディスク スペース量
Free	ファイル システム用の未使用のディスク スペース量
Use%	ファイル システムによって使用される、利用可能な総ディスク スペースの比率
Software RAID devices	存在する場合、ソフトウェア RAID デバイスを示し、次の各情報を提供します。
Device name	ディスク上のパーティションへのパス。パーティション名「md1」は、そのパーティションは RAID のパーティションであり、RAID タイプが RAID-1 であることを示します。
Type	RAID タイプ (たとえば、RAID-1)
Status	RAID デバイスの動作ステータス。ステータスには、NORMAL OPERATION または REBUILDING が含まれます
Physical devices and status	ディスク番号とディスクの動作ステータス ([GOOD] または [BAD] など)

次の例では、ディスク disk00 および disk01 のパーティション 04 とパーティション 05 は GOOD であり、RAID のパーティション /dev/md4 & /dev/md5 は NORMAL OPERATION である出力を示します。ただし、RAID のパーティション /dev/md8 の場合、ドライブの 1 つに問題があります。パーティション 00 のある disk04 は GOOD ですが、このパーティション上にペアがないのでステータスでは ONE OR MORE DRIVES ABNORMAL が表示されます。

```

/dev/md4      RAID-1   NORMAL OPERATION      disk00/04 [GOOD]
disk01/04 [GOOD]
/dev/md5      RAID-1   NORMAL OPERATION      disk00/05 [GOOD]
disk01/05 [GOOD]
...
/dev/md8      RAID-1   ONE OR MORE DRIVES ABNORMAL  disk04/00 [GOOD]

```

表 3-32 では、SMART をサポートする RAID-1 アプライアンスの **show disks tech-support** 出力の一般的な一部のフィールドについて説明します。SMART アトリビュートは、ベンダー依存です。ディスクベンダーごとに、異なる、サポート対象の SMART アトリビュートセットがあります。

表 3-32 show disks tech-support コマンドのフィールドの説明

フィールド	説明
disk00–disk05	WAE 7300 シリーズ アプライアンスは 6 つのディスクドライブの情報を示し、WAE 500 および 600 シリーズ アプライアンスは 2 つのディスクドライブの情報を示します。
Device	ディスクのベンダー番号とバージョン番号
Serial Number	ディスクのシリアル番号
Device type	デバイスのタイプはディスクです。
Transport protocol	物理レイヤ接続情報 (たとえば、Parallel SCSI [SPI-4])
Local time is	曜日、月、日付、時刻 (hh : mm : ss)、年、およびクロック標準。たとえば、Mon Mar 19 23:33:12 2007 UTC。
Device supports SMART and is Enabled	SMART サポートのステータス (Enabled または Disabled)
Temperature Warning Enabled	温度警告ステータス (Enabled または Disabled)
SMART Health Status:	ディスクのヘルス ステータス (OK または Failed)

表 3-33 では、SMART をサポートする RAID-1 アプライアンスの **show disks tech-support details** 出力のフィールドについて説明します。この出力の詳細は、ドライブ メーカーやドライブによって異なります。

表 3-33 show disks tech-support details コマンドのフィールドの説明

フィールド	説明
disk00–disk05	WAE 7300 シリーズ アプライアンスは 6 つのディスクドライブの情報を示し、WAE 500 および 600 シリーズ アプライアンスは 2 つのディスクドライブの情報を示します。
Device	ディスクのベンダー番号とバージョン番号
Serial Number	ディスクのシリアル番号
Device type	デバイスのタイプはディスクです。
Transport protocol	物理レイヤ接続情報 (たとえば、Parallel SCSI [SPI-4])
Local time is	曜日、月、日付、時刻 (hh : mm : ss)、年、およびクロック標準。たとえば、Mon Mar 19 23:33:12 2007 UTC。
Device supports SMART and is Enabled	SMART サポートのステータス (Enabled または Disabled)
Temperature Warning Enabled	温度警告ステータス (Enabled または Disabled)
SMART Health Status:	ディスクのヘルス ステータス (OK または Failed)
Current Drive Temperature	ドライブの温度 (摂氏)
Manufactured in week XX of year	製造の詳細
Current start stop count	デバイスが停止または開始した回数

表 3-33 show disks tech-support details コマンドのフィールドの説明 (続き)

フィールド	説明
Recommended maximum start stop count	ディスクの平均寿命をゲージするのに使用する、推奨の最大カウント
Error counter log	エラー カウント ログを表示するテーブル。さまざまなディスク エラー タイプのカウント

表 3-34 では、RAID-5 アプライアンスの **show disks tech-support** 出力のフィールドについて説明します。

表 3-34 show disks tech-support コマンドのフィールドの説明

フィールド	説明
Controllers found	検出した RAID コントローラの数
コントローラ情報	
Controller Status	コントローラの機能ステータス
Channel description	チャンネル トランスポート プロトコルの説明
Controller Model	コントローラのモデルを作成します。
Controller Serial Number	ServeRAID コントローラのシリアル番号
Physical Slot	スロット番号
Installed memory	ディスクのメモリ量
Copyback	copyback がイネーブルまたはディセーブルであるかのステータス
Data scrubbing	data scrubbing がイネーブルまたはディセーブルであるかのステータス
Defunct disk drive count	存在しないディスク ドライブの数
Logical drives/Offline/Critical	論理ドライブ数、オフラインであるドライブ数、およびクリティカルアラーム数
コントローラ バージョン情報	
BIOS	BIOS のバージョン番号
Firmware	Firmware のバージョン番号
Driver	Driver のバージョン番号
Boot Flash	Boot Flash のバージョン番号
コントローラ バッテリー情報	
Status	コントローラ バッテリーの機能ステータス
Over temperature	バッテリーの過熱状態
Capacity remaining	残りのバッテリー容量のパーセント
Time remaining (at current draw)	電流の消費量に基づく残りのバッテリー寿命の日数、時間数、および分秒
コントローラの Vital Product Data	
VPD Assigned#	コントローラの Vital Product Data (VPD) に割り当てられた番号
EC Version#	バージョン番号
Controller FRU#	コントローラの現場交換可能部品に割り当てられた番号
Battery FRU#	バッテリーの現場交換可能部品に割り当てられた番号

表 3-34 show disks tech-support コマンドのフィールドの説明 (続き)

フィールド	説明
論理ドライブ情報	
Logical drive number	情報が適用される論理ドライブを識別する番号
Logical drive name	論理ドライブ名
RAID level	論理ドライブの RAID レベル
Status of logical drive	論理ドライブの機能ステータス
Size	論理ドライブのサイズ (メガバイト単位)
Read-cache mode	read-cache モードの設定ステータス (Enabled または Disabled)
Write-cache mode	write-back の書き込みキャッシュ モードの設定ステータス (Enabled または Disabled)
Write-cache setting	write-back の書き込みキャッシュ設定の設定ステータス (Enabled または Disabled)
Partitioned	パーティションステート。値は Yes または No です。
Number of chunks	RAID-5 アレイに組み込まれたディスクの数
Stripe-unit size	ストライプユニットごとのデータストレージ量。デフォルトは、論理アレイのディスクごとに 256 KB です。パラメータは設定可能ではありません。
Stripe order (Channel,Device)	RAID アレイでグループ化された物理ドライブのグループにわたってストライプ化したデータの順序
Bad stripes	不良ストライプのフラグ。フラグの値は Yes または No です。
物理ドライブ情報	
Device #	情報が適用されるデバイス番号
Device is a xxxx	デバイスのタイプ
State	デバイスのステート (Online または Offline)
Supported	デバイスがサポートされているかを示すステータス
Transfer Speed	デバイス転送速度
Reported Channel,Device	RAID-5 アレイに組み込まれたディスクすべてにチャネル情報を提供します。
Reported Enclosure,Slot	デバイス番号とスロット番号
Vendor	ベンダー ID 番号
Model	モデル番号
Firmware	ファームウェア番号
Serial number	シリアル番号
Size	物理ドライブのサイズ (メガバイト単位)
Write Cache	書き込みキャッシュがイネーブルであるかのステータス
FRU	Field Replaceable Unit (FRU; 現場交換可能ユニット) 番号。提供された FRU 番号のある指定されたハードディスク ドライブが RAID 設定に失敗した場合に、RAID にドライブが存在しない FRU イベントが発生します。このフィールドのデフォルト値は NONE です。

表 3-34 show disks tech-support コマンドのフィールドの説明 (続き)

フィールド	説明
PFA	Predictive Failure Analysis (PFA; 事前障害分析機能) フラグ。フラグのデフォルト値は No です。RAID がドライブの障害を予測している場合、このフィールドは Yes に設定され、WAE でクリティカルアラームが生成されます。

関連コマンド[disk](#)[\(config\) disk error-handling](#)[show tech-support](#)

show egress-methods

設定され、特定の WAE で使用する出力方式を表示するには、**show egress-methods** EXEC コマンドを使用します。

```
show egress-methods
```

シンタックスの説明 このコマンドには引数やキーワードがありません。

コマンドモード EXEC

デバイスモード application-accelerator

例 表 3-35 では、**show egress-methods** 出力のフィールドについて説明します。

表 3-35 show egress-methods コマンドのフィールドの説明

フィールド	説明
Intercept method	パケットを WAE へ送信するのにルータが使用する代行受信方法
TCP Promiscuous 61 or 62	WCCP サービス番号
WCCP negotiated return method	WCCP は、ルータが使用する方法を戻します。値は、WCCP_GRE、WCCP_L2、NEG_RTN_PENDING (ネゴシエーションは保留中)、および UNKNOWN です。
Destination	この値は設定可能ではありません。このフィールドの値は常に ANY です。
Egress Method Configured	CLI で設定された出力方式
Egress Method Used	使用する出力方式

関連コマンド [show tfo egress-methods connection](#)
[\(config\) egress-method](#)

show flash

WAAS デバイスのフラッシュ メモリのバージョンと使用状況の情報を表示するには、**show flash EXEC** コマンドを使用します。

show flash

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-36 では、**show flash** 出力のフィールドについて説明します。

表 3-36 show flash コマンドのフィールドの説明

フィールド	説明
WAAS software version (disk-based code)	デバイスで動作する WAAS ソフトウェア バージョンとビルド番号
フラッシュ上のシステム イメージ	
Version	フラッシュ メモリに保存されるソフトウェアのバージョンとビルド番号
システム フラッシュ ディレクトリ	
System image	システム イメージが使用するセクターの数
Bootloader, rescue image, and other reserved areas	ブートローダが使用するセクターの数、回復用イメージ、および他の予約領域
XX sectors total, XX sectors free	ピアの総数。フリーセクターの数

show hardware

WAAS デバイスのシステム ハードウェアのステータスを表示するには、**show hardware EXEC** コマンドを使用します。

show hardware

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン **show hardware** コマンドは、バージョン番号、始動した日時、始動後の実行時間、マイクロプロセッサのタイプと速度、利用可能な物理メモリの量、ディスク ドライブのリストなど、システム ハードウェアのステータスを示します。

例 表 3-37 では、**show hardware** 出力のフィールドについて説明します。

表 3-37 show hardware コマンドのフィールドの説明

フィールド	説明
Cisco Wide Area Application Services Software (WAAS) Copyright (c) year by Cisco Systems, Inc. Cisco Wide Area Application Services Software Release XXX (build bXXX month day year)	ソフトウェア アプリケーション、著作権、リリース、およびビルド情報
Version	デバイスで動作するソフトウェアのバージョン番号
Compiled hour:minute:second month day year by cnbuild	ソフトウェア ビルドのコンパイル情報
System was restarted on day of week month day hour:minute:second year	システムが最後に起動した日付と時間
The system has been up for X hours, X minutes, X seconds	最後のリブート以降、システムが動作していた時間の長さ
CPU 0 is	CPU メーカーの情報
Total X CPU	デバイス上の CPU の数
XXXX Mbytes of Physical memory	デバイス上の物理メモリのメガバイト数
X CD ROM drive	デバイス上の CD-ROM ドライブの数
X GigabitEthernet interfaces	デバイス上のギガビットイーサネットの数

表 3-37 show hardware コマンドのフィールドの説明 (続き)

フィールド	説明
X InlineGroup interfaces	デバイス上の InlineGroup インターフェイスの数
X Console interface	デバイス上のコンソール インターフェイスの数
Manufactured As	製品 ID 情報
BIOS Information	BIOS に関する情報
Vendor	BIOS ベンダーの名前
Version	BIOS バージョン番号
Rel. 日付	(リリース日) BIOS がリリースされた日付
Cookie 情報	
SerialNumber	WAE のシリアル番号
SerialNumber (raw)	ASCII 値としての WAE のシリアル番号
TestDate	WAE がテストされた日付
ExtModel	デバイスのハードウェア モデル (たとえば、WAE612)
ModelNum (raw)	ExtModel 番号に対応する内部モデル番号 (ASCII 値)
HWVersion	現在のハードウェア バージョンの番号
PartNumber	実装されていません。
BoardRevision	現在のシステム ボードのリビジョン番号
ChipRev	現在のチップセットのリビジョン番号
VendID	cookie のベンダー ID
CookieVer	cookie のバージョン番号
Chksum	cookie のチェックサム。cookie が有効かどうかを示します。
すべてのディスク ドライブのリスト	
Physical disk information	番号別にリストされたディスク。WAE 7300 シリーズ アプライアンスは 6 つのディスク ドライブの情報を示し、WAE 500 および 600 シリーズ アプライアンスは 2 つのディスク ドライブの情報を示します。
disk00	ディスクのアベイラビリティ (Present、Not present or Not responding、または Not used [*]) ディスクの ID 番号およびタイプ (たとえば、h00c00i00 100 - DAS) メガバイトまたはギガバイト単位のディスク サイズ (たとえば、140011MB [136.7GB])
disk01	同じタイプの情報がディスクごとに表示されます。
Mounted filesystems	次のカラム ヘッドを含んだ表
Mount point	ファイル システムのマウント ポイント。たとえば、SYSFS のマウント ポイントは /local/local1 です。
Type	ファイル システムのタイプ。値には、root、internal、CONTENT、SYSFS、および PRINTSPOOL が含まれます。
Device	ディスク上のパーティションへのパス
Size	ファイル システムの総サイズ (メガバイト単位)

表 3-37 show hardware コマンドのフィールドの説明 (続き)

フィールド	説明
Inuse	ファイルシステムが使用するディスクスペース量
Free	ファイルシステム用の未使用のディスクスペース量
Use%	ファイルシステムによって使用される、利用可能な総ディスクスペースの比率
Software RAID devices	存在する場合、ソフトウェア RAID デバイスを示し、次の各情報を提供します。
Device name	ディスク上のパーティションへのパス。パーティション名「md1」は、そのパーティションが RAID のパーティションであり、RAID タイプが RAID-1 であることを示します (RAID-1 は WAAS でサポートされた唯一の RAID タイプです)。
Type	RAID タイプ (たとえば、RAID-1)
Status	RAID デバイスの動作ステータス。ステータスには、NORMAL OPERATION または REBUILDING が含まれます
Physical devices and status	ディスク番号とディスクの動作ステータス ([GOOD] または [BAD] など)

関連コマンド

[show disks](#)[show version](#)

show hosts

WAAS デバイスのホストを表示するには、**show hosts EXEC** コマンドを使用します。

show hosts

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン 次の **show hosts** コマンドは、ネームサーバと対応する IP アドレスをリストします。また、ホストテーブルサマリーとして、ホスト名、対応する IP アドレス、および対応するエイリアス（該当する場合）もリストします。

例 表 3-38 では、**show hosts** 出力のフィールドについて説明します。

表 3-38 show hosts コマンドのフィールドの説明

フィールド	説明
Domain names	IP アドレスを解決するために WAE が使用するドメイン名
Name Server(s)	Domain Name System (DNS; ドメインネームシステム) ネームサーバの IP アドレス
ホストテーブル	
hostname	現在のデバイスの FQDN (ホスト名およびドメイン)
inet address	現在のホストデバイスの IP アドレス
aliases	host グローバルコンフィギュレーションコマンドに基づき、現在のデバイス用に設定された名前

show inetd

WAAS デバイスの TCP/IP サービスのステータスを表示するには、**show inetd EXEC** コマンドを使用します。

show inetd

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン **show inetd EXEC** コマンドは、WAAS デバイスで TCP/IP サービスがイネーブルであるか、ディセーブルであるかのステータスを表示します。Trivial File Transfer Protocol (TFTP) は WAAS ではサポートされないため、TFTP サービス ステータスを無視できます。

例 表 3-39 では、**show inetd** 出力のフィールドについて説明します。

表 3-39 show inetd コマンドのフィールドの説明

フィールド	説明
Inetd service configurations:	
ftp	FTP サービスがイネーブルかディセーブルかどうかのステータス
rcp	RCP サービスがイネーブルかディセーブルかどうかのステータス
tftp	TFTP サービスがイネーブルかディセーブルかどうかのステータス

関連コマンド [\(config\) inetd enable](#)

show interface

WAAS デバイスのハードウェア インターフェイス情報を表示するには、**show interface EXEC** コマンドを使用します。

```
show interface {GigabitEthernet slot/port} | {ide control_num} | {InlineGroup slot/grpnumber} |
               {InlinePort slot/grpnumber/{lan | wan}} | {PortChannel port-num} | {scsi device_num}
               | {Standby group_num | usb}
```

シンタックスの説明

GigabitEthernet	ギガビット イーサネット インターフェイスのデバイス情報を表示します (適切に装備されたシステム上のみ)。
<i>slot/port</i>	ギガビット イーサネット インターフェイスのスロットおよびポート番号。スロットの範囲は 0 ~ 3 で、ポートの範囲は 0 ~ 3 です。スロットおよびポート番号はスラッシュ (/) で区切ります。
ide	IDE インターフェイスのデバイス情報を表示します。
<i>control_num</i>	IDE コントローラ番号 (0 ~ 1)
InlineGroup	インライン グループ情報を表示します。
<i>slot/grpnumber</i>	選択したインターフェイスのスロットおよびインライン グループ番号
InlinePort	インライン ポート情報を表示します。
<i>slot/grpnumber/</i>	選択したインターフェイスのスロットおよびインライン グループ番号
lan	LAN ポートのインライン ポート情報を表示します。
wan	WAN ポートのインライン ポート情報を表示します。
PortChannel	ポート チャネル インターフェイスのデバイス情報を表示します。
<i>port-num</i>	ポート チャネル インターフェイスのポート番号 (1 ~ 2)
scsi	SCSI インターフェイスのデバイス情報を表示します。
<i>device_num</i>	SCSI デバイス番号 (0 ~ 7)
Standby	スタンバイ グループ情報を表示します。
<i>group_num</i>	スタンバイ グループ番号 (1 ~ 4)
usb	USB インターフェイスのデバイス情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

例 表 3-40 では、`show interface GigabitEthernet` 出力のフィールドについて説明します。

表 3-40 show interface GigabitEthernet コマンドのフィールドの説明

フィールド	説明
Description	description option of the interface 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設定されたデバイスの説明
Type	インターフェイスのタイプ。常にイーサネットです。
Ethernet address	レイヤ 2 MAC アドレス
Internet address	このインターフェイスに設定されたインターネット IP アドレス
Broadcast address	このインターフェイスに設定されたブロードキャストアドレス
Netmask	このインターフェイスに設定されたネットマスク
Maximum Transfer Unit Size	現在設定された Maximum Transfer Unit (MTU) の値
Metric	インターフェイスのメトリック設定。デフォルトは 1 です。最適なルートを決定するために、ルーティング メトリックはルーティング プロトコルによって使用されます。メトリックは、宛先ネットワークまたはホストへの追加ホップとしてカウントされます。メトリック値が高いほどルートの優先度は低くなります。
Packets Received	このインターフェイスによって受信されるパケットの総数
Input Errors	このインターフェイス上の着信エラーの数
Input Packets Dropped	このインターフェイス上でドロップされた着信パケットの数
Input Packets Overruns	着信パケット オーバーラン エラーの数
Input Packets Frames	着信パケット フレーム エラーの数
Packet Sent	このインターフェイスから送信されたパケットの総数
Output Errors	発信パケット エラーの数
Output Packets Dropped	このインターフェイスによってドロップされた発信パケットの数
Output Packets Overruns	発信パケット オーバーラン エラーの数
Output Packets Carrier	発信パケット キャリア エラーの数
Output Queue Length	バイト単位の出力キューの長さ
Collisions	このインターフェイスでのパケット衝突の数
Interrupts	このインターフェイスでのパケット中断の数
Base address	基本的なアドレス。16 進数値
Flags	インターフェイス ステータス インジケータ。値には Up、Broadcast、Running、および Multicast が含まれます。
Mode	このインターフェイスの速度設定、送信モード、および送信速度

次の例は、WAE インライン ネットワーク アダプタで設定されたスロット 1 の inlineGroup 0 の情報を表示します。

```
WAE612# show interface inlineGroup 1/0
Interface is in intercept operating mode.
Standard NIC mode is off.
Disable bypass mode is off.
VLAN IDs configured for inline interception: All
Watchdog timer is enabled.
Timer frequency: 1600 ms.
Autoreset frequency 500 ms.
The watchdog timer will expire in 1221 ms.
```


表 3-41 では、**show interface InlinePort** 出力のフィールドについて説明します。

表 3-41 show interface InlinePort コマンドのフィールドの説明

フィールド	説明
Device name	インラインポート インターフェイスの識別情報番号 (eth0、eth1 など)
Packets Received	インラインポート インターフェイス上で受信されるパケットの総数
Packets Intercepted	代行受信されたパケットの総数 (TCP パケットのみが代行受信されます)
Packets Bridged	ブリッジングされるパケット数。代行受信されないパケットがブリッジングされます。
Packets Forwarded	インライン インターフェイスから送信されたパケット数
Packets Dropped	ドロップされたパケット数
Packets Received on native	ネイティブ (GigabitEthernet 1/0) インターフェイス上で受信され、インライン モジュールによって転送されたパケットの数
<i>n</i> flows through this interface	このインラインポート インターフェイス上でアクティブな TCP 接続の数
Ethernet Driver Status	
Type	インターフェイスのタイプ。常にイーサネットです。
Ethernet address	レイヤ 2 MAC アドレス
Maximum Transfer Unit Size	現在設定された MTU の値
Metric	インターフェイスのメトリック設定。デフォルトは 1 です。最適なルートを決定するために、ルーティング メトリックはルーティング プロトコルによって使用されます。メトリックは、宛先ネットワークまたはホストへの追加ホップとしてカウントされます。メトリック値が高いほどルートの優先度は低くなります。
Packets Received	このインターフェイスによって受信されるパケットの総数
Input Errors	このインターフェイス上の着信エラーの数
Input Packets Dropped	このインターフェイス上でドロップされた着信パケットの数
Input Packets Overruns	着信パケット オーバーラン エラーの数
Input Packets Frames	着信パケット フレーム エラーの数
Packet Sent	このインターフェイスから送信されたパケットの総数
Output Errors	発信パケット エラーの数
Output Packets Dropped	このインターフェイスによってドロップされた発信パケットの数
Output Packets Overruns	発信パケット オーバーラン エラーの数
Output Packets Carrier	発信パケット キャリア エラーの数
Output Queue Length	バイト単位の出力キューの長さ
Collisions	このインターフェイスでのパケット衝突の数
Base address	基本的なアドレス。16 進数値
Flags	インターフェイス ステータス インジケータ。値には Up、Broadcast、Running、および Multicast が含まれます。
Mode	このインターフェイスの速度設定、送信モード、および送信速度

表 3-42 では、`show interface PortChannel` 出力のフィールドについて説明します。

表 3-42 show interface PortChannel コマンドのフィールドの説明

フィールド	説明
Type	インターフェイスのタイプ。常にイーサネットです。
Ethernet address	レイヤ 2 MAC アドレス
Maximum Transfer Unit Size	現在設定された MTU の値
Metric	インターフェイスのメトリック設定。デフォルトは 1 です。ルーティング メトリックはルーティング プロトコルによって使用されます。メトリック値が高いほどルートの優先度が低くなります。メトリックは、宛先ネットワークまたはホストへの追加ホップとしてカウントされます。
Packets Received	このインターフェイスによって受信されるパケットの総数
Input Errors	このインターフェイス上の着信エラーの数
Input Packets Dropped	このインターフェイス上でドロップされた着信パケットの数
Input Packets Overruns	着信パケット オーバーランエラーの数
Input Packets Frames	着信パケット フレーム エラーの数
Packet Sent	このインターフェイスから送信されたパケットの総数
Output Errors	発信パケット エラーの数
Output Packets Dropped	このインターフェイスによってドロップされた発信パケットの数
Output Packets Overruns	発信パケット オーバーランエラーの数
Output Packets Carrier	発信パケット キャリア エラーの数
Output Queue Length	バイト単位の出力キューの長さ
Collisions	このインターフェイスでのパケット衝突の数
Flags	インターフェイス ステータス インジケータ。値には Up、Broadcast、Running、および Multicast が含まれます。

表 3-43 では、`show interface scsi` 出力のフィールドについて説明します。

表 3-43 show interface scsi コマンドのフィールドの説明

フィールド	説明
SCSI interface X	SCSI デバイス番号 X に関する情報。SCSI デバイスの製造、デバイス ID 番号、モデル番号、およびタイプを示します。

表 3-44 では、**show interface standby** 出力のフィールドについて説明します。

表 3-44 show interface standby コマンドのフィールドの説明

フィールド	説明
Standby Group	スタンバイ グループを識別する番号
説明	description option of the interface 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設定されたデバイスの説明
IP address, netmask	スタンバイ グループの IP アドレスおよびネットマスク
Member interfaces	スタンバイ グループのメンバー インターフェイス。スタンバイ グループの一部である物理 インターフェイスを示します。インターフェイスの定義を示します (GigabitEthernet 1/0 など)。
Active interface	現在、スタンバイ グループでアクティブであるインターフェイス

関連コマンド

[\(config\) interface](#)

[show running-config](#)

[show startup-config](#)

show inventory

WAAS デバイスのシステム コンポーネント情報を表示するには、**show inventory EXEC** コマンドを使用します。

show inventory

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン **show inventory EXEC** コマンドにより、WAAS デバイスの UDI を表示できます。ID 情報は、WAAS デバイスの不揮発性メモリに保存されています。

UDI は、製品のオペレーティング システムまたはネットワーク管理アプリケーションによって電子的にアクセスされ、固有のハードウェア デバイスの識別を可能にします。UDI のデータ整合性はお客様に不可欠です。WAAS デバイスの不揮発性メモリにプログラミングされている UDI は、製品ラベルおよび輸送用カートンのラベルに記載されている UDI と同じです。また、電子的手段で表示できるもの、およびお客様の目に触れるシステムやツールの UDI と同じです。現在は CLI でしか UDI にアクセスできません。SNMP が UDI 情報にアクセスすることはありません。

show tech-support EXEC コマンドを使用しても WAAS デバイスの UDI を表示できます。

例 表 3-45 では、**show inventory** 出力のフィールドについて説明します。

表 3-45 show inventory コマンドのフィールドの説明

フィールド	説明
PID	デバイスの製品識別 (ID) 番号
VID	デバイスのバージョン ID 番号。バージョン番号が使用できない場合、0 と表示されます。
SN	デバイスのシリアル番号

関連コマンド [show tech-support](#)

show ip access-list

WAAS デバイスの特定のインターフェイスまたはアプリケーションに対して定義、適用されるアクセス リストを表示するには、**show ip access-list EXEC** コマンドを使用します。

```
show ip access-list [acl-name | acl-num]
```

シンタックスの説明

<i>acl-name</i>	(オプション) 文字で始まる最大 30 文字の英数字の識別情報を使用する、特定のアクセス リストの情報
<i>acl-num</i>	(オプション) 数値の識別情報 (標準アクセス リストの場合は 0 ~ 99、拡張アクセス リストの場合は 100 ~ 199) を使用する、特定のアクセス リストの情報

デフォルト

すべての定義済みアクセス リストに関する情報を表示します。

コマンドモード

EXEC

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

WAAS デバイスで定義されているアクセス リストを表示するには、**show ip access-list EXEC** コマンドを使用します。名前または番号で特定のアクセス リストを識別しない限りは、次のセクションを含めて、すべての定義済みアクセス リストに関する情報が表示されます。

- 新しいリストおよび条件に利用可能なスペース
- 定義済みアクセス リスト
- インターフェイスおよびアプリケーションによる参照

例

表 3-46 では、**show ip access-list** 出力のフィールドについて説明します。

表 3-46 show ip access-list コマンドのフィールドの説明

フィールド	説明
利用可能なスペース	
XX access lists	許可された最大 50 のリストのうち残っているアクセス リストの数
XXX access list conditions	許可された最大 500 の条件のうち残っているアクセス リスト条件の数
Standard IP access list	設定された標準 IP アクセス リスト名。このリストに設定された条件のリストを表示します。
Extended IP access list	設定された拡張 IP アクセス リスト名。このリストに設定された条件のリストを表示します。

表 3-46 show ip access-list コマンドのフィールドの説明 (続き)

フィールド	説明
Interface access list references	<p>インターフェイスのリストと、インターフェイスが関連付けられたアクセスリスト。次のフォーマットで表示されます。</p> <p><i>interface slot/port</i></p> <p><i>interface direction</i></p> <p><i>access list number</i></p>
Application access list references	<p>アプリケーションのリストと、アプリケーションが関連付けられたアクセスリスト。次のフォーマットで表示されます。</p> <p><i>application type</i></p> <p><i>access list type and number</i></p> <p><i>associated port</i></p>

関連コマンド
clear**(config) ip access-list**

show ip routes

WAAS デバイスの IP ルーティング テーブルを表示するには、**show ip routes EXEC** コマンドを使用します。

show ip routes

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン このコマンドは IP ルート テーブルを表示します。これは WAE 上で設定された異なるルートのすべてをリストします。WAE はこのテーブルを使用して、ネクストホップを判別します。このテーブルには、WAE GigabitEthernet インターフェイス、ユーザ設定されたスタティック ルート、およびデフォルト ゲートウェイからのルートが含まれます。このテーブルの最後の行はデフォルトルートを示します。

例 表 3-47 では、**show ip routes** 出力のフィールドについて説明します。

表 3-47 show ip routes コマンドのフィールドの説明

フィールド	説明
Destination	ルートごとの宛先 IP アドレス
Gateway	ルートごとのゲートウェイアドレス
Netmask	ルートごとのネットマスク
Number of route cache entries	ルート キャッシュのエントリ数 ルート キャッシュは個別のエンティティで、このフィールドは IP ルート テーブルのエントリと関連付けられていません。ルート キャッシュのエンティティ数はオープンである接続の数によって異なります。

関連コマンド (config) ip
(config-if) ip

show kerberos

WAAS デバイスの Kerberos 認証設定を表示するには、**show kerberos EXEC** コマンドを使用します。

show kerberos

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン WAAS デバイスで発生したイベントに関する情報を表示するには、システム メッセージ ログを使用します。 *syslog.txt* ファイルは、*/local1* ディレクトリに格納されています。

例 表 3-48 では、**show kerberos** 出力のフィールドについて説明します。

表 3-48 show Kerberos コマンドのフィールドの説明

フィールド	説明
Kerberos の設定	
Local Realm	ローカル レalm 名
DNS suffix	レalm の DNS サフィックス
Realm for DNS suffix	このレalm の一部であるコンピュータの DNS アドレス
Name of host running KDC for realm	レalm の Key Distribution Center (KDC; 鍵発行局) を実行するホストの名前
Master KDC	プライマリまたはメイン KDC
Port	クライアントからの着信要求用に Kerberos サーバが使用するポート。デフォルトはポート 88 です。

関連コマンド [clear](#)

[\(config\) logging](#)

show key-manager

各 WAAS デバイスのキー マネージャ情報を表示するには、**show key-manager EXEC** コマンドを使用します。

```
show key-manager {key | status}
```

シンタックスの説明

key	Central Manager に登録されている各 WAE デバイスのキー マネージャの詳細情報を表示します。
status	暗号化ステータス情報全体を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

central-manager

例

表 3-49 では、**show key-manager key** 出力のフィールドについて説明します。

表 3-49 show key-manager key コマンドのフィールドの説明

フィールド	説明
WAE Device	デバイス名
Key ID	暗号キー ID 番号
Creation Time	キーが作成された日時
Encryption Algorithm	暗号化アルゴリズム

関連コマンド

[show statistics key-manager](#)

show logging

WAAS デバイスのシステム メッセージ ログ設定を表示するには、**show logging** EXEC コマンドを使用します。

show logging

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン WAAS デバイスで発生したイベントに関する情報を表示するには、システム メッセージ ログを使用します。*syslog.txt* ファイルは、*/local1* ディレクトリに格納されています。

例 次の例は、WAAS デバイス上の Syslog ホスト設定を表示します。

```
WAE# show logging
Syslog to host is disabled
Priority for host logging 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 disk file recycle size is set to 1000000
```

関連コマンド [clear](#)
[\(config\) logging](#)
[show sysfs volumes](#)

show memory

WAAS デバイスのメモリ ブロックおよび統計情報を表示するには、**show memory EXEC** コマンドを使用します。

show memory

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-50 では、**show memory** 出力のフィールドについて説明します。

表 3-50 show memory コマンドのフィールドの説明

フィールド	説明
Total physical memory	KB 単位の物理メモリの総量
Total free memory	総利用可能メモリ (KB 単位)
Total buffer memory	メモリ バッファのメモリ総量 (KB 単位)
Total cached memory	メモリ キャッシュのメモリ総量 (KB 単位)
Total swap	スワップ用途のメモリ総量 (KB 単位)
Total free swap	スワップ用途に利用可能な総メモリ (KB 単位)

show ntp

WAAS デバイスの NTP パラメータを表示するには、**show ntp EXEC** コマンドを使用します。

show ntp status

シンタックスの説明

status NTP ステータスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

例

表 3-51 では、**show ntp status** 出力のフィールドについて説明します。

表 3-51 show ntp status コマンドのフィールドの説明

フィールド	説明
NTP	NTP がイネーブルかディセーブルかを示します。
server list	NTP サーバ IP およびサブネット アドレス
remote	リモート NTP サーバの名前 (最初の 15 文字)
*	remote のカラムで、クロックを同期化するシステム ピアを識別します。
+	remote のカラムで、NTP 同期化に有効または適格なピアを識別します。
space	remote のカラムで、ピアが拒否されたことを示します (ピアは NTP サーバに到達できないか、到達の際、過度の遅延が発生しています)。
x	remote のカラムで、失敗したティックを示します。NTP サーバは、これを無視します。
-	remote のカラムで、クロックの許容制限を超えた読み込みを示します。NTP サーバは、これを無視します。
refid	リモート NTP サーバを同期化するクロック リファレンス ID
st	クロック サーバストラタムまたはレイヤ。この例では、ストラタム 1 は上位レイヤです。
t	ピアのタイプ (l (ローカル)、 u (ユニキャスト)、 m (マルチキャスト)、 b (ブロードキャスト))
when	サーバから最後のパケットを受信したタイミングを秒単位で示します。
poll	時間チェックまたは相関ポーリング インターバル (秒単位)
reach	8 ビット到達可能性レジスタ。最後のポーリング インターバル中にサーバに到達可能な場合は 1 が記録され、そうでない場合は 0 が記録されます。8 進数値 377 以上は、ポーリングがすべてサーバに到達したことを示します。
delay	要求側とサーバ間の推定遅延 (ミリ秒単位)

表 3-51 show ntp status コマンドのフィールドの説明 (続き)

フィールド	説明
offset	サーバを基準としたクロック オフセット
jitter	クロック ジッタ

関連コマンド[clock](#)[\(config\) clock](#)[\(config\) ntp](#)

show policy-engine application

WAE のアプリケーション ポリシー情報を表示するには、**show policy-engine application EXEC** コマンドを使用します。

```
show policy-engine application {classifier [app-classifier] | dynamic | name}
```

シンタックスの説明

classifier	指定されたアプリケーション分類機能に関する情報を表示します。分類機能を指定しないと、このコマンドはすべての分類機能に関する情報を表示します。単一一致を持つすべてのアプリケーション分類機能が 1 行に表示されます。
<i>app-classifier</i>	(オプション) アプリケーション分類機能の名前。名前は 30 文字以内です。
dynamic	アプリケーション動的一致情報を示します。
name	アプリケーション名リストを示します。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

リストに追加する自動検出 CIFS ファイル サーバを表示するには、**show policy-engine application dynamic** コマンドを使用します。サーバは、アクティビティが終了したあと、制限された時間（デフォルトでは 3 分）の間ダイナミック リストに表示され、別のクライアント要求により再度自動検出されるまで、ダイナミック リストからドロップされます。

例

表 3-52 では、**show policy-engine application classifier** 出力のフィールドについて説明します。

表 3-52 show policy-engine application classifier コマンドのフィールドの説明

フィールド	説明
Number of Application Classifiers:	設定されたアプリケーション分類機能の数
0 to N	アプリケーション名と、どのトラフィックに関心があるかを決定する一致ステートメントを含んだ番号付きのリスト。たとえば、 <pre>0) AFS match dst port range 7000 7009 1) Altiris-CarbonCopy match dst port eq 1680</pre>

表 3-53 では、`show policy-engine application dynamic` 出力のフィールドについて説明します。

表 3-53 show policy-engine application dynamic コマンドのフィールドの説明

フィールド	説明
ダイナミック一致フリーリスト情報	
Allocated	割り当て可能なダイナミック ポリシーの総数
In Use	現在使用しているダイナミック一致の数
Max In Use	最後のレポート以降に使用したダイナミック一致の最大数
Allocations	ダイナミック一致エントリが追加された回数
Individual Dynamic Match Information:	ダイナミック アプリケーション用に内部設定された一致値を表示します。ダイナミック アプリケーションは割り当てられたポートをスタティックに使用しませんが、ポートがアプリケーショントラフィックを処理するようネゴシエートします。
Number	リストの一致条件の数
Type	一致するトラフィックのタイプ。たとえば、Any-->Local は、送信元からローカル WAE へのトラフィックをテストします。
User Id	エントリを挿入したアクセラレータの数
Src	送信元の一致条件の値。値は ANY、LOCAL、IP アドレス、またはアプリケーションが適用されるポートです。
Dst	宛先一致条件の値。値は ANY、LOCAL、IP アドレス、またはアプリケーションが適用されるポートです。
Map Name	ダイナミック一致エントリが接続と一致した場合に呼び出されるポリシー エンジン アプリケーション マップ
Flags	異なる接続処理オプションを指定する動作フラグ
Seconds	ダイナミック一致エントリが終了する制限時間として指定された秒数
Remaining	ダイナミック一致エントリが期限切れになり、削除されるまでの残りの秒数
Hits	一致した接続の数

表 3-54 では、**show policy-engine application name** 出力のフィールドについて説明します。

表 3-54 show policy-engine application name コマンドのフィールドの説明

フィールド	説明
Number of Applications:X	デフォルト アプリケーションすべてを含んだ、WAE で定義されたアプリケーションの数。WAAS には 150 を越えるデフォルトのアプリケーション ポリシーが含まれます (デフォルト アプリケーション ポリシーのリストについては、『Cisco Wide Area Application Services Configuration Guide』の付録 A を参照してください)。 次に、名前別に WAE で定義された各アプリケーションを示します。
1) Authentication (15)	アプリケーション名と数値の内部 ID。ポリシー エンジンでアプリケーション名を管理するのに使用します。
2) Backup (18)	
3) Call-Management (17)	
4) Conferencing (8)	
5) Console (4)	
6) Content-Management (21)	
7) Directory-Services (6)	
8) Email-and-Messaging (12)	
9) Enterprise-Applications (13)	
10) File-System (2)	
11) File-Transfer (16)	
12) Instant-Messaging (22)	
13) Name-Services (25)	
14) Network-Analysis (26)	
15) P2P (7)	
16) Printing (14)	
17) Remote-Desktop (5)	
18) Replication (20)	
19) SQL (1)	
20) SSH (24)	
21) Storage (27)	
22) Streaming (11)	
23) Systems-Management (3)	
24) VPN (23)	
25) Version-Management (9)	
26) WAFS (10)	
27) Web (19)	
28) Other (0)	

関連コマンド

(config) policy-engine application classifier
(config) policy-engine application map adaptor EPM
(config) policy-engine application map adaptor WAFS transport
(config) policy-engine application map basic delete
(config) policy-engine application map basic disable
(config) policy-engine application map basic insert
(config) policy-engine application map basic list
(config) policy-engine application map basic move
(config) policy-engine application map basic name
(config) policy-engine application map other optimize DRE
(config) policy-engine application map other optimize full
(config) policy-engine application map other pass-through
(config) policy-engine application name
(config) policy-engine config

show policy-engine status

WAE のポリシー エンジンに関する高度な情報を表示するには、**show policy-engine status EXEC** コマンドを使用します。この情報にはアプリケーション名、分類機能および条件など利用可能なリソースの使用状況が含まれます。

show policy-engine status

コマンド モード EXEC

デバイス モード application-accelerator

例 表 3-55 では、**show policy-engine status** 出力のフィールドについて説明します。

表 3-55 show policy-engine status コマンドのフィールドの説明

フィールド	説明
Policy-engine resources usage:	表のカラムは Total、Used、および Available です。
Application names	アプリケーション名の総数。使用するアプリケーション名の数。利用可能なアプリケーション名の数
Classifiers	設定された分類機能の総数。使用する分類機能の数。利用可能な分類機能の数。許可された分類機能の最大数は 512 です。
Conditions	設定された条件の総数。使用する条件の数。利用可能な条件の数。許可された一致条件の最大数は 1024 です。
Policies	設定されたポリシーの総数。使用するポリシーの数。利用可能なポリシーの数。許可されたポリシーの最大数は 512 です。

関連コマンド

- [\(config\) policy-engine application classifier](#)
- [\(config\) policy-engine application map adaptor EPM](#)
- [\(config\) policy-engine application map adaptor WAFS transport](#)
- [\(config\) policy-engine application map basic delete](#)
- [\(config\) policy-engine application map basic disable](#)
- [\(config\) policy-engine application map basic insert](#)
- [\(config\) policy-engine application map basic list](#)
- [\(config\) policy-engine application map basic move](#)
- [\(config\) policy-engine application map basic name](#)
- [\(config\) policy-engine application map other optimize DRE](#)
- [\(config\) policy-engine application map other optimize full](#)
- [\(config\) policy-engine application map other pass-through](#)
- [\(config\) policy-engine application name](#)
- [\(config\) policy-engine config](#)

show print-services

WAAS デバイス上の設定権限、プリント サービスまたはプリント サービス プロセスにアクセスできる管理ユーザを表示するには、**show print-services EXEC** コマンドを使用します。

```
show print-services {drivers user username | process}
```

シンタックスの説明

process	プリント サーバおよびプリント スプーラに関する情報を表示します。
drivers	このプリント サーバのプリンタ ドライバを表示します。
user <i>username</i>	プリント管理グループに所属するユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

例

表 3-56 では、**show print-services process** 出力のフィールドについて説明します。

表 3-56 show print-services process コマンドのフィールドの説明

フィールド	説明
Print server is running.	プリント サーバの動作ステータス
Print spooler is running.	プリント スプーラの動作ステータス
プリント サーバのステータス	
Samba version 3.0.20	使用する Samba バージョン
PID	プロセス ID。WAE Linux アプライアンス上の Samba プロセスのプロセス ID 番号
Username	Samba プロセスを開始した UNIX ユーザ
Group	ユーザが所属する UNIX グループ
Machine	マシン名と IP アドレス。マシン名は NetBIOS 名と同じです。
Service	プリント サーバに接続するため、クライアントが使用する Remote procedure call (RPC; リモート プロシージャ コール) ポート。値は常に IPCS です。
pid	プロセス ID。WAE Linux アプライアンス上の Samba プロセスのプロセス ID 番号
machine	マシン名
Connected at	プリント サーバに接続する日時
No locked files	コメント行

表 3-56 show print-services process コマンドのフィールドの説明 (続き)

フィールド	説明
プリント スプーラのステータス	
scheduler is running	プリント スプーラ スケジューラの動作ステータス
system default destination	WAAS デフォルトプリント宛先 (VistaPrinterOnWAAS)
device for (VistaPrinterOnWAAS)	システム デフォルト プリント宛先のソケット アドレス
(VistaPrinterOnWAAS) accepting requests	システム デフォルト プリント宛先のアベイラビリティ ステータス
printer (VistaPrinterOnWAAS) is idle. enabled	システム デフォルト プリンタの動作ステータス

関連コマンド[\(config\) authentication](#)[\(config\) print-services](#)[show authentication](#)[windows-domain](#)[\(config\) windows-domain](#)

show processes

WAAS デバイスの CPU またはメモリ プロセスを表示するには、**show processes EXEC** コマンドを使用します。

```
show processes [cpu | debug pid | memory | system [delay 1-60 | count 1-100]]
```

シンタックスの説明

cpu	(オプション) CPU 利用率を表示します。
debug	(オプション) 指定されたプロセス識別情報のシステム コールと信号トレースを印刷して、システムの進行状況を表示します。
<i>pid</i>	プロセス ID
memory	(オプション) メモリ割り当てプロセスを表示します。
system	(オプション) アップデートに関してシステムのロード情報を表示します。
delay	(オプション) アップデート間の遅延を秒単位で指定します (1 ~ 60)。
count	(オプション) 表示されるアップデートの数を指定します (1 ~ 100)。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

ここに示す EXEC コマンドを使用して、システムの CPU 利用率を追跡して分析します。

show processes debug コマンドは、各プロセスによって作成された各システムコール (引数付き) の拡張内部システム コール情報と詳細なアカウント、および受信した信号を表示します。

show processes system コマンドを使用して、アップデートに関するシステムのロード情報を表示します。**delay** オプションは、アップデート間の遅延を秒単位で指定します。The **count option specifies the number of updates that are displayed.** このコマンドは次の項目を表示します。

- ワイド形式でのすべてのプロセスのリスト
- CPU リソースを利用するプロセスをリストした 2 つのテーブル。最初のテーブルは、CPU リソースの利用率の降順でのプロセスのリストを表示します。このリストは、プロセス システム (ps) 出力が表示されたあとに取られたスナップショットに基づきます。第 2 のテーブルは、最初のスナップショットの 5 秒後に取られたスナップショットに基づいて同じプロセスを表示します。
- 対応するプロセスが、1 秒で区切った一連の 5 つのスナップショットで使用する仮想メモリ。



(注)

これらのコマンドを使用すると、CPU 利用率とシステム パフォーマンスは深刻な影響を受けます。したがって、これらのコマンド、特に、**show processes debug** コマンドは、絶対に必要な場合以外には、使用しないようにしてください。

例 表 3-57 では、**show processes** 出力のフィールドについて説明します。

表 3-57 show processes コマンドのフィールドの説明

フィールド	説明
CPU Usage	ユーザ、システム オーバーヘッド、およびアイドルの各割合を示した CPU 利用率
PID	プロセス識別情報
STATE	対応するプロセスの現在の状態 R = 稼働中 S = 割り込み待機でスリープ状態 D = 割り込み以外の待機でスリープ状態またはスワッピング Z = ゾンビ T = 信号でトレースまたは停止
PRI	プロセスのプライオリティ
User T	ユーザ時間の使用量 (秒単位)
Sys T	システム時間の使用量 (秒単位)
COMMAND	プロセス コマンド
Total	総利用可能メモリ (バイト単位)
Used	現在使用されているメモリ (バイト単位)
Free	利用可能な空きメモリ (バイト単位)
Shared	現在使用されている共有メモリ (バイト単位)
Buffers	現在使用されているバッファ メモリ (バイト単位)
Cached	現在使用されているキャッシュ メモリ (バイト単位)
SwapTotal	スワップ用途に利用可能な総メモリ (バイト単位)

show radius-server

WAAS デバイスの RADIUS 設定情報を表示するには、**show radius-server EXEC** コマンドを使用します。

show radius-server

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-58 では、**show radius-server** 出力のフィールドについて説明します。

表 3-58 show radius-server コマンドのフィールドの説明

フィールド	説明
Login Authentication for Console/ Telnet Session	RADIUS サーバが、ログイン認証に対してイネーブルになっているかどうかを示します。
Configuration Authentication for Console/ Telnet Session	RADIUS サーバが、許可または設定認証に対してイネーブルになっているかどうかを示します。
Authentication scheme fail-over reason	プライマリ管理ログイン認証方式が失敗した場合はいつでも、管理ログイン認証のセカンダリ方式に WAAS デバイスがフェールオーバーするかどうかを示します。
RADIUS Configuration	RADIUS 認証設定
Key	RADIUS クライアント (WAAS デバイス) と RADIUS サーバ間のすべての通信の暗号化と認証に使用するキー
Timeout	WAAS デバイスが、タイムアウトを宣言するまで、指定された RADIUS 認証サーバからの応答を待つ秒数
Servers	WAAS デバイスが RADIUS 認証に使用する RADIUS サーバ
IP	RADIUS サーバのホスト名または IP アドレス
Port	RADIUS サーバが受信しているポート番号

関連コマンド (config) radius-server

show running-config

端末に WAAS デバイスの現在の実行コンフィギュレーション情報を表示するには、**show running-config** EXEC コマンドを使用します。このコマンドは **write terminal** コマンドに代わるものです。

show running-config

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン この EXEC コマンドは **show startup-config** コマンドと組み合わせて使用し、稼動中のメモリの情報と、起動中に使用される startup-config とを比較します。

例 次の例は、WAAS デバイスの現在実行中のコンフィギュレーションを表示します。

```
WAE# show running-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname waas-cm
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
...
```

関連コマンド [configure](#)
[copy running-config](#)
[copy startup-config](#)

show services

WAAS デバイスのサービス関連情報を表示するには、**show services EXEC** コマンドを使用します。

```
show services {ports [port-num] | summary}
```

シンタックスの説明

ports	サービスをポート番号別に表示します。
<i>port-num</i>	(オプション) 最大 8 つのポート番号 (1 ~ 65535)
summary	サービス要約を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

例

次の例は、サービスの要約を表示します。

```
WAE# show services summary
```

```
Service          Ports
-----
                CMS          1100 5256
                NLM          4045
                WAFS          1099
                emdb          5432
                MOUNT          3058
                MgmtAgent      5252
                WAFS_tunnel    4050
                CMS_db_vacuum    5257
```

show smb-conf

Samba 設定ファイル *smb.conf* の WAAS デバイスの現在値を表示するには、**show smb-conf EXEC** コマンドを使用します。

show smb-conf

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン このコマンドは、トラブルシューティングの目的で、*smb.conf* ファイルの `global`、`print$`、および `printers` パラメータの値を表示します。これらのパラメータの説明とその値については、[「\(config\) smb-conf」](#) コマンドを参照してください。

例 次の例は、現在の設定におけるすべてのパラメータ値を表示します。

```
WAE# show smb-conf

Current smb-conf configurations -->

smb-conf section "global" name "ldap ssl" value "start_tls"
smb-conf section "printers" name "printer admin" value "root"

Output of current smb.conf file on disk -->

=====

# File automatically generated

[global]
idmap uid = 70000-200000
idmap gid = 70000-200000
winbind enum users = no
winbind enum groups = no
winbind cache time = 10
winbind use default domain = yes
printcap name = cups
load printers = yes
printing = cups
cups options = "raw"
force printername = yes
lpq cache time = 0
log file = /local/local1/errorlog/samba.log
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
smb ports = 50139
```

```
local master = no
domain master = no
preferred master = no
dns proxy = no
template homedir = /local/local1/
template shell = /admin-shell
ldap ssl = start_tls
comment = Comment:
netbios name = MYFILEENGINE
realm = ABC
wins server = 10.10.10.1
password server = 10.10.10.10
security = domain

[print$]
path = /state/samba/printers
guest ok = yes
browseable = yes
read only = yes
write list = root

[printers]
path = /local/local1/spool/samba
browseable = no
guest ok = yes
writable = no
printable = yes
printer admin = root

=====
```

関連コマンド

[\(config\) smb-conf](#)

[windows-domain](#)

[\(config\) windows-domain](#)

show snmp

WAAS デバイスの SNMP 通信のステータスを確認するには、**show snmp EXEC** コマンドを使用します。

```
show snmp {alarm-history | engine ID | event | group | stats | user}
```

シンタックスの説明

alarm-history	SNMP アラーム履歴情報を表示します。
engineID	ローカル SNMP エンジンの ID を表示します。
event	Event MIB を介して設定されたイベントを表示します。
group	SNMP グループを表示します。
stats	SNMP 統計情報を表示します。
user	SNMP ユーザを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドは、さまざまな SNMP 変数に関する情報と、SNMP 動作に関する統計情報を提供します。

例

表 3-59 では、**show snmp alarm-history** 出力のフィールドについて説明します。

表 3-59 show snmp alarm-history コマンドのフィールドの説明

フィールド	説明
Index	リストされているアラームのシリアル番号を表示します。
Type	アラームが発生 (R) したかクリア (C) されたかを示します。
Sev	アラーム重大度のレベル: クリティカル (Cr)、メジャー (Ma)、マイナー (Mi)
Alarm ID	WAE によって送信されるトラップには、数値のアラーム ID が含まれます。
ModuleID	WAE によって送信されるトラップには、数値のモジュール ID が含まれます (モジュール名をモジュール ID にマップする場合は、表 3-60 を参照してください)。
Category	WAE によって送信されるトラップには、数値のカテゴリ ID が含まれます (カテゴリ名をカテゴリ ID にマップする場合は、表 3-61 を参照してください)。
Descr	WAAS ソフトウェア アラームとアラームを生成したアプリケーションの説明を提供します。

表 3-60 では、モジュール ID へのモジュール名のマッピングを要約します。

表 3-60 モジュール名の ID 番号への要約

モジュール名	モジュール ID
AD_DATABASE	8000
NHM	1
NHM/NHM	2500
nodemgr	2000
standby	4000
sysmon	1000
UNICAST_DATA_RECEIVER	5000
UNICAST_DATA_SENDER	6000

表 3-61 では、カテゴリ ID へのカテゴリ名のマッピングを要約します。

表 3-61 カテゴリ名の ID 番号への要約

カテゴリ名	カテゴリ ID
Communications	1
Service Quality	2
Processing Error	3
Equipment	4
Environment	5
Content	6

表 3-62 では、**show snmp engineID** 出力のフィールドについて説明します。

表 3-62 show snmp engineID コマンドのフィールドの説明

フィールド	説明
Local SNMP Engine ID	ローカルデバイス上の SNMP のコピーを識別するストリング

表 3-63 では、**show snmp event** 出力のフィールドについて説明します。**show snmp event** コマンドは、「snmp trigger」コマンドを使用して設定された SNMP イベントに関する情報を表示します。

表 3-63 show snmp event コマンドのフィールドの説明

フィールド	説明
Mgmt Triggers	管理トリガーの出力。1、2、3 などの番号で識別されます。
(1): Owner:	トリガーを設定した人物の名前。「CLI」はデフォルトのオーナーです。システムには設定されたデフォルトのトリガーがあります。
(1):	トリガーの名前。この名前はローカルに一意で、管理上割り当てられています。たとえば、このフィールドには「isValid」というトリガー名が含まれています。番号は、 show 出力にリストされた最初の管理トリガーであることを示します。
Comment:	トリガーの機能および使用方法の説明。たとえば、WAFS ライセンスファイルは有効ではありません。

表 3-63 show snmp event コマンドのフィールドの説明 (続き)

フィールド	説明
Sample:	テスト サンプルを評価する基準。たとえば、Abs (Absolute) または Delta です。
Freq:	頻度。トリガーのサンプリングを待機する秒数。サンプリングでの一貫性を推奨するため、チェックの開始から次のチェックの開始までのインターバルを測定し、チェックが完了したときではなく、期限が満了するとただちにタイマーを再開します。
Test:	設定された SNMP トリガーに基づいて実行するトリガー検査のタイプ。Test フィールドには次の検査タイプが含まれます。 Absent — 不在検査 Boolean — ブール値検査 Equal — 等価しきい値検査 Falling — 下限しきい値検査 Greater-than — しきい値を越える検査 Less-than — しきい値未満の検査 On-change — 変動の有無についての検査 Present — 存在検査 Rising — 上限しきい値検査
ObjectOwner:	snmp trigger create グローバル コンフィギュレーション コマンドまたは SNMP インターフェイスを使用してトリガーを作成したオブジェクト オーナーの名前。「CLI」はデフォルトのオーナーです。
Object:	オブジェクトを識別するストリング ブール エントリ
Value:	トリガーを実行するかどうかを判断するためサンプリングする MIB オブジェクトの object identifier (OID; オブジェクト ID)
Cmp:	比較。実行するブール比較のタイプ。1 ~ 6 の番号は次のブール比較に対応します。 unequal (1) equal (2) less (3) lessOrEqual (4) greater (5) greaterOrEqual (6)
Start:	このインスタンスを発生させる開始値
ObjOwn:	オブジェクト オーナー
Obj:	オブジェクト
EveOwn:	イベント オーナー
Eve:	イベント。SNMP イベントのタイプ。たとえば、CLI_EVENT です。
Delta Value Table:	デルタ サンプリングに関するトリガー情報を含んだテーブル

表 3-63 show snmp event コマンドのフィールドの説明 (続き)

フィールド	説明
(0):	
Thresh:	トリガー タイプがしきい値であるかチェックするしきい値
Exis:	実行する存在検査のタイプ。値は 1 または 0 です。
Read:	MIB インスタンスがクエリーされたかどうかを示します。
OID:	オブジェクト ID (MIB インスタンスと同じ)
val:	値の ID
(2):	トリガーが設定されている MIB インスタンス。これは、 show 出力に示された 2 番目の管理トリガーです。このフィールドは、この show コマンドで示されたインスタンスごとに繰り返されます。

表 3-64 では、**show snmp group** 出力のフィールドについて説明します。

表 3-64 show snmp group コマンドのフィールドの説明

フィールド	説明
groupname	SNMP グループの名前、または一般的なアクセス ポリシーを持ったユーザの集まり
security_model	グループが使用するセキュリティ モデル (v1、v2c、または v3 のいずれか)
readview	グループの読み取りビューを識別するストリング
writeview	グループの書き込みビューを識別するストリング
notifyview	グループの通知ビューを識別するストリング

表 3-65 では、**show snmp stats** 出力のフィールドについて説明します。

表 3-65 show snmp stats コマンドのフィールドの説明

フィールド	説明
SNMP packets input	入力された SNMP パケットの総数
Bad SNMP version errors	SNMP のバージョンが無効なパケットの数
Unknown community name	未知のコミュニティ名の SNMP パケットの数
Illegal operation for community name supplied	そのコミュニティで許可されていない動作を要求するパケットの数
Encoding errors	誤って符号化されている SNMP パケットの数
Number of requested variables	SNMP マネージャによって要求されている変数の数
Number of altered variables	SNMP マネージャによって変更されている変数の数
Get-request PDUs	受信した GET 要求の数
Get-next PDUs	受信した GET-NEXT 要求の数
Set-request PDUs	受信した SET 要求の数
SNMP packets output	ルータによって送信された SNMP パケットの総数
Too big errors	最大パケットサイズより大きな SNMP パケットの数
Maximum packet size	SNMP パケットの最大サイズ
No such name errors	存在しない MIB オブジェクトを指定した SNMP 要求の数

表 3-65 show snmp stats コマンドのフィールドの説明 (続き)

フィールド	説明
Bad values errors	MIB オブジェクトの無効な値を指定した SNMP SET 要求の数
General errors	その他のエラーが原因で失敗した SNMP SET 要求の数 (No such name error、Bad values error など特定されているエラー以外のエラー)
Response PDUs	要求に対応して送信された応答数
Trap PDUs	送信された SNMP トラップの数

表 3-66 では、`show snmp user` 出力のフィールドについて説明します。

表 3-66 show snmp user コマンドのフィールドの説明

フィールド	説明
User name	SNMP ユーザの名前を識別するストリング
Engine ID	デバイス上の SNMP のコピー名を識別するストリング
Group Name	SNMP グループの名前、または一般的なアクセス ポリシーを持ったユーザの集まり

関連コマンド

[\(config\) snmp-server community](#)
[\(config\) snmp-server contact](#)
[\(config\) snmp-server enable traps](#)
[\(config\) snmp-server group](#)
[\(config\) snmp-server host](#)
[\(config\) snmp-server location](#)
[\(config\) snmp-server mib persist event](#)
[\(config\) snmp-server notify inform](#)
[\(config\) snmp-server user](#)
[\(config\) snmp-server view](#)
[snmp trigger](#)

show ssh

WAAS デバイスの Secure Shell (SSH; セキュア シェル) サービスのステータスと設定情報を表示するには、**show ssh** EXEC コマンドを使用します。

show ssh

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-67 では、**show ssh** 出力のフィールドについて説明します。

表 3-67 show ssh コマンドのフィールドの説明

フィールド	説明
SSH server supports SSH2 protocol (SSH1 compatible).	プロトコルがステートメントをサポートします。
SSH service is not enabled.	SSH サービスがイネーブルであるかどうかのステータス
Currently there are no active SSH sessions.	アクティブな SSH セッションの数
Number of successful SSH sessions since last reboot:	最後のリブート以降、成功した SSH セッションの数
Number of failed SSH sessions since last reboot:	最後のリブート以降、失敗した SSH セッションの数
SSH key has not been generated or previous key has been removed.	SSH キーのステータス
SSH login grace time value is 300 seconds.	ログインに許可された時間
Allow 3 password guess(es).	許可されるパスワード推測の数

関連コマンド (config) ssh-key-generate

(config) sshd

show standby

WAAS デバイスのスタンバイ インターフェイスに関する情報を表示するには、**show standby EXEC** コマンドを使用します。

show standby

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン 特定のスタンバイ グループ設定に関する情報を表示するには、**show interface standby standby group_num EXEC** コマンドを入力します。

例 表 3-68 では、**show standby** 出力のフィールドについて説明します。

表 3-68 show standby コマンドのフィールドの説明

フィールド	説明
Standby Group	スタンバイ グループを識別する番号
説明	description option of the interface 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設定されたデバイスの説明
IP address	スタンバイ グループの IP アドレス
netmask	スタンバイ グループのネットマスク
Member interfaces	スタンバイ グループのメンバー インターフェイス。スタンバイ グループの一部である物理インターフェイスを示します。インターフェイスの定義を示します (GigabitEthernet 1/0 など)。
priority	各インターフェイスのプライオリティ ステータス
Active interface	現在、スタンバイ グループでアクティブであるインターフェイス
Maximum errors allowed on the active interface	アクティブ インターフェイス上で許可されたエラーの最大数

関連コマンド [show interface](#)

[show running-config](#)

[show startup-config](#)

[\(config-if\) standby](#)

show startup-config

WAAS デバイスの startup-config を表示するには、**show startup-config** EXEC コマンドを使用します。

show startup-config

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン この EXEC コマンドを使用して、初期起動中に使用される設定（NVRAM [不揮発性 RAM] にストア）を表示します。このコマンドと、**show running-config** コマンドの出力の違いに注意してください。

例 次の例は、WAAS デバイスの始動時に使用するために保存された設定を表示します。

```
WAE# show startup-config
! WAAS version 4.0.0
!
device mode central-manager
!
!
hostname Edge-WAE1
!
!
!
!
exec-timeout 60
!
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
 ip address 10.10.10.33 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
...
```

関連コマンド [configure](#)
[copy running-config](#)
[show running-config](#)

show statistics authentication

WAAS デバイスの認証統計情報を表示するには、**show statistics authentication EXEC** コマンドを使用します。

show statistics authentication

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン 記録された認証アクセス要求、拒否、許可の数を表示するには、**show statistics authentication** コマンドを使用します。

例 次の例は、WAAS デバイスでの認証に関連する統計情報を表示します。

```
WAE# show statistics authentication
Authentication Statistics
-----
Number of access requests:      115
Number of access deny responses: 12
Number of access allow responses: 103
```

関連コマンド [\(config\) authentication](#)
[clear](#)
[show authentication](#)

show statistics cifs

CIFS 統計情報を表示するには、**show statistics cifs EXEC** コマンドを使用します。

```
show statistics cifs {cache eviction | requests}
```

シンタックスの説明

cache	CIFS キャッシュの統計情報を表示します。
eviction	CIFS キャッシュ除去のステータスを表示します。
requests	CIFS 要求の統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

要求タイプ別に項目化された CIFS トラフィックの詳細を表示するには、**show statistics cifs EXEC** コマンドを使用します。このコマンドは、システムの使用方法を理解する場合に便利です。たとえば、要求にはデータ転送、ブラウジング、データベース アクティビティ、または他の目的のためのものなどがあります。トラブルシューティング目的で、これらの統計情報とパフォーマンス問題を関連付けられます。または、これらの統計情報を使用して、どの特定のパフォーマンス最適化を設定するかを決定することもできます。

例

表 3-69 では、**show statistics cifs requests** 出力のフィールドについて説明します。

表 3-69 show statistics cifs requests コマンドのフィールドの説明

フィールド	説明
Statistics gathering period	統計情報収集期間の時間、分、秒、およびミリ秒の数
Total	CIFS 要求の総数
Remote	ローカル キャッシュから処理されなかった CIFS 要求の数
ALL_COMMANDS	表示された CIFS コマンドすべてのエイリアス
total	すべてのコマンドの要求の総数
remote	すべてのコマンドのリモート要求の数
async	すべてのコマンドの async 要求の数
avg local	すべてのコマンドのローカル要求の平均時間 (ミリ秒単位)
avg remote	すべてのコマンドのリモート要求の平均時間 (ミリ秒単位)
CONNECT	接続チェック コマンド
total	このコマンドの要求の総数
remote	このコマンドのリモート要求の数
async	このコマンドの async 要求の数
avg local	このコマンドのローカル要求の平均時間 (ミリ秒単位)
avg remote	このコマンドのリモート要求の平均時間 (ミリ秒単位)

表 3-69 show statistics cifs requests コマンドのフィールドの説明 (続き)

フィールド	説明
NB_SESSION_REQ	NetBIOS セッション要求コマンド
VFN_LIVELINESS	Liveliness チェック コマンド

関連コマンド

[cifs](#)

[show cifs](#)

show statistics content-distribution-network

WAAS Central Manager に登録されている WAE または デバイス グループのステータスを表示するには、**show statistics content-distribution-network EXEC** コマンドを使用します。このコマンドは WAAS Central Manager だけで利用できます。

```
show statistics content-distribution-network device status device_id
```

シンタックスの説明

device status	WAAS Central Manager に登録されている WAE または デバイス グループのステータスを表示します。
device_id	デバイスまたはデバイス グループの名前または ID

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

central-manager

使用上のガイドライン

show statistics content-distribution-network EXEC コマンドを使用し、デバイス グループ内の WAE に関する ID 詳細情報を表示し、WAE がオンラインになっているか確認します。

例

次の例は、WAAS Central Manager に登録されている WAE の ID 詳細情報を表示します。

```
WAE# show statistics content-distribution-network device status edge-wae-11
Device id="CdmConfig_142" name="edge-wae-11" status="Online";
```

show statistics dre

WAE の Data Redundancy Elimination (DRE) 一般統計情報を表示するには、**show statistics dre EXEC** コマンドを使用します。

show statistics dre

コマンドモード EXEC

デバイスモード application-accelerator

例 表 3-70 では、**show statistics dre** 出力のフィールドについて説明します。このコマンドは、すべての接続の集約された統計情報を表示します。

表 3-70 show statistics dre コマンドのフィールドの説明

フィールド	説明
Cache	集約された DRE キャッシュ データ統計情報
Status	現在の DRE ステータス。Status 値には、Initializing、Usable、Temporarily Fail、および Fail が含まれます。
Oldest Data (age)	DRE データが、日 (d)、時間 (h)、分 (m)、および秒 (s) 形式でキャッシュに保存された時間 たとえば、「1d1h」は 1 日、1 時間を意味します。
Total usable disk size	DRE キャッシュに割り当てられた総ディスク スペース
Used (%)	使用する総 DRE キャッシュ ディスク スペースの比率
Hash table RAM size	DRE ハッシュ テーブルに割り当てられたメモリ量
Used (%)	DRE ハッシュ テーブルに使用する割り当てメモリの比率
完了した接続	
Total (cumulative):	処理された累積接続の数
Active:	まだオープンである接続の数
Encode	圧縮されたメッセージの統計情報
Overall:[msg in out ratio]	圧縮されたメッセージの集約情報 msg = メッセージの総数 in = 圧縮までのバイト数 out = 圧縮後のバイト数 ratio = 圧縮された総バイト数の比率
DRE:[msg in out ratio]	DRE メッセージ数
DRE bypass	圧縮のためバイパスされた DRE メッセージの数
LZ:[msg in out ratio]	LZ メッセージの数
	 (注) DRE 圧縮が適用されたあとに LZ 圧縮が適用されます (必ず DRE 圧縮が最初に適用されます)。
LZ Bypass:[msg in out ratio]	圧縮のためバイパスされた LZ メッセージの数

表 3-70 show statistics dre コマンドのフィールドの説明 (続き)

フィールド	説明
Average Latency	DRE と LZ 両方のメッセージ 1 つを圧縮する平均時間 (ミリ秒 [ms] 単位)
Message size distribution	各サイズのグループに分類されるメッセージの比率 (message size フィールドは 6 つのサイズのグループに分割されます)
Decode	圧縮解除されたメッセージの統計情報
Overall:[msg in out ratio]	圧縮解除されたメッセージの集約統計情報 msg = メッセージの総数 in = 圧縮解除までのバイト数 out = 圧縮解除後のバイト数 ratio = 圧縮解除された総バイト数の比率
DRE:[msg in out ratio]	DRE メッセージ数
DRE Bypass [msg in]	圧縮解除のためバイパスされた DRE メッセージの数
LZ:[msg in out ratio]	LZ メッセージの数
LZ Bypass:[msg in]	圧縮解除のためバイパスされた LZ メッセージの数
Latency (Last 3 sec):[max avg]	DRE と LZ 両方のメッセージ 1 つを圧縮解除する最大時間 (ミリ秒単位) DRE と LZ 両方のメッセージ 1 つを圧縮解除する平均時間 (ミリ秒単位)
Message size distribution	各サイズのグループに分類されるメッセージの比率 (message size フィールドは 6 つのサイズのグループに分割されます)

関連コマンド

[debug](#)[show statistics dre connection](#)[show statistics dre peer](#)

show statistics dre connection

WAE の Data Redundancy Elimination (DRE) 接続統計情報を表示するには、**show statistics dre connection EXEC** コマンドを使用します。

```
show statistics dre connection [active [client-ip {ip_address | hostname} | client-port port |
id connection_id | last | peer-no peer_id | server-ip {ip_address | hostname} | server-port port] |
client-ip {ip_address | hostname} | client-port port | id connection_id | last | peer-no peer_id |
server-ip {ip_address | hostname} | server-port port]
```

シンタックスの説明

active	(オプション) すべてのアクティブな接続の統計情報を表示します。
client-ip	(オプション) 指定された IP アドレスまたはホスト名をもつクライアントの接続統計情報を表示します。
<i>ip_address</i>	クライアントまたはサーバの IP アドレス
<i>hostname</i>	クライアントまたはサーバのホスト名
client-port	(オプション) 指定されたポート番号をもつクライアントの接続統計情報を表示します。
<i>port</i>	クライアントまたはサーバのポート番号 (1 ~ 65535)
id	(オプション) 指定された識別情報をもつ接続の接続統計情報を表示します。
<i>connection_id</i>	接続を識別する 0 ~ 4294967295 の数字
last	(オプション) 直近の接続の統計情報を表示します。
peer-no	(オプション) 指定された識別情報をもつピアの接続統計情報を表示します。
<i>peer_id</i>	ピアを識別する 0 ~ 4294967295 の数字
server-ip	(オプション) 指定された IP アドレスとホスト名をもつサーバの接続統計情報を表示します。
server-port	(オプション) 指定されたポート番号をもつサービスの接続統計情報を表示します。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

このコマンドは DRE 圧縮が適用されている個々の TCP 接続の統計情報を表示します。この情報はリアルタイムでアップデートされます。

オプションなしでこのコマンドを使用すると、DRE が適用される WAE 上のすべての TCP 接続のオンライン要約を表示します。ある接続の詳細統計情報を取得するには、コマンドオプションを使用して接続を絞り込みます。大半のフィルタは詳細統計情報を表示します。一部のフィルタ (ピア番号など) はサマリー情報を表示し、詳細は表示しません。

例 表 3-71 では、**show statistics dre connection** 出力のフィールドについて説明します。

表 3-71 show statistics dre connection コマンドのフィールドの説明

フィールド	説明
Conn-ID	接続ごとにデバイスによって割り当てられた接続 ID
Peer No.	ピア圧縮デバイスに割り当てられた番号
Client-ip:port	TCP 接続を初期化したクライアント デバイスの IP アドレスとポート (ユーザの PC やノート型パソコンなど)
Server-ip:port	サーバの IP アドレスおよびポート
Encode-in	圧縮によるバイト数
Decode-in	圧縮解除によるバイト数
PID	ピア ID。ピア デバイスの MAC アドレス
Status	接続ステートおよびステートの時間可能な値は Active または Closed です。 A = アクティブ C = クローズド たとえば、C(22h) は接続が 22 時間の間、閉じていたことを示します。

関連コマンド

[debug](#)

[show statistics dre connection](#)

show statistics dre peer

WAE の Data Redundancy Elimination (DRE) ピア統計情報を表示するには、**show statistics dre peer** EXEC コマンドを使用します。

```
show statistics dre peer {context context-value [ip ip-address | peer-id peer-id |
peer-no peer-no] | ip ip-address [context context-value | ip ip-address | peer-id peer-id | peer-no
peer-no] | peer-id peer-id [context context-value | ip ip-address | peer-no peer-no] |
peer-no peer-no [context context-value | ip ip-address | peer-id peer-id]}
```

シンタックスの説明

context	指定されたコンテキストのピア統計情報を表示します。
context-value	コンテキスト (0 ~ 4294967295)
ip	(オプション) ピアの IP アドレスを指定します。
ip_address	ピアの IP アドレス
peer-id	(オプション) ピアの MAC アドレスを指定します。
peer-id	ピア ID (0 ~ 4294967295)
peer-no	(オプション) ピア番号を指定します。
peer-no	ピア番号

コマンドモード

EXEC

デバイスモード

application-accelerator

例

表 3-72 では、**show statistics dre peer** 出力のフィールドについて説明します。このコマンドは DRE ピア デバイス接続情報を表示します。

表 3-72 show statistics dre peer コマンドのフィールドの説明

フィールド	説明
Peer-No	ピア圧縮デバイスに割り当てられた番号
Context	DRE デバッグ トレースのコンテキスト ID
Peer-ID	ピア デバイスの MAC アドレス
Hostname	ピア デバイスのホスト名
Cache	ピアが示す DRE キャッシュ データ統計情報
Used disk:	DRE キャッシュのディスク上で使用する MB 数
Age:	DRE データが、日 (d)、時間 (h)、分 (m)、および秒 (s) 形式でキャッシュに保存された時間
接続	
Total (cumulative):	処理された累積接続の数
Active:	まだオープンである接続の数
同時接続 (最後の 2 分)	
max	最後の 2 分間での同時接続の数
avg	最後の 2 分間での同時接続の平均数

表 3-72 show statistics dre peer コマンドのフィールドの説明 (続き)

フィールド	説明
Encode	圧縮されたメッセージの統計情報
Overall:[msg in out ratio]	圧縮されたメッセージの集約統計情報 msg = メッセージの総数 in = 圧縮解除までのバイト数 out = 圧縮解除後のバイト数 ratio = 圧縮された総バイト数の比率
DRE:[msg in out ratio]	DRE メッセージ数
DRE Bypass:[msg in]	圧縮のためバイパスされた DRE メッセージの数
LZ:[msg in out ratio]	LZ メッセージの数
LZ Bypass:[msg in]	圧縮のためバイパスされた LZ メッセージの数
Message size distribution	各サイズのグループに分類されるメッセージの比率 (message size フィールドは6つのサイズのグループに分割されます)
Decode	圧縮解除されたメッセージの統計情報
Overall:[msg in out ratio]	圧縮解除されたメッセージの集約統計情報 msg = メッセージの総数 in = 圧縮解除までのバイト数 out = 圧縮解除後のバイト数 ratio = 圧縮解除された総バイト数の比率
DRE:[msg in out ratio]	DRE メッセージ数
DRE Bypass:[msg in]	圧縮解除のためバイパスされた DRE メッセージの数
LZ:[msg in out ratio]	LZ メッセージの数
LZ Bypass:[msg in]	圧縮解除のためバイパスされた LZ メッセージの数
Latency (Last 3 sec):[max avg]	DRE と LZ 両方のメッセージ 1 つを圧縮解除する最大時間 (ミリ秒単位) DRE と LZ 両方のメッセージ 1 つを圧縮解除する平均時間 (ミリ秒単位)
Message size distribution	各サイズのグループに分類されるメッセージの比率 (message size フィールドは6つのサイズのグループに分割されます)

関連コマンド

[debug](#)[show statistics dre connection](#)

show statistics epm

WAE の EndPoint Mapper (EPM) 統計情報を表示するには、**show statistics epm EXEC** コマンドを使用します。

show statistics epm

コマンドモード EXEC

デバイスモード application-accelerator

使用上のガイドライン このコマンドは記録された要求と応答の総数を表示します。

例 表 3-73 では、**show statistics epm** 出力のフィールドについて説明します。

表 3-73 show statistics epm コマンドのフィールドの説明

フィールド	説明
Total requests	EPM アダプタによって処理された要求の数 (接続ごとに 1 回増加)
success	EPM アダプタによって正常に解析された EPM 要求の数
fault	不良クライアント要求 (または EPM アダプタによる処理を必要としない有効な要求) により、正常に処理されなかった接続の数
Total responses	EPM アダプタによって処理された応答の数 (接続ごとに 1 回増加)
policy match	EPM アダプタによって正常に処理された接続の数 (たとえば、作成されたダイナミック一致など)
UUID not configured	ポリシー エンジンに設定されていないサービスを、クライアントが要求した回数
service unavailable	サーバが利用できないことを通知するサービスを、クライアントが要求した回数
fault	不良クライアント応答またはクライアント応答の処理中に発生した内部エラーにより、正常に処理されなかった接続の数

関連コマンド [\(config\) policy-engine application map adaptor EPM](#)

show statistics flow

WAAS デバイスのフロー統計情報を表示するには、**show statistics flow EXEC** コマンドを使用します。

```
show statistics flow {filters | monitor tcpstat-v1}
```

シンタックスの説明

<i>filters</i>	フロー フィルタ統計情報を表示します。
monitor	パフォーマンス統計情報を表示します。
tcpstat-v1	tcpstat-v1 コレクタの統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

例

表 3-74 では、**show statistics flow filters** 出力のフィールドについて説明します。

表 3-74 show statistics flow filters コマンドのフィールドの説明

フィールド	説明
Number of Filters	フィルタの数
Status	フィルタがイネーブルまたはディセーブルであるかどうかのステータス
Capture Mode	フィルタの動作。値には FILTER または PROMISCUOUS が含まれます。混合モード動作は、WAAS では利用できません。
Server	フローを監視するサーバの IP アドレス リスト
Flow Hits	サーバ別のフロー ヒットの数
Flags	フローを識別するフラグ CSN : 非最適化されたクライアント側 (エッジ) SSO : 最適化されたサーバ側 (エッジ) CSO : 最適化されたクライアント側 (コア) SSN : 非最適化されたサーバ側 (コア) PT : パススルー (Edge/Core/Intermediate) IC : 内部クライアント

表 3-75 では、**show statistics flow monitor** 出力のフィールドについて説明します。

表 3-75 show statistics flow monitor コマンドのフィールドの説明

フィールド	説明
ホスト接続	
Configured host address	接続用 tcpstat-v1 コンソールの IP アドレス
Connection State	接続のステート
Connection Attempts	接続試行の数
Connection Failures	接続失敗の数
Last connection failure	最後に接続が失敗した日時
Last configuration check sent	最後の設定チェックが送信された日時
Last registration occurred	最後の登録が行われた日時
Host Version	接続用 tcpstat-v1 コンソールのバージョン番号
コレクタ接続	
Collector host address:port	ホスト接続を通じて特定された tcpstat-v1 アグリゲータの IP アドレスおよびポート番号
Connection State	接続のステート
Connection Attempts	接続試行の数
Connection Failures	接続失敗の数
Last connection failure	最後に接続が失敗した日時
Last configuration check sent	最後の設定チェックが送信された日時
Last update sent	最後のアップデートが送信された日時
Updates sent	送信されたアップデートの数
Summaries discarded	ストレージ用に割り当てられたディスク スペースが限界に達し、廃棄されたサマリーの数 このフィールドの数は、サマリーをコレクタに転送する能力より高速で収集している場合を示します。 このフィールドのカウンタは、data_update アラームを生成します。
Last registration occurred	最後の登録が行われた日時
Host Version	接続用 tcpstat-v1 アグリゲータのバージョン番号
収集統計情報	
Collection State	サマリー収集動作のステート
Summaries collected	収集されたサマリーの数。サマリーは、監視されるトラフィックの packets digests です。
Summaries dropped	ドロップされたサマリーの総数。これは次のサブカテゴリの合計です。
Dropped by TFO	メモリを割り当てることができないなどのエラーにより、TFO によってドロップされたパケットの数
Dropped due to backlog	キュー制限に達したことによりドロップされたパケットの数 このカウンタは、フロー モニタ アプリケーションが受信されるサマリーの数に対応可能かどうかを示します。

表 3-75 show statistics flow monitor コマンドのフィールドの説明 (続き)

フィールド	説明
Summary backlog	WAE のコレクタ モジュールによって読み取られるために、キューで待機するパケットの数
Last drop occurred	最後のパケットがドロップされた日時

関連コマンド**clear**

show statistics icmp

WAAS デバイスの ICMP 統計情報を表示するには、**show statistics icmp EXEC** コマンドを使用します。

show statistics icmp

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-76 では、**show statistics icmp** 出力のフィールドについて説明します。

表 3-76 show statistics icmp コマンドのフィールドの説明

フィールド	説明
ICMP messages received	エンティティが受信した Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) メッセージの総数。ICMP 入力エラーとしてカウントされたメッセージすべてを含みます。
ICMP messages receive failed	エンティティが受信したにもかかわらず、ICMP 固有のエラー (不良 ICMP チェックサム、長さ不良など) があると判断した ICMP メッセージの数
Destination unreachable	受信したこのタイプの ICMP メッセージの数
Timeout in transit	受信したこのタイプの ICMP メッセージの数
Wrong parameters	受信したこのタイプの ICMP メッセージの数
Source quenches	受信したこのタイプの ICMP メッセージの数
Redirects	受信したこのタイプの ICMP メッセージの数
Echo requests	受信したこのタイプの ICMP メッセージの数
Echo replies	受信したこのタイプの ICMP メッセージの数
Timestamp requests	受信したこのタイプの ICMP メッセージの数
Timestamp replies	受信したこのタイプの ICMP メッセージの数
Address mask requests	受信したこのタイプの ICMP メッセージの数
Address mask replies	受信したこのタイプの ICMP メッセージの数
ICMP messages sent	このエンティティが送信しようとした ICMP メッセージの総数。このカウンタには、ICMP 出力エラーとしてカウントされたメッセージがすべて含まれます。

表 3-76 show statistics icmp コマンドのフィールドの説明 (続き)

フィールド	説明
ICMP messages send failed	バッファの不足などの ICMP 内の問題により、このエンティティが送信しなかった ICMP メッセージの数
Destination unreachable	送信したこのタイプの ICMP メッセージの数
Time exceeded	送信したこのタイプの ICMP メッセージの数
Wrong parameters	送信したこのタイプの ICMP メッセージの数
Source quenches	送信したこのタイプの ICMP メッセージの数
Redirects	送信したこのタイプの ICMP メッセージの数
Echo requests	送信したこのタイプの ICMP メッセージの数
Echo replies	送信したこのタイプの ICMP メッセージの数
Timestamp requests	送信したこのタイプの ICMP メッセージの数
Timestamp replies	送信したこのタイプの ICMP メッセージの数
Address mask requests	送信したこのタイプの ICMP メッセージの数
Address mask replies	送信したこのタイプの ICMP メッセージの数

関連コマンド

clear

show statistics ip

WAAS デバイスの IP 統計情報を表示するには、**show statistics ip EXEC** コマンドを使用します。

show statistics ip

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

例 表 3-77 では、**show statistics ip** 出力のフィールドについて説明します。

表 3-77 show statistics ip コマンドのフィールドの説明

フィールド	説明
IP 統計情報	
Total packets in	インターフェイスから受信した入力データグラムの総数。入力エラーとしてカウントされたデータグラムすべてを含みます。
with invalid address	IP ヘッダー宛先フィールドの IP アドレスが、このエンティティで受信される有効なアドレスでなかったことにより、廃棄された入力データグラムの数。この数には、無効なアドレス (0.0.0.0 など) と、サポートされていないクラス (クラス E など) のアドレスが含まれます。IP ゲートウェイではなく、データグラムを転送しないエンティティの場合、宛先アドレスがローカルアドレスではないので、このカウンタには廃棄されたデータグラムが含まれます。
with invalid header	IP ヘッダのエラー (不良チェックサム、バージョン番号の不一致、その他の形式エラー、Time-to-Live (TTL; 存続可能時間) 超過エラー、IP オプションの処理中に検出されたエラーなどを含む) により、廃棄された入力データグラムの数
forwarded	このエンティティが最終の IP 宛先ではなかった入力データグラムの数。結果的に最終の宛先に転送するためのルートを検出しようとしています。IP ゲートウェイとして機能しないエンティティでは、このカウンタには、このエンティティ経由でソースルートであったパケットのみが含まれます。ソースルート オプションは正常に処理されます。
unknown protocol	プロトコルが不明であるか、サポートされていないので、正常に受信したものの廃棄されたローカル アドレス データグラムの数

表 3-77 show statistics ip コマンドのフィールドの説明 (続き)

フィールド	説明
discarded	処理の続行を妨げる問題がなかったにもかかわらず、(バッファスペースの不足などにより) 廃棄された入力 IP データグラムの数。この数には、再構成の待機中に廃棄されたデータグラムは含まれません。
delivered	IP ユーザ プロトコル (ICMP を含む) に正常に配信された入力 IP データグラムの総数
Total packets out	ローカル IP ユーザ プロトコル (ICMP を含む) が送信要求に対して提供した、IP データグラムの総数。この数には、転送フィールドでカウントされたデータグラムは含まれません。
dropped	宛先への送信を妨げる問題がなかったにもかかわらず、(バッファスペースの不足などにより) 廃棄された出力 IP データグラムの数。パケットがこの廃棄基準 (任意) を満たしている場合、このカウントには転送フィールドでカウントされたデータグラムが含まれます。
dropped (no route)	宛先に送信するためのルートが検出できなかったので廃棄された IP データグラムの数。このカウントには、このルート基準を満たさない、転送フィールドでカウントされたパケットや、デフォルト ゲートウェイがすべてダウンしているため、ホストがルーティングできなかったデータグラムが含まれます。
Fragments dropped after timeout	このエンティティで再構成の待機中に受信したフラグメントが保持される最大秒数
Reassemblies required	このエンティティで受信した、再構成する必要がある IP フラグメントの数
Packets reassembled	正常に再構成した IP データグラムの数
Packets reassemble failed	IP 再構成アルゴリズムが検出した障害の数 (タイムアウト、エラーなど理由は問いません)。このカウントは、必ずしも、廃棄された IP フラグメントのカウントではありません。これは、一部のアルゴリズム (特に、RFC 815 のアルゴリズム) では、フラグメントの受信時に結合するので、フラグメント数を追跡できなくなるからです。
Fragments received	このエンティティで正常にフラグメント化された IP データグラムの総数
Fragments failed	このエンティティでフラグメント化する必要があったにもかかわらず、フラグメント化できなかった (Don't Fragment フラグが設定されていた) ので、廃棄された IP データグラムの数
Fragments created	このエンティティでのフラグメンテーションの結果として生成された IP データグラム フラグメントの数

関連コマンド

[clear](#)[\(config\) ip](#)[\(config-if\) ip](#)[show ip routes](#)

show statistics key-manager

各 WAAS デバイスのキー マネージャ情報を表示するには、**show statistics key-manager EXEC** コマンドを使用します。

show statistics key-manager

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード central-manager

例 [表 3-78](#) では、**show statistics key-manager** 出力のフィールドについて説明します。

表 3-78 show statistics key-manager コマンドのフィールドの説明

フィールド	説明
Count of Retrieve key	取得した暗号キーの数
Count of Create new key	作成した新しいキーの数

関連コマンド **show statistics key-manager**

show statistics netstat

WAAS デバイスのインターネット ソケット接続統計情報を表示するには、**show statistics netstat EXEC** コマンドを使用します。

show statistics netstat

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-79 では、**show statistics netstat** 出力のフィールドについて説明します。

表 3-79 show statistics netstat コマンドのフィールドの説明

フィールド	説明
Active Internet connections (w/o servers)	この WAR との間のすべてのオープンなインターネット接続のリスト
Proto	TCP や UDP などのインターネット接続で使用するレイヤ 4 プロトコル
Recv-Q	接続上の受信方向のレイヤ 4 プロトコル スタックによってバッファリングされたデータ量
Send-Q	接続上の送信方向のレイヤ 4 プロトコル スタックによってバッファリングされたデータ量
Local Address	接続の WAE エンドポイントで使用する IP アドレスおよびレイヤ 4 ポート
Foreign Address	接続のリモートエンドポイントで使用する IP アドレスおよびレイヤ 4 ポート
State	接続のレイヤ 4 ステート。TCP ステートには、ESTABLISHED、TIME-WAIT、LAST-ACK、CLOSED、CLOSED-WAIT、SYN-SENT、SYN-RCVD、SYN-SENT、SYN-ACK-SENT、および LISTEN が含まれます。

show statistics radius

WAAS デバイスの RADIUS 認証統計情報を表示するには、**show statistics radius EXEC** コマンドを使用します。

show statistics radius

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-80 では、**show statistics radius** 出力のフィールドについて説明します。

表 3-80 show statistics radius コマンドのフィールドの説明

フィールド	説明
RADIUS 統計情報	
認証	
Number of access requests	アクセス要求の数
Number of access deny responses	アクセス拒否応答の数
Number of access allow responses	アクセス許可応答の数
許可	
Number of authorization requests	許可要求の数
Number of authorization failure responses	許可失敗応答の数
Number of authorization success responses	許可成功応答の数
アカウントिंग	
Number of accounting requests	アカウントिंग要求の数
Number of accounting failure responses	アカウントング失敗応答の数
Number of accounting success responses	アカウントング成功応答の数

関連コマンド [clear](#)
[\(config\) radius-server](#)
[show radius-server](#)

show statistics services

WAAS デバイスのサービス統計情報を表示するには、**show statistics services EXEC** コマンドを使用します。

show statistics services

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-81 では、**show statistics services** 出力のフィールドについて説明します。

表 3-81 show statistics services コマンドのフィールドの説明

フィールド	説明
Port Statistics	WAAS デバイス上の各ポートのサービス関連統計情報
Port	ポート番号
Total Connections	接続の総数

関連コマンド [show services](#)

show statistics snmp

WAAS デバイスの SNMP 統計情報を表示するには、**show statistics snmp EXEC** コマンドを使用します。

show statistics snmp

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-82 では、**show statistics snmp** 出力のフィールドについて説明します。

表 3-82 show statistics snmp コマンドのフィールドの説明

フィールド	説明
SNMP packets input	入力された SNMP パケットの総数
Bad SNMP version errors	SNMP のバージョンが無効なパケットの数
Unknown community name	未知のコミュニティ名の SNMP パケットの数
Illegal operation for community name supplied	そのコミュニティで許可されていない動作を要求するパケットの数
Encoding errors	誤って符号化されている SNMP パケットの数
Number of requested variables	SNMP マネージャによって要求されている変数の数
Number of altered variables	SNMP マネージャによって変更されている変数の数
Get-request PDUs	受信した GET 要求の数
Get-next PDUs	受信した GET-NEXT 要求の数
Set-request PDUs	受信した SET 要求の数
SNMP packets output	ルータによって送信された SNMP パケットの総数
Too big errors	最大パケット サイズより大きな SNMP パケットの数
Maximum packet size	SNMP パケットの最大サイズ
No such name errors	存在しない MIB オブジェクトを指定した SNMP 要求の数
Bad values errors	MIB オブジェクトの無効な値を指定した SNMP SET 要求の数
General errors	その他のエラーが原因で失敗した SNMP SET 要求の数 (No such name error、Bad values error など特定されているエラー以外のエラー)

表 3-82 show statistics snmp コマンドのフィールドの説明 (続き)

フィールド	説明
Response PDUs	要求に対応して送信された応答数
Trap PDUs	送信された SNMP トラップの数

関連コマンド[show snmp](#)[\(config\) snmp-server user](#)[\(config\) snmp-server view](#)

show statistics tacacs

WAAS デバイスの TACACS+ 認証および許可統計情報を表示するには、**show statistics tacacs EXEC** コマンドを使用します。

show statistics tacacs

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
 replication-accelerator
 central-manager

例 表 3-83 では、**show statistics tacacs** 出力のフィールドについて説明します。

表 3-83 show statistics tacacs コマンドのフィールドの説明

フィールド	説明
TACACS+ 統計情報	
認証	
Number of access requests	アクセス要求の数
Number of access deny responses	アクセス拒否応答の数
Number of access allow responses	アクセス許可応答の数
許可	
Number of authorization requests	許可要求の数
Number of authorization failure responses	許可失敗応答の数
Number of authorization success responses	許可成功応答の数
アカウントिंग	
Number of accounting requests	アカウントिंग要求の数
Number of accounting failure responses	アカウントING失敗応答の数
Number of accounting success responses	アカウントING成功応答の数

関連コマンド [clear](#)
[\(config\) tacacs](#)
[show tacacs](#)

show statistics tcp

WAAS デバイスの TCP 統計情報を表示するには、**show statistics tcp EXEC** コマンドを使用します。

show statistics tcp

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

例 表 3-84 では、**show statistics tcp** 出力のフィールドについて説明します。

表 3-84 show statistics tcp コマンドのフィールドの説明

フィールド	説明
TCP 統計情報	
Server connection openings	TCP 接続が CLOSED ステートから SYN-SENT ステートに直接移行した回数
Client connection openings	TCP 接続が LISTEN ステートから SYN-RCVD ステートに直接移行した回数
Failed connection attempts	TCP 接続が SYN-SENT ステートまたは SYN-RCVD ステートのいずれかから CLOSED ステートに直接移行した回数。および TCP 接続が SYN-RCVD ステートから LISTEN ステートに直接移行した回数
Connections established	現在のステートが ESTABLISHED または CLOSE-WAIT のいずれかである TCP 接続の数
Connections resets received	TCP 接続が ESTABLISHED ステートまたは CLOSE-WAIT ステートのいずれかから CLOSED ステートに直接移行した回数
Connection resets sent	RST フラグを含む、送信された TCP セグメントの数
Segments received	受信したセグメントの総数。受信エラーのあったものを含みます。このカウントには、現在確立されている接続で受信したセグメントが含まれます。
Segments sent	送信されたセグメントの総数。現在の接続上で送信されたものを含みますが、再送信されたオクテットのみを含んだものは除外します。
Bad segments received	受信した不良セグメントの数

表 3-84 show statistics tcp コマンドのフィールドの説明 (続き)

フィールド	説明
Segments retransmitted	再送信されたセグメントの総数。すなわち、すでに送信済みの1つまたは複数のオクテットを含む、送信されたTCPセグメントの数
Retransmit timer expirations	再送信タイマーの満了によって再送信されたTCPパケットの数
Server segments received	サーバから受信したTCPパケットの数
Server segments sent	サーバに送信されたTCPパケットの数
Server segments retransmitted	サーバに再送信されたTCPパケットの数
Client segments received	クライアントから受信したTCPパケットの数
Client segments sent	クライアントに送信されたTCPパケットの数
Client segments retransmitted	クライアントに再送信されたTCPパケットの数
TCP 拡張統計情報	
Sync cookies sent	SYNパケットに応じてSYN cookieを使用して送信されたSYN-ACKパケットの数
Sync cookies received	デバイスによってSYN-ACKパケットで送信された正しいSYN cookieを使用して、受信したACKパケットの数
Sync cookies failed	デバイスによってSYN-ACKパケットで送信された不正なSYN cookieを使用して、受信したACKパケットの数
Embryonic connection resets	TCP接続がSYN-RCVDステート、SYN-SENTステート、またはSYN-ACK-SENTステートのいずれかからCLOSEDステートに直接移行した回数
Prune message called	デバイスが、接続用に割り当てられたメモリプールを超過した回数
Packets pruned from receive queue	メモリオーバーランにより、接続の受信キューからドロップされたパケットの数
Out-of-order-queue pruned	メモリオーバーランにより、out-of-orderキューがプルーニングされた回数
Out-of-window Icmp messages	受信したウィンドウからの、TCP接続上で受信したICMPパケットの数
Lock dropped Icmp messages	ソケットがビジー状態なのでドロップされたICMPパケットの数
Arp filter	ARPフィルタによりドロップされたICMP応答の数
Time-wait sockets	TCP接続がTIME-WAITステートからCLOSEDステートに移行した回数
Time-wait sockets recycled	TCP接続がTIME-WAITステートからCLOSEDステートに移行した回数
Time-wait sockets killed	TCP接続がTIME-WAITステートからCLOSEDステートに移行した回数
PAWS passive	PAWSチェックの失敗によりドロップされた着信SYNパケットの数
PAWS active	PAWSチェックの失敗によりドロップされた着信SYN-ACKパケットの数
PAWS established	PAWSチェックの失敗によりESTABLISHEDステートでドロップされたパケットの数

表 3-84 show statistics tcp コマンドのフィールドの説明 (続き)

フィールド	説明
Delayed acks sent	送信された遅延 ACK の数
Delayed acks blocked by socket lock	ソケットのビジー状態により延期された遅延 ACK の数
Delayed acks lost	失われた遅延 ACK の数
Listen queue overflows	傍受サーバキューのオーバーフローにより、ドロップされた着信 TCP 接続の数
Connections dropped by listen queue	内部エラーによりドロップされた着信 TCP 接続の数
TCP packets queued to prequeue	プロセスに事前にキューイングされた着信 TCP パケットの数
TCP packets directly copied from backlog	backlog キューからプロセスに直接コピーされた着信 TCP パケットの数
TCP packets directly copied from prequeue	prequeue からプロセスに直接コピーされた着信 TCP パケットの数
TCP prequeue dropped packets	TCP prequeue から削除されたパケットの数
TCP header predicted packets	TCP ヘッダー予測パケットの数
Packets header predicted and queued to user	ヘッダー予測され、ユーザにキューイングされた TCP パケットの数
TCP pure ack packets	データなしで受信した ACK パケットの数
TCP header predicted acks	ヘッダー予測された TCP ACK パケットの数
TCP Reno recoveries	TCP Reno リカバリの数
TCP SACK recoveries	TCP SACK リカバリの数
TCP SACK renegeing	TCP SACK 違反の数
TCP FACK reorders	TCP FACK reorder の数
TCP SACK reorders	TCP SACK reorder の数
TCP Reno reorders	TCP Reno reorder の数
TCP TimeStamp reorders	TCP TimeStamp reorder の数
TCP full undos	TCP full undo の数
TCP partial undos	TCP partial undo の数
TCP DSACK undos	TCP DSACK undo の数
TCP loss undos	TCP loss undo の数
TCP losses	TCP 損失の数
TCP lost retransmit	TCP の失われた再送信の数
TCP Reno failures	TCP Reno 障害の数
TCP SACK failures	TCP SACK 障害の数
TCP loss failures	TCP 損失障害の数
TCP fast retransmissions	TCP 高速再送信の数
TCP forward retransmissions	TCP 転送再送信の数
TCP slowstart retransmissions	TCP スロースタート再送信の数
TCP Timeouts	TCP タイムアウトの数
TCP Reno recovery fail	TCP Reno リカバリ失敗の数
TCP Sack recovery fail	TCP SACK リカバリ失敗の数
TCP scheduler failed	TCP スケジューラ障害の数
TCP receiver collapsed	TCP レシーバー コラプスト障害の数

表 3-84 show statistics tcp コマンドのフィールドの説明 (続き)

フィールド	説明
TCP DSACK old packets sent	送信された TCP DSACK の古いパケットの数
TCP DSACK out-of-order packets sent	送信された TCP DSACK out-of-order パケットの数
TCP DSACK packets received	受信した TCP DSACK パケットの数
TCP DSACK out-of-order packets received	受信した TCP DSACK out-of-order パケットの数
TCP connections abort on sync	sync で打ち切られた TCP 接続の数
TCP connections abort on data	データで打ち切られた TCP 接続の数
TCP connections abort on close	close で打ち切られた TCP 接続の数
TCP connections abort on memory	メモリで打ち切られた TCP 接続の数
TCP connections abort on timeout	タイムアウトで打ち切られた TCP 接続の数
TCP connections abort on linger	リンガーで打ち切られた TCP 接続の数
TCP connections abort failed	失敗した TCP 接続打ち切りの数
TCP memory pressures	デバイスが TCP スタック用に割り当てられたメモリプールを処理する回数

関連コマンド

[clear](#)[show tcp](#)[\(config\) tcp](#)

show statistics tfo

WAE の Traffic Flow Optimization (TFO; トラフィック フロー最適化) 統計情報を表示するには、**show statistics tfo** EXEC コマンドを使用します。

```
show statistics tfo [application app-name | pass-through | peer | saving app-name]
```

シンタックスの説明

application	(オプション) アプリケーションごとに統計情報を表示します。
<i>app-name</i>	アプリケーション名
pass-through	(オプション) パススルー統計情報を表示します。
peer	(オプション) ピア情報を表示します。
saving	(オプション) すべてのアプリケーションの保存情報を表示します。

コマンドモード

EXEC

デバイスモード

application-accelerator

例

表 3-85 では、**show statistics tfo** コマンドのフィールドについて説明します。

表 3-85 show statistics tfo コマンドのフィールドの説明

フィールド	説明
Total number of optimized connections	最後の TFO 統計情報リセット以降に最適化された TCP 接続の総数
No. of active connections	最適化された TCP 接続の総数
No. of pending (to be accepted) connections	最適化されますが、現在はセットアップ段階である TCP 接続の数
No. of connections closed normally	TCP FIN を使用して問題なく終了した、最適化された接続の数
No. of connections closed with error	問題が発生して、または TCP RST を使用して終了した、最適化された接続の数
Total number of peers	アクティブなピア WAE の数(接続ごとに2つの WAE [この WAE とピア WAE] の間で最適化されます)
No. of entries into overload mode	WAE が過負荷状態になった回数。過負荷状態では、新しい接続はパススルーに設定されます。この状態は、同時接続数が最大に達した場合など、さまざまな理由で発生します。
No. of connections reset due to	エラーが発生して終了した接続数の詳細
Socket write failure	ソケットでの書き込みに失敗しました (LAN 側または WAN 側)。
Socket read failure	ソケットでの読み込みに失敗しました (LAN 側または WAN 側)。
Opt socket close while waiting to write	書き込みが完了する前に終了した2つの WAE の間のソケット (WAN ソケット)
Unopt socket close while waiting to write	書き込みが完了する前に終了した、WAE とクライアント/サーバの間のソケット (LAN ソケット)

表 3-85 show statistics tfo コマンドのフィールドの説明 (続き)

フィールド	説明
Opt socket error close while waiting to read	読み込みが完了する前に終了した2つのWAEの間のソケット (WAN ソケット)
Unopt socket error close while waiting to read	読み込みが完了する前に終了した、WAE とクライアント / サーバの間のソケット (LAN ソケット)
DRE decode failure	データのデコード中の DRE 内部エラー (発生してはいけません)
DRE encode failure	データの符号化中の DRE 内部エラー (発生してはいけません)
Connection init failure	自動ディスカバリは正常に終了しましたが、接続のセットアップに失敗しました。
Opt socket unexpected close while waiting to read	読み込みが完了する前に終了した2つのWAEの間のソケット (WAN ソケット)
Exceeded maximum number of supported connections	WAE がスケーラビリティ制限に達したので、途中で終了した接続
Buffer allocation or manipulation failed	内部メモリ割り当てエラー (発生してはいけません)
Peer received reset from end host	サーバまたはクライアントによって送信された TCP RST (通常の動作で、必ずしも問題を示すものではありません)
DRE connection state out of sync	DRE 内部エラー (発生してはいけません)
Memory allocation failed for buffer heads	内部メモリ割り当てエラー (発生してはいけません)

関連コマンド

[show tfo accelerators](#)

[show tfo bufpool](#)

[show tfo connection](#)

[show tfo status](#)

show statistics udp

WAAS デバイスの User Datagram Protocol (UDP; ユーザ データグラム プロトコル) 統計情報を表示するには、**show statistics udp EXEC** コマンドを使用します。

show statistics udp

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-86 では、**show statistics udp** 出力のフィールドについて説明します。

表 3-86 show statistics udp コマンドのフィールドの説明

フィールド	説明
UDP 統計情報	
Packets received	UDP ユーザに配信される UDP データグラムの総数
Packets to unknown port received	宛先ポートにアプリケーションがなかった受信 UDP データグラムの総数
Packet receive error	宛先ポートにアプリケーションが存在しないという理由以外で、配信できなかった受信 UDP データグラムの数
Packet sent	このエンティティから送信された UDP データグラムの総数

show statistics wccp

WAE の WCCP 統計情報を表示するには、**show statistics wccp EXEC** コマンドを使用します。

```
show statistics wccp gre
```

シンタックスの説明

gre	WCCP Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) パケット関連の統計情報を表示します。
------------	---

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

GRE は、WCCP 対応ルータでデータグラムを IP パケットにカプセル化し、その後 WAE (透過型プロキシサーバ) にリダイレクトできるレイヤ 3 技術です。この中間宛先で、データグラムは非カプセル化されたあとオリジンサーバにルーティングされ、キャッシュミスが発生した場合に要求に応えます。そのとき、オリジンサーバへのトリップは内部データグラムに 1 ホップとして現れます。通常、GRE を使用してリダイレクトされたトラフィックは GRE トンネルトラフィックと呼ばれます。GRE を使用すると、すべてのリダイレクションはルータソフトウェアにより取り扱われます。

WCCP リダイレクションを使用した場合、Cisco ルータは接続の宛先ポートで WCCP がイネーブルになっているため、TCP SYN パケットを宛先に転送しません。その代わりに、WCCP 対応ルータが GRE トンネリングを使用してパケットをカプセル化し、それをこの WCCP 対応ルータからリダイレクトされたパケットを受け付けるように設定された WAE に送信します。

リダイレクトされたパケットを受信後、WAE は次のような処置を行います。

1. パケットから GRE レイヤを取り除きます。
2. このリダイレクトされたパケットを受け付けるべきか決定し、コンテンツの要求を次のように処理します。
 - a. WAE が要求を受け付けた場合は、クライアントに TCP SYN ACK パケットを送信します。この応答パケットで、WAE は送信元アドレスとして指定された本来の宛先 (オリジンサーバ) の IP アドレスを使用して WAE がクライアントに見えないよう (トランスペアレント) に、クライアントの TCP SYN パケットが到達しようとした宛先であるかのように動作します。
 - b. WAE が要求を受け付けない場合は、TCP SYN パケットを GRE に再カプセル化し、それを WCCP 対応ルータに戻します。ルータは、WAE がこの接続に関心がないとみなし、パケットを本来の宛先 (オリジンサーバ) に転送します。

たとえば、WAE は、特定のクライアントから発信されたり特定のサーバへ送信される要求をバイパスするように設定されている場合は、要求を受け付けません。

例

表 3-87 では、show statistics wccp gre 出力のフィールドについて説明します。

表 3-87 show statistics wccp gre コマンドのフィールドの説明


フィールド	説明
Transparent GRE packets received	WCCP により代行受信されたかどうかに関係なく、WAE により受信された GRE パケットの総数。GRE は、WAE へのパスにルータが何台あってもパケットが WAE に到達できるようにするレイヤ 3 技術です。
Transparent non-GRE packets received	WAE に要求を透過的にリダイレクトするレイヤ 2 またはレイヤ 4 スイッチング (コンテンツ スイッチング モジュール [CSM]) でルータ ハードウェアのトラフィック 代行受信およびリダイレクト機能のどちらかを使用して、WAE により受信された非 GRE パケットの数
Transparent non-GRE packets passed through	レイヤ 4 スイッチにより透過的に代行受信され、WAE にリダイレクトされる非 GRE パケットの数
Total packets accepted	クライアントのコンテンツ要求に応えるため、透過的に代行受信され、WAE にリダイレクトされるパケットの総数
Invalid packets received	リダイレクトされたパケットが GRE パケットで WCCP GRE ヘッダーのデータが無効である、またはリダイレクトされたパケットの IP ヘッダーが無効であるため、ドロップされるパケットの数
Packets received with invalid service	無効な WCCP サービス番号が格納されている WCCP バージョン 2 GRE リダイレクト パケットの数
Packets received on a disabled service	WAE でイネーブルになっていないサービスの WCCP サービス番号を指定する WCCP バージョン 2 GRE リダイレクト パケットの数。たとえば、HTTPS キャッシング サービス (サービス 70) がイネーブルになっていない場合に WAE にリダイレクトされる HTTPS 要求
Packets received too small	WAE にリダイレクトされ、WCCP GRE ヘッダーに必要な最小限のデータが格納されていない GRE パケットの数
Packets dropped due to zero TTL	リダイレクトされたパケットの IP ヘッダーの TTL がゼロのため、WAE によりドロップされる GRE パケットの数
Packets dropped due to bad buckets	不良マスクまたはハッシュ バケット判定により WCCP フロー リダイレクションを実行できなかったため、WAE によりドロップされるパケットの数  (注) バケットは、WAE クラスタ内の各 WAE へ割り当てられた割り当てハッシュのある一部と定義されます。この環境に WAE が 1 つだけ存在する場合は、256 個のバケットが割り当てられています。
Packets dropped due to no redirect address	フロー リダイレクションの宛先 IP アドレスを判別できなかったため、ドロップされるパケットの数
Packets dropped due to loopback redirect	宛先 IP アドレスがループバック アドレスと同じ場合に WAE によりドロップされるパケットの数

表 3-87 show statistics wccp gre コマンドのフィールドの説明 (続き)

フィールド	説明
Pass-through pkts dropped on assignment update	TFO パススルー宛ですが、デバイスがバケットを所有していないので代わりにドロップされるパケットの数
Connections bypassed due to load	WAE が過負荷の場合、バイパスされる接続フローの数。過負荷バイパス オプションがイネーブルになっている場合、WAE はバケットをバイパスし、過負荷トラフィックを再ルーティングします。負荷が高いままの場合、さらにもう 1 つのバケットもバイパスされ、WAE が負荷を処理できるようになるまでバイパスが続きます。
Packets sent back to router	要求を受け取った WCCP 対応ルータに WAE により戻される要求の数。ルータはこのあとフローを、ブラウザから直接オリジン Web サーバへ送信し、WAE をバイパスします。
Packets sent to another WAE	WCCP サービス グループの別の WAE にリダイレクトされるパケットの数。サービス グループは最大 32 個の WAE と 32 個の WCCP 対応ルータで構成されます。どちらのパケット転送方式でも、ハッシュ パラメータが、WCCP サービス グループの WAE 間でのリダイレクトされたトラフィックのロード バランシング方法を指定します。
GRE fragments redirected	WAE により受信され、断片化された GRE パケットの数。これらのパケットはルータにリダイレクトされます。
GRE encapsulated fragments received	WAE が受信する GRE カプセル化フラグメントの数。tcp-promiscuous サービスはポート情報を検査しないので、ルータまたはスイッチが IP フラグメントを GRE カプセル化し、WAE にリダイレクトします。これらのフラグメントはパケットに再構成されてから、処理されます。
Packets failed encapsulated reassembly	再構成された GRE カプセル化パケットで、再構成健全性チェックに失敗したためドロップされた数。再構成された GRE カプセル化パケットは、複数の GRE カプセル化フラグメントで構成されます。このフィールドは、以前の統計に関連しています。
Packets failed GRE encapsulation	GRE ヘッダー付きパケットのカプセル化中に問題が発生してリダイレクトできなかつたため、WAE によりドロップされる GRE パケットの数
Packets dropped due to invalid fwd method	GRE を使用してリダイレクトされたが、WCCP サービスでレイヤ 2 リダイレクションが設定されていたため、WAE によりドロップされる GRE パケットの数
Packets dropped due to insufficient memory	GRE パケットの取り扱いに必要な付加メモリ リソースの割り当てに失敗したため、WAE によりドロップされる GRE パケットの数

表 3-87 show statistics wccp gre コマンドのフィールドの説明 (続き)

フィールド	説明
Packets bypassed, no conn at all	傍受している TCP ポートがなかったため、存在するフローと関連付けできなかったパケットの数。WCCP は非対称パケットフローを取り扱うこともでき、WCCP サービスグループ (クラスタ内の最大 32 個の WAE と通信する最大 32 個のルータまたはスイッチ) で使用されるスイッチまたはルータの数に関係なく、常にキャッシュへの Web サーバの一貫したマッピングを維持します。
Packets bypassed, no pending connection	初期ハンドシェイクが完了しなかったため、保留中の接続と関連付けできなかったパケットの数
Packets due to clean wccp shutdown	クリーンな WCCP シャットダウンのためバイパスされる接続フローの数。WCCP の適切なシャットダウン中、WAE は処理中のフローについては引き続きサービスを提供する一方で、新しいフローのバイパスを開始します。フローの数が 0 になると、WAE は、リード WAE に自分のパケットを他の WAE へ再割り当てさせることで、自分自身はクラスタから脱退します。
Packets bypassed due to bypass-list lookup	バイパス リスト エントリによりバイパスされる接続フローの数。WAE はオリジン サーバからエラー応答を受信すると、サーバのエントリをそのバイパス リストに追加します。バイパスされたサーバに存在するコンテンツの次の要求を受信した場合は、パケットをバイパスゲートウェイにリダイレクトします。バイパスゲートウェイが設定されていない場合、パケットはリダイレクトしているレイヤ 4 スイッチに戻されます。
Packets received with client IP addresses	スプーフィングされている接続フローに関連するパケットの数。クライアントの IP アドレスをスプーフィングして WAE はクライアント IP (WAE 自身の IP アドレスとは別のもの) を持つパケットを受信し、そのパケットを待機している正しいアプリケーションに送信できます。
Conditionally Accepted connections	条件付き受け付け機能のため、WAE によって受け付けられる接続フローの数
Conditionally Bypassed connections	条件付き受け付け機能のため、WAE によってバイパスされる接続フローの数
Packets dropped due to received on loopback	パケットがループバック インターフェイスで受信されましたが、デバイスのローカルアドレス宛ではなかったため、WCCP L2 インターセプト レイヤによってドロップされたパケットの数。パケットには有効でない、または使用しないルートがあります。
Packets w/WCCP GRE received too small	レイヤ 2 で WCCP 対応ルータによって透過的に代行受信されたあと WAE に送信され、GRE を使用してパケットをリダイレクトするために断片化が必要なパケットの数。WAE は IP ヘッダーをカプセル化できないので、パケットをドロップします。
Packets dropped due to IP access-list deny	WAE が WCCP GRE カプセル化パケットに適用する IP アクセス リストが WCCP アプリケーションのアクセスを拒否している場合 (<code>wccp access-list</code> コマンド)、WAE によりドロップされるパケットの数

表 3-87 show statistics wccp gre コマンドのフィールドの説明 (続き)

フィールド	説明
Packets fragmented for bypass	IP ヘッダーを保持する十分なデータが格納されていない GRE パケットの数
Packet pullups needed	パケットを処理の一部として統合する回数。パケットがフラグメントとして受信され、最初のフラグメントに処理に必要な情報がすべて含まれていない場合に、統合が必要になります。
Packets dropped due to no route found	WAE がルートを発見できないため、ドロップされるパケットの数

関連コマンド[\(config\) wccp access-list](#)[\(config\) wccp flow-redirect enable](#)[\(config\) wccp router-list](#)[\(config\) wccp shutdown](#)[\(config\) wccp tcp-promiscuous](#)[\(config\) wccp tcp-promiscuous](#)

show statistics windows-domain

WAAS デバイスの Windows ドメイン サーバ情報を表示するには、**show statistics windows-domain EXEC** コマンドを使用します。

show statistics windows-domain

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン **show statistics windows-domain EXEC** コマンドを使用して Windows ドメイン サーバ統計情報を表示したあと、**clear statistics windows-domain EXEC** コマンドを入力すると、これらの統計情報のカウンタをクリアできます。

例 表 3-88 では、**show statistics windows-domain** 出力のフィールドについて説明します。

表 3-88 show statistics windows-domain コマンドのフィールドの説明

フィールド	説明
Windows ドメイン統計情報	
認証	
Number of access requests	アクセス要求の数
Number of access deny responses	アクセス拒否応答の数
Number of access allow responses	アクセス許可応答の数
許可	
Number of authorization requests	許可要求の数
Number of authorization failure responses	許可失敗応答の数
Number of authorization success responses	許可成功応答の数
アカウントティング	
Number of accounting requests	アカウントティング要求の数
Number of accounting failure responses	アカウントティング失敗応答の数
Number of accounting success responses	アカウントティング成功応答の数

関連コマンド [windows-domain](#)
[\(config\) windows-domain](#)

show sysfs volumes

WAAS デバイスのシステム ファイル システム (sysfs) 情報を表示するには、**show sysfs volumes** EXEC コマンドを使用します。

show sysfs volumes

シンタックスの説明 このコマンドには引数やキーワードがありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン システム ファイル システム (sysfs) はトランザクション ログ、Syslog、内部デバッグ ログなどのログ ファイルを保存します。システム イメージ ファイルとオペレーティング システム ファイルも保存します。

例 表 3-89 では、**show sysfs volumes** 出力のフィールドについて説明します。

表 3-89 show sysfs volumes コマンドのフィールドの説明

フィールド	説明
sysfs 00-04	システム ファイル システム および ディスク 番号
/local/local1-5	ボリュームの マウント ポイント
nnnnnnKB	ボリュームの サイズ (KB 単位)
nn% free	SYSFS パーティションのフリー スペースの比率

関連コマンド [disk](#)
[\(config\) disk error-handling](#)

show tacacs

WAAS デバイスの TACACS+ 認証プロトコル設定情報を表示するには、**show tacacs EXEC** コマンドを使用します。

show tacacs

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-90 では、**show tacacs** 出力のフィールドについて説明します。

表 3-90 show tacacs コマンドのフィールドの説明

フィールド	説明
Login Authentication for Console/ Telnet Session	TACACS+ サーバが、ログイン認証に対してイネーブルになっているかどうかを示します。
Configuration Authentication for Console/ Telnet Session	TACACS+ サーバが、許可または設定認証に対してイネーブルになっているかどうかを示します。
TACACS+ Configuration	TACACS+ サーバパラメータ
TACACS+ Authentication	WAAS デバイスで TACACS+ 認証がイネーブルかどうかを示します。
Key	WAE が TACACS+ サーバとの通信に使用する秘密鍵。TACACS+ キーの最大文字数は、印字可能 ASCII 文字（タブは除く）で 99 文字を超えてはなりません。
Timeout	WAAS デバイスが、タイムアウトを宣言するまで、指定された TACACS+ 認証サーバからの応答を待つ秒数
Retransmit	TACACS+ タイムアウト インターバルを超過した場合に、WAAS デバイスが TACACS+ に接続を再送信する回数
Password type	パスワード認証のメカニズム。デフォルトでは、Password Authentication Protocol (PAP; パスワード認証プロトコル) がパスワード認証のメカニズムです。
Server	TACACS+ サーバのホスト名または IP アドレス
Status	サーバがプライマリまたはセカンダリ ホストであるかどうかを示します。

関連コマンド

clear

show statistics tacacs

show tacacs

(config) tacacs

show tcp

WAAS デバイスの TCP 設定情報を表示するには、**show tcp EXEC** コマンドを使用します。

show tcp

シンタックスの説明

このコマンドには引数やキーワードがありません。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

replication-accelerator

central-manager

例

表 3-91 では、**show tcp** 出力のフィールドについて説明します。このコマンドは、**tcp** 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設定された設定を表示します。

表 3-91 show tcp コマンドのフィールドの説明

フィールド	説明
TCP 設定	
TCP keepalive timeout XX sec	WAAS デバイスが接続を切断するまで開いたままにするよう設定された時間の長さ
TCP keepalive probe count X	接続が失敗したとみなされるまで、WAAS デバイスが接続を再試行する時間数
TCP keepalive probe interval XX sec	WAAS デバイスがアイドル接続を開いたままにするよう設定された時間の長さ (秒単位)
TCP explicit congestion notification disabled	TCP の Explicit Congestion Notification (ECN; 明示的輻輳通知) 機能の設定ステータス。値は enabled または disabled です。
TCP cwnd base value X	送信輻輳ウィンドウの値 (セグメント単位)
TCP initial slowstart threshold value X	スロー スタートのしきい値 (セグメント単位)
TCP increase (multiply) retransmit timer by X	再送信タイマーの基準値を増やすよう設定された回数

表 3-91 show tcp コマンドのフィールドの説明 (続き)

フィールド	説明
TCP memory_limit	
Low water mark	メモリ プレッシャ モードの下限 (MB 単位)。これより低いと TCP が通常のメモリ割り当てモードに入ります。
High water mark (pressure)	通常のメモリ割り当てモードの上限 (MB 単位)。これを越えると TCP がメモリ プレッシャ モードに入ります。
High water mark (absolute)	TCP のメモリ使用状況 (MB 単位) の絶対限界

関連コマンド
[clear](#)[show statistics tcp](#)[\(config\) tcp](#)

show tech-support

TAC のサポートを利用するのに必要な情報を表示するには、**show tech-support EXEC** コマンドを使用します。

show tech-support [page]

シンタックスの説明

page (オプション) ページごとの出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

このコマンドを使用して、使用している WAAS デバイスについて TAC のサポートを得るのに必要なシステム情報を表示します。出力をディスク ファイルにロギングすることを推奨します ([「\(config\) logging」](#) コマンドを参照)。

例

次の例は、テクニカル サポート情報を表示します。



(注)

show tech-support コマンドの出力は長くなる可能性があるため、この例では一部を示します。

```
WAE# show tech-support
----- version and hardware -----

Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
...
Version: ce510-4.0.0.180

Compiled 18:08:17 Feb 16 2006 by cnbuild

System was restarted on Fri Feb 17 23:09:53 2006.
The system has been up for 5 weeks, 3 days, 2 hours, 9 minutes, 49 seconds.

CPU 0 is GenuineIntel Intel(R) Celeron(R) CPU 2.40GHz (rev 2) running at 2401MHz
.
Total 1 CPU.
512 Mbytes of Physical memory.
...
BIOS Information:
Vendor                : IBM
Version               : - [PLEC52AUS-C.52] -
Rel. Date             : 05/19/03
...
List of all disk drives:
Physical disk information:
```

■ show tech-support

```

disk00: Normal                (IDE disk)                76324MB ( 74.5GB)
disk01: Normal                (IDE disk)                76324MB ( 74.5GB)

```

Mounted filesystems:

MOUNT POINT	TYPE	DEVICE	SIZE	INUSE	FREE	USE%
/	root	/dev/root	31MB	26MB	5MB	83%
/sw	internal	/dev/md0	991MB	430MB	561MB	43%
/swstore	internal	/dev/md1	991MB	287MB	704MB	28%
/state	internal	/dev/md2	3967MB	61MB	3906MB	1%
/disk00-04	CONTENT	/dev/md4	62539MB	32MB	62507MB	0%
/local/local1	SYSFS	/dev/md5	3967MB	197MB	3770MB	4%
.../local1/spool	PRINTSPOOL	/dev/md6	991MB	16MB	975MB	1%

Software RAID devices:

DEVICE NAME	TYPE	STATUS	PHYSICAL DEVICES AND STATUS	
/dev/md0	RAID-1	NORMAL OPERATION	disk00/00 [GOOD]	disk01/00 [GOOD]
/dev/md1	RAID-1	NORMAL OPERATION	disk00/01 [GOOD]	disk01/01 [GOOD]
/dev/md0	RAID-1	NORMAL OPERATION	disk00/00 [GOOD]	disk01/00 [GOOD]
/dev/md1	RAID-1	NORMAL OPERATION	disk00/01 [GOOD]	disk01/01 [GOOD]
/dev/md2	RAID-1	NORMAL OPERATION	disk00/02 [GOOD]	disk01/02 [GOOD]

```

...
Currently content-filefilesystems RAID level is not configured to change.

```

```

----- running configuration -----

```

```

! WAAS version 4.0.0
!
!
...

```

```

----- processes -----

```

```

CPU average usage since last reboot:

```

```

cpu: 0.00% User, 1.79% System, 3.21% User(nice), 95.00% Idle

```

```

-----
PID  STATE  PRI  User  T  SYS  T  COMMAND
-----
1    S      0    20138 21906 (init)
2    S      0      0      0 (migration/0)
3    S     19      0      0 (ksoftirqd/0)
4    S    -10      0      0 (events/0)
5    S    -10      0      0 (khelper)
17   S    -10      0      0 (kacpid)
93   S    -10      0      0 (kblockd/0)
...

```

関連コマンド

[show version](#)

[show hardware](#)

[show disks details](#)

[show running-config](#)

[show processes](#)

[show processes memory](#)

[show memory](#)

[show interface](#)

[show cdp entry](#)

show cdp neighbors
show statistics wcep
show alarms all
show statistics tfo
show statistics tfo application
show statistics tfo saving
show statistics tfo pass-through
show statistics tfo peer
show tfo auto-discovery
show tfo status
show tfo accelerators
show tfo bufpool accounting
show policy-engine status
show policy-engine application
show statistics dre
show statistics dre peer
show statistics tep
show statistics ip
show statistics icmp
show standby
show statistics netstat
show disks SMART-info
show disks SMART-info details
show disks failed-sectors

show telnet

WAAS デバイスの Telnet サービス設定を表示するには、**show telnet EXEC** コマンドを使用します。

show telnet

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト 有効

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

例 次の例は、WAAS デバイスで Telnet がイネーブルになっているかどうかを表示します。

```
WAE# show telnet
telnet service is enabled
```

関連コマンド [telnet](#)
[\(config\) telnet enable](#)
[\(config\) exec-timeout](#)

show tfo accelerators

WAE の Traffic Flow Optimization (TFO) アクセラレータ情報を表示するには、**show tfo accelerators** EXEC コマンドを使用します。

```
show tfo accelerators
```

シンタックスの説明 このコマンドには引数やキーワードがありません。

コマンドモード EXEC

デバイスモード application-accelerator

例 次の例は WAE の TFO アクセラレータ情報を表示します。

```
WAE# show tfo accelerators
Name: TFO                               State: Registered, Handling Level: 100%
  Keepalive timeout: 3.0 seconds, Session timeouts: 0, Total timeouts: 0
  Last keepalive received 00.5 Secs ago
  Last registration occurred 11:21:43:38.4 Days:Hours:Mins:Secs ago
Name: EPM                               State: Registered, Handling Level: 100%
  Keepalive timeout: 5.0 seconds, Session timeouts: 0, Total timeouts: 0
  Last keepalive received 00.2 Secs ago
  Last registration occurred 11:21:43:36.7 Days:Hours:Mins:Secs ago
Name: CIFS                              State: Not Registered, Handling Level: 0%
  Keepalive timeout: 0.0 seconds, Session timeouts: 0, Total timeouts: 0
  Last keepalive received -Never-
  Last Registration occurred -Never-
```

関連コマンド [show tfo auto-discovery](#)

[show tfo bufpool](#)

[show tfo connection](#)

[show tfo filtering](#)

[show tfo status](#)

show tfo auto-discovery

WAE の Traffic Flow Optimization (TFO) 自動探索統計情報を表示するには、**show tfo auto-discovery** EXEC コマンドを使用します。

```
show tfo auto-discovery [blacklist {entries [netmask netmask] [] | statistics []}] [list] [] {begin regex [regex] | exclude regex [regex] | include regex [regex]}
```

シンタックスの説明

blacklist	(オプション) ブラックリスト サーバテーブルを表示します。
entries	自動探索ブラックリスト サーバテーブルのエントリすべてを表示します。
netmask	テーブル出力をフィルタリングするネットワーク マスクを表示します。
<i>netmask</i>	一致するアドレスを表示するネットワーク マスク (A.B.C.D/)
statistics	自動探索ブラックリスト サーバテーブルの管理統計情報を表示します。
list	(オプション) WAE が現在最適化またはパススルーしている TCP フローをリストします。
	(オプション) 出力修飾子
begin	正規表現と一致する行で開始します。
<i>regex</i>	一致する正規表現。複数の表現を入力できます。
exclude	正規表現と一致する行を除外します。
include	正規表現と一致する行を含めます。

コマンド モード

EXEC

デバイス モード

application-accelerator

例 次の例は WAE の TFO 自動探索統計情報を表示します。

```

WAE# show tfo auto-discovery
Auto discovery structure:
  Allocation Failure:                0
  Allocation Success:                6615
  Deallocations:                    6615
  Timed Out:                          0
Auto discovery table:
  Bucket Overflows:                  0
  Table Overflows:                    0
  Entry Adds:                        6615
  Entry Drops:                       6615
  Entry Count:                        0
  Lookups:                            6624
Bind hash add failures:               0
Route Lookup:
  Failures:                           0
  Success:                             0
Socket:
  Allocation failures:                0
  Accept pair allocation failures:     0
  Unix allocation failures:           0
  Connect lookup failures:            0
Packets:
  Memory allocation failures:         0
  Total Sent:                          6624
  Total Received:                     13228
  Incorrect length or checksum received: 0
  Invalid filtering tuple received:    0
  Received for dead connection:       0
  Ack dropped in synack received state: 0
  Non Syn dropped in nostate state:    0
Auto discovery failure:
  No peer or asymmetric route:       6604
  Insufficient option space:          0
  Invalid connection state:           0
  Missing Ack conf:                   0
Auto discovery success TO:
  Internal server:                     0
  External server:                     0
Auto discovery success FOR:
  Internal client:                     0
  External client:                     0
Auto discovery success SYN retransmission:
  Zero retransmit:                     0
  One retransmit:                      0
  Two+ retransmit:                     0
Auto discovery Miscellaneous:
  Intermediate device:                 0
  RST received:                       0
  SYNs found with our device id:      0
  SYN retransmit count resets:        0

```

関連コマンド

[show statistics tfo](#)
[show tfo accelerators](#)
[show tfo bufpool](#)
[show tfo connection](#)
[show tfo filtering](#)
[show tfo status](#)

show tfo bufpool

WAE の Traffic Flow Optimization (TFO) バッファ プール情報を表示するには、**show tfo bufpool** EXEC コマンドを使用します。

```
show tfo bufpool {accounting | from-index index | owner-connection conn-id |
  owner-module {RElib | tcpproxy} [from-index index | owner-connection conn-id |
  state {free | in-use} [from-index index | owner-connection conn-id | to-index index] |
  to-index index] | state {free | in-use} [from-index index | owner-connection conn-id |
  to-index index] | to-index index}
```

シンタックスの説明

accounting	バッファ プール全体の使用状況を表示します。
from-index	バッファ ユニットの開始インデックスを表示します。
<i>index</i>	バッファ ユニットのインデックス (0 ~ 4294967295)
owner-connection	バッファ ユニットのオーナー接続を表示します。
<i>conn-id</i>	接続 ID (0 ~ 4294967295)
owner-module	バッファ ユニットのオーナー モジュールを表示します。
RElib	RE ライブラリが所有するバッファ ユニットの示します。
tcpproxy	TCP プロキシが所有するバッファ ユニットの示します。
state	バッファ ユニットの状態 (フリーまたは使用) を表示します。
free	フリーのバッファ ユニットの示します。
in-use	使用中のバッファ ユニットの示します。
to-index	バッファ ユニットの終了インデックスを表示します。

コマンド モード

EXEC

デバイス モード

application-accelerator

例

次の例は WAE の TFO バッファ プール情報を表示します。

```
WAE# show tfo bufpool accounting
Total buffer pool size: 80740352 bytes
Free buffer: 80740352 bytes, in 78848 units (unit size: 1024 bytes)
Used buffer: 0 bytes, in 0 units
  Buffer usage by module:
    Tcpproxy: using 0 bytes, in 0 units
    RElib: using 0 bytes, in 0 units
    LZlib: using 0 bytes, in 0 units
  Buffer usage by connection:
```

関連コマンド

[show tfo accelerators](#)
[show tfo auto-discovery](#)
[show tfo connection](#)
[show tfo filtering](#)
[show tfo status](#)
[show statistics tfo](#)

show tfo connection

WAE の Traffic Flow Optimization (TFO) 接続情報を表示するには、**show tfo connection** EXEC コマンドを使用します。

```
show tfo connection [[summary] | [client-ip host-address | client-port port | peer-id mac |
server-ip host-address | server-port port]]
```

シンタックスの説明

summary	(オプション) 接続の要約 リストを表示します。
client-ip	(オプション) 送信元 IP アドレス
<i>host-address</i>	ホスト名または IP アドレス
client-port	(オプション) 送信元クライアントの IP アドレス
<i>port</i>	クライアントまたはサーバのポート番号
peer-id	(オプション) 特定ピアの接続統計情報を表示します。
<i>mac</i>	ピア ホストの MAC (メディア アクセス制御) アドレス
server-ip	(オプション) 宛先サーバの IP アドレス
server-port	(オプション) 宛先ポート番号

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

オプションなしでこのコマンドを使用すると、WAE の TFO 接続それぞれに関する詳細情報を表示します。接続の要約 リストを表示するには、**summary** オプションを使用します。

リスト中の F、D または L 最適化ポリシーを持つ接続では、**show statistics dre connection** コマンドと特定の接続 ID を識別する **id** オプションを使用して DRE 統計情報に関する補足情報を検索できます。

例

次の例は、WAE の TFO 最適化接続の要約を表示します。

```
WAE# show tfo connection summary

Optimized Connection List
Policy summary order: Our's, Peer's, Negotiated, Applied
F: Full optimization, D: DRE only, L: LZ Compression, T: TCP Optimization

Local-IP:Port      Remote-IP:Port      ConId  PeerId      Policy
10.77.156.99:59950  10.77.156.106:10005  21     00:11:25:ac:3e:04  F,F,F,F
10.77.156.99:59951  10.77.156.106:10007  22     00:11:25:ac:3e:04  F,F,F,F
10.77.156.99:59952  10.77.156.106:10008  23     00:11:25:ac:3e:04  F,F,F,F
10.77.156.99:59953  10.77.156.106:10009  24     00:11:25:ac:3e:04  F,F,F,F
10.77.156.99:59954  10.77.156.106:10010  25     00:11:25:ac:3e:04  F,F,F,F
```

関連コマンド

[show statistics dre connection](#)

[show statistics tfo](#)

[show tfo accelerators](#)

[show tfo auto-discovery](#)[show tfo bufpool](#)[show tfo filtering](#)[show tfo status](#)

show tfo egress-methods connection

WAE の接続セグメントに関する詳細な出力方式関連情報を表示するには、**show tfo egress-methods connection EXEC** コマンドを使用します。

```
show tfo egress-methods connection [local-ip ipaddress | local-port port | remote-ip ipaddress |
remote-port port]
```

シンタックスの説明

egress-methods	出力方式に関する詳細情報を表示します。
connection	接続の出力方式関連の統計情報を表示します。
local-ip	(オプション) 接続タブルのローカル IP アドレス
ipaddress	IP アドレス
local-port	(オプション) 接続タブルのローカル ポート番号
port	ポート番号
remote-ip	(オプション) 接続タブルのリモート IP アドレス
ipaddress	IP アドレス
remote-port	(オプション) 接続タブルのリモート ポート番号
port	ポート番号

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

オプションなしでこのコマンドを使用すると、WAE の TFO 接続それぞれに関する詳細情報を表示します。

このコマンドは、開始点から終了点までのデータ フローが複数のデバイスによって透過的に代行受信される環境において、接続セグメントに関する出力方式関連情報を表示します。接続タブルは、WAAS デバイス (WAE) が処理のため代行受信するエンドツーエンド接続の 1 つのセグメントを表します。

たとえば、単一のクライアント サーバ接続には次の 3 つのセグメントがあります (図 3-1 を参照)。

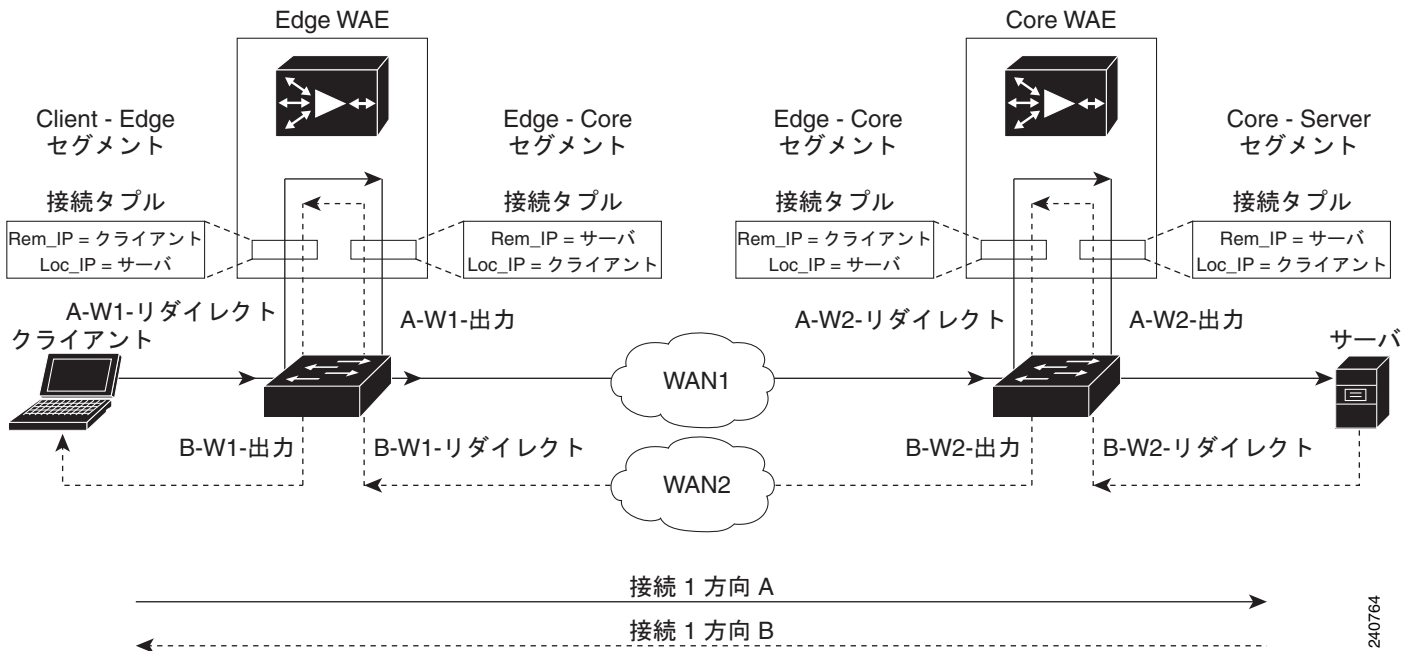
- クライアントと Edge WAE の間
- Edge WAE と Core WAE の間
- Core WAE とサーバの間

この例では、Edge WAE が参加するセグメント 2 つに次の接続タブル 2 つがあります。

- Client — Edge セグメントを表す接続タブル
- Edge — Core セグメントを表す接続タブル

出力表示では、これらの2つの接続タプルは TUPLE と MATE と表示されます (表 3-92 を参照)。表示する重要情報とは、接続タプルのローカルおよびリモート IP アドレスであり、TUPLE または MATE とマーク付けされているかどうかではありません。

図 3-1 3つのセグメントのあるトポロジと対応する接続タプル



WAAS デバイスは接続のクライアントエンドと接続のサーバエンド両方に対して透過的であるので、接続タプルのローカル IP アドレスはエンドツーエンド トポロジのセグメントによって異なります。

たとえば、WAAS がクライアントからパケットを代行受信する場合、このパケットは Client — Edge セグメントを表す接続タプルに入力します。このタプルでは、WAAS デバイスはサーバであるかのようにクライアントに表示されます。この接続タプルのローカル IP アドレスはサーバの IP アドレスに、リモート IP アドレスはクライアントの IP アドレスになります。同様に、Edge WAE がデータをクライアントに送信する場合、パケットはサーバから発信したかのように、この接続タプルから出力します。

WAAS がパケットをサーバに送信する場合、パケットは Edge — Core セグメントを表す接続タプルから出力します。このタプルでは、WAAS デバイスはクライアントであるかのようにサーバに表示されます。この接続タプルのローカル IP アドレスはクライアントの IP アドレスに、リモート IP アドレスはサーバの IP アドレスになります。同様に、Edge WAE が Core WAE からパケットを代行受信する場合、この接続タプルのデータはサーバから発信したかのように表示されます。

例 表 3-92 に、`show tfo egress-methods connection` 出力のフィールドについて説明します。

表 3-92 show tfo egress-methods connection コマンドのフィールドの説明

フィールド	説明
TUPLE	
Local-IP:Port	接続タプルのローカル デバイスの IP アドレスおよびポート番号
Remote-IP:Port	接続タプルのリモート デバイスの IP アドレスおよびポート番号
MATE	
Local-IP:Port	メイト接続タプルのローカル デバイスの IP アドレスおよびポート番号
Remote-IP:Port	メイト接続タプルのリモート デバイスの IP アドレスおよびポート番号
Egress method	使用する出力方式
WCCP Service Bucket	接続タプルおよびメイト接続タプルの WCCP サービス番号とバケット番号
Tuple Flags	代行受信方式および代行受信メカニズムのフラグ。このフィールドには、代行受信方式としての WCCP または NON-WCCP、代行受信メカニズムとしての L2 または GRE、このタプルがフロー保護メカニズムを通じてパケットを受信するかどうかを示す PROT の値が含まれます。
代行受信デバイス (ID)	
ID IP address	代行受信デバイスの IP アドレス
ID MAC address	代行受信デバイスの MAC (メディア アクセス制御) アドレス
ID IP address updates	代行受信デバイスの IP アドレス変更の数
ID MAC address updates	代行受信デバイスの MAC アドレス変更の数
Memory address	メモリアドレス

パケットが接続タプルに入力するたびに代行受信デバイスの IP アドレスまたは MAC アドレスが記録されます。コマンド出力の `updates` フィールドでは、代行受信デバイスの IP アドレスまたは MAC アドレスが記録されたかどうかを示します。たとえば、`ID MAC address updates` フィールドがゼロ (0) の場合、MAC アドレスは記録されず、`ID MAC address` フィールドはブランクになります。記録された代行受信デバイスの情報は、パケットが WAE から出力するとき使用されます。

接続タプルの出力方式が IP フォワーディングの場合、代行受信デバイス情報は必要なく、IP フォワーディング出力方式にも記録されないため、`updates` フィールドは常にゼロ (0) になります。

代行受信方式が WCCP GRE リダイレクトで、出力方式が WCCP GRE である場合、IP address フィールドのみが更新および記録されます。GRE ヘッダーの宛先アドレスは IP アドレスのみを受け付けるため、MAC アドレス情報は必要ではなく、記録もされません。

代行受信方式が WCCP L2 リダイレクトで出力方式が WCCP GRE である場合、着信 WCCP L2 パケットには MAC ヘッダーのみが含まれるため、MAC address および IP address フィールドは両方ともアップデートおよび記録されます。MAC アドレスは記録され、代行受信デバイスの IP アドレスは逆 ARP ルックアップから取得され、これも記録されます。この状況でパケットが接続タプルを出力する場合、パケットには記録された代行受信デバイスの宛先 IP アドレスのある GRE ヘッダーが含まれます。

アップデート回数は、特定のトポロジでは1より大きくなります。たとえば、冗長ルータ トポロジでは、2つのホスト間で同じ接続の同じ方向に、異なる代行受信ルータからパケットが着信します。パケットが着信するたびに、代行受信デバイスの MAC アドレスまたは IP アドレスは最後に記録されたアドレスと比較されます。MAC アドレスまたは IP アドレスが変更されると、updates フィールドは増加し、新しい MAC アドレスまたは IP アドレスが記録されます。

関連コマンド[show egress-methods](#)[show statistics tfo](#)

show tfo filtering

WAE が現在持っている着信および発信 TFO フローに関する情報を表示するには、**show tfo filtering EXEC** コマンドを使用します。

```
show tfo filtering [list [| {begin regex [regex] | exclude regex [regex] | include regex [regex]}]] [| {begin
regex [regex] | exclude regex [regex] | include regex [regex]}]
```

シンタックスの説明

list	(オプション) WAE が現在最適化またはパススルーしている TCP フローをリストします。
	(オプション) 出力修飾子
begin	正規表現と一致する行で開始します。
<i>regex</i>	一致する正規表現。複数の表現を入力できます。
exclude	正規表現と一致する行を除外します。
include	正規表現と一致する行を含めます。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

このコマンドは WAE が現在最適化している TCP フローをリストします。WAE によって最適化されず、パススルーされる TCP フローも含まれます。State 欄の「P」はパススルーされたフローを示します。

例

次の例は WAE の TFO 接続情報を表示します。

```
WAE# show tfo filtering
Number of filtering tuples:                2
Packets dropped due to ttl expiry:         0
Packets dropped due to bad route:         0
Syn packets dropped with our own id in the options: 0
Syn packets received and dropped on estab. conn: 0
Syn-Ack packets received and dropped on estab. conn: 0
Packets recvd on in progress conn. and not handled: 0
Packets dropped due to peer connection alive: 0
Packets dropped due to invalid TCP flags: 0
Packets dropped by FB packet input notifier: 0
Packets dropped by FB packet output notifier: 0
Number of errors by FB tuple create notifier: 0
Number of errors by FB tuple delete notifier: 0
Dropped WCCP GRE packets due to invalid WCCP service: 0
Dropped WCCP L2 packets due to invalid WCCP service: 0
```

```
WAE# show tfo filtering list
```

```
E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough
B: Bypass, T: Timedout, C: Closed
```

Local-IP:Port	Remote-IP:Port	Tuple (Mate)	State
10.99.11.200:1398	10.99.22.200:80	0xcba709c0 (0xcba70a00)	E
10.99.11.200:1425	10.99.22.200:80	0xcba70780 (0xcba707c0)	E
10.99.11.200:1439	10.99.22.200:5222	0xcba703c0 (0xcba70b40)	Sr
10.99.11.200:1440	10.99.22.200:5222	0xcba70400 (0xcba70440)	Sr
10.99.22.200:1984	10.99.11.200:80	0xcba70600 (0xcba70640)	E
10.99.22.200:1800	10.99.11.200:23	0xcba70480 (0x0)	PE
10.99.11.200:1392	10.99.22.200:80	0xcba70f80 (0x0)	E
10.99.22.200:20	10.99.11.200:1417	0xcba701c0 (0xcba70180)	E
10.99.11.200:1417	10.99.22.200:20	0xcba70180 (0x0)	E
10.99.22.200:1987	10.99.11.200:80	0xcba70240 (0xcba70200)	E
10.99.11.200:1438	10.99.22.200:5222	0xcba70900 (0xcba70580)	Sr
10.99.22.200:1990	10.99.11.200:80	0xcba70100 (0xcba70140)	E
10.99.22.200:80	10.99.11.200:1426	0xcba70740 (0xcba70700)	E
10.99.22.200:80	10.99.11.200:1425	0xcba707c0 (0xcba70780)	E
10.99.22.200:1985	10.99.11.200:80	0xcba70a40 (0xcba70a80)	E
10.99.22.200:80	10.99.11.200:1410	0xcba70500 (0xcba70540)	E
10.99.22.200:80	10.99.11.200:1398	0xcba70a00 (0xcba709c0)	E
10.99.22.200:80	10.99.11.200:1392	0xcba70f40 (0xcba70f80)	E
10.0.19.5:54247	10.1.242.5:80	0xc9e5b400 (0xc9e5b100)	ED



(注)

一部のステータスは凡例に記述されていません。D = 完了です。「ED」ステータスはペアのうち1つのソケットが終了 (D) したものの、メイトがまだ確立されている (E) 場合に発生します。

関連コマンド

[show tfo accelerators](#)

[show tfo auto-discovery](#)

[show tfo bufpool](#)

[show tfo connection](#)

[show tfo status](#)

show tfo status

WAE のグローバル Traffic Flow Optimization (TFO) ステータス情報を表示するには、**show tfo status** EXEC コマンドを使用します。

show tfo status

コマンドモード EXEC

デバイスモード application-accelerator

例 次の例は WAE のグローバル TFO ステータス情報を表示します。

```
WAE# show tfo status
Optimization Status:
  Configured: optimize full
  Current: optimize full
TFO is up since Sat Feb 25 13:18:51 2006
TFO is functioning normally.
Total number of optimized connections since start:      0
Number of active connections:                          0
Total number of peers:                                  0
```

関連コマンド

- [show statistics tfo](#)
- [show tfo accelerators](#)
- [show tfo auto-discovery](#)
- [show tfo bufpool](#)
- [show tfo connection](#)
- [show tfo filtering](#)

show tfo synq

SynQ モジュールの累積統計情報を表示するには、**show tfo synq** EXEC コマンドを使用します。

```
show tfo synq [list [| {begin regex [regex] | exclude regex [regex] | include regex [regex]}] [| {begin
regex [regex] | exclude regex [regex] | include regex [regex]}]
```

シンタックスの説明

list	(オプション) SynQ モジュールでトラッキングした接続を示します。
	(オプション) 出力修飾子
begin	正規表現と一致する行で開始します。
<i>regex</i>	一致する正規表現。複数の表現を入力できます。
exclude	正規表現と一致する行を除外します。
include	正規表現と一致する行を含めます。

コマンドモード

EXEC

デバイスモード

application-accelerator

使用上のガイドライン

SynQ モジュールで現在、トラッキングされている接続をリストするには、**show tfo synq list** コマンドを使用します。

例

次の例は、**show tfo synq** コマンドの出力を示します。

```
WWAE# show tfo synq
Synq structures allocations success:          0
Synq structures allocations failure:         0
Synq structures deallocations:               0
Synq table entry adds:                       0
Synq table entry drops:                     0
Synq table entry lookups:                   0
Synq table overflows:                       0
Synq table entry count:                     0
Packets received by synq:                   0
Packets received with invalid filtering tuple: 0
Non-syn packets received:                   0
Locally originated/terminating syn packets received: 0
Retransmitted syn packets received while in Synq: 0
Synq user structure allocations success:     0
Synq user structure allocations failure:     0
Synq user structure deallocations:          0
```

show transaction-logging

WAE のトランザクション ログ コンフィギュレーション設定とアーカイブされたトランザクション ログ ファイルのリストを表示するには、**show transaction-logging EXEC** コマンドを使用します。

show transaction-logging

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC

デバイス モード application-accelerator

使用上のガイドライン WAE のトランザクション ログの現在の設定に関する情報を表示するには、**show transaction-log** または **show transaction-logging EXEC** コマンドを使用します。この EXEC コマンドは両方とも同じ出力を表示します。HTTP と WMT MMS キャッシュ プロキシトランザクションおよび TFTP と ICAP トランザクションのトランザクション ログ ファイル情報が表示されます。



(注) セキュリティ上、**show transaction-log EXEC** コマンドの出力にパスワードは表示されません。

例 次の例は、WAE 上のトランザクション ログの現在の設定に関する情報を表示します。

```
WAAE# show transaction-logging
Transaction log configuration:
-----
TFO Logging is disabled.
TFO Archive interval: every-day every 1 hour
TFO Maximum size of archive file: 2000000 KB

TFO logging to remote syslog host is disabled.
TFO remote syslog host is not configured.
TFO facility is the default "*" which is "user".

Exporting files to ftp servers is disabled.
```

関連コマンド

- [clear](#)
- [transaction-log](#)
- [\(config\) transaction-logs](#)

show user

WAAS デバイスの特定ユーザのユーザ識別番号とユーザ名情報を表示するには、**show user EXEC** コマンドを使用します。

```
show user {uid number | username name}
```

シンタックスの説明

uid	ユーザの識別番号に基づいてユーザ情報を表示します。
<i>number</i>	識別番号 (0 ~ 65535)
username	ユーザの名前に基づいてユーザ情報を表示します。
<i>name</i>	ユーザの名前

コマンドのデフォルト設定

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

例

表 3-93 に、**show user** 出力のフィールドについて説明します。

表 3-93 show user コマンドのフィールドの説明

フィールド	説明
Uid	ユーザ ID 番号
Username	ユーザ名
Password	ログインパスワード。このフィールドは実際のパスワードを表示しません。
Privilege	ユーザの特権レベル
Configured in	ログイン認証が設定されているデータベース

関連コマンド

clear
show users administrative
(config) username

show users administrative

管理特権を持つユーザまたはロックアウトされたユーザを表示するには、**show users administrative EXEC** コマンドを使用します。

```
show users administrative {history | logged-in | locked-out}
```

シンタックスの説明

history	以前、アプライアンス CLI にログインしたことのあるユーザのリストを表示します。
logged-in	現在、アプライアンス CLI にログインしているユーザのリストを表示します。
locked-out	CLI からロックアウトされるユーザのリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

例

次に、以前アプライアンスにログインしたことのあるユーザのリストを表示する例を示します。

```
WAE# show users administrative history
<username>    <line>      <ip address/host>  <login details>
<username>    <line>      <ip address/host>  <login details>
<username>    <line>      <ip address/host>  <login details>
```

表 3-94 に、**show users administrative history** 出力のフィールドについて説明します。

表 3-94 show users administrative history コマンドのフィールドの説明

フィールド	説明
Username	履歴期間中にこのアプライアンスの CLI にログインしたユーザ
Line	このアプライアンスへのアクセスに使用する端末のタイプ
IP address/Host	このアプライアンスにログインしたユーザの IP アドレスおよびホスト名
Login details	曜日、月、日付、時間、およびユーザがログインしていないかまだログインしているか。

次に、現在アプライアンスにログインしているユーザのリストを表示する例を示します。

```
WAE# show users administrative logged-in
<username>    <line>      <ip address/host>  <login details>
<username>    <line>      <ip address/host>  <login details>
<username>    <line>      <ip address/host>  <login details>
```


表 3-95 に、**show users administrative logged-in** 出力のフィールドについて説明します。

表 3-95 show users administrative logged-in コマンドのフィールドの説明

フィールド	説明
Username	アプライアンスの CLI に現在ログインしたユーザ
Line	このアプライアンスへのアクセスに使用する端末のタイプ
IP address/Host	このアプライアンスにログインしたユーザの IP アドレスおよびホスト名
Login details	各ユーザがログインした曜日、月、日付、および時間

次に、アプライアンスからロックアウトされたユーザのリストを表示する例を示します。

```
WAE# show users administrative locked-out
  <username>
  <username>
```

clear users locked-out username username EXEC モード コマンドにより、ユーザ名データを使用できます。「[clear users](#)」を参照してください。

関連コマンド

[clear](#)

[clear users](#)

[\(config\) username](#)

show version

WAAS デバイスで動作中の WAAS ソフトウェアのバージョン情報を表示するには、**show version EXEC** コマンドを使用します。

show version [last | pending]

シンタックスの説明

last	最後に保存されたイメージのバージョン情報を表示します。
pending	保留中のアップグレードイメージのバージョン情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

例

表 3-96 に、**show version** 出力のフィールドについて説明します。

表 3-96 show version コマンドのフィールドの説明

フィールド	説明
Cisco Wide Area Application Services Software (WAAS) Copyright (c) year by Cisco Systems, Inc. Cisco Wide Area Application Services Software Release XXX (build bXXX month day year)	ソフトウェア アプリケーション、著作権、リリース、およびビルド情報
Version	デバイスで動作するソフトウェアのバージョン番号
Compiled hour:minute:second month day year by cnbuild	ソフトウェア ビルドのコンパイル情報
System was restarted on day of week month day hour:minute:second year	システムが最後に起動した日付と時間
The system has been up for X hours, X minutes, X seconds	最後のレポート以降、システムが動作していた時間の長さ

show wccp

WAE の Web Cache Connection Protocol (WCCP) 情報を表示するには、**show wccp EXEC** コマンドを使用します。

```

show wccp wide-area-engines
show wccp flows {tcp-promiscuous} [summary]
show wccp gre
show wccp masks {tcp-promiscuous} [summary]
show wccp routers
show wccp services [detail]
show wccp slowstart {tcp-promiscuous} [summary]
show wccp status

```

シンタックスの説明

wide-area-engines	どの WAE がどのルータに認識されているかを表示します。
flows	WCCP パケット フローを表示します。
tcp-promiscuous	TCP-PROMISCUOUS キャッシング サービスのパケット フローを表示します。
summary	(オプション)TCP-PROMISCUOUS キャッシング サービス パケット フローに関する要約情報を表示します。
gre	WCCP Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) パケット関連の情報を表示します。
masks	所定のサービスの WCCP マスク割り当てを表示します。
routers	この WAE が認識するルータとそうでないルータを表示します。
services	設定された WCCP サービスを表示します。
detail	(オプション) サービスの詳細を表示します。
slowstart	選択したサービスの WCCP スロースタート状態を表示します。
status	イネーブル化され、実行している WCCP のバージョンを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator

例

次の例は、**show wccp services** コマンドの出力を示します。

```

WAE# show wccp services
Services configured on this File Engine
      TCP Promiscuous 61
      TCP Promiscuous 62

```

次の例は、**show wccp services detail** コマンドの出力の一部を示します。

```

WAE# show wccp services detail
Service Details for TCP Promiscuous 61 Service
  Service Enabled           : Yes
  Service Priority          : 34
  Service Protocol          : 6
  Application               : Unknown
  Service Flags (in Hex)   : 501
  Service Ports             :      0      0      0      0
                          :      0      0      0      0

  Security Enabled for Service : No
  Multicast Enabled for Service : No
  Weight for this Web-CE       : 0
  Negotiated forwarding method : GRE
  Negotiated assignment method : HASH
  Negotiated return method    : GRE
  Received Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 0
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0
  Calculated Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 1741
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0

Service Details for TCP Promiscuous 62 Service
  Service Enabled           : Yes
  Service Priority          : 34
  Service Protocol          : 6
  Application               : Unknown
  Service Flags (in Hex)   : 502
  Service Ports             :      0      0      0      0
                          :      0      0      0      0

  Security Enabled for Service : No
  Multicast Enabled for Service : No
  Weight for this Web-CE       : 0
  Negotiated forwarding method : GRE
  Negotiated assignment method : HASH
  Negotiated return method    : GRE
  Received Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 0
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0
  Calculated Values:
  Source IP mask (in Hex)     : 0
  Destination IP mask (in Hex) : 1741
  Source Port mask (in Hex)   : 0
  Destination Port mask (in Hex) : 0

```

次の例は、**show wccp routers** コマンドの出力を示します。

```
WAE# show wccp routers
Router Information for Service: TCP Promiscuous 61
  Routers Configured and Seeing this File Engine(1)
    Router Id      Sent To      Recv ID
    0.0.0.0        10.10.20.1  00000000
  Routers not Seeing this File Engine
    10.10.20.1
  Routers Notified of but not Configured
  -NONE-
  Multicast Addresses Configured
  -NONE-
Router Information for Service: TCP Promiscuous 62
  Routers Configured and Seeing this File Engine(1)
    Router Id      Sent To      Recv ID
    0.0.0.0        10.10.20.1  00000000
  Routers not Seeing this File Engine
    10.10.20.1
  Routers Notified of but not Configured
  -NONE-
  Multicast Addresses Configured
  -NONE-
```

次の例は、**show wccp status** コマンドの出力を示します。

```
WAE# show wccp status
WCCP version 2 is enabled and currently active
```

表 3-97 に、**show wccp gre** 出力のフィールドについて説明します。

表 3-97 show wccp gre コマンドのフィールドの説明

フィールド	説明
Transparent GRE packets received	WCCP により代行受信されたかどうかに関係なく、WAE により受信された GRE パケットの総数。GRE は、WAE へのパスにルータが何台あってもパケットが WAE に到達できるようにするレイヤ 3 技術です。
Transparent non-GRE packets received	WAE に要求を透過的にリダイレクトするレイヤ 2 またはレイヤ 4 スイッチング (コンテンツ スイッチング モジュール [CSM]) でルータ ハードウェアのトラフィック代行受信およびリダイレクト機能のどちらかを使用して、WAE により受信された非 GRE パケットの数
Transparent non-GRE packets passed through	レイヤ 4 スイッチにより透過的に代行受信され、WAE にリダイレクトされる非 GRE パケットの数
Total packets accepted	クライアントのコンテンツ要求に応えるため、透過的に代行受信され、WAE にリダイレクトされるパケットの総数
Invalid packets received	リダイレクトされたパケットが GRE パケットで WCCP GRE ヘッダーのデータが無効である、またはリダイレクトされたパケットの IP ヘッダーが無効であるため、ドロップされるパケットの数
Packets received with invalid service	無効な WCCP サービス番号が格納されている WCCPバージョン 2 GRE リダイレクトパケットの数

表 3-97 show wccp gre コマンドのフィールドの説明 (続き)


フィールド	説明
Packets received on a disabled service	WAE でイネーブルになっていないサービスの WCCP サービス番号を指定する WCCP バージョン 2 GRE リダイレクト パケットの数。たとえば、HTTPS キャッシング サービス (サービス 70) がイネーブルになっていない場合に WAE にリダイレクトされる HTTPS 要求
Packets received too small	WAE にリダイレクトされ、WCCP GRE ヘッダーに必要な最小限のデータが格納されていない GRE パケットの数
Packets dropped due to zero TTL	リダイレクトされたパケットの IP ヘッダーの TTL がゼロのため、WAE によりドロップされる GRE パケットの数
Packets dropped due to bad buckets	不良マスクまたはハッシュ バケット判定により WCCP フロー リダイレクションを実行できなかったため、WAE によりドロップされるパケットの数  (注) バケットは、WAE クラスタ内の各 WAE へ割り当てられた割り当てハッシュのある一部と定義されます。この環境に WAE が1つだけ存在する場合は、256 個のバケットが割り当てられています。
Packets dropped due to no redirect address	フロー リダイレクションの宛先 IP アドレスを判別できなかったため、ドロップされるパケットの数
Packets dropped due to loopback redirect	宛先 IP アドレスがループバック アドレスと同じ場合に WAE によりドロップされるパケットの数
Pass-through pkts dropped on assignment update	TFO パススルー宛ですが、デバイスがバケットを所有していないので代わりにドロップされるパケットの数
Connections bypassed due to load	WAE が過負荷の場合、バイパスされる接続フローの数。過負荷バイパス オプションがイネーブルになっている場合、WAE はバケットをバイパスし、過負荷トラフィックを再ルーティングします。負荷が高いままの場合、さらにもう1つのバケットもバイパスされ、WAE が負荷を処理できるようになるまでバイパスが続きます。
Packets sent back to router	要求を受け取った WCCP 対応ルータに WAE により戻される要求の数。ルータはこのあとフローを、ブラウザから直接オリジン Web サーバへ送信し、WAE をバイパスします。
Packets sent to another WAE	WCCP サービス グループの別の WAE にリダイレクトされるパケットの数。サービス グループは最大 32 個の WAE と 32 個の WCCP 対応ルータで構成されます。どちらのパケット転送方式でも、ハッシュ パラメータが、WCCP サービス グループの WAE 間でのリダイレクトされたトラフィックのロード バランシング方法を指定します。
GRE fragments redirected	WAE により受信され、断片化された GRE パケットの数。これらのパケットはルータにリダイレクトされます。
GRE encapsulated fragments received	WAE が受信する GRE カプセル化フラグメントの数。tcp-promiscuous サービスはポート情報を検査しないので、ルータまたはスイッチが IP フラグメントを GRE カプセル化し、WAE にリダイレクトします。これらのフラグメントはパケットに再構成されてから、処理されます。

表 3-97 show wccp gre コマンドのフィールドの説明 (続き)

フィールド	説明
Packets failed encapsulated reassembly	再構成された GRE カプセル化パケットで、再構成健全性チェックに失敗したためドロップされた数。再構成された GRE カプセル化パケットは、複数の GRE カプセル化フラグメントで構成されます。このフィールドは、以前の統計に関連しています。
Packets failed GRE encapsulation	GRE ヘッダー付きパケットのカプセル化中に問題が発生してリダイレクトできなかつたため、WAE によりドロップされる GRE パケットの数
Packets dropped due to invalid fwd method	GRE を使用してリダイレクトされたが、WCCP サービスでレイヤ 2 リダイレクションが設定されていたため、WAE によりドロップされる GRE パケットの数
Packets dropped due to insufficient memory	GRE パケットの取り扱いに必要な付加メモリ リソースの割り当てに失敗したため、WAE によりドロップされる GRE パケットの数
Packets bypassed, no conn at all	傍受している TCP ポートがなかったため、存在するフローと関連付けできなかったパケットの数。WCCP は非対称パケットフローを取り扱うこともでき、WCCP サービスグループ(クラスタ内の最大 32 個の WAE と通信する最大 32 個のルータまたはスイッチ) で使用されるスイッチまたはルータの数に関係なく、常にキャッシュへの Web サーバの一貫したマッピングを維持します。
Packets bypassed, no pending connection	初期ハンドシェイクが完了しなかったため、保留中の接続と関連付けできなかったパケットの数
Packets due to clean wccp shutdown	クリーンな WCCP シャットダウンのためバイパスされる接続フローの数。WCCP の適切なシャットダウン中、WAE は処理中のフローについては引き続きサービスを提供する一方で、新しいフローのバイパスを開始します。フローの数が 0 になると、WAE は、リード WAE に自分のパケットを他の WAE へ再割り当てさせることで、自分自身はクラスタから脱退します。
Packets bypassed due to bypass-list lookup	バイパス リスト エントリによりバイパスされる接続フローの数。WAE はオリジン サーバからエラー応答を受信すると、サーバのエントリをそのバイパス リストに追加します。バイパスされたサーバに存在するコンテンツの次の要求を受信した場合は、パケットをバイパス ゲートウェイにリダイレクトします。バイパス ゲートウェイが設定されていない場合、パケットはリダイレクトしているレイヤ 4 スイッチに戻されます。
Packets received with client IP addresses	スプーフィングされている接続フローに関連するパケットの数。クライアントの IP アドレスをスプーフィングして WAE はクライアント IP (WAE 自身の IP アドレスとは別もの) を持つパケットを受信し、そのパケットを待機している正しいアプリケーションに送信できます。
Conditionally Accepted connections	条件付き受け付け機能のため、WAE によって受け付けられる接続フローの数

表 3-97 show wccp gre コマンドのフィールドの説明 (続き)

フィールド	説明
Conditionally Bypassed connections	条件付き受け付け機能のため、WAE によってバイパスされる接続フローの数
Packets dropped due to received on loopback	パケットがループバック インターフェイスで受信されましたが、デバイスのローカル アドレス宛ではなかったため、WCCP L2 インターセプト レイヤによってドロップされたパケットの数。パケットには有効でない、または使用しないルートがあります。
Packets w/WCCP GRE received too small	レイヤ 2 で WCCP 対応ルータによって透過的に代行受信されたあと WAE に送信され、GRE を使用してパケットをリダイレクトするために断片化が必要なパケットの数。WAE は IP ヘッダーをカプセル化できないので、パケットをドロップします。
Packets dropped due to IP access-list deny	WAE が WCCP GRE カプセル化パケットに適用する IP アクセス リストが WCCP アプリケーションのアクセスを拒否している場合 (<code>wccp access-list</code> コマンド)、WAE によりドロップされるパケットの数
Packets fragmented for bypass	IP ヘッダーを保持する十分なデータが格納されていない GRE パケットの数
Packet pullups needed	パケットを処理の一部として統合する回数。パケットがフラグメントとして受信され、最初のフラグメントに処理に必要な情報がすべて含まれていない場合に、統合が必要になります。
Packets dropped due to no route found	WAE がルートを発見できないため、ドロップされるパケットの数

関連コマンド

[\(config\) wccp access-list](#)[\(config\) wccp flow-redirect enable](#)[\(config\) wccp router-list](#)[\(config\) wccp shutdown](#)[\(config\) wccp tcp-promiscuous](#)[\(config\) wccp version](#)

show windows-domain

WAAS デバイスの Windows ドメイン設定情報を表示するには、**show windows-domain EXEC** コマンドを使用します。

show windows-domain

シンタックスの説明 このコマンドには引数やキーワードがありません。

コマンド モード EXEC

デバイス モード application-accelerator
replication-accelerator
central-manager

例 表 3-98 では、**show windows-domain** 出力のフィールドについて説明します。

表 3-98 show windows-domain コマンドのフィールドの説明

フィールド	説明
Login Authentication for Console/ Telnet Session:	セッションのプライマリ ログイン認証方式のステータス。enabled または disabled です。
Configuration Authentication for Console/ Telnet Session:enabled (secondary)	セッションのセカンダリ ログイン認証方式のステータス。enabled または disabled です。
Windows domain Configuration:	Windows ドメイン設定を表示します。
Workgroup	ワークグループ識別ストリング
Comment	コメント行
Net BIOS	WAE の Windows NetBIOS 名
Realm	Kerberos レalm (Windows ドメイン名と類似、Kerberos は除く)
WINS Server	WINS サーバの IP アドレス
Password Server	Kerberos サーバの Domain Name System (DNS; ドメインネーム システム) 名
Security	設定された認証のタイプ。NTLM の「Domain」または Kerberos の「ADS」のいずれか。
管理グループ	
Super user group	Active Directory (AD) ドメイン名。このグループのユーザには管理権限があります。
Normal user group	AD グループ名。このグループのユーザは、WAE の通常 / デフォルトの特権レベルを持っています。

関連コマンド [windows-domain](#)
[\(config\) windows-domain](#)

shutdown

WAAS デバイスをシャットダウンするには、**shutdown EXEC** コマンドを使用します。

shutdown [poweroff]

シンタックスの説明

poweroff (オプション) すべてのアプリケーションとオペレーティング システムを閉じたあと、電源を切断します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

制御シャットダウンとは、デバイスの電源を切断しないで WAAS デバイスを正常にシャットダウンするプロセスを指します。制御シャットダウンでは、すべてのアプリケーションアクティビティとオペレーティング システムが WAE で正常に停止しますが、電源は投入されたままです。WAAS デバイスの制御シャットダウンにより、WAAS デバイスが処理されているときのダウンタイムを最小限にできます。



注意

制御シャットダウンが実行されていない場合、WAAS のファイル システムは破損する可能性があります。WAAS デバイスが正常にシャットダウンされていない場合、リブートするのに長くかかります。



(注)

ソフトウェアによる電源切断後は、WAAS デバイスは WAAS ソフトウェアを使用して電源を再度投入できません。1 度電源ボタンを押して、WAAS デバイスをオンラインに戻す必要があります。

shutdown EXEC コマンドは、WAAS デバイスの正常なシャットダウンを助けるコマンドで、すべての WAE ハードウェア モデルでサポートされています。**shutdown poweroff** コマンドも、ACPI をサポートするので、すべての WAE ハードウェア モデルでサポートされています。

shutdown コマンドはすべてのアプリケーションを終了し、すべてのシステム アクティビティを停止しますが、電源は投入したままに維持します。ファンは動作し続け、電源 LED は点灯し、デバイスに電源がまだ入っていることを示します。シャットダウンプロセスが完了すると、デバイスのコンソールに次のメニューが表示されます。

```
===== SHUTDOWN SHELL =====
System has been shut down.
```

You can

0. Power down system by pressing and holding power button
 1. Reload system by software
 2. Power down system by software
- [1-2]?

shutdown poweroff コマンドはすべてのアプリケーションとオペレーティング システムを終了し、すべてのシステム アクティビティを停止し、電源を切断します。ファンは動作を停止し、電源 LED は点滅し始め、デバイスの電源が切断されていることを示します。



(注)

shutdown または **shutdown poweroff** コマンドを使用すると、次の電源投入時とデバイスのブート時に、ファイル システムのチェックが行われません。

表 3-99 に、WAAS デバイスに対する **shutdown** のみの動作と **shutdown poweroff** の動作について説明します。

表 3-99 shutdown コマンド動作の説明

アクティビティ	プロセス
ユーザが WAE でシャットダウン操作を実行	shutdown poweroff WAE# shutdown poweroff
WAE をオンラインに戻すためユーザが手動操作	shutdown poweroff の実行後、電源ボタンを 1 度押して WAAS デバイスをオンラインに戻す必要があります。
ファイル システムのチェック	電源を再度投入して WAAS デバイスをリブートしたあとは、実行されません。

コンソールセッションまたはリモートセッションから **shutdown EXEC** コマンドを入力することで (Telnet または SSH バージョン 1 あるいは SSH バージョン 2)、WAAS デバイスに対してシャットダウンを実行できます。

WAAS デバイスに対してシャットダウンを実行するには、次のように **shutdown EXEC** コマンドを入力します。

```
WAE# shutdown
```

システム設定を保存するか尋ねられたら、**yes** を入力します。

```
System configuration has been modified. Save? [yes]: yes
```

シャットダウンを進めるか尋ねられたら、**Enter** を押してシャットダウンの操作を進めます。

```
Device can not be powered on again through software after shutdown.
Proceed with shutdown? [confirm]
```

メッセージが表示され、この WAE のすべてのサービスがシャットダウン中であることを通知します。

```
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

システムをシャットダウンすると（システムが停止する）、WAAS ソフトウェアのシャットダウンシェルが、コンソール上にシステムの現在の状態を表示します（例：「System has been shut down」）。ソフトウェアによる電源切断を実行するか（**Power down system by software** オプション）、ソフトウェアを介してシステムをリロードするか尋ねられます。

```
===== SHUTDOWN SHELL =====
System has been shut down.
You can either
    Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

WAAS デバイスの電源を切断するには、WAAS デバイスの電源ボタンを押し続けるか、次のいずれかの方法で **shutdown poweroff** を実行します。

- コンソールのコマンドラインで、次のように要求があった場合、**2** を入力します。

```
===== SHUTDOWN SHELL =====
System has been shut down.
You can either
    Power down system by pressing and holding power button
or
1. Reload system through software
2. Power down system through software
```

- WAAS CLI で、次のように **shutdown poweroff EXEC** コマンドを入力します。

```
WAE# shutdown poweroff
```

システム設定を保存するか尋ねられたら、**yes** を入力します。

```
System configuration has been modified. Save?[yes]:yes
```

決定の確認を求められたら、**Enter** キーを押します。

```
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

例 次の例では、**shutdown** コマンドを使用して、すべてのアプリケーションを終了し、すべてのシステムアクティビティを停止します。

```
WAE1# shutdown
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after shutdown.
Proceed with shutdown?[confirm]
Shutting down all services, will timeout in 15 minutes.
shutdown in progress ..System halted.
```

次の例では、**shutdown poweroff** コマンドを使用して、すべてのアプリケーションを終了し、すべてのシステム アクティビティを停止、WAAS デバイスの電源を切断します。

```
WAE2# shutdown poweroff
System configuration has been modified. Save?[yes]:yes
Device can not be powered on again through software after poweroff.
Proceed with poweroff?[confirm]
Shutting down all services, will timeout in 15 minutes.
poweroff in progress ..Power down.
```

snmp trigger

WAAS デバイスで監視目的でユーザが選択した MIB オブジェクトのしきい値を設定するには、**snmp trigger EXEC** コマンドを使用します。設定をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
snmp trigger {create mibvar [wildcard] [wait-time [absent [LINE | mibvar1 mibvar1] [LINE | mibvar2
mibvar2] [LINE | mibvar3 mibvar3] [LINE] | equal [absolute value [[LINE | mibvar1 mibvar1]
[LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1 mibvar1]
[LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | falling [absolute value [LINE |
mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE
| mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] |
greater-than [absolute value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE |
mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1 mibvar1] [LINE | mibvar2 mibvar2] [LINE
| mibvar3 mibvar3] [LINE]] | less-than [absolute value [LINE | mibvar1 mibvar1] [LINE | mibvar2
mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1 mibvar1] [LINE | mibvar2
mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | on-change [[LINE | mibvar1 mibvar1][LINE |
mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]] | present [LINE | mibvar1 mibvar1] [LINE |
mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | rising [absolute value [LINE | mibvar1
mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE] | delta value [LINE | mibvar1
mibvar1] [LINE | mibvar2 mibvar2] [LINE | mibvar3 mibvar3] [LINE]]] | delete mibvar}
```

シンタックスの説明

create	MIB オブジェクトのしきい値を設定します。
<i>mibvar</i>	監視対象の MIB オブジェクトの名前、またはモニタリングしきい値を削除する MIB オブジェクトの名前
wildcard	(オプション) 指定された MIB 変数名を、ワイルドカードが含まれているものとして取り扱います。
<i>wait-time</i>	(オプション) トリガー サンプルの間で待機する秒数 (60 ~ 600)
absent	(オプション) 不在検査を適用します。
<i>LINE</i>	(オプション) 作成されるしきい値の説明
mibvar1、mibvar2、mibvar3	(オプション) MIB オブジェクトを通知に追加します。
<i>mibvar1、mibvar2、mibvar3</i>	通知に追加する MIB オブジェクトの名前
equal	等価しきい値検査を適用します。
absolute	(オプション) 絶対サンプル タイプを使用します。
<i>value</i>	(オプション) サンプルの絶対またはデルタ値
delta	デルタ サンプル タイプを使用します。
falling	下限しきい値検査を適用します。
greater-than	しきい値を越える検査を適用します。

less-than	しきい値未満の検査を適用します。
on-change	変動の有無についての検査を適用します。
present	存在検査を適用します。
rising	上限しきい値検査を適用します。
delete	MIB オブジェクトのしきい値を削除します。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン **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、特定の設定に関連している他の MIB オブジェクトに対して追加の SNMP トラップを定義できます。すべてのサポート MIB の中から任意の MIB オブジェクトを、トラップとして選択できます。トラップは次に示す各種の検査に基づいて生成できます。

- **absent** — 最後のサンプリング時点で存在していた指定の MIB オブジェクトが、現在のサンプリング時点でもはや存在しない。
- **equal** — 指定した MIB オブジェクトの値が、指定したしきい値と等しい。
- **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ている。この条件に対してトラップが生成されると、サンプリングした MIB オブジェクトの値がしきい値を超えて上昇し、ふたたび下限しきい値を下回らない限り、同じ条件の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、指定したしきい値より大きい。
- **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来変動している。
- **Present** — 以前のサンプリング時点で不在だった指定の MIB オブジェクトが、現在のサンプリング時点で存在する。
- **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ている。この条件に対してトラップが生成されると、サンプリングした MIB オブジェクトの値がしきい値より低くなり、ふたたび上限しきい値を上回らない限り、同じ条件の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くことができます。絶対サンプルタイプは、0 ~ 4294967295 の間の固定整数値に対して、検査が評価されたサンプルタイプです。デルタ サンプル タイプは、現在のサンプリングと以前のサンプリングの間における MIB オブジェクトの値の変動に対して、検査が評価されたサンプルタイプです。

SNMP トラップの設定後、作成したばかりのイベント トラップが生成されるようにするには、**snmp-server enable traps event** グローバル コンフィギュレーション コマンドを使用する必要があります。また、システムをリブートしても SNMP トラップ設定を保持するには、**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永続性を設定し、**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。

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

```
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 Equality 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
```

WAE が SNMP トラップを送信するように設定すると、この新たに作成されたトラップの結果を、**show snmp events EXEC** コマンドを使用して表示できます。

ユーザ作成の SNMP トラップを削除することもできます。次の例は、前の例で作成した *esConTabIsConnected* に対して設定されたトラップを削除する方法を示します。

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

関連コマンド

- [\(config\) snmp-server community](#)
- [\(config\) snmp-server contact](#)
- [\(config\) snmp-server enable traps](#)
- [\(config\) snmp-server group](#)
- [\(config\) snmp-server host](#)
- [\(config\) snmp-server location](#)
- [\(config\) snmp-server mib persist event](#)
- [\(config\) snmp-server notify inform](#)
- [\(config\) snmp-server user](#)
- [\(config\) snmp-server view](#)

ssh

セキュアでないネットワークを介して信頼できないクライアント マシンと WAAS デバイス間のセキュアな暗号化コミュニケーションを可能にするには、**ssh EXEC** コマンドを使用します。

ssh options

シンタックスの説明

options **ssh EXEC** コマンドと併用するオプション。利用できるオプションの詳細は、Request for Comments (RFC 4254) (<http://www.rfc-archive.org/getrfc.php?rfc=4254>) を参照してください。

デフォルト

デフォルトでは、WAAS デバイスの Secure Shell (SSH; セキュア シェル) 機能はディセーブルになっています。

コマンド モード

EXEC

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

SSH は、サーバとクライアント プログラムで構成されます。Telnet と同様、クライアント プログラムを使用して SSH サーバが稼働するマシンにリモートでログインできますが、クライアントとサーバ間を転送されるメッセージが暗号化される点が Telnet と異なります。SSH の機能には、ユーザ認証、メッセージの暗号化、およびメッセージ認証があります。



(注)

Telnet デーモンは今までもおり WAAS デバイスで利用できます。SSH は Telnet に取って代わるものではありません。

関連コマンド

(config) sshd
(config) ssh-key-generate

tcpdump

ネットワーク トラフィックをダンプするには、**tcpdump** EXEC コマンドを使用します。

tcpdump [*LINE*]

シンタックスの説明

LINE (オプション) ダンプ オプション

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

TCPdump は、ネットワーク インターフェイスを通過するパケットを代行受信してキャプチャできるようにするユーティリティです。ネットワーク アプリケーションのトラブル シューティングに利用できます。

通常のネットワーク動作中は、ネットワーク インターフェイスにアドレス指定されたパケットだけが代行受信されて、TCP/IP プロトコル レイヤ スタックの上位レイヤに渡されます。インターフェイスにアドレス指定されていないパケットは無視されます。混合モードでは、インターフェイスによって受信される予定のないパケットも代行受信され、プロトコル スタックの上位レベルに渡されます。TCPdump は、ネットワーク インターフェイスを混合モードにすると作動します。TCPdump は、フリーの libpcap (パケット キャプチャ ライブラリ) を使用します。

この例に示すように、利用可能なオプションを表示するには、**-h** オプションを使用します。

```
WAE# tcpdump -h
tcpdump version 3.8.1 (jlemon)
libpcap version 0.8
Usage: tcpdump [-aAdDeflLnNOPqRStuUvX] [-c count] [-C file_size ]
               [-E algo:secret ] [-F file ] [-i interface ] [-r file ]
               [-s snaplen ] [-T type ] [-w file ] [-y datalinktype ]
               [ expression ]
```

例

次の例では、ファイル *tcpdump.txt* へのネットワーク トラフィックのダンプを開始します。

```
WAE# tcpdump -w tcpdump.txt
```

関連コマンド

[less](#)

[ping](#)

[tetherreal](#)

[traceroute](#)

telnet

Telnet クライアントを使用して WAAS デバイスにログインするには、**telnet EXEC** コマンドを使用します。

```
telnet {hostname | ip-address} [portnum]
```

シンタックスの説明

<i>hostname</i>	ネットワーク デバイスのホスト名
<i>ip-address</i>	ネットワーク デバイスの IP アドレス
<i>portnum</i>	(オプション) ポート番号 (1 ~ 65535)。デフォルトのポート番号は 23 です。

デフォルト

デフォルトのポート番号は 23 です。

コマンドモード

EXEC

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

escape や **suspend** コマンドなどの UNIX シェル機能は、Telnet クライアントでは利用できません。また、マルチ Telnet セッションはサポートされていません。Telnet クライアントでは宛先ポートを指定できます。

例

次の例は、Telnet クライアントを使用して WAAS デバイスにログインする方法を示します。

```
WAE# telnet cisco-wae
WAE# telnet 10.168.155.224
WAE# telnet cisco-wae 2048
WAE# telnet 10.168.155.224 2048
```

関連コマンド

[\(config\) telnet enable](#)

terminal

コンソール ウィンドウに表示される行数を設定したり、現在のコンソールの **debug** コマンドの出力を表示したりするには、**terminal EXEC** コマンドを使用します。

```
terminal {length length | monitor [disable]}
```

シンタックスの説明

length	端末上の表示の長さを設定します。
<i>length</i>	端末上の表示の長さ (0 ~ 512)。長さを 0 に設定するということは、中断がないということです。
monitor	デバッグ出力を現在の端末にコピーします。
disable	(オプション) 指定された端末でのモニタリングをディセーブルにします。

デフォルト

デフォルトは 24 行です。

コマンドモード

EXEC

デバイスモード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

length パラメータとして 0 を入力すると、画面への出力は中断されません。 *length* の 0 以外のすべての値について、出力の行数が指定された *length* の数に達すると、**-More-** プロンプトが表示されます。**-More-** プロンプトは出力行を考慮します。次の画面を表示するには、**Spacebar** を押します。一度に 1 行を表示するには、**Enter** キーを押します。

terminal monitor コマンドにより、Telnet セッションは、コンソールに表示される **debug** コマンドの出力を表示できます。Telnet セッションが終了するまで、モニタリングは継続します。

例

次の例は、表示される行数を 20 に設定します。

```
WAE# terminal length 20
```

次の例は、端末を中断なしに設定します。

```
WAE# terminal length 0
```

関連コマンド

すべての **show** コマンド

tethereal

コマンドラインからネットワーク トラフィックを分析するには、**tethereal** EXEC コマンドを使用します。

```
tethereal [LINE]
```

シンタックスの説明	<i>LINE</i> (オプション) オプション
デフォルト	デフォルトの動作や値はありません。
コマンド モード	EXEC
デバイス モード	application-accelerator replication-accelerator central-manager
使用上のガイドライン	Tethereal は、ネットワーク トラフィック アナライザ ツール Ethereal のコマンドラインバージョンです。TCPdump と同様、パケット キャプチャ ライブラリ (libpcap) を使用します。ネットワーク トラフィックの分析とは別に、Tethereal はパケット デコード機能も備えています。

次の例は、WAAS **tetherreal** コマンドで利用できるオプションを示します。

```
WAE# tetherreal -h
This is GNU tetherreal 0.10.6
(C) 1998-2004 Gerald Combs <gerald@ethereal.com>
Compiled with GLib 1.2.9, with libpcap 0.6, with libz 1.1.3, without libpcrc,
without UCD-SNMP or Net-SNMP, without ADNS.
NOTE: this build does not support the "matches" operator for Ethereal filter
syntax.
Running with libpcap (version unknown) on Linux 2.4.16.

tetherreal [ -vh ] [ -DlInpqSVx ] [ -a <capture autostop condition> ] ...
[ -b <number of ring buffer files>[:<duration>] ] [ -c <count> ]
[ -d <layer_type>==<selector>,<decode_as_protocol> ] ...
[ -f <capture filter> ] [ -F <output file type> ] [ -i <interface> ]
[ -N <resolving> ] [ -o <preference setting> ] ... [ -r <infile> ]
[ -R <read filter> ] [ -s <snaplen> ] [ -t <time stamp format> ]
[ -T pdml|ps|psml|text ] [ -w <savefile> ] [ -y <link type> ]
[ -z <statistics string> ]
Valid file type arguments to the "-F" flag:
libpcap - libpcap (tcpdump, Ethereal, etc.)
rh6_1libpcap - RedHat Linux 6.1 libpcap (tcpdump)
suse6_3libpcap - SuSE Linux 6.3 libpcap (tcpdump)
modlibpcap - modified libpcap (tcpdump)
nokialibpcap - Nokia libpcap (tcpdump)
lanalyzer - Novell LANalyzer
ngsniffer - Network Associates Sniffer (DOS-based)
snoop - Sun snoop
netmon1 - Microsoft Network Monitor 1.x
netmon2 - Microsoft Network Monitor 2.x
ngwsniffer_1_1 - Network Associates Sniffer (Windows-based) 1.1
ngwsniffer_2_0 - Network Associates Sniffer (Windows-based) 2.00x
visual - Visual Networks traffic capture
5views - Accellent 5Views capture
niobserverv9 - Network Instruments Observer version 9
default is libpcap
```

関連コマンド

[tcpdump](#)

traceroute

WAAS デバイスからリモート ホストへのルートを追跡するには、**traceroute** EXEC コマンドを使用します。

```
traceroute {hostname | ip-address}
```

シンタックスの説明

<i>hostname</i>	リモート ホストの名前
<i>ip-address</i>	リモート ホストの IP アドレス

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

traceroute はほとんどのオペレーティング システムで広範に利用できるユーティリティです。PING と同様、ネットワークの接続を判別する貴重なツールです。PING では、2 つのエンド システム間で接続があるかどうか検出できます。Traceroute もこれを行います。2 つのシステム間の中間ルータもリストします。したがって、パケットがあるシステムから別のシステムへと取る可能性のあるルートを確認できます。ホスト名か IP アドレスがわかっているときに、**traceroute** を使用してリモート ホストへのルートを検出します。

例

次の例は、WAAS デバイスと IP アドレスが 10.0.0.0 のデバイス間のルートをトレースします。

```
WAE# traceroute 10.0.0.0
traceroute to 10.0.0.0 (10.0.0.0), 30 hops max, 38 byte packets
 1 sblab2-rtr.abc.com (192.168.10.1)  0.959 ms  0.678 ms  0.531 ms
 2 192.168.1.1 (192.168.1.1)  0.665 ms  0.576 ms  0.492 ms
 3 172.24.115.66 (172.24.115.66)  0.757 ms  0.734 ms  0.833 ms
 4 sjc20-sbb5-gw2.abc.com (192.168.180.93)  0.683 ms  0.644 ms  0.544 ms
 5 sjc20-rbb-gw5.abc.com (192.168.180.9)  0.588 ms  0.611 ms  0.569 ms
 6 sjce-rbb-gw1.abc.com (172.16.7.249)  0.746 ms  0.743 ms  0.737 ms
 7 sj-wall-2.abc.com (172.16.7.178)  1.505 ms  1.101 ms  0.802 ms
 8 * * *
 9 * * *
 .
 .
 .
29 * * *
30 * * *
```

関連コマンド

[ping](#)

transaction-log

トランザクション ログを強制的にエクスポートまたはアーカイブするには、**transaction-log EXEC** コマンドを使用します。

```
transaction-log {export | tfo force archive}
```

シンタックスの説明

export	WAE のトランザクション ファイルを強制的にアーカイブします。
tfo force archive	Traffic Flow Optimization (TFO) トランザクション ファイルを強制的にアーカイブします。

コマンド モード

EXEC

デバイス モード

application-accelerator

例

次の例は、WAE のトランザクション ファイルを強制的にアーカイブします。

```
WAE# transaction-log export
```

次の例は、WAE の TFO トランザクション ログ ファイルを強制的にアーカイブします。

```
WAE# transaction-log tfo force archive
```

関連コマンド

[\(config\) transaction-logs](#)

[show transaction-logging](#)

type

ファイルを表示するには、**type EXEC** コマンドを使用します。

type filename

シンタックスの説明

<i>filename</i>	ファイルの名前
-----------------	---------

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドを使用して、WAAS デバイスの任意のファイル ディレクトリ内のファイルのコンテンツを表示します。このコマンドを使用して、トランザクション ロギングやシステム ロギング (Syslog) などの機能のモニタもできます。

例

次の例は、*syslog.txt* ファイルのコンテンツの表示方法を示します。

```
WAB# type /local1/syslog.txt
```

関連コマンド

[cpfile](#)
[dir](#)
[lls](#)
[ls](#)
[pwd](#)
[rename](#)

type-tail

ログ ファイルの終わりから指定された行数分を表示したり、ファイルに新しい行が追加されるごとに継続してファイルの終わりを表示したり、ファイルの特定の行から開始したり、ファイルの特定の行を組み入れまたは除外したりするには、EXEC モードで **type-tail** コマンドを使用します。

```
type-tail filename [line | follow || {begin LINE | exclude LINE | include LINE}]
```

シンタックスの説明

<i>filename</i>	調べる対象のファイル
<i>line</i>	(オプション) ファイルの終わりからの表示する行数 (1 ~ 65535)
follow	(オプション) ファイルに新しい行が追加されるごとに継続してファイルの終わりを表示します。
	(オプション) begin 、 exclude 、 include の各出力修飾子に基づいてファイルのコンテンツを表示します。
begin	ファイルの表示を開始する行を特定します。
<i>LINE</i>	表示を開始する、または表示に組み入れまたは除外する、ファイル内の位置を指示する正規表現
exclude	ファイルの表示から除外される行を指示します。
include	ファイルの表示に組み入れる行を指示します。

デフォルト

最後の 10 行が表示されます。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

この EXEC コマンドにより、ファイルの終わりを表示することでログ ファイルを監視できます。表示するファイルの終わりからの行数を指定することも、新しい情報がログに記録されるたびにファイルの最後の行を追うこともできます。**follow** オプションにより最後の行が継続的にスクロールされるのを中止するには、キー シーケンスの **Ctrl-C** を使用します。

さらに、出力修飾子を使用すれば、表示する情報のタイプの指示もできます。出力修飾子により、特定の行の組み入れや除外、ファイルの表示の開始位置の指示ができます。

例 次の例は、*/local1* ディレクトリ内のログ ファイルのリストを検索し、*syslog.txt* ファイルの最後の 10 行を表示します。この例では、表示される行数が指定されていないので、デフォルトの 10 行が使用されています。

```
WAE# ls /local1
actona
core_dir
crash
dbupgrade.log
downgrade
errorlog
logs
lost+found
sa
service_logs
spool
syslog.txt
syslog.txt.1
syslog.txt.2
syslog.txt.3
syslog.txt.4
var
wdd.sh.signed
```

```
WAE# type-tail /local1/syslog.txt
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get https
equest throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/ftp connection 5
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/ftp' from dataserver
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: unable to get ftp-ov
er-http request throughput stats(error 4)
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: setValues getMethod
all ...
Apr 17 00:21:09 edge-wae-11 java: %CE-CMS-4-700001: setValues found...
Apr 17 00:21:48 edge-wae-11 java: %CE-CMS-4-700001: ds_getStruct got err
r : 4 for key stat/cache/http/perf/throughput/requests/sum connection 5
Apr 17 00:21:48 edge-wae-11java: %CE-CMS-4-700001: ds_getStruct: unable
to get `stat/cache/http/perf/throughput/requests/sum' from dataserver
Apr 17 00:21:48 edge-wae-11 java: %CE-CMS-4-700001: unable to get http r
quest throughput stats(error 4)
Apr 17 00:23:20 edge-wae-11 java: %CE-TBD-3-100000: WCCP_COND_ACCEPT: TU
LE DELETE conditional accept tuple {Source IP [port] = 0.0.0.0 [0] Destinatio
IP [port] = 32.60.43.2 [53775] }returned error: -1 errno 9
```

次の例では、ファイルの増大に伴って *syslog.txt* ファイルを追います。

```
WAE# type-tail /local1/syslog.txt follow
```

undebug

デバッグ機能をディセーブルにするには、**undebug EXEC** コマンドを使用します (**debug EXEC** コマンドの **no** 形式も参照)。

application-accelerator デバイス モードでは、**undebug** コマンドは次のとおりです。

```
undebug aaa accounting
undebug all
undebug authentication {content-request | user | windows-domain}
undebug buf {all | dmbuf | dmsg}
undebug cdp {adjacency | events | ip | packets}
undebug cli {all | bin | parser}
undebug cms
undebug dataserver {all | clientlib | server}
undebug dhcp
undebug dre {aggregation | all | cache | connection {aggregation [acl] | cache [acl] | core [acl] |
message [acl] | misc [acl] | acl} | core | lz | message | misc}
undebug epm
undebug flow monitor tcpstat-v1
undebug logging all]
undebug ntp
undebug print-spooler {all | brief | errors | warnings}
undebug rbc
undebug snmp {all | cli | main | mib | traps}
undebug tfo {buffer-mgr | connection [auto-discovery [acl] | comp-mgr [acl] | conn-mgr [acl] |
egress-method [acl] | filtering [acl] | netio-engine [acl] | policy-engine [acl] | synq [acl] | acl] |
stat-mgr | translog}
undebug translog export
undebug wafs {{all | core-fe | edge-fe | manager | utilities} {debug | error | info | warn}}
undebug wccp {all | detail | error | events | keepalive | packets | slowstart}
```



(注)

dre、*epm*、*flow*、*print-spooler*、*rbc*、*tfo*、*translog*、*wafs*、および *wccp* コマンド オプションは application-accelerator デバイス モードのみでサポートされます。

central manager デバイス モードでは、**undebug** コマンドは次のとおりです。

```
undebug aaa accounting
undebug all
undebug authentication {content-request | user | windows-domain}
undebug buf {all | dmbuf | dmsg}
undebug cdp {adjacency | events | ip | packets}
```

```

undebg cli {all | bin | parser}
undebg cms
undebg dataserver {all | clientlib | server}
undebg dhcp
undebg emdb [level [levelnum]]
undebg logging all
undebg ntp
undebg rpc {detail | trace}
undebg snmp {all | cli | main | mib | traps}

```



(注)

emdb、*key-manager*、および *rpc* コマンド オプションは、*central manager* デバイス モードでのみサポートされます。

シンタックスの説明

aaa accounting	(オプション) AAA アカウンティング アクションをディセーブルにします。
all	(オプション) すべてのデバッグ オプションをディセーブルにします。
authentication	(オプション) 認証デバッグをディセーブルにします。
content-request	コンテンツ要求認証のデバッグをディセーブルにします。
user	システム認証に対するユーザ ログインのデバッグをディセーブルにします。
windows-domain	Windows ドメイン認証のデバッグをディセーブルにします。
buf	(オプション) バッファ マネージャのデバッグをディセーブルにします。
all	すべてのバッファ マネージャのデバッグをディセーブルにします。
dmbuf	dmbuf デバッグのみをディセーブルにします。
dmsg	dmsg デバッグのみをディセーブルにします。
cdp	(オプション) CDP デバッグをディセーブルにします。
adjacency	CDP ネイバー情報のデバッグをディセーブルにします。
events	CDP イベントのデバッグをディセーブルにします。
ip	CDP IP のデバッグをディセーブルにします。
packets	パケット関連 CDP のデバッグをディセーブルにします。
cli	(オプション) CLI デバッグをディセーブルにします。
all	すべての CLI のデバッグをディセーブルにします。
bin	CLI コマンド バイナリ プログラムのデバッグをディセーブルにします。
parser	CLI コマンド パーサーのデバッグをディセーブルにします。
cms	(オプション) CMS デバッグをディセーブルにします。
dataserver	(オプション) データ サーバのデバッグをディセーブルにします。
all	すべてのデータ サーバのデバッグをディセーブルにします。
clientlib	データ サーバ クライアント ライブラリ モジュールのデバッグをディセーブルにします。
server	データ サーバ モジュールのデバッグをディセーブルにします。
dhcp	(オプション) DHCP デバッグをディセーブルにします。

dre	(オプション) DRE デバッグをディセーブルにします。
aggregation	DRE チャンク集約のデバッグをディセーブルにします。
all	すべての DRE コマンドのデバッグをディセーブルにします。
cache	DRE キャッシュのデバッグをディセーブルにします。
connection	DRE 接続のデバッグをディセーブルにします。
aggregation [acl]	指定された接続の DRE チャンク集約のデバッグをディセーブルにします。
cache [acl]	指定された接続の DRE キャッシュのデバッグをディセーブルにします。
core [acl]	指定された接続の DRE コアのデバッグをディセーブルにします。
message [acl]	指定された接続の DRE メッセージのデバッグをディセーブルにします。
misc [acl]	指定された接続のその他の DRE デバッグをディセーブルにします。
acl	トレースされた接続を制限する ACL
core	DRE コアのデバッグをディセーブルにします。
message	DRE メッセージのデバッグをディセーブルにします。
misc	その他の DRE デバッグをディセーブルにします。
epm	(オプション) DCE-RPC EPM デバッグをディセーブルにします。
flow	(オプション) ネットワーク トラフィック フローのデバッグをイネーブルにします。
monitor	モニタ フロー パフォーマンスのデバッグ コマンドをイネーブルにします。
tcpstat-v1	tcpstat-v1 のデバッグをイネーブルにします。
logging	(オプション) ロギングのデバッグをディセーブルにします。
all	すべてのロギングのデバッグをディセーブルにします。
ntp	(オプション) NTP デバッグをディセーブルにします。
print-spooler	(オプション) プリント スプーラのデバッグをディセーブルにします。
all	すべてのデバッグ機能を使用して、プリント スプーラのデバッグをディセーブルにします。
brief	簡潔なデバッグ メッセージのみを使用して、プリント スプーラのデバッグをディセーブルにします。
errors	エラー条件のみを使用して、プリント スプーラのデバッグをディセーブルにします。
warnings	警告条件のみを使用して、プリント スプーラのデバッグをディセーブルにします。
rbcp	(オプション) RBCP デバッグをディセーブルにします。
snmp	(オプション) SNMP デバッグ コマンドをディセーブルにします。
all	すべての SNMP デバッグ コマンドをディセーブルにします。
cli	SNMP CLI のデバッグをディセーブルにします。
main	SNMP のメイン デバッグをディセーブルにします。
mib	SNMP MIB のデバッグをディセーブルにします。
traps	SNMP トラップのデバッグをディセーブルにします。
tfo	(オプション) TFO デバッグをディセーブルにします。
buffer-mgr	TFO バッファ マネージャのデバッグをディセーブルにします。
connection	TFO 接続のデバッグをディセーブルにします。

auto-discovery [<i>acl</i>]	(オプション) 自動ディスカバリ モジュールの TFO 接続のデバッグをディセーブルにします。
comp-mgr [<i>acl</i>]	(オプション) 圧縮モジュールの TFO 接続のデバッグをディセーブルにします。
conn-mgr [<i>acl</i>]	(オプション) Connection Manager の TFO 接続のデバッグをディセーブルにします。
egress-method [<i>acl</i>]	(オプション) 出力方式の TFO 接続のデバッグをディセーブルにします。
filtering [<i>acl</i>]	(オプション) フィルタリング モジュールの TFO 接続のデバッグをディセーブルにします。
netio-engine [<i>acl</i>]	(オプション) ネットワーク入出力モジュールの TFO 接続のデバッグをディセーブルにします。
policy-engine [<i>acl</i>]	(オプション) アプリケーション ポリシーの TFO 接続のデバッグをディセーブルにします。
synq [<i>acl</i>]	(オプション) SynQ モジュールの TFO 接続のデバッグをディセーブルにします。
acl	(オプション) TFO 接続を制限する ACL
stat-mgr	TFO 統計情報マネージャのデバッグをディセーブルにします。
translog	TFO トランザクション ログのデバッグをディセーブルにします。
translog	(オプション) transaction logging デバッグ コマンドをディセーブルにします。
export	トランザクション ログ FTP エクスポートのデバッグをディセーブルにします。
wafs	(オプション) WASS ソフトウェア コンポーネントとユーティリティからのメッセージがロギングされる通知レベル (debug、info、warn、error) をアンセットします。
all	すべてのソフトウェア コンポーネントとユーティリティのロギング レベルを同時にアンセットします。
core-fe	Core File Engine として機能する WAE のロギング レベルをアンセットします。
edge-fe	Edge File Engine として機能する WAE のロギング レベルをアンセットします。
manager	Device Manager のロギング レベルをアンセットします。
utilities	WAAS ユーティリティのロギング レベルをアンセットします。
wccp	(オプション) WCCP 情報のデバッグをディセーブルにします。
all	すべての WCCP デバッグ機能をディセーブルにします。
detail	WCCP の詳細なデバッグをディセーブルにします。
error	WCCP エラーのデバッグをディセーブルにします。
events	WCCP イベントのデバッグをディセーブルにします。
keepalive	アプリケーションに送信される WCCP キープアライブのデバッグをディセーブルにします。
packets	WCCP パケット関連情報のデバッグをディセーブルにします。
slowstart	WCCP スロースタートのデバッグをディセーブルにします。

次の構文表では、central manager デバイス モードで使用するオプションについて説明します。

emdb	(オプション) 組み込みデータベースのデバッグをディセーブルにします。
level	(オプション) EMDB サービスの指定されたデバッグ レベルをディセーブルにします。
levelnum	(オプション) ディセーブルにするデバッグ レベル (レベル 0 はデバッグをディセーブルにします)
key-manager	(オプション) Central Manager のキー マネージャのデバッグをディセーブルにします。
rpc	(オプション) Remote Procedure Call (RPC; リモート プロシージャ コール) ログをディセーブルにします。
detail	プライオリティ レベルが「detail」以上の RPC ログをディセーブルにします。
trace	プライオリティ レベルが「trace」以上の RPC ログをディセーブルにします。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイス モード

- application-accelerator
- replication-accelerator
- central-manager

使用上のガイドライン **debug** および **undebug** コマンドは、シスコシステムズのテクニカル サポートの担当者から指示があった場合にだけ使用することを推奨します。

関連コマンド

- [debug](#)
- [show debugging](#)

wafs

WAE で Wide Area File Services (WAFS; ワイドエリア ファイル サービス) 関連のネットワーク設定、およびファイル サーバ、プリンタ、ユーザなどの設定をバックアップ、復元または作成するには、**wafs EXEC** コマンドを使用します。

```
wafs {backup-config filename | restore-config filename |
      sysreport [filename | date-range from_date end_date filename]}
```



(注)

wafs sysreport コマンドを実行すると、一時的に WAE のパフォーマンスに影響を与える可能性があります。

シンタックスの説明

backup-config	ファイルに現在の WAFS 関連の設定情報をコピーします。
<i>filename</i>	WAFS 設定の保存先である <i>xxxx.tar.gz</i> フォーマットのファイルの名前。このファイルは <i>/local/local1</i> ディレクトリに保存されます。
restore-config	保存されている WAFS 関連の設定情報をファイルからロードします。
<i>filename</i>	(オプション) ロードする WAFS 設定情報が保存された <i>xxxx.tar.gz</i> フォーマットのファイルの名前。このファイルは <i>/local/local1</i> ディレクトリになければいけません。
sysreport	廃止予定。 copy sysreport を使用します。
<i>date-range</i>	(オプション) システム レポートの対象となる時間の範囲を表示します。
<i>from_date</i>	作成されたシステム レポート内の情報の開始日
<i>to_date</i>	作成されたシステム レポート内の情報の終了日
<i>filename</i>	システム情報が保存先である <i>xxxx.tar.gz</i> フォーマットのファイルの名前

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator

使用上のガイドライン

wafs backup-config EXEC コマンドは、基本ネットワーク設定のバックアップが十分でない場合 (**copy running-config** コマンドを使用して実行) に使用します。たとえば WAAS CLI グローバル コンフィギュレーション モードを使用して変更を行う前にシステム設定をバックアップしたり、誤った操作で現在の設定のデータを損失しないよう保護する場合などです。

wafs restore-config は自動的にリロード機能を実行します。このコマンドの完了時、WAE を再登録することを推奨します。

この **wafs** コマンドは、WAAS Central Manger GUI からバックアップとシステムの復元、またはシステム レポートの作成を利用できない場合にも役立ちます。

例

次の例では、WAFS 設定情報のバックアップ ファイルを作成します。

```
WAE# wafs ?
  backup-config  backup system configurations to a file.
  restore-config restore system configurations from a file. WARNING: After
                  restoring configuration, the system needs to be restarted and
                  re-registered.
  sysreport      system report to a file

WAE# wafs backup-config backup.tar.gz
      system configuration is stored in file /local/local1/backup.tar.gz
```

次の例は、以前に保存された WAFS 設定情報でシステムを復元します。

```
WAE# wafs restore-config backup.tar.gz
Restoring configurations ...
After upload is completed the File Engine will be reloaded. We strongly recommend you
re-register after the engine is reloaded.
```

関連コマンド

[copy running-config](#)

whoami

現在のユーザのユーザ名を表示するには、**whoami EXEC** コマンドを使用します。

whoami

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンドモード EXEC

デバイスモード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン この EXEC コマンドを使用して現在のユーザのユーザ名を表示します。

例 次の例はユーザ名を表示します。

```
WAE# whoami  
admin
```

関連コマンド [pwd](#)

windows-domain

WAAS デバイスの Windows ドメイン ユーティリティにアクセスするには、**windows-domain EXEC** コマンドを使用します。

windows-domain diagnostics {findsmb | getent | net | nmblookup | smbclient | smbstatus | smbtree | tdbbackup | tdbdump | testparm | wbinfo}

シンタックスの説明

diagnostics	Windows ドメイン診断ユーティリティの選択をイネーブルにします。
findsmb	NetBIOS 名前解決およびブラウズのトラブルシューティング用ユーティリティを表示します。
getent	ローカルと PDC 両方のユーザとグループの統合リストを取得するためのユーティリティを表示します。
net	リモート CIFS サーバの管理用ユーティリティを表示します。
nmblookup	NetBIOS 名前解決およびブラウズのトラブルシューティング用ユーティリティを表示します。
smbclient	Windows 環境および統合のトラブルシューティング用ユーティリティを表示します。
smbstatus	Samba サーバのステータス、接続されたクライアントなどの検査用ユーティリティを表示します。
smbtree	Windows ネットワーク ネイバーフッド構造およびコンテンツの検査用ユーティリティを表示します。
tdbbackup	Samba データベース ファイルのバックアップ、確認、復元用ユーティリティを表示します。
tdbdump	Samba データベース ファイルの検査用ユーティリティを表示します。
testparm	<i>smb.conf</i> ファイルの正確さを検証するためのユーティリティを表示します。
wbinfo	Winbind およびドメイン統合のトラブルシューティング用ユーティリティを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

このコマンドを使用して選択した Windows ドメイン診断ユーティリティをアクティブにします。

例

次の例は、Get Entity ユーティリティで利用可能なオプションを示します。

```
WAE# windows-domain diagnostics getent --help
Usage: getent [OPTION...] database [key ...]
getent - get entries from administrative database.

-s, --service=CONFIG      Service configuration to be used
-?, --help                Give this help list
    --usage                Give a short usage message
-V, --version              Print program version
```

Mandatory or optional arguments to long options are also mandatory or optional for any corresponding short options.

```
Supported databases:
aliases ethers group hosts netgroup networks passwd protocols rpc
services shadow
```

次の例は、NetBIOS 名前解決およびブラウザのトラブルシューティング用の NMB Lookup ユーティリティで利用可能なオプションを示します。

```
WAE# windows-domain diagnostics nmblookup -h
Usage: [-?TV] [--usage] [-B BROADCAST-ADDRESS] [-f VAL] [-U STRING] [-M VAL]
      [-R VAL] [-S VAL] [-r VAL] [-A VAL] [-d DEBUGLEVEL] [-s CONFIGFILE]
      [-l LOGFILEBASE] [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP]
      [-i SCOPE] <NODE> ...
```

次の例は、Windows 環境および統合のトラブルシューティング用の Samba Client ユーティリティで利用可能なオプションを示します。

```
WAE# windows-domain diagnostics smbclient -h
Usage: [-?EgVnkP] [--usage] [-R NAME-RESOLVE-ORDER] [-M HOST] [-I IP] [-L HOST]
      [-t CODE] [-m LEVEL] [-T <c|x>IXFqgbNan] [-D DIR] [-c STRING] [-b BYTES]
      [-p PORT] [-d DEBUGLEVEL] [-s CONFIGFILE] [-l LOGFILEBASE]
      [-O SOCKETOPTIONS] [-n NETBIOSNAME] [-W WORKGROUP] [-i SCOPE]
      [-U USERNAME] [-A FILE] [-S on|off|required] service <password>
```

次の例は、TDB Backup ユーティリティで利用可能なオプションを示します。

```
WAE# windows-domain diagnostics tdbbackup -h
Usage: tdbbackup [options] <fname...>

-h                this help message
-s suffix         set the backup suffix
-v                verify mode (restore if corrupt)
```

次の例は、Windows ドメインに登録されているユーザに関する情報を表示する WinBiind ユーティリティの `-u` オプションの使い方を示します。

```
WAE# windows-domain diagnostics wbinfo -u
administrator
guest
user98
tuser1
```

```
WAE# show user username user98
Uid          : 70012
Username     : user98
Password     : *****
Privilege    : super user
Configured in : Windows Domain database
```

```
WAE# show user uid 70012
Uid          : 70012
Username     : user98
Password     : *****
Privilege    : super user
Configured in : Windows Domain database
```

次の例は、Windows ドメインの登録方法を示します。

```
WAE# windows-domain diagnostics
      net join -S<domain server> -U<domain admin username>%<domain admin password>
```

関連コマンド

[\(config\) windows-domain](#)

write

WAAS デバイスでスタートアップ コンフィギュレーションを保存するには、**write EXEC** コマンドを使用します。

write [erase | memory | mib-data | terminal]

シンタックスの説明

erase	(オプション) NVRAM (不揮発性 RAM) から startup-config を削除します。
memory	(オプション) コンフィギュレーションを NVRAM に書き込みます。これは始動情報のデフォルトの保存場所です。
mib-data	(オプション) MIB の固定コンフィギュレーション データをディスクに書き込みます。
terminal	(オプション) コンフィギュレーションをターミナルセッションに出力します。

デフォルト

コンフィギュレーションはデフォルトで NVRAM に書き込まれます。

コマンド モード

EXEC

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

このコマンドを使用すると、NVRAM に実行コンフィギュレーションを保存したり、メモリ内の設定を消去したりできます。**write erase** コマンドを実行すると、メモリ内にコンフィギュレーションは保持されず、WAAS デバイスのリブート後に、設定の各項目の入力を求めるプロンプトが表示されます。

write terminal コマンドを使用すると、ターミナルセッション ウィンドウに現在の実行コンフィギュレーションが表示されます。同等のコマンドが **show running-config** です。

例

次の例は、現在の startup-config をメモリに保存します。

```
WAE# write memory
```

関連コマンド

[copy running-config](#)
[copy startup-config](#)
[show running-config](#)
[show startup-config](#)

コンフィギュレーションモード コマンド

グローバル コンフィギュレーションモードは、デバイス全体に対する WAAS ソフトウェア機能の設定、表示、テストに使用します。このモードを開始するには、特権 EXEC モードから **configure** コマンドを入力します。グローバル コンフィギュレーションモードのプロンプトは、WAE のホスト名とそのあとに続く (config) およびポンド記号 (#) からなります。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には、グローバル コンフィギュレーションモードを開始しておく必要があります。

```
WAE# configure  
WAE(config)#
```

グローバル コンフィギュレーションモードで入力されたコマンドは、入力されると同時に実行コンフィギュレーション ファイルをアップデートします。この変更が **startup-config** ファイルに保存されるのは、**copy running-config startup-config** EXEC モード コマンドの入力後です。設定が保存されると、WAE の再起動後も保持されます。

グローバル コンフィギュレーションモードを使用して特定のコンフィギュレーションモードを開始することもできます。グローバル コンフィギュレーションモードからインターフェイス コンフィギュレーションモード、標準 ACL 設定モードまたは拡張 ACL 設定モードに入ることができます。

グローバル コンフィギュレーションモードを終了して特権レベル EXEC モードに戻るには、**exit** または **end** 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。

```
WAE(config)# exit  
WAE#
```

(config) aaa accounting

WAAS デバイスで AAA アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。

```
aaa accounting {commands {0 | 15} default {start-stop | stop-only | wait-start} tacacs | exec default
{start-stop | stop-only | wait-start} tacacs | system default {start-stop | stop-only} tacacs}
```

シンタックスの説明

commands	指定された特権レベルで、すべてのコマンドのアカウントティングを設定します。
0	標準ユーザのユーザ特権レベル
15	管理ユーザのユーザ特権レベル
デフォルト	デフォルトのアカウントティング リストを使用するように AAA アカウンティングを設定します。
start-stop	プロセスの開始時にアカウントティング開始通知を、プロセスの終了時にアカウントティング終了通知を送信します。アカウントティング開始記録はバックグラウンドで送信されます。要求されたユーザ プロセスは、アカウントティング サーバがアカウントティング開始通知を受信したかどうかに関係なく開始されます。
stop-only	ユーザによって要求されたプロセスの終了時にアカウントティング終了通知を送信します。
wait-start	アカウントティング サーバに開始と終了の両方のアカウントティング通知を送信します。ただし、要求されたユーザ サービスは、アカウントティング開始通知が確認応答されるまで開始されません。ユーザは、記録されるまでは CLI コマンドまたはログインを実行できません。 アカウントティング終了通知も送信されますが、確認応答は不要です。
tacacs	アカウントティング用に TACACS+ が使用できるようにします。
exec	ユーザ EXEC プロセス (ユーザ シェル) のアカウントティングを有効にします。有効になると、EXEC シェル アカウンティングは、EXEC ターミナルセッション (ユーザ シェル) イベントと管理者による EXEC シェルへのログインおよびログアウトをレポートします。
system	ユーザに関連付けられていないシステムレベルのイベント (リロードなど) のアカウントティングを有効にします。

デフォルト

AAA アカウンティングはデフォルトで無効に設定されています。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

AAA アカウンティング機能により、管理ユーザのアクティビティ、ユーザがアクセスするサービス、およびユーザが消費するネットワーク リソースの量 (たとえば、接続時間や転送されるバイト) を追跡できます。また、AAA アカウンティング機能を使用して、課金、監査、レポート、またはセキュリティを目的として、ユーザのアクティビティを追跡することもできます。WAAS は

TACACS+ を使用して AAA アカウンティングを実装します。一方、RADIUS は現在サポートされていません。AAA アカウンティングが有効になると、WAAS デバイスは、アカウンティング レコードの形式で TACACS+ セキュリティ サーバにユーザのアクティビティをレポートします。このデータは、ネットワーク管理、クライアント課金、および監査用に分析できます。

次のタイプのイベントのアカウンティングをアクティブにできます。

- EXEC — EXEC シェル アカウンティングを使用して、Telnet、FTP、または SSH (SSH バージョン 1 または バージョン 2) を介した EXEC シェルへの管理者のログインおよびログアウトをレポートします。このタイプのアカウンティングは、WAAS デバイスでのユーザ EXEC ターミナルセッション (ユーザ シェル) に関する情報を記録します。この情報には、ユーザ名、日付、各セッションの開始および終了時刻、時間帯、WAAS デバイスのアクセスに使用したシステムの IP アドレスなどがあります。EXEC シェル アカウンティング情報には、TACACS+ サーバ上のアカウンティング ログ ファイルを介してアクセスできます。このログ ファイルは、このタイプのアカウンティング情報に対して次のレポート形式を使用します。

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#Service
```

- Command — WAAS デバイスは、WAAS デバイス上で実行された CLI コマンドに関する情報を記録します。各コマンドのアカウンティング レコードには、実行されたコマンドの構文、そのコマンドを実行したユーザの名前、そのユーザの特権レベル、各コマンドを実行した日付と時刻が含まれています。WAAS デバイスでは、0 と 15 の 2 つの特権レベルをサポートします。これはそれぞれ標準ユーザと管理ユーザを表します。コマンド アカウンティング情報には、TACACS+ サーバ上のアカウンティング ログ ファイルを介してアクセスできます。このログ ファイルは、このタイプのアカウンティング情報に対して次のレポート形式を使用します。

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#Service#PrivilegeLevel#CLICommand
```

- System — WAAS デバイスは、システムレベルのイベント (たとえば、システムが再起動するタイミング) すべてに関する情報を記録します。システム アカウンティング情報には、TACACS+ サーバ上のアカウンティング ログ ファイルを介してアクセスできます。このログ ファイルは、このタイプのアカウンティング情報に対して次のレポート形式を使用します。

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#SystemService#SystemAccountingEvent#EventReason
```

WAAS ソフトウェアは、デフォルトのアカウンティング リストのみサポートします。



注意

wait-start オプションを使用する前に、WAAS デバイスで TACACS+ サーバが設定され、サーバと正常にコンタクトをとれることを確認してください。WAAS デバイスが設定された TACACS+ サーバにコンタクトできない場合は、おそらく無応答になっています。

WAAS ソフトウェアは **wait-start** オプションが設定されていると、次の警告メッセージを表示します。

```
Warning:The device may become non-responsive if it cannot contact a configured TACACS+
server.
```

管理者は、次のプロンプトに対して「yes」を入力するまで、設定を確認するよう繰り返し求められます。

```
Are you sure you want to proceed?[yes]
```

例 次の例では WAAS デバイスに TACACS+ を設定し、プロセスの開始時にアカウント開始通知を、プロセスの終了時にアカウント終了通知を送信するように指定します。また、アカウント開始通知がサーバに受信されたかどうかに関係なく要求されたユーザプロセスが開始するように指定します。

```
WAE(config)# tacacs key abc
WAE(config)# tacacs server 192.168.50.1 primary
WAE(config)# aaa accounting system default start-stop tacacs
WAE# show aaa accounting
Accounting Type   Record event(s)  Protocol
-----
Exec shell        unknown          unknown
Command level 0   unknown          unknown
Command level 15  unknown          unknown
System            start-stop       TACACS+
```

次の例では、WAAS デバイスはすべてのユーザ EXEC セッションを記録するよう設定されます。また、このコマンドは、セッションの終了時にアカウント終了通知を TACACS+ サーバに送信するように指定します。

```
WAE(config)# aaa accounting exec default stop-only tacacs
```

次の例では、WAAS デバイスは標準ユーザによって実行されたすべての CLI コマンドを記録するよう設定されます。また、このコマンドは、標準ユーザによって実行されたすべての CLI コマンドの終了時に、アカウント終了通知を TACACS+ サーバに送信するように指定します。

```
WAE(config)# aaa accounting commands 0 default stop-only tacacs
```

次の例では、WAAS デバイスは管理ユーザによって実行されたすべての CLI コマンドを記録するよう設定されます。また、このコマンドは、プロセスの開始時にアカウント開始通知を、プロセスの終了時にアカウント終了通知を TACACS+ サーバに送信するように指定します。管理ユーザによって実行された CLI コマンドは、アカウント開始通知が確認応答されるまで続行されません。

```
WAE(config)# aaa accounting commands 15 default wait-start tacacs
```

次の例は、TACACS+ サーバ上で使用可能な EXEC シェル アカウンティング レポートを示しています。

```
Wed Apr 14 11:19:19 2004 172.16.0.0 super10 pts/0 172.31.0.0 start
start_time=1081919558 task_id=3028 timezone=PST service=shell
Wed Apr 14 11:19:23 2004 172.16.0.0 super10 pts/0 172.31.0.0
stop stop_time=1081919562 task_id=3028 timezone=PST service=shell
Wed Apr 14 11:22:13 2004 172.16.0.0 normal20 pts/0 via5.abc.com start
start_time=1081919732 task_id=3048 timezone=PST service=shell
Wed Apr 14 11:22:16 2004 172.16.0.0 normal20 pts/0 via5.abc.com stop
stop_time=1081919735 task_id=3048 timezone=PST service=shell
Wed Apr 14 11:25:29 2004 172.16.0.0 admin ftp via5.abc.com start start_time=1081919928
task_id=3069 timezone=PST service=shell
Wed Apr 14 11:25:33 2004 172.16.0.0 admin ftp via5.abc.com stop stop_time=1081919931
task_id=3069 timezone=PST service=shell
```

次の例は、TACACS+ サーバ上で使用可能なシステム アカウンティング レポートを示しています。

```
Wed Apr 14 08:37:14 2004 172.16.0.0 unknown unknown 0.0.0.0 start
start_time=1081909831
task_id=2725 timezone=PST service=system event=sys_acct reason=reload
Wed Apr 14 10:19:18 2004 172.16.0.0 admin ttyS0 0.0.0.0 stop stop_time=1081915955
task_id=5358 timezone=PST service=system event=sys_acct reason=shutdown
```

次の例は、TACACS+ サーバ上で使用可能なコマンド アカウンティング レポートを示しています。

```
Wed Apr 14 12:35:38 2004 172.16.0.0 admin ttyS0 0.0.0.0 start start_time=1081924137
task_id=3511 timezone=PST service=shell -lvl=0 cmd=logging console enable
Wed Apr 14 12:35:39 2004 172.16.0.0 admin ttyS0 0.0.0.0 stop stop_time=1081924137
task_id=3511 timezone=PST service=shell priv-lvl=0 cmd=logging console enable
```

コマンド アカウンティングに加えて、WAAS デバイスは、実行された CLI コマンドをシステム ログ (*syslog.txt*) に記録します。メッセージフォーマットは次のとおりです。

```
ce_syslog(LOG_INFO, CESM_PARSER, PARSER_ALL, CESM_350232,
          "CLI_LOG %s: %s \n", __FUNCTION__, pd->command_line);
```

関連コマンド

[debug](#)

[show aaa accounting](#)

(config) adapter

EndPoint Mapper (EPM) サービスを有効にするには、**adapter** 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。EPM サービスを無効にするには、このコマンドの **no** 形式を使用します。

adapter epm enable

シンタックスの説明

epm	Microsoft PortMapper アダプタを指定します。
enable	EPM サービスを有効にします。

デフォルト

EPM サービスは、WAAS ソフトウェア リリース 4.0.3 およびそれ以降のリリースにアップグレードするときにデフォルトで有効になります。また、新しい WAE アプライアンス上または工場出荷時のデフォルト設定に戻す場合は、デフォルトで無効になります。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

Microsoft PortMapper アダプタが設置されている場合に、EPM サービスを有効にするには、**adapter epm enable** コマンドを使用します。

例

次の例では、EPM サービスを有効にします。

```
WAE(config)# adapter epm enable
```

関連コマンド


[show adapter](#)
[show statistics epm](#)

(config) alarm overload-detect

アラーム過負荷状態を検出するには、**alarm overload-detect** 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。

```
alarm overload-detect {clear 1-999 [raise 10-1000] | enable | raise 10-1000 [clear 1-999]}
```

シンタックスの説明

clear	WAAS デバイス上のアラーム過負荷状態がクリアされるしきい値を指定します。アラームがこのしきい値より低下すると、アラームはクリアされ SNMP トラップとアラーム通知が再度 NMS へ送信されます。
	 (注) alarm overload-detect clear の値は、 alarm overload-detect raise の値より小さくする必要があります。
<i>1-999</i>	アラーム過負荷状態を終了させる 1 秒当たりのアラーム数
raise	(オプション) WAAS デバイスがアラーム過負荷状態を開始し、ネットワーク管理ステーション (NMS) への SNMP トラップおよびアラーム通知が一時停止するしきい値を指定します。
enable	アラーム過負荷状態の検出を有効にします。
<i>10-1000</i>	アラーム過負荷を発生させる 1 秒当たりのアラーム数

デフォルト

clear : 1 秒当たり 1 アラーム

raise : 1 秒当たり 10 アラーム

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

WAAS デバイス上で実行している複数のアプリケーションで同時に問題が発生した場合、多数のアラームが同時に発生し、WAAS デバイスは応答を停止します。**alarm overload-detect** 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、ノードヘルス管理からの着信アラームに対する過負荷の限度を設定できます。アラーム数が許容されているアラーム数の最大値を超えた場合、WAAS デバイスはアラーム過負荷状態に入り、アラーム数が **clear** オプションで定義された数に低下するまで、その状態が続きます。

WAAS デバイスがアラーム過負荷状態に入ると、次のイベントが発生します。

- アラーム過負荷通知が SNMP および NMS に送信される。**clear** および **raise** の値も SNMP および NMS に伝達されます。
- 以降のアラーム発生およびクリア動作に対する SNMP トラップと NMS 通知は、一時停止する。
- アラーム過負荷クリア通知が送信される。
- WAAS デバイスは、着信アラームの割合が **clear** の値に低下するまで、アラーム過負荷状態を維持する。



(注) アラーム過負荷状態では、アプリケーションはアラームを発生させ続け、アラームは WAAS デバイス内に記録されます。**show alarms** および **show alarms history EXEC** コマンドは、アラーム過負荷状態でもすべてのアラームを表示します。

例

次の例はアラーム過負荷状態の検出を有効にします。

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

次の例は、1 秒当たり 100 アラームでアラーム過負荷状態が発生するしきい値を設定します。

```
WAE(config)# alarm overload-detect raise 100
```

次の例は、1 秒当たり 10 アラームでアラーム過負荷状態が解除されるレベルを設定します。

```
WAE(config)# alarm overload-detect clear 10
```

関連コマンド

[show alarms](#)

(config) asset

監査タグ文字列のタグ名を設定するには、**asset** 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。監査タグ名を削除するには、このコマンドの **no** 形式を使用します。

asset tag name

シンタックスの説明

tag	監査タグを設定します。
name	監査タグ名文字列

デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

例

次の例は、WAAS デバイスで監査タグ文字列のタグ名を設定する方法を示します。

```
WAE(config)# asset tag entitymib
```


(config) authentication

WAAS デバイスの管理ログイン認証および許可方式を指定するには、**authentication** グローバル コンフィギュレーション モード コマンドを使用します。選択的にオプションを無効にするには、このコマンドの **no** 形式を使用します。

```
authentication {configuration {local | radius | tacacs | windows-domain} enable [primary |
secondary | tertiary | quaternary] | fail-over server-unreachable | login {local | radius | tacacs |
windows-domain} enable [primary | secondary | tertiary| quaternary] | content-request
windows-domain disconnected-mode enable}
```

シンタックスの説明

configuration	WAAS デバイスの管理ログイン許可 (設定) パラメータを設定します。
local	WAAS デバイスのログイン許可 (設定) 方式としてローカル データベース方式を選択します。
radius	WAAS デバイスのログイン許可 (設定) 方式として RADIUS 方式を選択します。
tacacs	WAAS デバイスのログイン許可 (設定) 方式として TACACS+ 方式を選択します。
windows-domain	WAAS デバイスのログイン許可 (設定) 方式として Windows ドメイン コントローラ方式を選択します。
enable	WAAS デバイスの指定された管理ログイン許可方式を有効にします。
primary	(オプション) WAAS デバイスが最初に使用する管理ログイン許可方式を指定します。
secondary	(オプション) 最初の方式が失敗した場合に WAAS デバイスが 2 番めに使用する管理ログイン許可方式を指定します。
tertiary	(オプション) 最初と 2 番めの方式が失敗した場合に WAAS デバイスが 3 番めに使用する管理ログイン許可方式を指定します。
<i>quaternary</i>	(オプション) 最初と 2 番め、3 番めの方式が失敗した場合に WAAS デバイスが 4 番めに使用する管理ログイン許可方式を指定します。
fail-over server-unreachable	プライマリ認証サーバに到達不能な場合に WAAS デバイスがセカンダリ認証データベースをクエリーするよう指定します。
login	WAAS デバイスの管理ログイン認証パラメータを設定します。
local	WAAS デバイスの管理ログイン認証方式としてローカル データベース方式を選択します。
radius	WAAS デバイスの管理ログイン認証方式として RADIUS 方式を選択します。
tacacs	WAAS デバイスの管理ログイン認証方式として TACACS+ 方式を選択します。
windows-domain	WAAS デバイスの管理ログイン認証方式として Windows ドメイン コントローラ方式を選択します。
enable	WAAS デバイスの選択された管理ログイン認証方式を有効にします。
primary	(オプション) WAAS デバイスが最初に使用する管理ログイン認証方式を指定します。

secondary	(オプション) 最初の方式が失敗した場合に WAAS デバイスが 2 番めに使用する管理ログイン認証方式を指定します。
tertiary	(オプション) 最初の方式が失敗した場合に WAAS デバイスが 2 番めに使用する管理ログイン認証方式を指定します。
quaternary	(オプション) 最初と 2 番め、3 番めの方式が失敗した場合に WAAS デバイスが 4 番めに使用する管理ログイン認証方式を指定します。
content-request	コンテンツの要求を認証します。
	
	(注) このオプションは application-accelerator デバイス モードだけで利用できます。
windows-domain	ドメイン サーバ認証用の Windows ドメイン コントローラを選択します。
disconnected-mode	切断モードで認証します。
enable	切断モードでの認証を有効にします。

デフォルト

ローカル認証方式は、デフォルト設定で有効になっています。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

authentication コマンドは、認証と許可の両方式を設定し、この方式により WAAS デバイスへのログインと設定アクセスを統制します。

**(注)**

WAAS デバイスに対する管理ログイン認証および許可の設定には、可能な場合には WAAS CLI ではなく WAAS Central Manager GUI を使用することを強く推奨します。WAAS Central Manager GUI を使用して WAAS Central Manager に登録されている単一 WAE または WAE グループで管理ログイン認証および許可を一元的に設定する方法については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

authentication login コマンドは、ユーザがどのレベルの WAAS デバイス アクセス権限を持っているか判断します。**authentication configuration** コマンドは、WAAS デバイスへの特権アクセス (設定アクセス) をユーザに許可します。

authentication login local および **authentication configuration local** コマンドは、認証および許可にローカル データベースを使用します。

authentication login tacacs および **authentication configuration tacacs** コマンドは、リモート TACACS+ サーバを使用してユーザのアクセス レベルを判断します。WAAS ソフトウェアがサポートするのは TACACS+ のみで、TACACS や Extended TACACS はサポートしません。

TACACS+ を設定するには、**authentication** および **tacacs** コマンドを使用します。TACACS+ を有効にするには、**tacacs enable** コマンドを使用します。TACACS+ 認証の詳細については、「(config) tacacs」コマンドを参照してください。

authentication login radius および **authentication configuration radius** コマンドは、リモート RADIUS サーバを使用してユーザのアクセス レベルを判断します。

デフォルトで、ローカル方式は有効になっていますが、TACACS+ および RADIUS はともにログインと設定が無効になっています。TACACS+ および RADIUS が無効になっている場合、ローカルは自動的に有効になっています。TACACS+、RADIUS、およびローカル方式は、同時に有効にできます。

primary オプションは、ログインと設定の両方の認証を試みる最初の方式を指定します。また、**secondary** オプションは、最初の（プライマリ）方式が失敗した場合に使用する方式を指定します。**tertiary** オプションは、プライマリとセカンダリの方式がともに失敗した場合に使用する方式を指定します。**quaternary** オプションは、プライマリ、セカンダリ、ターシャリ方式が失敗した場合に使用する方式を指定します。**authentication login** または **authentication configuration** コマンドのすべての方式がプライマリとして設定されている場合、あるいはセカンダリまたはターシャリとして設定されている場合、ローカル方式が最初に試行され、次に TACACS+、その次に RADIUS となります。

プライマリ方式による認証の実行

authentication fail-over server-unreachable グローバル コンフィギュレーション コマンドにより、プライマリ認証サーバが到達不能な場合のみ、セカンダリ認証方式へのフェールオーバーが発生するように指定できます。この機能によりユーザは、リモート認証サーバ（TACACS+ または RADIUS）が到達不能なときだけ、ローカル データベースを使用して WAAS デバイスにアクセスできるようになります。たとえば、TACACS+ サーバが、ユーザ認証フェールオーバーが設定された状態で認証に対して有効なとき、ローカル データベースで定義されたアカウントでユーザが WAAS デバイスにログインしようとする、ログインは失敗します。ログインが成功するのは、TACACS+ サーバが到達不能なときだけです。

ローカル データベースを介したログイン認証および許可

ローカル認証および許可では、ローカルに設定されたログインおよびパスワードを使用して管理ログイン試行を認証します。ログインおよびパスワードは各 WAAS デバイスに対してローカルで、各ユーザ名にはマッピングされません。

デフォルトでは、ローカル ログイン認証は最初、有効に設定されています。ローカル ログイン認証を無効にできるのは、他の管理ログイン認証方式を 1 つ以上有効にした後です。ただし、ローカル ログイン認証が無効になっている場合に残りすべての管理ログイン認証方式を無効にすると、ローカル ログイン認証は自動的に再度有効になります。

RADIUS 認証および許可設定の指定

WAAS デバイスで RADIUS 認証を設定するには、**radius-server** 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、WAAS デバイス上で一連の RADIUS 認証サーバ設定をまず設定する必要があります（「(config) radius-server」コマンドを参照）。

authentication login radius 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、通常のログインモードの RADIUS 認証を有効にします。

authentication configuration radius 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、RADIUS 許可を有効にします。

WAAS デバイスでの RADIUS 認証および許可を無効にするには、**authentication** グローバル コンフィギュレーション コマンドの **no** 形式を使用します（たとえば、**no authentication login radius enable** コマンドを使用して RADIUS 認証を無効にします）。

TACACS+ 認証および許可設定の指定

WAAS デバイスで TACACS+ 認証を設定するには、**tacacs** 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、WAAS デバイス上で一連の TACACS+ 認証設定を設定する必要があります (「(config) tacacs」コマンドを参照)。

サーバの冗長性

認証サーバは、**tacacs host** または **radius-server host** グローバル コンフィギュレーション コマンドで指定できます。TACACS+ サーバの場合、**tacacs host hostname** コマンドを使用して追加サーバを設定します。このような追加サーバは、特に WAAS デバイス ロード バランシング方式がサーバ間で均等に要求を分散するとき、認証の冗長性とスループットの向上を実現します。WAAS デバイスがいずれかの認証サーバに接続できない場合、認証は発生せず、以前に認証されていないユーザはアクセスを拒否されます。

Windows ドメイン ログイン認証の指定

デバイスまたはデバイス グループの管理ログイン認証方式および許可方式として Windows ドメインを有効にできます。Windows 認証を有効にする前に、**windows-domain wins-server** 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、まず Windows ドメイン コントローラを設定する必要があります (「(config) windows-domain」コマンドを参照)。

WAAS CLI ではなく、WAAS Central Manager GUI を使用して WAAS ドメイン コントローラ設定を設定することを推奨します。『Cisco Wide Area Application Services Configuration Guide』の Chapter 6 を参照してください。

例

プライマリ認証サーバに到達不能な場合にセカンダリ認証データベースをクエリーするには、次のコマンドを入力します。この機能はサーバ不到達時フェールオーバー機能と呼ばれます。

```
WAE(config)# authentication fail-over server-unreachable
```

WAAS デバイスでサーバ不到達時フェールオーバー機能が有効になっている場合、WAAS デバイスでは2つのログイン認証方式 (プライマリおよびセカンダリ方式) だけを設定できます。WAAS デバイスは指定された認証サーバに到達不能な場合にのみ、プライマリ認証方式からセカンダリ認証方式へフェールオーバーします。

ローカル、TACACS+、RADIUS または Windows データベースを使用して認証権限を有効にし、次に管理ログイン認証の順序を指定するには、**authentication login** 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、RADIUS がプライマリ方式、TACACS+ がセカンダリ方式、Windows が3番めの方式、ローカルデータベースが4番めの方式として指定されています。この例で、WAAS デバイス上でサーバ不到達時フェールオーバー機能が有効になっていないため、4つのログイン認証方式が指定されています。

```
WAE(config)# authentication login radius enable primary
WAE(config)# authentication login tacacs enable secondary
WAE(config)# authentication login windows-domain enable tertiary
WAE(config)# authentication login local enable quaternary
```



(注) WAAS デバイスでサーバ不到達時フェールオーバー機能を有効にした場合は、認証のプライマリ方式として **TACACS+** または **RADIUS** を指定し、認証のセカンダリ方式としてローカルを指定してください。

ローカル、TACACS+、RADIUS または Windows データベースを使用して許可権限を有効にし、次に管理ログイン許可（設定）の順序を指定するには、**authentication configuration** 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。



(注) 許可権限はコンソールと Telnet の接続試行、セキュア FTP (SFTP) セッションおよび Secure Shell (SSH; セキュア シェル、バージョン 1 と 2) セッションに適用されます。

管理ログイン認証および許可方式は、同じ順序で設定することを強く推奨します。たとえば、管理ログイン認証および許可の両方に対して RADIUS をプライマリ ログイン方式とし、TACACS+ をセカンダリ ログイン方式、Windows をターシャリ方式、そしてローカル方式をクワターナリ方式として使用するよう WAAS デバイスを設定します。

次の例では、RADIUS がプライマリ方式、TACACS+ がセカンダリ方式、Windows が 3 番めの方式、ローカル データベースが 4 番めの方式として指定されています。この例で、WAAS デバイス上でサーバ不到達時のフェールオーバー機能が有効になっていないため、4 つのログイン許可（設定）方式が指定されています。

```
WAE(config)# authentication configuration radius enable primary
WAE(config)# authentication configuration tacacs enable secondary
WAE(config)# authentication configuration windows-domain enable tertiary
WAE(config)# authentication configuration local enable quaternary
```



(注) WAAS デバイスでサーバ不到達時フェールオーバー機能を有効にした場合は、許可（設定）のプライマリ方式として **TACACS+** または **RADIUS** を指定し、許可（設定）のセカンダリ方式としてローカルを指定してください。

次の例は **show authentication** コマンドの出力結果を示します。

```
WAE# show authentication user

Login Authentication:      Console/Telnet/Ftp/SSH Session
-----
local                      enabled (primary)
Windows domain            enabled
Radius                    disabled
Tacacs+                   disabled

Configuration Authentication: Console/Telnet/Ftp/SSH Session
-----
local                      enabled (primary)
Radius                    disabled
Tacacs+                   disabled
```

関連コマンド

(config) radius-server

show authentication

show statistics radius

show statistics tacacs

(config) tacacs

windows-domain

(config) windows-domain

(config) authentication strict-password-policy

WAAS デバイス上でストロング パスワード ポリシーをアクティブにするには、**authentication strict-password-policy** 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。WAAS デバイス上で、ストロング パスワード ポリシーを無効にし、標準パスワード ポリシーを使用するには、このコマンドの **no** 形式を使用します。

authentication strict-password-policy

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト WAAS デバイス上でストロング パスワード ポリシーは有効に設定されています。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン 強度の強いパスワード ポリシーが有効な場合、ユーザ パスワードは次の要件を満たしている必要があります。

- パスワードは、最低 11 の文字長である必要があります。
- パスワードには、大文字と小文字の両方 (A ~ Z および a ~ z)、数字 (0 ~ 9)、および特殊文字 (~!@#\$%^&*()_+=[\]{};:;</> など) を使用できます。
- パスワードを、すべて同じ文字 (99999 など) とすることはできません。
- パスワードを、連続する文字 (12345 など) とすることはできません。
- パスワードをユーザ名と同じにすることはできません。
- ユーザ パスワードは 90 日以内に期限満了となります。新しいパスワードは、それぞれ 12 個前までのパスワードと異なるものにする必要があります。
- パスワードには、' ' | (アポストロフィ、二重引用符、パイプ) または制御文字を使用できません。

ストロング パスワード ポリシーが無効な場合、ユーザ パスワードは次の要件を満たす必要があります。

- パスワードは、1 ~ 34 の文字長である必要があります。
- パスワードには、大文字と小文字の両方 (A ~ Z および a ~ z)、および数字 (0 ~ 9) を使用できます。
- パスワードには、' ' | (アポストロフィ、二重引用符、パイプ) または制御文字を使用できません。



(注)

強度の強いパスワード ポリシーが有効な場合、既存の標準ポリシー パスワードも動作しています。ただし、これらのパスワードは強いパスワード ポリシーの下で期限満了となる場合があります。

■ (config) authentication strict-password-policy

例

次の例では、強度の強いパスワード ポリシーを有効にします。

```
WAE(config)# authentication strict-password-policy
```

次の例では、強度の強いパスワード ポリシーを無効にします。

```
WAE(config)# no authentication strict-password-policy
```

関連コマンド

[clear users](#)

[\(config\) authentication](#)

(config) auto-register

Dynamic Host Configuration Protocol (DHCP) を介してファストイーサネットまたはギガビットイーサネット WAE のディスカバリおよび WAAS Central Manager への自動登録を有効にするには、**auto-register** 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。WAE 上の自動登録機能が無効にするには、このコマンドの **no** 形式を使用します。

auto-register enable [FastEthernet slot/port | GigabitEthernet slot/port]

シンタックスの説明

enable	DHCP を使用した WAAS Cenral Manager へのデバイス自動登録を有効にします。
FastEthernet	(オプション) DHCP を使用して自動登録を行うファストイーサネットインターフェイスを選択します。
<i>slot/port</i>	ファストイーサネットスロット (0 ~ 3) およびポート番号
GigabitEthernet	(オプション) DHCP を使用して自動登録を行うギガビットイーサネットインターフェイスを選択します。
<i>slot/port</i>	ギガビットイーサネットスロット (1 ~ 2) およびポート番号

デフォルト

デフォルトでは、WAE は DHCP を使用した自動登録が有効になっています。

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

使用上のガイドライン

自動登録は自動的にネットワーク設定を設定し、WAE を WAAS Central Manager に登録します。ブートアップ時、実行中の WAAS ソフトウェア (WAAS Central Manager 自身は除く) は自動的に WAAS Central Manager を検出して登録します。管理者がデバイス上で手動設定を行う必要はありません。WAE を登録した後、管理者はデバイスを承認し、WAAS Central Manager GUI を使用してリモートで設定します。

auto-register enable コマンドにより、ファストイーサネットまたはギガビットイーサネット WAE は DHCP を介して WAAS Central Manager のホスト名を検出し、デバイスを自動的に WAAS Central Manager に登録できます。ディスカバリと登録はブートアップ時に行われます。

interface GigabitEthernet slot/port コマンドを使用して固定 IP アドレスを割り当てるには、**no auto-register enable** コマンドを使用して DHCP を介したデバイスの自動登録を無効にしておく必要があります。デフォルトでは DHCP を介した自動登録が有効になっています。

自動登録を動作させるには、WAAS Central Manager のホスト名が設定され、ベンダー クラス オプション 43 を処理できる DHCP サーバが必要です。



(注)

自動登録に使用される DHCP の形式は、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを介して設定可能なインターフェイスレベル DHCP と同じではありません。

DHCP サーバは WAAS デバイスに、RFC 2132 の規定どおりカプセル化されたベンダー固有オプションの形式でベンダー クラス オプション (オプション 43) 情報を送信する必要があります。RFC 2132 の該当セクション、セクション 8.4 をここに複写します。

カプセル化されたベンダー固有のオプションフィールドは、次の例外はありますが DHCP オプションと同じ構文の一連の code/length/value フィールドとして符号化する必要があります。

1. カプセル化されたベンダー固有の拡張フィールドに「マジック クッキー」フィールドがあってはけません。
2. ベンダーはカプセル化されたベンダー固有の拡張フィールドで 0 または 255 以外のコードを定義できますが、セクション 2 で規定された tag-length-value 構文に準拠する必要があります。
3. コード 255 (END) がある場合、ベンダー拡張フィールドの終わりではなく、カプセル化されたベンダー拡張フィールドの終わりを表します。コード 255 がない場合は、囲みのベンダー特有情報フィールドの終わりはカプセル化されたベンダー拡張フィールドの終わりとみなされます。

RFC 標準に従い、DHCP サーバは WAAS Central Manager ホスト名情報を code/length/value 形式で送信する必要があります (コードおよび長さは 1 オクテットです)。WAAS Central Manager ホスト名のコードは 0x01 です。DHCP サーバの管理および設定は自動登録機能の対象範囲ではありません。

WAAS デバイスはオプション 60 のベンダー クラス識別情報として DISCOCDN を送信し、カスタマー別のデバイス グループ化を容易にします。

自動登録 DHCP ではまた、有効とみなされるように DHCP サーバのオファーに次のオプションを入れる必要もあります。

- Subnet-mask (オプション 1)
- Routers (オプション 3)
- Domain-name (オプション 15)
- Domain-name-servers (オプション 6)
- Host-name (オプション 12)

インターフェイスレベル DHCP でオファーが有効とみなされるには subnet-mask (オプション 1) および routers (オプション 3) だけが必要で、domain-name (オプション 15)、domain-name-servers (オプション 6) および host-name (オプション 12) はオプションです。以上のすべてのオプションは domain-name-servers (オプション 6) を除き、システムの既存の設定を置換します。

domain-name-servers オプションはネーム サーバの既存リストに追加されます。ただしネーム サーバは最大 8 つという制約があります。

自動登録は、デバイスの最初のインターフェイス上では、デフォルトで有効になっています。最初のインターフェイスは次のように WAE モデルによって異なります。

- WAE-511、WAE-512、WAE-611、WAE-612 および WAE-7320 では、GigabitEthernet 1/0 を使用します。

DHCP サーバがない場合、デバイスは自動登録を完了できず、最終的にタイムアウトします。自動登録はデバイスのブート後であればいつでも無効にでき、手動のセットアップおよび登録を実行できます。

例

次の例はギガビットイーサネット ポート 2/0 での自動登録を有効にします。

```
WAE(config)# auto-register enable GigabitEthernet 2/0
```

次の例は、WAE に設定されたすべてのインターフェイスで自動登録を無効にします。

```
WAE(config)# no auto-register enable
```


関連コマンド

[show auto-register](#)[show running-config](#)[show startup-config](#)

(config) banner

EXEC、ログイン、および Message-of-The-Day (MOTD) のバナーを設定するには、**banner** 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。バナー機能を無効にするには、このコマンドの **no** 形式を使用します。

```
banner enable | {{exec | login | motd} [message text]}
```

シンタックスの説明

enable	WAE のバナー サポートを有効にします。
exec	EXEC バナーを設定します。
message	(オプション) EXEC プロセスが作成されると表示されるメッセージを指定します。
text	1 行のメッセージ テキスト。バナーがユーザに表示されるときに、WAE によってメッセージの \n 部分が新しい行に変換されます。
login	ログイン バナーを設定します。
motd	MOTD バナーを設定します。

デフォルト

バナー サポートはデフォルトで無効です。

コマンド モード

グローバル コンフィギュレーション

使用上のガイドライン

次の 3 つのタイプのバナーを任意のデバイス モードで設定できます。

- MOTD バナーは、MOTD を設定します。このメッセージは、ログインを試みるときに表示される最初のメッセージです。
- ログイン バナーは、MOTD バナーが表示されてから、実際のログイン プロンプトが表示される前に表示されます。
- EXEC バナーは、EXEC CLI シェルの起動後に表示されます。

**(注)**

上記のすべてのバナーはコンソール、Telnet、または Secure Shell (SSH; セキュア シェル) バージョン 2 セッションで有効です。

message キーワードはオプションです。**message** キーワードを指定せずに Carriage Return (CR; 復帰) を入力すると、メッセージ テキストを入力するように要求されます。1 行以上のメッセージ テキストの場合は、**Return** キーを押すか、デリミタ (\n) を入力して、新しい行にメッセージが表示されるように指定します。新しい行の文字 (\n) を含め、最大 980 文字を入力できます。新しい行の最初にピリオド (.) を入力し、メッセージを保存して、グローバル コンフィギュレーション モードのプロンプトに戻ります。



(注) EXEC バナーのコンテンツは、入力を求めるプロンプトが表示されたあとにユーザが入力する、コマンドライン入力から取得されます。

バナーの設定後、**banner enable** 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、アプリケーションのバナー サポートを有効にします。**show banner EXEC** コマンドを入力して、設定したバナーに関する情報を表示します。



(注) SSH バージョン 1 クライアントを実行していて、WAE にログインする場合は、MOTD バナーとログイン バナーは表示されません。WAE にログインする場合は、SSH バージョン 2 を使用してバナーを表示する必要があります。

例

次の例は、**banner motd message** 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、MOTD バナーを設定する方法を示します。この例では、MOTD メッセージは 1 行のテキストで構成されず。

```
WAE(config)# banner motd message This is a WAAS 4.0.7 device
```

次の例は、**banner motd message** 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、1 行を超える MOTD メッセージを設定する方法を示します。この場合、MOTD メッセージがユーザに表示されるときに、WAE によってメッセージの \n 部分が新しい行に変換されます。

```
WAE(config)# banner motd message "This is the motd message.
\nThis is a WAAS 4.0.7 device\n"
```

次の例は、**banner login message** 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、1 行を超えるログイン メッセージを設定する方法を示します。この場合、WAE A は、ユーザに表示されるログイン メッセージの新しい行に、メッセージの \n 部分を変換します。

```
WAE(config)# banner login message "This is login banner.
\nUse your password to login\n"
```

次の例は、バナー サポートを有効にする方法を示します。

```
WAE(config)# banner enable
```

次の例は、**banner exec** 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、インタラクティブなバナーを設定する方法を示します。**banner exec** コマンドは **banner motd message** コマンドに類似していますが、**banner exec** コマンドでは、入力を求めるプロンプトが表示されたあとにユーザが入力する、コマンドライン入力からバナー コンテンツが取得される点が異なります。

```
WAE(config)# banner exec
Please type your MOTD messages below and end it with '.' at beginning of line:
(plain text only, no longer than 980 bytes including newline)
This is the EXEC banner.\nUse your WAAS username and password to log in to this WAE.\n
.
Message has 99 characters.
WAE(config)#
```

WAE に MOTD、ログイン、および EXEC のバナーが設定されているとします（上記の例を参照）。ユーザが SSH セッションを使用して WAE にログインすると、MOTD バナーおよびログイン バナーを含むログインセッションが表示されます。ログインバナーは、次のようにログインパスワードを入力するようにユーザに要求します。

```
This is the motd banner.  
This is a WAAS 4.0.7 device  
This is login banner.  
Use your password to login.  
  
Cisco Wide Area Application Services Engine  
  
admin@wae's password:
```

ユーザが有効なログインパスワードを入力すると、EXEC バナーが表示され、次のように WAAS ユーザ名とパスワードを入力するように要求されます。

```
Last login: Fri Oct 1 14:54:03 2004 from client  
System Initialization Finished.  
This is the EXEC banner.  
Use your WAAS username and password to log in to this WAE.
```

有効な WAAS ユーザ名とパスワードを入力すると、WAE CLI が表示されます。CLI プロンプトは、ログインアカウントの特権レベルに応じて異なります。次の例では、ユーザが管理特権を持つユーザ名とパスワード（特権レベル 15）を入力したため、EXEC モードの CLI プロンプトが表示されます。

```
WAE#
```

関連コマンド

[show banner](#)

(config) bypass

WAE で静的なバイパス リストを設定するには、**bypass** 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。バイパス機能を無効にする（静的なバイパス リストを消去する）には、このコマンドの **no** 形式を使用します。

```
bypass static {clientip | any-client} {serverip | any-server}
```

シンタックスの説明

static	バイパス リストにスタティック エントリを追加します。
<i>clientip</i>	この IP アドレスからの要求は WAE をバイパスします。
any-client	任意のクライアントから特定のサーバに向けられたトラフィックをバイパスします。
<i>serverip</i>	この IP アドレスからの要求は WAE をバイパスします。
any-server	指定されたクライアントから任意のサーバへの要求は WAE をバイパスします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

静的なバイパス リストを使用して、WAE による設定可能な一連のクライアントおよびファイルサーバ間のトラフィック フローの処理をバイパスできます。Edge WAE でスタティック バイパス エントリを設定することにより、ルータ コンフィギュレーションを変更せずにトラフィックの代行受信を制御できます。別個に、必要であれば、先にトラフィックを Edge WAE にリダイレクトせずにバイパスさせる IP アクセス リストをルータ上で設定できます。通常、WCCP 受け入れリストはキャッシュに格納されるファイル サーバ（およびキャッシュに格納されないファイル サーバ）のグループを定義します。静的なバイパスは、WAAS が特定クライアントから特定ファイル サーバ（または特定クライアントからすべてのファイル サーバ）への接続をキャッシングさせたくない場合などまれなケースで使用できます。

bypass static コマンドは、指定された発信元からのトラフィックが WAE をバイパスすることを許可します。クライアントまたはサーバのどの IP アドレスでも、ワイルドカードはサポートされていません。



(注)

WCCP 対応ルータでは静的なバイパス機能ではなく、IP アクセス リストを使用することを推奨します。アクセス リストの方が効率的です。

例

次の例では、指定されたクライアントから指定されたサーバへのトラフィックに、強制的に WAE をバイパスさせます。

```
WAE(config)# bypass static 10.1.17.1 172.16.7.52
```

次の例では、指定されたサーバ向けの全トラフィックに、強制的に WAE をバイパスさせます。

```
WAE(config)# bypass static any-client 172.16.7.52
```

次の例では、指定されたクライアントから任意のファイルサーバへの全トラフィックに、強制的に WAE をバイパスさせます。

```
WAE(config)# bypass static 10.1.17.1 any-server
```

送信元と宛先のアドレスの静的リストにより、問題を引き起こすクライアントとサーバのインスタンスを隔離できます。静的設定リストの項目を表示するには、次のように **show bypass list** コマンドを使用します。

```
WAE# show bypass list
Client          Server          Entry type
-----
10.1.17.1:0     172.16.7.52:0  static-config
any-client:0    172.16.7.52:0  static-config
10.1.17.2:0     any-server:0    static-config
```

関連コマンド

[show bypass](#)

(config) cdp

すべての WAAS デバイス インターフェイスに対して Cisco Discovery Protocol (CDP; シスコ検出プロトコル) オプションをグローバルに設定するには、グローバル コンフィギュレーション モードで **cdp** コマンドを使用します。

```
cdp {enable | holdtime seconds | timer seconds}
```

シンタックスの説明

enable	グローバルに CDP を有効にします。
holdtime	受信者が CDP パケットを廃棄するまで保持する時間の長さを秒単位で設定します。デフォルトは 180 秒です。
<i>seconds</i>	受信者が CDP パケットを保持する、秒単位での時間の長さ (10 ~ 255)
timer	CDP アドバタイズの間隔 (秒単位)。デフォルトは 60 秒です。
<i>seconds</i>	秒単位での間隔 (5 ~ 254)

デフォルト

holdtime : 180 秒

timer : 60 秒

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

cdp enable コマンドによって有効になると、CDP プロトコルは隣接デバイスのプロトコルアドレスを取得し、そのデバイスのプラットフォームを検出します。また、デバイスが使用するインターフェイスに関する情報も表示します。CDP はメディアおよびプロトコルから独立しており、シスコの機器で稼働します。

CDP MIB とともに SNMP を使用することにより、ネットワーク管理アプリケーションは、デバイス タイプと隣接デバイスの SNMP エージェント アドレスを学習し、そのようなデバイスに SNMP クエリーを送信できます。Cisco Discovery Protocol は CISCO-CDP-MIB を使用します。

CDP 用に設定された各デバイスは、アドバタイズとも呼ばれる定期的なメッセージをマルチキャスト アドレスに送信します。**cdp timer seconds** コマンドは、CDP パケットが送信されるレートを指定します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。アドバタイズには、Time-To-Live (TTL; 存続可能時間) または保持時間の情報も含まれています。保持時間を設定するには、**cdp holdtime seconds** コマンドを使用して、受信者が CDP パケットを保持する時間を秒単位で指定します。各デバイスは、他のデバイスから送信される定期的な CDP メッセージも受信して、隣接デバイスについて学習します。

例

次の例では、まず CDP を有効にし、CDP パケット保持時間を 10 秒に設定し、次に CDP パケットの送信レート (15 秒) を設定します。

```
WAE(config)# cdp enable
WAE(config)# cdp holdtime 10
WAE(config)# cdp timer 15
```

関連コマンド

(config-if) cdp

clear

show cdp

(config) central-manager

WAAS Central Manager の役割およびポート番号を指定するには、central-manager デバイス モードで **central-manager** 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。WAE を登録する WAAS Central Manager の IP アドレスまたはホスト名を指定するには、application-accelerator デバイス モードで **central-manager** 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。これらのアクションを打ち消すには、このコマンドの **no** 形式を使用します。

```
central-manager {address {hostname | ip-address} | role {primary | standby} | ui port port-num}
```

シンタックスの説明

address	WAE が登録する WAAS Central Manager のホスト名または IP アドレスを指定します。
hostname	WAE が登録する WAAS Central Manager のホスト名
ip-address	WAE が登録する WAAS Central Manager の IP アドレス
role	WAAS Central Manager の役割をプライマリまたはスタンバイに設定します。
primary	WAAS Central Manager を登録されている WAE に対するプライマリ WAAS Central Manager に設定します。
standby	WAAS Central Manager を登録されている WAE に対するセカンダリ WAAS Central Manager に設定します。
ui	WAAS Central Manager GUI ポート アドレスを設定します。
port	WAAS Central Manager GUI ポートを設定します。デフォルトはポート 8443 です。
port-num	ポート番号 (1 ~ 65535)



(注) **address** オプションは application-accelerator デバイス モードでのみ有効です。**role** および **ui port** オプションは central-manager デバイス モードでのみ有効です。

デフォルト WAAS Central Manager GUI はポート 8443 を使用するように事前設定されています。

コマンド モード グローバル コンフィギュレーション

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

central-manager address グローバル コンフィギュレーション コマンドは WAE デバイスを WAAS Central Manager と関連付けるので、デバイスは WAAS ネットワークの一部として承認されます。デバイスで WAAS Central Manager の IP アドレスが設定された後、デバイスは自己署名セキュリティ証明書および IP アドレスまたはホスト名、ディスク スペース割り当てなど他の基本情報を WAAS Central Manager に提示します。

WAAS Central Manager で **cms enable** 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 WAAS Central Manager 上の cms サービスを有効にした場合、WAAS Central Manager GUI のポート番号を変更すると、WAAS Central Manager で Centralized Management System (CMS; 中央集中型管理システム) サービスが自動的に再起動されます。

NAT 内側のデバイスの設定

WAAS ネットワークでは、WAAS Central Manager に登録されている WAAS デバイス (WAE またはスタンバイ WAAS Central Manager) は次の 2 つの方法でプライマリ WAAS Central Manager から設定情報を取得します。最初の方式では、デバイスがプライマリ WAAS Central Manager をポート 443 で定期的にポーリングし、設定アップデートを要求します。このポート番号は設定できません。バックアップ方式は、WAAS Central Manager が登録済みデバイスにポート 443 で通知を発行することにより、できるだけ速く登録済みデバイスに設定アップデートを転送する場合です。この方式では変更をよりタイムリーに有効にできます。バックアップ方式を使用する場合でも、このポート番号は設定できません。WAAS Central Manager に登録されているデバイスが WAAS Central Manager をポーリングして設定アップデートを要求できない場合、WAAS ネットワークの動作は信頼できません。

上記の方式はすべて Network Address Translation (NAT; ネットワーク アドレス変換) ファイアウォールがある場合は複雑になります。WAAS デバイス (ネットワークのエッジにある WAE およびプライマリまたはスタンバイ WAAS Central Manager) が NAT ファイアウォールの内側にある場合、同じ NAT 内にあるデバイスは 1 つの IP アドレス (インサイド側ローカル IP アドレス) を使用してデバイスをアクセスし、NAT の外側にあるデバイスは別の IP アドレス (インサイド側グローバル IP アドレス) を使用してデバイスをアクセスします。中央管理対象デバイスはそのインサイド側ローカル IP アドレスだけを WAAS Central Manager にアドバタイズします。NAT 内側のその他のすべてのデバイスはインサイド側ローカル IP アドレスを使用して、NAT 内部にある中央管理対象デバイスにコンタクトします。中央管理対象デバイスと同じ NAT 内にはないデバイスは特殊な設定なしでは中央管理対象デバイスとコンタクトできません。

プライマリ WAAS Central Manager が NAT 内にある場合、その NAT で WAAS Central Manager のインサイド側ローカル IP アドレスに対するスタティック変換 (インサイド側グローバル IP アドレス) を設定し、デバイスを WAAS Central Manager に登録するときに **central manager address ip-address** グローバル コンフィギュレーション コマンドで WAAS Central Manager のインサイド側ローカル IP アドレスではなく、このアドレスを使用することにより、NAT 外側のデバイスが Central Manager をポーリングして **getUpdate** を要求できるようになります。WAAS デバイスが NAT 内側にあり、WAAS Central Manager が NAT 外側にある場合、その NAT で WAE デバイスのインサイド側ローカル IP アドレスに対するスタティック変換 (インサイド側グローバル IP アドレス) を設定して、このアドレスを Device Activation ウィンドウの NAT Configuration 見出しの下の IP Address フィールドに指定することにより、WAAS デバイスが **getUpdate** 要求をポーリングできるようになります。

**(注)**

スタティック変換はインサイド側ローカル アドレスとインサイド側グローバル アドレスの 1 対 1 マッピングを確立します。スタティック変換は、インサイド側のホストがアウトサイド側から固定アドレスでアクセス可能にする必要がある場合に便利です。

スタンバイ WAAS Central Manager

シスコ WAAS ソフトウェアはスタンバイ WAAS Central Manager を実装します。このプロセスにより WAAS ネットワーク設定のコピーを保存できます。プライマリ WAAS Central Manager が故障した場合、プライマリの代わりにスタンバイを使用できます。

相互運用性のため、スタンバイ WAAS Central Manager を使用する場合は、完全な WAAS Central Manager 設定を保存するためプライマリ WAAS Central Manager と同じソフトウェア バージョンでなければいけません。そうしないと、スタンバイ WAAS Central Manager はこのステータスを検出し、問題が修正されるまでプライマリ WAAS Central Manager から受信した設定アップデートを処理しません。

**(注)**

先にスタンバイ WAAS Central Manager をアップデートし、その後プライマリ WAAS Central Manager をアップデートすることを推奨します。またソフトウェアをアップデートする前に、プライマリ WAAS Central Manager でデータベースのバックアップを作成し、そのデータベース バックアップ ファイルを安全な場所にコピーすることも推奨します。

ウォーム スタンバイからプライマリへ WAAS Central Manager の切り替え

プライマリ WAAS Central Manager が動作不能になると、手動でウォーム スタンバイ WAAS Central Manager の 1 つをプライマリ WAAS Central Manager に再設定できます。**central-manager role primary** グローバル コンフィギュレーション コマンドを次のように使用して新しいロールを設定します。

```
WAE# configure
WAE(config)# central-manager role primary
```

このコマンドはロールをスタンバイからプライマリに変更した後、管理サービスを再起動して変更を認識させます。

**注意**

プライマリ WAAS Central Manager がまだオンラインのままアクティブなときにウォーム スタンバイ WAAS Central Manager をプライマリに切り替えると、両方の WAAS Central Manager が互いに検出し、自動的にシャットダウンして管理サービスを無効にします。WAAS Central Manager は停止状態になり、これは自動的にフラッシュ メモリに保存されます。停止状態の WAAS Central Manager をオンライン ステータスに戻す方法については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

**注意**

WAAS Central Manager をプライマリからスタンバイに切り替える場合、Central Manager の設定が消去されます。スタンバイに切り替わった Central Manager は、現在プライマリである Central Manager からの設定情報の複製を開始します。スイッチング ロールの前にスタンバイ ユニットとスタンバイ ユニットが同期を行っていないと、重要な設定情報が紛失する可能性があります。このコマンドを使用する前に、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

例 次の例は、WAAS デバイス、waas-cm が WAAS ネットワークに対するプライマリ WAAS Central Manager として機能するように指定します。

```
waas-cm(config)# central-manager role primary
```

次の例は WAE が IP アドレス 10.1.1.1 の WAAS Central Manager に登録するよう指定します。このコマンドは WAE をプライマリ WAAS Central Manager と関連付けるので、WAE は WAAS ネットワークの一部として承認されます。

```
WAE(config)# central-manager address 10.1.1.1
```

次の例は、WAAS Central Manager GUI をアクセスするための新しい GUI ポートを設定します。

```
WAE(config)# central-manager ui port 8550
```

次の例は、WAAS Central Manager をスタンバイ WAAS Central Manager に設定します。

```
WAE(config)# central-manager role standby  
Switching CDM to standby will cause all configuration settings made on this CDM to be  
lost.  
Please confirm you want to continue [no]?yes  
Restarting CMS services
```

(config) clock

表示目的で夏時間と時間帯を設定するには、**clock** 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。この機能を無効にするには、このコマンドの **no** 形式を使用します。

```
clock {summertime timezone {date startday startmonth startyear starthour endday endmonth endyear
offset | recurring {1-4 startweekday startmonth starthour endweekday endmonth endhour offset |
first startweekday startmonth starthour endweekday endmonth endhour
offset | last startweekday startmonth starthour endweekday endmonth endhour offset}} | timezone
{timezone houroffset minutesoffset}}
```

シンタックスの説明

summertime	夏時間を設定します。
<i>timezone</i>	夏時間帯の名前
date	絶対夏時間を設定します。
<i>startday</i>	開始の日付 (1 ~ 31)
<i>startmonth</i>	開始の月 (January ~ December)
<i>startyear</i>	開始の年 (1993 ~ 2032)
<i>starthour</i>	時間:分 (hh:mm) 形式の開始時間 (0 ~ 23)
<i>endday</i>	終了の日付 (1 ~ 31)
<i>endmonth</i>	終了の月 (January ~ December)
<i>endyear</i>	終了の年 (1993 ~ 2032)
<i>endhour</i>	時間:分 (hh:mm) 形式の終了時間 (0 ~ 23)
<i>offset</i>	UTC からオフセット (「 使用上のガイドライン 」セクションのテーブルを参照) する分数 (0 ~ 59)
recurring	反復夏時間を設定します。
1-4	開始の週番号 (1 ~ 4) を設定します。
first	反復夏時間が始まる月の最初の週を設定します。
last	反復夏時間が始まる月の最後の週を設定します。
<i>startweekday</i>	開始する曜日 (Monday ~ Friday)
<i>startmonth</i>	開始の月 (January ~ December)
<i>starthour</i>	時間:分 (hh:mm) 形式の開始時間 (0 ~ 23)
<i>endweekday</i>	終了する曜日 (Monday ~ Friday)
<i>endmonth</i>	終了の月 (January ~ December)
<i>endhour</i>	時間:分 (hh:mm) 形式の終了時間 (0 ~ 23)
<i>offset</i>	UTC からオフセット (「 使用上のガイドライン 」セクションのテーブルを参照) する分数 (0 ~ 59)
timezone	標準時間帯を設定します。
<i>timezone</i>	時間帯の名前 (「 使用上のガイドライン 」セクションのテーブルを参照)
<i>houroffset</i>	UTC からオフセット (「 使用上のガイドライン 」セクションのテーブルを参照) する時間 (-23 ~ +23)
<i>minutesoffset</i>	UTC からオフセット (「 使用上のガイドライン 」セクションのテーブルを参照) する分数 (0 ~ 59)

デフォルト

デフォルトの動作や値はありません。

コマンドモード グローバル コンフィギュレーション

デバイスモード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン NTP サーバなしで現地および UTC の現在時刻を設定および表示するには、**clock set** コマンドとともに **clock timezone** コマンドを使用します。**clock timezone** パラメータで、**clock set EXEC** コマンドで設定した UTC 時間と現地時間の間の差異を指定します。UTC 時間 と現地時間は、**show clock detail EXEC** コマンドで表示します。

clock timezone offset コマンドを使用して時間帯を設定します。ここで、*timezone* は下記のテーブルの目的の時間帯エントリであり、*00* は、時間と分形式の、UTC とのオフセット（進めるまたは遅らせる）です（UTC は以前は Greenwich mean time [GMT; グリニッジ標準時]）と呼ばれていました。

```
WAE(config)# clock timezone timezone 0 0
```



(注)

時間帯エントリは大文字、小文字を区別するので、表 3-100 に記載されているとおりに正確に指定する必要があります。時間帯表から時間帯エントリを使用すると、夏時間用に自動的に調整されます。

表 3-100 時間帯 — UTC からのオフセット

時間帯	UTC からのオフセット
Africa/Algiers	+1
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Nairobi	+3
America/Buenos_Aires	-3
America/Caracas	-4
America/Mexico_City	-6
America/Lima	-5
America/Santiago	-4
Atlantic/Azores	-1
Atlantic/Cape_Verde	-1
Asia/Almaty	+6
Asia/Baghdad	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6

表 3-100 時間帯 — UTC からのオフセット (続き)

時間帯	UTC からのオフセット
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2
Asia/Kabul	+4.30
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	-4
Canada/Newfoundland	-3.30
Canada/Saskatchewan	-6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2
Europe/London	0
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10

表 3-100 時間帯 — UTC からのオフセット (続き)

時間帯	UTC からのオフセット
Pacific/Kwajalein	-12
Pacific/Samoa	-11
US/Alaska	-9
US/Central	-6
US/Eastern	-5
US/East-Indiana	-5
US/Hawaii	-10
US/Mountain	-7
US/Pacific	-8

例 次の例は、UTC から 8 時間遅れのオフセットを持つ太平洋標準時を現地の時間帯として指定します。

```
WAE(config)# clock timezone US/Pacific -8 0
```

次の例では、WAAE デバイス上の時間帯設定を無効にします。

```
WAE(config)# no clock timezone
```

次の例では夏時間を設定します。

```
WAE(config)# clock summertime US/Pacific date 10 October 2005 23:59 29 April 2006
23:59 60
```

関連コマンド

[clock](#)

[show clock](#)

(config) cms

WAAS デバイス上でメンテナンスのスケジューリングを行って Centralized Management System (CMS; 中央集中型管理システム) を有効にするには、**cms** 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。これらのアクションを打ち消すには、このコマンドの **no** 形式を使用します。

```
cms {database maintenance {full {enable | schedule weekday at time} | regular {enable | schedule
weekday at time}} | enable | rpc timeout {connection 5-1800 | incoming-wait 10-600 | transfer
10-7200}}
```

シンタックスの説明

database maintenance	組み込みデータベースのクリーンまたはリインデックス メンテナンス ルーチンを設定します。
full	フル メンテナンス ルーチンを設定し、組み込みデータベース テーブルをクリーンします。
enable	組み込みデータベース テーブルで行うフル メンテナンス ルーチンを有効にします。
schedule	メンテナンス ルーチンを行うためのスケジュールを設定します。
<i>weekday</i>	メンテナンス ルーチンを開始する曜日 every-day 毎日 Mon 毎月曜日 Tue 毎火曜日 Wed 毎水曜日 Thu 毎木曜日 Fri 毎金曜日 Sat 毎土曜日 Sun 毎日曜日
at	メンテナンス ルーチンを開始するメンテナンス スケジュール時間を設定します。
<i>time</i>	メンテナンス ルーチンを開始する時間 (0 ~ 23:0 ~ 59) (hh:mm) at メンテナンス時間 Mon 毎月曜日 Tue 毎火曜日 Wed 毎水曜日 Thu 毎木曜日 Fri 毎金曜日 Sat 毎土曜日 Sun 毎日曜日
regular	定期メンテナンス ルーチンを設定し、組み込みデータベース テーブルをリインデックスします。
enable	WAAS デバイス上で CMS プロセスを有効にします。
rpc timeout	リモート プロシージャ コール接続のタイムアウト値を設定します。
connection	接続作成時の最大待機時間を指定します。
<i>5-1800</i>	タイムアウト時間 (秒単位)。WAAS Central Manager のデフォルトは 30 秒で、WAE のデフォルトは 180 秒です。
incoming-wait	クライアント応答の最大待機時間を指定します。
<i>10-600</i>	タイムアウト時間 (秒単位)。デフォルトは 30 秒です。

transfer	接続をオープンのままにしておく最大時間を指定します。
<i>10-7200</i>	タイムアウト時間 (秒単位)。デフォルトは 300 秒です。

デフォルト

database maintenance regular : enabled (有効)

database maintenance full : enabled (有効)

connection : WAAS Central Manager は 30 秒で、WAE は 180 秒です。

incoming wait : 30 秒

transfer : 300 秒

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

cms database maintenance 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、組み込みデータベースのフル メンテナンス クリーニング (バキューミング) または定期メンテナンス リンデックス ルーチンのスケジューリングを行います。フル メンテナンス ルーチンはディスクが 90 パーセント以上フルの場合のみ実行され、週に一度だけ実行されます。テーブルをクリーニングすることでデータベース システムのスペースを再利用できます。

cms enable グローバル コンフィギュレーション コマンドは自動的にノードをデータベース管理テーブルに登録し、CMS プロセスを有効にします。**no cms enable** グローバル コンフィギュレーション コマンドは WAAS デバイス上の管理サービスを停止させるだけです。WAAS ネットワークから WAAS デバイスの登録を解除 (削除) するには、**cms deregister EXEC** コマンドを使用します。

例

次の例は、WAAS デバイスで毎金曜日、午後 11 時の定期 (リンデックス) メンテナンス ルーチンをスケジューリングします。

```
WAE(config)# cms database maintenance regular schedule Fri at 23:00
```

次の例は、WAAS デバイスで CMS プロセスを有効にする方法を示します。

```
WAE(config)# cms enable
Generating new RPC certificate/key pair
Restarting RPC services

Creating database backup file emerg-debug-db-01-25-2006-15-31.dump
Registering Wide Area Central Manager...
Registration complete.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in Wide Area Central Manager UI.
management services enabled
```

関連コマンド

cms

show cms

(config) device mode

WAAS デバイスのデバイス モードを設定するには、**device mode** 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。WAAS デバイス上で動作モードをリセットするには、このコマンドの **no** 形式を使用します。

device mode {application-accelerator | replication accelerator | central-manager}

シンタックスの説明

application-accelerator	WAAS デバイスが WAAS アクセラレータとして機能するように設定します。すべての Edge WAE および Core WAE はこのモードまたは replication-accelerator モードで動作しなければいけません。
replication-accelerator	WAAS デバイスが、データ センターのレプリケーション アプリケーション用の WAAS アクセラレータとして機能するように設定します。レプリケーションに参加する Core WAE はすべて、replication-accelerator モードにする必要があります。
central-manager	WAAS デバイスが WAAS Central Manager として機能するように設定します。

デフォルト

デフォルトのデバイス動作モードは application-accelerator です。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

WAAS Central Manager は専用アプライアンスで展開する必要があります。WAAS 4.0 ソフトウェア リリースではデバイス モード機能が追加されました。これにより WAAS デバイスを WAAS Central Manger または WAE のどちらかで展開できます。WAAS デバイスは、いずれか 1 つのデバイス モードでのみ動作できます。利用できる一連の WAAS CLI コマンドは WAAS デバイスのデバイス モードに基づいて異なります。



(注)

WAAS Central Manager は、WAAS ネットワークのデバイス管理ステーションです。これにより、WAE の中央集中型の設定、管理、および監視が可能になります。

デフォルトでは、WAAS デバイスは application-accelerator モードを使用し、Wide Area Application Engine (WAE) として動作します。WAAS CLI を使用して WAAS Central Manager のネットワーク設定を行う前に、デバイス モードを central-manager に変更する必要があります。

デバイス モードを central-manager に変更してから、**cms enable** 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、WAAS ネットワーク関連アプリケーションおよびサービスを有効にします。WAAS ネットワークを無効にするには、このコマンドの **no** 形式を使用します。

WAE ネットワーク モジュール (デバイスの任意の NME-WAE ファミリ) を Central Manager として設定できません。

インライン WAE を Central Manager として設定できますが、インライン機能は使用できません。

例

次の例では、WAAS デバイスのデバイス モードとして、`central-manager` を指定します。

```
WAE(config)# device mode central-manager
```

次の例では、WAAS デバイスのデバイス モードとして、`application-accelerator` を指定します。

```
WAE(config)# device mode application-accelerator
```

次の例では、WAAS デバイスのデバイス モードとして、`replication-accelerator` を指定します。

```
WAE(config)# device mode replication-accelerator
```

次の例では、デバイス モードを `central-manager` から `application-manager` または `replication-manager` に変更します。

**(注)**

最初に EXEC モードで `cms deregister force` コマンドを使用して、Central Manager 上の Centralized Management System (CMS; 中央集中型管理システム) を無効にしてから、グローバル コンフィギュレーション モードで `device mode` コマンドを使用します。

```
WAE# cms deregister force
WAE(config)# device mode application-accelerator
WAE# copy running-config startup-config
```

関連コマンド

[show device-mode](#)

(config) disk disk-name

オンラインでの取り外しのためディスクを無効にするには、**disk disk-name** 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。ディスクを再度有効にするには、このコマンドの **no** 形式を使用します。

```
disk disk-name diskxx shutdown [force]
```

シンタックスの説明

<i>diskxx</i>	ディスクの名前 (disk00 ~ disk05)
shutdown	メンテナンスのためディスクを無効にします。
force	(オプション) このコマンドの no 形式とともに使用する場合は、ディスクを強制的に再度有効にします。 このオプションは RAID-5 システムでは利用できません。

デフォルト

ディスクは有効です。

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

このコマンドは **disk mark EXEC** モード コマンドに代わるものです。

このコマンドは WAE-7341 および WAE-7371 モデルでは利用できません。代わりに、**disk disk-name diskxx replace EXEC** モード コマンドを使用します。

RAID-1 による論理ディスク処理

RAID-1 はソフトウェア機能として WAAS に実装されています。RAID-1 WAAS デバイスは信頼性の向上のため 2 つのディスク ドライブを使用できます。RAID-1 はディスク ミラーリングを提供します (データは 2 つ以上のドライブに重複して書き込まれます)。冗長性による信頼性の向上が目的です。RAID-1 の場合、1 つのディスク 書き込みを 2 つのディスク ドライブに対して行う必要があるため、ファイル システムの書き込みパフォーマンスに影響を与えます。RAID-1 (ミラーリング) は RAID-1 デバイス上のすべてのファイル システムに使用されます。この設定により、いかなる場合にも信頼性のあるソフトウェアの実行が保証されます。



(注)

WAAS ソフトウェアは、Wide Area File Services (WAFS) ファイル システムおよび、Data Redundancy Elimination (DRE) キャッシュの両方に CONTENT ファイル システムを使用します。

WAE-612、WAE-7326、WAE-7341、および WAE-7371 ディスク ドライブのホットスワップ

このリリースの WAAS では、障害のあるディスクの交換およびスケジュールされたディスク メンテナンスのためにホットスワップ機能がサポートされています。WAE-612 および WAE-7326 では、**disk disk-name diskxx shutdown** 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、スケ

ジュールされたディスク メンテナンスのためにディスクを手動でシャットダウンします。WAE-7341 および WAE-7371 では、**disk disk-name diskxx replace EXEC** コマンドを使用して、スケジュールされたディスク メンテナンスのためにディスクを手動でシャットダウンします(予定ディスク メンテナンス プロシージャについては、『Cisco Wide Area Application Services Configuration Guide』の Chapter 14 章を参照してください)。

ディスクが完全にシャットダウンされるまで待ってから、ディスクを WAE から物理的に取り外してください。RAID の取り外し処理が終了すると、WAAS はディスク障害アラームおよびトラップを生成します。さらに、syslog ERROR メッセージがログに記録されます。

RAID 再構築プロセス中に障害のあるディスクがソフトウェアで削除された場合は、RAID 再構築エラーのアラームが生成されます。RAID 再構築プロセス中にディスクを管理上のシャットダウンにした場合は、代わりに RAID 再構築の中断アラームが生成されます。

RAID の再構築プロセス中に削除イベントが発生した場合は、RAID 削除プロセスの正常終了に1分ほどかかる場合があります。このプロセスにかかる実際の時間は、ディスクのサイズによって異なります。

RAID-1 での障害ディスクの自動処理

クリティカル ディスク アラームがシステムで1つ検出されると、障害ディスクはディスクのホットスワップ機能により自動的に無効にされます。ソフトウェアでは **disk error-handling** の設定に関係なく、障害ディスクを自動的に削除します。

障害ディスクの交換

取り外しのためディスクを管理上無効にするには、グローバル コンフィギュレーション モードで **disk disk-name** コマンドを使用します。交換後にディスクを管理的に再度有効にするには、このコマンドの **no** 形式を使用します。

ディスクを手動でシャットダウンする場合は、**no disk disk-name diskxx shutdown** コマンドを入力するまでシャットダウンされたままとなります。

RAID-1 デバイスの場合は、グローバル コンフィギュレーション モードで **disk disk-name diskxx shutdown force** コマンドを使用することにより、以前に不良ディスクとして識別されたディスクを交換し、不良ステータスを手動で上書きすることができます。

ディスク情報

障害ディスクまたは不良ディスクとされているディスクを識別するには、**show disks failed-disk-id EXEC** コマンドを使用します。このリストに示されたシリアル番号を持つディスクを再度挿入しないでください。



(注) **show disks failed-disk-id EXEC** コマンドは WAE-7341 および WAE-7371 モデルでは利用できません。

関連コマンド

(config) [disk error-handling](#)

(config) [disk logical shutdown](#)

[disk](#)

[show disks](#)

(config) disk encrypt enable

ディスク暗号化をイネーブルにするには、**disk encrypt enable** 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。ディスク暗号化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。

disk encrypt enable

シンタックスの説明

このコマンドには、キーワードや引数がありません。

デフォルト

ディスク暗号化はデフォルトでディセーブルに設定されています。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

ディスク暗号化機能は、導入されている ACE service module システムを流れ、ACE service module 永久ストレージにストアされる機密情報の安全な保護に対するニーズに対応します。ディスクの暗号化には、WAE ディスク上での実際のデータ暗号化およびキーのストレージと管理の 2 つの機能が 있습니다。

ディスク暗号化をイネーブルにすると、ACE service module 永久ストレージ内のすべてのデータが暗号化されます。暗号化されたデータのロックを解除する暗号キーは Central Manager にストアされ、キー管理は Central Manager によって行われます。ディスク暗号化の設定後に WAE をリポートすると、WAE は Central Manager からキーを自動的に取得し、ACE service module 永久ストレージにストアされているデータに通常どおりアクセスできるようにします。

ディスク暗号化の要件は次のとおりです。

- Central Manager をネットワークで使用するように設定しておく必要があります。
- WAE デバイスを Central Manager に登録する必要があります。
- WAE デバイスを Central Manager でオンラインにする（接続をアクティブにしておく）必要があります。この要件は、ディスク暗号化をイネーブルにしている場合にのみ適用されます。
- ディスク暗号化設定を有効にするには WAE をリポートする必要があります。

WAE をリポートすると、新しいキーを使用して暗号化パーティションが作成され、既存のデータがこのパーティションから削除されます。

ディスク暗号化設定（暗号化をイネーブルにするかディセーブルにするか）に変更があると、ディスクのキャッシュがクリアされます。この機能によって、WAE が盗難された場合にも、カスタマーの機密データの暗号が解読されてアクセスされるのを防ぎます。

ディスク暗号化をイネーブルにしてから、この機能をサポートしていないソフトウェアのバージョンにダウングレードすると、ディスク パーティションを使用できなくなります。このような場合は、ダウングレードを行ってからディスク パーティションを削除する必要があります。

ディスク暗号化をイネーブルまたはディセーブルにするには、**disk encrypt** 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。ディスク暗号化をイネーブルまたはディセーブルにすると、その後の初回リポート中にファイル システムが再初期化されます。再初期化には、ディスクパーティションのサイズによって 10 分から数時間ほどかかる場合があります。この間、WAE にはアクセス可能ですが、WAE のサービスを利用することはできません。

Central Manager の IP アドレスを変更するか、Central Manager の位置を変更するか、Central Manager を別の Central Manager と交換したが元の Central Manager の一部の情報をコピーしていない場合、ディスク暗号化をイネーブルにして WAE をリロードすると、WAE ファイル システムは再初期化プロセスを完了することができないか、Central Manager から暗号キーを取得できません。

WAE が暗号キーを取得できない場合は、CLI の **disk encrypt disable** 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ディスク暗号化をディセーブルにし、WAE をリロードします。ディスク暗号化をイネーブルにして WAE をリロードする前に、Central Manager に接続できることを確認してください。このプロセスによってディスク キャッシュがクリアされます。

暗号化ステータスの詳細を表示するには、**show disks details EXEC** コマンドを使用します。ファイルシステムによる初期化中は、**show disks details** によって [System initialization is not finished, please wait...] というメッセージが表示されます。ディスク暗号化ステータスは、イネーブルであってもディセーブルであっても、Central Manager GUI の Device Home ウィンドウで表示することもできます。

関連コマンド**disk****show disks**

(config) disk error-handling

WAAS デバイスでディスク エラーの処理方法を設定し、ディスク エラー処理のしきい値を定義するには、**disk error-handling** 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。デフォルトのエラー処理しきい値に戻すには、このコマンドの **no** 形式を使用します。

```
disk error-handling {reload | remap | threshold number}
```

シンタックスの説明

reload	disk00 のシステム ファイル システム (SYSFS) に問題がある場合、ディスクをリロードします。
remap	ディスク エラーを自動的にリマップするようにディスクを設定します。
threshold	ディスクが不良としてマーク付けされるまでに許容されるディスク エラーの数を設定します。
<i>number</i>	ディスクが不良としてマーク付けされるまでに許容されるディスク エラーの数 (0 ~ 100)。デフォルト値は 10 です。0 を設定した場合、ディスクは不良としてマーク付けされません。

デフォルト

```
error-handling threshold number : 10
```

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

2 ドライブ システムの場合、RAID ソフトウェアは、SYSFS を単一ドライブ障害から保護し、アプリケーションが I/O エラーを認識しないようにします。このような設定では、エラー処理は指定する必要がありません。その他のすべての設定では、エラー処理は指定する必要があります。

正常に動作するには、WAAS デバイスは disk00 という名前のディスク ドライブを備えている必要があります。また、WAAS デバイスは、SYSFS (システム ファイル システム) の第 1 パーティションを格納するディスク ドライブを備えている必要もあります。SYSFS パーティションは、システム ログや内部デバッグ ログなどのログ ファイルを保存するために使用します。WAAS デバイスのイメージ ファイルやコンフィギュレーション ファイルのストアにも使用できます。disk00 は常に SYSFS パーティションを格納します。ソフトウェア RAID を適用した場合、SYSFS パーティションには disk00 と disk01 の両方が格納されています。いずれにしても、disk00 のディスクおよび SYSFS の第 1 パーティションを格納するディスクは、クリティカル ドライブと呼ばれ、WAAS デバイスの正常な動作に必要です。

WAE をブートし、クリティカルディスク ドライブがシステムの始動時に検出されないと、WAAS デバイスはサービス低下の状態で作動します。クリティカルディスク ドライブの 1 つが実行時に動作不能になった場合、WAAS デバイスは、アプリケーションの誤動作や失敗などの症状を示すことがあります。あるいは WAAS デバイスが応答を停止することもあります。WAAS デバイスのクリティカルディスク ドライブを監視して、ディスク ドライブ エラーがあれば TAC にレポートする必要があります。

WAAS デバイスでは、ディスク デバイス エラーは次のいずれかのイベントとして定義されます。

- SCSI または IDE デバイス エラーが、Linux カーネルによって出力される。
- 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) システム コール）が、EIO エラー コードで失敗する。
- 始動時に存在したディスク デバイスが、実行時にアクセスできない。

ディスクの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。WAAS デバイスのディスク ドライブでエラーが発生すると、SYSFS パーティションがまだ損なわれ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、WAAS デバイスで 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 エラー処理のしきい値の指定

WAAS デバイスでディスク デバイス エラー処理のしきい値を定義できます。ディスク デバイス エラーの数が指定されたしきい値に達した場合は、対応するディスク デバイスは自動的に不良としてマーク付けされます。デフォルトでは、このしきい値は 10 に設定されています。デバイスでは、不良ディスク デバイスの使用をすぐには止めません。次にリポートしたあとに、不良ディスク ドライブの使用を中止します。

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 ドライブを不良としてマーク付けさせたくない場合は、0 を指定します。

指定されたしきい値を超えた場合は、WAAS デバイス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ディスク ドライブであり、自動リロード機能 (**disk error-handling reload** コマンド) が有効な場合、WAAS ソフトウェアはディスク ドライブを不良としてマーク付けし、WAAS デバイスが自動的にリロードされます。WAAS デバイスがリロードされると、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、WAAS デバイスの自動リロード機能は無効になっています。自動リロード機能を有効にするには、**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有効にした後、無効にするには、**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。

例

次の例では、特定のディスク ドライブ（たとえば、disk00）に対して、ディスク ドライブが不良として自動的にマーク付けされるまでに許容されるエラーの最大数を 5 ディスク ドライブ エラーとして設定しています。

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

関連コマンド

disk

show disks

(config) disk logical shutdown

RAID-5 論理ディスク ドライブをシャットダウンするには、**disk logical shutdown** 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。RAID-5 論理ディスク ドライブを再度有効にするには、このコマンドの **no** 形式を使用します。

disk logical shutdown

シンタックスの説明 このコマンドには、キーワードや引数がありません。

デフォルト RAID-5 アレイはデフォルトで有効に設定されます。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator

使用上のガイドライン このコマンドは WAE-7341 および WAE-7371 モデルでのみサポートされます。

このコマンドを使用して WAE-7341 または WAE-7371 をディスクレス モードで動作させます。ディスクレス モードでは、パーティションおよびディスクはマウントされず、使用できません。

このコマンドを有効にするには、デバイスをリロードする必要があります。

(config) egress-method

代行受信された接続の出力方式を設定するには、**egress-method** 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。

```
egress-method {ip-forwarding | negotiated-return} intercept-method wccp
```

シンタックスの説明

ip-forwarding	出力方式を IP 転送に設定します。
negotiated-return	出力方式を WCCP ネゴシエーション リターンに設定します。
intercept-method	出力方式の設定時にどの代行受信方式を使用するかを選択します。
wccp	WCCP 代行受信の出力方式を設定します。

デフォルト

デフォルトの出力方式は IP 転送です。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

WCCP 代行受信モードでは、IP 転送とネゴシエーション リターンの 2 つの出力設定オプションをサポートします。ネゴシエーション リターンは、WCCP GRE を WCCP 出力方式としてサポートします。

WCCP GRE パケット リターンによって、複数の WAE をクライアントおよびサーバとして同じ VLAN またはサブネット上に配置できます。このトポロジは、IP 転送の出力方式を使用している場合には許可されません。フローを最適化するために、WCCP GRE パケット リターンはまた、冗長ルータおよびルータのロード バランシングを「ベストエフォート」方式でサポートしています。

WCCP GRE を出力方式として設定すると、WAAS はルータのロード バランシングがネットワークで使用されている場合に、元のルータ選択を維持するよう最大限の努力を払います。WAAS は、WCCP GRE に対してルータ選択において次のロジックを適用します。

- WAAS が TCP フローに DRE および圧縮を適用している場合は、最適化されたデータを伝送する単一のパケットが、別のルータからリダイレクトされた複数のパケットで受信した元のデータを表す可能性があることから、送信されたパケット数が少なくなることがあります。この最適化されたデータ伝送パケットは、WAE から前回パケットを WAE にリダイレクトしたルータに、そのフローの方向で出力されます。
- WAE が最適化されたデータを受信する場合、データは別々のルータから複数のパケットで到達することがあります。WAAS は最適化されたデータを展開して元のデータに戻し、複数のパケットとして送信します。この元のデータ伝送パケットが、WAE から前回パケットを WAE にリダイレクトしたルータに、そのフローの方向で出力されます。

ネゴシエーション リターンは、WCCP GRE を唯一の WCCP 出力方式としてサポートします。WCCP が WCCP L2 リターンをネゴシエーションする場合は、WAE は出力方式として IP 転送をデフォルトで使用します。ネゴシエーションされた出力方式がデフォルトで IP 転送である場合は、何の通知も受け取りませんが、このような場合には Syslog メッセージが生成されます。

デフォルトの出力方式は IP 転送です。**negotiated-return** オプションを設定しない場合は、IP 転送が使用されます。

ただし WCCP バイパス フローは、CLI 設定に関係なく WCCP ネゴシエーション リターン方式を使用し、IP 転送を使用しません。



(注) WCCP GRE 出力方式はインライン動作モードに適用されません。

例 WCCP 代行受信モードの出力方式を Central Manager GUI から設定するには、**Devices > Devices > Interception > Egress Methods** を選択します。

次の例では、WCCP GRE パケット リターン の代行受信および出力方式を CLI から設定します。

```
WAE(config)# egress-method negotiated-return intercept-method wccp
```

次の例では、IP 転送の代行受信および出力方式を CLI から設定します。

```
WAE(config)# egress-method ip-forwarding intercept-method wccp
```

特定の WAE 上で設定され使用されている出力方式を表示するには、**show egress-methods EXEC** コマンドまたは **show tfo egress-methods connection EXEC** コマンドを使用します。

関連コマンド

[show egress-methods](#)

[show tfo egress-methods connection](#)

[\(config\) wccp tcp-promiscuous](#)

(config) end

グローバル コンフィギュレーション モードを終了するには、**end** 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。

end

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン 実行コンフィギュレーションへの変更を完了した後は常に、**end** コマンドを使用してグローバル コンフィギュレーション モードを終了します。NVRAM への新しいコンフィギュレーションを保存するには、**write** コマンドを使用します。

Ctrl-Z コマンドもグローバル コンフィギュレーション モードを終了します。

例 次の例は、WAAS デバイスでグローバル コンフィギュレーション モードを終了する方法を示します。

```
WAE(config)# end  
WAE#
```

関連コマンド [\(config\) exit](#)

(config) exec-timeout

WAAS デバイスで非アクティブな Telnet または SSH セッションを開いたままにしておく時間の長さを設定するには、**exec-timeout** 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。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

exec-timeout *timeout*

シンタックスの説明

timeout タイムアウト (分単位) (0 ~ 44640)

デフォルト

デフォルトは 15 分です。

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

WAAS デバイスでの Telnet または Secure Shell (SSH; セキュア シェル) セッションは、**exec-timeout** コマンドによって指定されたインターバルの間、非アクティブな状態で開いたままにしておくことができます。**exec-timeout** によるインターバルが経過すると、WAAS デバイスでは自動的に Telnet または SSH セッションを閉じます。

例

次の例は、タイムアウトを 100 分に設定します。

```
WAE(config)# exec-timeout 100
```

次の例では、設定された 100 分のタイムアウトを無効にし、デフォルトの 15 分に戻します。

```
WAE(config)# no exec-timeout
```

関連コマンド

[\(config\) telnet enable](#)

(config) exit

グローバル コンフィギュレーション モードを終了させて特権レベル EXEC モードに戻るには、**exit** コマンドを使用します。

exit

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード すべてのモード

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン このコマンドは、**Ctrl-Z** または **end** コマンドと同じです。

例 次の例は、グローバル コンフィギュレーション モードを終了して特権レベル EXEC モードに戻ります。

```
WAE(config)# exit  
WAE#
```

関連コマンド [\(config\) end](#)

(config) external-ip

WAE で最大 8 つの外部 Network Address Translation (NAT; ネットワーク アドレス変換) IP アドレスを設定するには、**external-ip** 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。NAT IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

external-ip ip-addresses

シンタックスの説明

ip-addresses 最大 8 つの外部または IP アドレスを設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

使用上のガイドライン

このコマンドを使用して WAE で最大 8 つの NAT IP アドレスを設定して、ルータが最大 8 つの内部アドレスを一意的に登録済みアドレスに変換したり、外部登録済みアドレスをプライベートネットワークに一意的なアドレスに変換できるようにします。

WAAS ネットワークでは、WAAS Central Manager に登録されている WAE は次の 2 つの方法でプライマリ WAAS Central Manager から設定情報を取得します。最初の方式では、デバイスがプライマリ WAAS Central Manager をポート 443 で定期的にポーリングし、設定アップデートを要求します。このポート番号は設定できません。バックアップ方式は、WAAS Central Manager が登録済みデバイスにポート 443 で通知を発行することにより、できるだけ速く登録済みデバイスに設定アップデートを転送する場合です。この方式では変更をよりタイムリーに有効にできます。バックアップ方式を使用する場合でも、このポート番号は設定できません。WAAS Central Manager に登録されているデバイスが WAAS Central Manager をポーリングして設定アップデートを要求できない場合、WAAS ネットワークの動作は信頼できません。

WAAS デバイス（ネットワークのエッジにある WAE およびプライマリまたはスタンバイ WAAS Central Manager）が NAT ファイアウォールの内側にある場合、同じ NAT の内側にあるデバイスは 1 つの IP アドレス（インサイド側ローカル IP アドレス）を使用してデバイスをアクセスし、NAT の外側にあるデバイスは別の IP アドレス（NAT IP アドレスまたはインサイド側グローバル IP アドレス）を使用してデバイスをアクセスします。中央管理対象デバイスはそのインサイド側ローカル IP アドレスだけを WAAS Central Manager にアドバタイズします。NAT 内側のその他のすべてのデバイスはインサイド側ローカル IP アドレスを使用して、NAT 内部にある中央管理対象デバイスにコンタクトします。中央管理対象デバイスと同じ NAT 内にはないデバイスは特殊な設定なしでは中央管理対象デバイスとコンタクトできません。

プライマリ WAAS Central Manager が NAT 内側にある場合、その NAT で WAAS Central Manager のインサイド側ローカル IP アドレスに対するスタティック変換（NAT IP アドレスまたはインサイド側 IP アドレス）を設定し、WAAS デバイスを WAAS Central Manager に登録するときに **central manager address ip-address** グローバル コンフィギュレーション コマンドで WAAS Central Manager のインサイド側ローカル IP アドレスではなく、このアドレスを使用することにより、NAT 外側にある WAAS デバイスが Central Manager をポーリングして **getUpdate** を要求できるようになります。WAAS デバイスが NAT 内側にあり、WAAS Central Manager が NAT 外側にある場合、その NAT

■ (config) external-ip

で WAE インサイド側ローカルアドレスに対するスタティック変換 (NAT IP アドレスまたはインサイド側グローバル IP アドレス) を設定することにより、WAAS デバイスは getUpdate 要求をポーリングできるようになります。

**(注)**

スタティック変換はインサイド側ローカルアドレスとインサイド側グローバルアドレスの 1 対 1 マッピングを確立します。スタティック変換は、インサイド側のホストがアウトサイド側から固定アドレスでアクセス可能にする必要がある場合に便利です。

例

次の例は、WAAS デバイスで 4 つの外部 NAT IP アドレスを設定します。

```
WAE(config)# external-ip 192.168.43.1 192.168.43.2 192.168.43.3 192.168.43.4
```

関連コマンド

[\(config\) interface](#)

[\(config\) ip](#)

[\(config-if\) ip](#)

(config) flow monitor

ネットワークトラフィックフローモニタリングを有効にし、トラフィック分析のために WAE を tcpstat-v1 コレクタに登録するには、**flow monitor** 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。ネットワークトラフィックフロー設定を無効にするには、このコマンドの **no** 形式を使用します。

```
flow monitor tcpstat-v1 {enable | host ip_address}
```

シンタックスの説明

monitor	フローパフォーマンスを監視します。
tcpstat-v1	tcpstat-v1 コレクタを設定します。
enable	フローモニタリングを有効にします。
host	収集制御エージェントを指定します。
<i>ip_address</i>	収集制御エージェントの IP アドレス

デフォルト

デフォルトの設定ではホストアドレスは設定されておらず、この機能は無効になっています。

コマンドモード

グローバルコンフィギュレーション

デバイスモード

application-accelerator

使用上のガイドライン

WAE でフローモニタリングを設定する手順については、『*Cisco Wide Area Application Services Configuration Guide*』の Chapter 15 を参照してください。

NetQoS SuperAgent コンソールの使用および NetQoS SuperAgent エンティティの設定に関する情報については、次の Web サイトにアクセスしてください。 <http://www.netqos.com>

(config) help

コマンドライン インターフェイスのオンライン ヘルプを取得するには、**help** 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。

help

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード EXEC およびグローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン コマンド内のどの位置でも疑問符 (?) を入力すればヘルプが得られます。一致するものがない場合、ヘルプ リストは空なので、利用できるオプションが表示されるまで、? の位置を前にずらして入力する必要があります。

次の2つのヘルプ スタイルが提供されます。

- コマンド引数を入力する準備ができている場合、完全ヘルプを使って (たとえば **show ?**)、可能な引数を表示させることができます。
- コマンドを簡略化して入力し、どんな引数が入力に一致するか知りたい場合 (たとえば、**show stat?**)、部分ヘルプを使用します。

例 次の例は、**help** グローバル コンフィギュレーション コマンドの出力を示します。

```
WAE# configure
WAE(config)# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.
```

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered.

次の例は、完全ヘルプを使用して、利用可能な WCCP コマンド引数を確認する方法を示しています。

```
WAE# configure
WAE(config)# wccp ?
  access-list      Configure an IP access-list for inbound WCCP encapsulate
                   traffic
  flow-redirect    Redirect moved flows
  router-list      Router List for use in WCCP services
  shutdown        Wccp Shutdown parameters
  slow-start       accept load in slow-start mode
  tcp-promiscuous  TCP promiscuous mode service
  version          WCCP Version Number
```

次の例は、部分ヘルプを使用して、WCCP 引数の構文を確認する方法を示しています。

```
WAE(config)# wccp tcp ?
mask                Specify mask used for CE assignment
router-list-num     Router list number
```

(config) hostname

WAAS デバイスでネットワーク ホスト名を設定するには、**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。デフォルト設定のホスト名にリセットするには、このコマンドの **no** 形式を使用します。

hostname *name*

シンタックスの説明

<i>name</i>	WAAS デバイスの新しいホスト名で、大文字、小文字を区別します。名前には 1 ～ 30 の英数字を使用できます。
-------------	---

デフォルト

デフォルトのホスト名は WAAS デバイスのモデル番号 (たとえば、WAE-511、WAE-611、WAE-7326 など) です。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

このコマンドを使用して WAAS デバイスのホスト名を設定します。ホスト名は、コマンドプロンプトとデフォルトのコンフィギュレーション ファイル名に使用されます。この名前はルーティングにも使用されるので、次の規則に準拠します。

- 英数字とハイフン (-) のみ、使用可能
- 長さは最大 30 文字
- 次の文字は無効とみなされるため、デバイスに名前を付けるときは使用不可: @、#、\$、%、^、&、*、()、\、/、<

例

次の例は、WAAS デバイスのホスト名を *sandbox* に変更します。

```
WAE-511(config)# hostname sandbox
Sandbox(config)#
```

次の例では、ホスト名を削除します。

```
Sandbox(config)# no hostname
WAE-511(config)#
```

関連コマンド

[dnslookup](#)
[\(config\) ip](#)
[\(config-if\) ip](#)
[show hosts](#)

(config) inetd enable

WAAS デバイスで FTP および RCP サービスを有効にするには、**inetd enable** 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。上記のサービスを無効にするには、このコマンドの **no** 形式を使用します。

```
inetd enable {ftp | rcp}
```

シンタックスの説明

ftp	FTP サービスを有効にします。
rcp	RCP サービスを有効にします。

デフォルト

FTP は有効で、RCP は無効です。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

Inetd (Internet daemon = インターネット デーモンの略で「アイ ネット ディー」と発音) は、特定ポートの接続要求またはメッセージを受信するプログラムで、このようなポートに関連付けられたサービスを実行するサーバプログラムを起動します。**inetd enable** コマンドを **ftp** および **rcp** キーワードとともに使用して WAAS デバイスでのサービスを有効または無効にします。サービスを無効にするには、**no** 形式で **inetd enable** コマンドを入力します。現在の **inetd** セッションが有効か無効か確認するには、**show inetd EXEC** コマンドを使用します。

例

次の例は、WAAS デバイスで FTP サービス セッションを有効にします。

```
WAE(config)# inetd enable ftp
```

次の例では、FTP サービスを無効にします。

```
WAE(config)# no inetd enable ftp
```

関連コマンド

[show inetd](#)

(config) interface

ギガビット イーサネット、InlineGroup、ポート チャネル、またはスタンバイ インターフェイスを設定するには、**interface** 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。選択したオプションを無効にしたり、デフォルト値に戻したり、シャットダウン インターフェイスを有効にしたりするには、このコマンドの **no** 形式を使用します。


```
interface GigabitEthernet slot/port [autosense | bandwidth {10 | 100 | 1000} | cdp enable |
channel-group {1} | description text | full-duplex | half-duplex | ip {access-group {acl-num |
acl_name} {in | out} | address {ip_address netmask [secondary]} | dhcp [client-id id hostname
name | hostname name client-id id]} | mtu mtusize | shutdown | standby grpnumber [priority
priority]]
```

```
interface InlineGroup slot/grpnumber [autosense | bandwidth {10 | 100 | 1000} | failover timeout {1 |
3 | 5} | full-duplex | half-duplex | inline [vlan {all | native | vlan_list}] | shutdown]
```

```
interface PortChannel {1} [description text | ip {access-group {acl-num | acl_name} {in | out} |
address ip-address netmask} | shutdown]
```

```
interface Standby grpnumber {description text | errors max-error-number | ip ip_address | no
{description text | errors max-error-number | ip ip_address | shutdown} | shutdown}
```

シンタックスの説明

GigabitEthernet	設定するギガビットイーサネットインターフェイスを選択します。
<i>slot/port</i>	選択したインターフェイスのスロットおよびポート番号。スロットの範囲は0～2で、ポートの範囲は0～3です。スロットおよびポート番号はスラッシュ (/) で区切ります。
autosense	(オプション) ギガビットイーサネットインターフェイスが自動的にインターフェイスの速度を感知するように設定します。
bandwidth	(オプション) 指定されたインターフェイスの帯域幅を設定します。
10	インターフェイスの帯域幅を 10 Mbps に設定します。
100	インターフェイスの帯域幅を 100 Mbps に設定します。
1000	インターフェイスの帯域幅を 1000 Mbps に設定します。このオプションはすべてのポートで利用できるわけではなく、自動感知と同じです。
cdp enable	(オプション) 指定されたインターフェイスで Cisco Discovery Protocol (CDP; シスコ検出プロトコル) を有効にします。
channel-group	(オプション) EtherChannel グループを設定します。
1	インターフェイスの EtherChannel をグループ 1 に設定します。
description	インターフェイスの説明を入力します。
<i>text</i>	このインターフェイスについて説明するテキスト
full-duplex	(オプション) インターフェイスを全二重動作に設定します。
half-duplex	(オプション) インターフェイスを半二重動作に設定します。
	
	(注) WAE またはルータ、スイッチ、もしくはその他のデバイス上で半二重接続を使用しないことを強く推奨します。
ip	(オプション) インターフェイスの IP コンフィギュレーション コマンドを有効にします。
access-group	Access Control List (ACL; アクセス コントロール リスト) を使用して、このインターフェイスの IP パケットに対してアクセス コントロールを設定します。

<i>acl_num</i>	現在のインターフェイスに適用する ACL を識別する数値の ID。有効な範囲は、標準の ACL では 1 ~ 99、拡張 ACL では 100 ~ 199 です。
<i>acl_name</i>	最大 30 文字の英数字の ID で、文字で始まります。現在のインターフェイスに適用する ACL を識別します。
in	指定された ACL を現在のインターフェイスの着信パケットに適用します。
out	指定された ACL を現在のインターフェイスの発信パケットに適用します。
address	インターフェイスの IP アドレスを設定します。
<i>ip-address</i>	このインターフェイスの IP アドレス
<i>netmask</i>	このインターフェイスのネットマスク
secondary	(オプション) 設定されたアドレスがセカンダリ IP アドレスであることを指定します。このキーワードを省略した場合、設定されたアドレスはプライマリ IP アドレスです。
dhcp	(オプション) Dynamic Host Configuration Protocol (DHCP) でネゴシエーションされたものに IP アドレスを設定します。
client-id	(オプション) クライアントの識別情報を指定します。
<i>id</i>	クライアントの識別情報
hostname	(オプション) ホスト名を指定します。
<i>name</i>	ホスト名
mtu	(オプション) インターフェイスの最大伝送ユニット (maximum transmission unit; MTU) サイズを設定します。
<i>mtusize</i>	MTU サイズ (バイト単位で 88 ~ 1500)
shutdown	(オプション) このインターフェイスをシャットダウンします。
standby	(オプション) スタンバイ インターフェイス コンフィギュレーション コマンドを設定します。
<i>grpnumber</i>	スタンバイ グループ番号 (1 ~ 4)
priority	(オプション) スタンバイ グループのインターフェイスのプライオリティを設定します。
<i>priority</i>	スタンバイ グループのインターフェイスのプライオリティ (0 ~ 4294967295)
InlineGroup	設定するインターフェイスの InlineGroup を設定します。
<i>slot/grpnumber</i>	選択したインターフェイスのスロットおよびインライン グループ番号インライン機能のグループ番号は 0 か 1 のいずれかです (各アダプタにはグループ化された 2 つのペアがあります)。
failover	(オプション) フェールオーバー パラメータを変更します。
timeout	障害が発生してからトラフィックを別のポートに転送するまでのインターフェイスのインライングループの最大時間を設定します。
1	フェールオーバーが発生するまでの秒数
3	フェールオーバーが発生するまでの秒数
5	フェールオーバーが発生するまでの秒数
inline	(オプション) インターフェイスの InlineGroup のインライン代行受信を有効にします。
vlan	(オプション) VLAN リストのパラメータを変更します。
all	すべてのタグ付きパケットとタグなしパケットにコマンドを適用します。
native	タグなしパケットを指定します。
<i>vlan_list</i>	カンマ区切りの VLAN ID のリスト。指定された VLAN セットにインライン機能を制限します。

PortChannel	設定するインターフェイスの EtherChannel を選択します。
1	ポートチャンネルインターフェイス番号を 1 に設定します。
errors	最大エラー数を指定します。
<i>max-error-number</i>	エラーの最大数
ip	インターフェイスの IP アドレスを指定します。
<i>ip_address</i>	インターフェイスの IP アドレス

デフォルト

デフォルトの動作や値はありません。

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

interface コマンドには **FibreChannel** のオプションが含まれますが、ファイバチャンネル インターフェイスは WAAS デバイスではサポートされていません。**interface FibreChannel** コマンドは、このコマンドリファレンスには記載されていません。

WAAS デバイスでインターフェイスの帯域幅を設定するには、**bandwidth** インターフェイス コンフィギュレーション コマンドを使用します。帯域幅は、Mbps 単位で指定します。**1000 Mbps** オプションはすべてのポートで利用できるわけではありません。このオプションを使用すると、インターフェイスで自動的に自動感知が有効になります。光ギガビットイーサネット インターフェイスを備えている WAE-7320 モデルのインターフェイス速度は変更できません。ギガビットイーサネット インターフェイスは、WAE-7320 で 1000 Mbps でのみ動作します。銅線を利用するギガビットイーサネット インターフェイスを備えているより新しい WAAS デバイス モデル（たとえば WAE-611 または WAE-7326）では、この制約は当てはまりません。これらのギガビットイーサネット インターフェイスは 10、100 または 1000 Mbps で動作するように設定できます。より新しい WAAS モデルでは、1000 Mbps 設定は自動感知を含みます。たとえば、ギガビットイーサネット インターフェイスを 1000 Mbps、半二重で動作するよう設定することはできません。

グローバル コンフィギュレーション モードで **cdp enable** コマンドを使用すると、すべてのインターフェイス上でグローバルに CDP を有効にします。インターフェイスごとに CDP の動作を制御するには、インターフェイス コンフィギュレーション モードで **cdp enable** コマンドを使用します。インターフェイス レベルの制御は、グローバル制御を上書きします。

インターフェイス ID（たとえば、ギガビットイーサネット 1/0）を表示するには、**show running-config** または **show startup-config** コマンドを使用します。**autosense**、**bandwidth**、**full-duplex**、**half-duplex**、**ip**、および **shutdown** コマンドは、このコマンドリファレンスでは別々にリストしています。

単一物理インターフェイスでの複数のセカンダリ IP アドレスの設定

interface secondary 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、同一インターフェイスに複数の IP アドレスを設定します。単一インターフェイスに複数の IP アドレスを設定することで、WAAS デバイスは複数のサブネットに存在できます。この設定により、ルータを介してリダイレクトすることなく、コンテンツが直接 WAAS デバイスから要求クライアントに行くので、応答時間を最適化できます。クライアントは、WAAS デバイスと同じサブネット上に設定されているので、WAAS デバイスを認識できるようになります。

1つのインターフェイスに最大4つのセカンダリアドレスを割り当てできます。このようなアドレスがアクティブになるのは、プライマリアドレスが設定された後だけです。同一のサブネットでは、2つのインターフェイスが同一のIPアドレスを持つことはできません。このようなセカンダリIPアドレスを設定するには、**ip address** コマンドを使用します。

複数のセカンダリIPアドレスが割り当てられた物理インターフェイスを1つWAASデバイスが備えている場合、出力トラフィックは、IPルーティングによって選択された送信元IPアドレスを使用します。WAASデバイスのセカンダリIPアドレスがプライマリIPアドレスと同一のサブネットにある場合、出力トラフィックはプライマリIPアドレスしか使用しません。対照的に、セカンダリIPアドレスがプライマリIPアドレスと別のサブネットにある場合、宛先IPアドレスにより、WAASデバイス上のどのIPアドレスを出力トラフィックに使用するかが決定されます。

DHCP に対するインターフェイスの設定

WAASデバイスの初期設定時に、WAASデバイスに静的IPアドレスを設定するか、インターフェイスレベルのDHCPを使用してWAE上のインターフェイスに動的にIPアドレスを割り当てるか選択できます。

WAASデバイス上でインターフェイスレベルのDHCPを有効にしていない場合は、手動でWAASデバイスの静的IPアドレスとネットワークマスクを指定する必要があります。WAASデバイスを、ネットワークの別の部分の別の場所に移動する場合は、手動でWAASデバイスの新しい静的IPアドレスとネットワークマスクを入力する必要があります。

インターフェイスは、**ip address dhcp [client_id | hostname]** インターフェイス コンフィギュレーション コマンドを使用すると、DHCPに対して有効にできます。クライアントIDはASCII値です。WAASデバイスは、ネットワーク情報要求の際、設定済みのクライアントIDとホスト名をDHCPに送信します。DHCPサーバは、WAASデバイスが送信しているクライアントID情報とホスト名情報を識別し、WAASデバイスに割り当てられた特定のネットワーク コンフィギュレーションを送り返すように設定できます。



(注) 手動でDHCPのインターフェイスを設定するまでは、自動登録は無効にしておく必要があります。自動登録は、デバイスの最初のインターフェイス上では、デフォルトで有効になっています。

インターフェイスの説明の定義

WAASデバイス上の特定のインターフェイスについて簡潔な説明を指定できます。**description text** インターフェイス コンフィギュレーション コマンドを使用して特定のインターフェイスの説明を入力します。説明のテキストの長さは最大240文字です。この機能は、ギガビットイーサネット、ポートチャネル、およびスタンバイインターフェイスでサポートされています。



(注) この機能は現在、SCSIやIDEインターフェイスに対してはサポートされていません。

インターフェイスの説明の定義後、**show EXEC** コマンドを使用して定義したインターフェイスの説明を表示させます。WAE上の特定のインターフェイスの定義した説明を表示するには、**show interface interface type slot/port EXEC** コマンドを使用します。

ポートチャネル (EtherChannel) インターフェイス

WAAS 対応の EtherChannel ソフトウェアは、2つの同一速度ネットワーク インターフェイスが1つの仮想インターフェイスにグループ化することをサポートします。この設定により、2つの統合型ギガビット イーサネット インターフェイスで構成される仮想インターフェイスの設定または削除が可能になります。EtherChannel は、シスコルータ、スイッチ、および EtherChannel、ロードバランシング、各インターフェイスの現在のリンク ステータスに基づく自動障害検出およびリカバリをサポートするその他のネットワーク デバイスまたはホストとの相互運用性も提供します。



(注)

WAE インライン ネットワーク アダプタのインライン イーサネット インターフェイスを使用して EtherChannel を形成できません。

InlineGroup インターフェイス

InlineGroup インターフェイスは、オプションの4ポートインラインネットワークアダプタカードに物理的に含まれているペアのイーサネットポートの論理グループです。インラインネットワークアダプタは、WAAS 4.0.7 リリース以降のすべての WAAS アプライアンス プラットフォームでサポートされています。最大2つの InlineGroup インターフェイスを使用できます。これにより、バイパスが有効な2つパスによりトラフィックが WAE アプライアンスを通過できるようになり、複数のルータによる構成が可能になります。InlineGroup インターフェイスはフェールオーバー機能を提供し、任意の VLAN セットに割り当てることができます (InlineGroup インターフェイスの設定例については、「(config-if) inline」コマンドを参照してください)。

InlineGroup インターフェイスに、リンク速度 (**bandwidth** または **autosense**) および動作モード (**half-duplex** または **full-duplex**) を設定できます。



(注)

WAE またはルータ、スイッチ、もしくはその他のデバイス上で半二重接続を使用しないことを強く推奨します。半二重を使用すると、パフォーマンスを改善するシステムの機能が妨げられるため、適切ではありません。各 Cisco WAE インターフェイスおよび隣接デバイス (ルータ、スイッチ、ファイアウォール、WAE) のポート設定を再度チェックし、全二重が設定されていることを確認します。

例

次の例は、1つの CLI コマンドでインターフェイスの属性を設定します。

```
WAE(config)# interface GigabitEthernet 1/0 full-duplex
```

次の例は、一連の CLI コマンドでインターフェイスを設定できることを示しています。

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# full-duplex
WAE(config-if)# exit
WAE(config)#
```

次の例では、シャットダウン インターフェイスを有効にします。

```
WAE(config)# no interface GigabitEthernet 1/0 shutdown
```

次の例では、EtherChannel を作成します。ポートチャネルはポートチャネル 1 で、10.10.10.10 の IP アドレスと 255.0.0.0 のネットマスクを割り当てられています。

```
WAE# configure
WAE(config)# interface PortChannel 1
WAE(config-if)# ip address 10.10.10.10 255.0.0.0
WAE(config-if)# exit
```

次の例では、EtherChannel を削除します。

```
WAE(config)# interface PortChannel 1
WAE(config-if)# no ip address 10.10.10.10 255.0.0.0
WAE(config-if)# exit
WAE(config)# no interface PortChannel 1
```

次の例では、チャンネルグループにインターフェイスを追加します。

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# channel-group 1
WAE(config-if)# exit
```

次の例では、チャンネルグループからインターフェイスを削除します。

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# no channel-group 1
WAE(config-if)# exit
```

次の例では、**ip address** インターフェイス コンフィギュレーション コマンドを使用して、WAAS デバイス上のギガビットイーサネットにセカンダリ IP アドレスを割り当てます。

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# ip address 10.10.10.10 255.0.0.0 secondary
```

次の例では、ギガビットイーサネットインターフェイスに対して説明を設定します。

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# description This is a GigabitEthernet interface.
```

次の例は、**show running-config EXEC** コマンドのサンプル出力を示します。

```
WAE# show running-config
.
.
.
interface GigabitEthernet 1/0
  description This is an interface to the WAN
  ip address dhcp
  ip address 192.168.1.200 255.255.255.0
  no autosense
  bandwidth 100
  full-duplex
  exit
.
.
.
```

次の例は **show interface** コマンドのサンプル出力を示します。

```
WAE# show interface GigabitEthernet 1/0
Description: This is the interface to the lab
type: Ethernet
.
.
.
```

関連コマンド

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config) ip

ネットワーク デバイスの初期設定を変更するには、**ip** 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。これらの設定を削除または無効にするには、このコマンドの **no** 形式を使用します。

```
ip default-gateway ip-address
ip domain-name name1 name2 name3
ip name-server ip-addresses
ip path-mtu-discovery enable
ip route dest_addr net_addr gateway_addr
```

シンタックスの説明

default-gateway	デフォルト ゲートウェイを指定します(ルーティング IP でない場合)。
<i>ip-address</i>	デフォルト ゲートウェイの IP アドレス
domain-name	ドメイン名を指定します。
<i>name1 ~ name3</i>	ドメイン名 (最大3つまで指定できます)
name-server	ネーム サーバのアドレスを指定します。
<i>ip-addresses</i>	ネーム サーバの IP アドレス (最大8個)
path-mtu-discovery	RFC 1191 Path 最大伝送ユニット (Maximum Transmission Unit; MTU) discovery を設定します。
enable	Path MTU discovery を有効にします。
route	ネット ルートを指定します。
<i>dest_addr</i>	宛先のルート アドレス
<i>net_addr</i>	ネットマスク アドレス
<i>gateway_addr</i>	ゲートウェイ アドレス

デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

```
application-accelerator
replication-accelerator
central-manager
```

使用上のガイドライン

デフォルト ゲートウェイを定義するには、**ip default-gateway** コマンドを使用します。設定できるデフォルト ゲートウェイは1つだけです。IP デフォルト ゲートウェイを削除するには、このコマンドの **no** 形式を使用します。WAAS デバイスは、宛先への明確なルートが見つからない場合、デフォルト ゲートウェイを使用して IP パケットをルーティングします。

デフォルト ドメイン名を定義するには、**ip domain-name** コマンドを使用します。IP デフォルト ドメイン名を削除するには、このコマンドの **no** 形式を使用します。ドメイン名は最大3つまで入力できます。ホスト名にドメイン名が追加されていない状態で要求が着信した場合、プロキシは *name1*、*name2*、および *name3* をこの順序で追加して、これらの名前のいずれかが成功するまで、ホスト名を解決しようとします。

WAAS デバイスは、設定されたドメイン名を、ドメイン名が入っていない IP ホスト名すべてに追加します。追加された名前は DNS によって解決され、ホスト テーブルに追加されます。ホスト名解決を正常に動作させるには、WAAS デバイスに最低限 1 つのドメイン ネーム サーバが指定されている必要があります。

複数のネーム サーバのアドレスを指定して名前とアドレスの解決に使用するには、**ip name-server ip-addresses** コマンドを使用します。IP ネーム サーバを無効にするには、このコマンドの **no** 形式を使用します。ホスト名を IP アドレスに、または IP アドレスをホスト名に正しく解決するため、WAAS デバイスでは DNS サーバを使用します。**ip name-server** コマンドを使用して、WAAS デバイスを特定の DNS サーバにポイントします。最大 8 つのサーバを設定できます。

Path MTU 自動ディスカバリは MTU を検出し、自動的に正しい値を設定します。この自動ディスカバリユーティリティを起動するには、**ip path-mtu-discovery enable** コマンドを使用します。デフォルトでは、この機能は有効に設定されています。この機能が無効にされると、送信側デバイスは、576 バイトより小さいパケット サイズとネクストホップ MTU を使用します。既存の接続は、この機能が有効または無効になっても影響を受けません。

WAAS ソフトウェアは、RFC 1191 に定義されている IP Path MTU Discovery をサポートしています。有効に設定されている場合、Path MTU Discovery は、転送パスに沿ったさまざまなリンク間で許容される最大 IP パケット サイズを検出し、パケット サイズに対して自動的に正しい値を設定します。リンクが搬送する最大の MTU を使用することで、送信側デバイスは送信する必要のあるパケットの数を最小限にできます。



(注)

IP Path MTU discovery は、ネットワーク内のリンクがダウンし、強制的に、別の異なる MTU にサイズ調整したリンクを使用させられる場合に便利です。また、IP Path MTU discovery は、最初に接続が確立され、送信側に仲介リンクに関する情報がまったくない場合にも便利です。

IP Path MTU Discovery は、送信側デバイスによって開始されます。サーバが IP Path MTU discovery をサポートしていない場合、受信側デバイスには、サーバによって生成されるデータグラムの断片化を避けるのに利用できるメカニズムがありません。

ip route コマンドを使用して、ネットワークまたはホストについて特定のスタティック ルートを追加します。指定の宛先が示された IP パケットはすべて、設定済みのルートを使用します。

スタティック IP ルーティングを設定するには、**ip route** コマンドを使用します。ルートを削除するには、このコマンドの **no** 形式を使用します。**ip route 0.0.0.0 0.0.0.0** コマンドを使用してデフォルトゲートウェイを設定しないでください。代わりに、**ip default-gateway** コマンドを使用してください。

例

次の例は、WAAS デバイスのデフォルトゲートウェイを設定します。

```
WAE(config)# ip default-gateway 192.168.7.18
```

次の例では、デフォルトゲートウェイを無効にします。

```
WAE(config)# no ip default-gateway
```

次の例では、WAAS デバイスのスタティック IP ルートを設定します。

```
WAE(config)# ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

■ (config) ip

次の例では、スタティック IP ルートを無効にします。

```
WAE(config)# no ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

次の例は、WAAS デバイスのデフォルト ドメイン名を設定します。

```
WAE(config)# ip domain-name cisco.com
```

次の例は、WAAS デバイスのデフォルト ドメイン名を無効にします。

```
WAE(config)# no ip domain-name
```

次の例は、WAAS デバイスのネーム サーバを設定します。

```
WAE(config)# ip name-server 10.11.12.13
```

次の例は、WAAS デバイスのネーム サーバを無効にします。

```
WAE(config)# no ip name-server 10.11.12.13
```

関連コマンド

[show ip routes](#)

(config) ip access-list

WAAS デバイスでインターフェイスまたはアプリケーションへのアクセス制御のためのアクセスリストを作成および変更するには、**ip access-list** 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。アクセスリストを無効にするには、このコマンドの **no** 形式を使用します。

```
ip access-list {standard | extended} {acl-name | acl-num}
```

シンタックスの説明

standard	標準 ACL コンフィギュレーション モードを有効にします。CLI が標準 ACL コンフィギュレーション モードを開始すると、それ以降に入力するコマンドはすべて、現在の標準アクセス リストに適用されます。(config-std-nacl) プロンプトが表示されます。 WAE(config-std-nacl)# 標準アクセス リストのエントリの処理および標準 ACL コンフィギュレーション モード (config-std-nacl)# から利用できるコマンドについては、「(config) ip access-list」を参照してください。
extended	拡張 ACL コンフィギュレーション モードを有効にします。CLI は、拡張 ACL コンフィギュレーション モードを開始します。このモードでは、以降のすべてのコマンドが現在の拡張アクセス リストに適用されます。次の (config-ext-nacl) プロンプトが表示されます。 WAE (config-ext-nacl) # 拡張アクセス リストのエントリの処理および拡張 ACL コンフィギュレーション モード (config-ext-nacl)# から利用できるコマンドについては、「(config) ip access-list」セクションを参照してください。
acl-name	ACL コンフィギュレーション モードから入力されたすべてのコマンドが適用するアクセスリスト。最大30文字の英数字文字列を使用し、文字で始まります。
acl-num	アクセス リスト コンフィギュレーション モードから入力されたすべてのコマンドが適用するアクセス リスト。数値 ID を使用します。有効な範囲は、標準のアクセス リストでは 1 ~ 99、拡張アクセス リストでは 100 ~ 199 です。

デフォルト

アクセス リストは、少なくとも 1 つ **permit** エントリが設定されていないかぎり、すべてのパケットをドロップします。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

アクセス リストは、WAAS デバイスの特定のアプリケーションまたはインターフェイスへのアクセスを制御するために使用してください。アクセス コントロール リストは、パケットの種類を指定する複数のエントリで構成され、WAAS デバイスはこのパケットをドロップするかさらに処理するため受け入れます。WAAS デバイスは、アクセス リストに出現する順序で各エントリを適用します。この順序はデフォルトでは、エントリが設定された順序です。



(注)

ルータに定義されている IP ACL は、WAE に定義されている IP ACL より優先されます。WAE に定義されている IP ACL は、WAE に定義されている WAAS アプリケーション定義ポリシーより優先されます。

ACL コンフィギュレーション モード内では、編集コマンド (**list**、**delete**、**move**) を使用して、現在の条件エントリを表示したり、特定のエントリを削除したり、エントリの評価順序を変更したりできます。グローバル コンフィギュレーション モードに戻るには、ACL コンフィギュレーション モードプロンプトで **exit** を入力します。

エントリを作成するには、**deny** または **permit** キーワードを使用して、WAAS デバイスにドロップさせる、またはさらに処理するために受け入れさせるパケットのタイプを指定します。デフォルトでは、アクセス リストはすべてを拒否します。アクセス リストが暗黙の **deny any** エントリで終了しているためです。したがって、少なくとも 1 つ **permit** エントリを指定して、有効なアクセス リストを作成する必要があります。

アクセス リストを作成した後、**access-group** コマンドを使用してアクセス リストをアクセス グループに組み入れることができます。このコマンドはアクセス リストの適用方法を決定します。アクセス リストは、当該のコマンドを使用すれば特定のアプリケーションにも適用できます。存在しないアクセス リストの参照は、**permit any** 条件文と同等です。

アクセス リストを処理するには、**ip access-list standard** または **ip access-list extended** グローバル コンフィギュレーション コマンドを実行します。新しいまたは既存のアクセス リストは、文字または数字で始まる、最大 30 文字の長さの名前を付けて識別します。数字を使用して標準アクセス リストを識別する場合は、1 ~ 99 の範囲にしてください。拡張アクセス リストの場合は、100 ~ 199 の数字を使用します。SNMP サーバまたは TFTP ゲートウェイ / サーバのアクセスには標準アクセス リストを使用する必要があります。ただし、WCCP アプリケーションへのアクセスには、標準アクセス リストまたは拡張アクセス リストのどちらでも使用できます。

アクセス リストを識別すると、CLI により適切なコンフィギュレーション モードが開始され、以降のコマンドはすべて、指定されたアクセス リストに適用されます。各コンフィギュレーション モードのプロンプトを次の例に示します。

```
WAE(config)# ip access-list standard test
WAE(config-std-nacl)# exit
WAE(config)# ip access-list extended test2
WAE(config-ext-nacl)#
```

例

次の例は、WAAS デバイスでアクセス リストを作成する方法を示します。このアクセス リストを作成することで、WAAS デバイスにリダイレクトされるすべての Web トラフィックを受け入れ、SSH を使用したホスト管理アクセスを制限します。

```
WAE(config)# ip access-list extended example
WAE(config-ext-nacl)# permit tcp any any eq www
WAE(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

次の例は、インターフェイスのアクセス リストをアクティブにします。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group example in
WAE(config-if)# exit
```


次の例は、**show running-configuration** コマンドを実行したときに、この設定がどう表示されるかを示します。

```
...
!  
interface GigabitEthernet 1/0  
 ip address 10.1.1.50 255.255.0.0  
 ip access-group example in  
 exit  
...  
ip access-list extended example  
 permit tcp any any eq www  
 permit tcp host 10.1.1.5 any eq ssh  
 exit  
...  
...
```

関連コマンド

clear

(config-if) ip access-group

show ip access-list

(config) kerberos

Kerberos データベースで定義されているユーザを認証するには、**kerberos** 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。認証を無効にするには、このコマンドの **no** 形式を使用します。

```
kerberos {local-realm kerberos-realm | realm {dns-domain | host} kerberos-realm | server
kerberos-realm {hostname | ip-address} [port-number]}
```



(注)

Windows ドメイン サーバでこのコマンドを正常に実行させるにはリバース DNS ゾーンを設定する必要があります。

シンタックスの説明

local-realm	WAAS のデフォルト レルムを表示します。スイッチが Kerberos データベースで定義されたユーザを認証するように設定します。
<i>kerberos-realm</i>	Kerberos レルムの IP アドレスまたは名前 (大文字) デフォルト値はヌル ストリングです。
realm	Kerberos レルムにホスト名または DNS ドメイン名をマップします。
<i>dns-domain</i>	Kerberos レルムにマップする DNS ドメイン名
	(注) ドメイン名は必ず先行ドット (.) で開始します。
<i>host</i>	Kerberos ホスト レルムにマップするホスト IP アドレスまたは名前
server	指定の Kerberos レルムで使用する Key Distribution Center (KDC; 鍵発行局) およびオプションで KDC がモニタリングするポート番号を指定します。
<i>hostname</i>	KDC を実行しているホストの名前
<i>ip-address</i>	KDC を実行しているホストの IP アドレス
<i>port-number</i>	(オプション) KDC サーバのポート番号

デフォルト

kerberos-realm :ヌル ストリング
port-number : 88

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

すべての Windows 2000 ドメインも Kerberos レルムです。Windows 2000 ドメイン名は DNS ドメイン名でもあるので、Windows 2000 ドメイン名の Kerberos レルム名は必ず大文字です。この大文字使用は Kerberos Version 5 プロトコル ドキュメント (RFC-1510) の DNS 名をレルム名として使用するための勧告に従っており、他の Kerberos ベースの環境との相互運用性にも影響します。

Kerberos 認証が設定された KDC サーバおよびすべてのホストは 5 分以内にやり取りしないと、認証は失敗します。すべてのホスト、特に KDC は NTP を実行している必要があります。NTP の設定については、「(config) ntp」コマンドを参照してください。

KDC サーバおよび管理サーバは同じ IP アドレスを持っている必要があります。両方のサーバのデフォルトのポート番号はポート 88 です。

kerberos コマンドは krb5.conf ファイルを変更します。

例 次の例は、WAAS デバイスが指定された Kerberos レalmにある指定された KDC で認証するように設定する方法を示します。設定はあとで確認されています。

```
WAE(config)# kerberos ?
  local-realm  Set local realm name
  realm       Add domain to realm mapping
  server      Add realm to host mapping
WAE(config)# kerberos local-realm WAE.ABC.COM
WAE(config)# kerberos realm wae.abc.com WAE.ABC.COM
WAE(config)# kerberos server wae.abc.com 10.10.192.50
WAE(config)# exit
WAE# show kerberos
Kerberos Configuration:
-----
  Local Realm: WAE.ABC.COM
  DNS suffix: wae.abc.com
  Realm for DNS suffix: WAE.ABC.COM
  Name of host running KDC for realm:
  Master KDC: 10.10.192.50
  Port: 88
```

関連コマンド[show kerberos](#)

(config) kernel kdb

カーネル デバッガ (kdb) へのアクセスを有効にするには、**kernel kdb** 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。kdb は、有効にしておくと、カーネルの問題が発生した場合に自動的にアクティブ化します。または、WAAS デバイスのローカル コンソールから、必要なキーシーケンスを押して手動でアクティブにできます。カーネル デバッガへのアクセスを無効にするには、このコマンドの **no** 形式を使用します。

kernel kdb

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト カーネル デバッガは、デフォルトで無効に設定されています。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン kdb は、有効にしておくと、カーネルの問題が発生した場合に自動的にアクティブ化します。アクティブ化すると、kdb が手動で無効にされるまで、WAAS デバイスのすべての通常機能は一時停止します。kdb のプロンプトは次のようになります。

```
[0]kdb>
```

kdb を無効にするには、kdb プロンプトに **go** を入力します。カーネルの問題のため kdb が自動的にアクティブになった場合、システムはコア ダンプを生成して再起動します。診断目的で kdb を手動でアクティブにした場合、kdb をアクティブにしたときの状態に関係なく、システムは通常の機能を再開します。いずれの場合も、**reboot** を入力するとシステムは再起動し、通常の動作を再開します。

kdb はデフォルトで無効に設定されているので、有効にするには、グローバル コンフィギュレーション モードで **kernel kdb** コマンドを入力します。kdb が有効になっている場合は、**no kernel kdb** 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と無効になります。kdb を有効にしたら、**Ctrl_** のあとに続いて **Ctrl-B** を押すと、ローカル コンソールから手動でアクティブ化できます。

カーネル デバッガを無効にする理由は次のとおりです。WAAS デバイスは多くのサイトで無人になることが多く、コア ダンプの生成後、ユーザの手動操作を必要とせず、WAAS デバイスが自動的にレポートするのが望ましい。カーネル デバッガを無効にすると、自動回復が可能になります。

例 次の例は、カーネル デバッガへのアクセスを有効にし、次に無効にします。

```
WAE(config)# kernel kdb
WAE(config)# no kernel kdb
```

(config) line

端末回線設定を指定するには、**line** 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。WAAS デバイスがキャリア検知信号をチェックしないように設定するには、このコマンドの **no** 形式を使用します。

line console carrier-detect

シンタックスの説明

console	コンソールの端末回線設定を設定します。
carrier-detect	キャリア検知信号をチェックしてからコンソールに書き込むように、デバイスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

replication-accelerator

central-manager

例

次の例は、WAAS デバイスがキャリア検知信号をチェックするように設定します。

```
WAE(config)# line console carrier-detect
```



(config) logging

システム ロギングを設定するには、**logging** 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。ロギング機能を無効にするには、このコマンドの **no** 形式を使用します。

```
logging {console {enable | priority loglevel} | disk {enable | filename filename | priority loglevel |
  recycle size} | facility facility | host {hostname | ip-address} [port port_num | priority loglevel |
  rate-limit message_rate]}
```

シンタックスの説明

console	コンソールへのシステム ロギングを設定します。
enable	コンソールへのシステム ロギングを有効にします。
priority	どのプライオリティ レベルのメッセージを Syslog ファイルに送るかを設定します。
<i>loglevel</i>	次のいずれかのキーワードを使用します。 <ul style="list-style-type: none"> • alert — ただちに対策が必要です。プライオリティ 1 • critical — ただちに対策が必要です。プライオリティ 2 • debug — デバッグ メッセージ。プライオリティ 7 • emergency — システムは利用不能です。プライオリティ 0 • error — エラー状態。プライオリティ 3 • information — 情報メッセージ。プライオリティ 6 • notice — 正常ではあるが注意を要する状況。プライオリティ 5 • warning — 警告状態。プライオリティ 4
disk	ディスク ファイルへのシステム ロギングを設定します。
enable	ディスク ファイルへのシステム ロギングを有効にします。
filename	Syslog ファイルの名前を設定します。
<i>filename</i>	Syslog ファイルの名前
recycle	<i>syslog.txt</i> がリサイクル サイズを超える場合、上書きします。
<i>size</i>	バイト単位の Syslog ファイルのサイズ (1000000 ~ 50000000)
facility	Syslog メッセージのファシリティ パラメータを設定します。

<i>facility</i>	次のいずれかのキーワードを使用します。 <ul style="list-style-type: none"> • auth — 許可システム • daemon — システム デーモン • kernel — カーネル • local0 — ローカル使用 • local1 — ローカル使用 • local2 — ローカル使用 • local3 — ローカル使用 • local4 — ローカル使用 • local5 — ローカル使用 • local6 — ローカル使用 • local7 — ローカル使用 • mail — メール システム • news — USENET ニュース • syslog — Syslog 自身 • user — ユーザ プロセス • uucp — UUCP システム
host	リモートホストにシステム ロギングを設定します。
<i>hostname</i>	リモート Syslog ホストのホスト名。最大 4 つまでリモート Syslog ホストを指定します。
	 (注) 複数の Syslog ホストを指定するには、複数のコマンドラインを使用します。1 つのコマンドにつき 1 つのホストを指定します。
<i>ip-address</i>	リモート Syslog ホストの IP アドレス。最大 4 つまでリモート Syslog ホストを指定します。
	 (注) 複数の Syslog ホストを指定するには、複数のコマンドラインを使用します。1 つのコマンドにつき 1 つのホストを指定します。
port	(オプション) ホストにロギングする際に使用するポートを指定します。
<i>port_num</i>	ホストにロギングする際に使用するポート。デフォルト ポートは 514 です。
priority	(オプション) ホストにメッセージをロギングする際の、メッセージのプライオリティ レベルを設定します。デフォルト プライオリティは warning です。
<i>loglevel</i>	次のいずれかのキーワードを使用します。 <ul style="list-style-type: none"> • alert — ただちに対策が必要です。プライオリティ 1 • critical — ただちに対策が必要です。プライオリティ 2 • debug — デバッグ メッセージ。プライオリティ 7 • emergency — システムは利用不能です。プライオリティ 0 • error — エラー状態。プライオリティ 3 • information — 情報メッセージ。プライオリティ 6 • notice — 正常ではあるが注意を要する状況。プライオリティ 5 • warning — 警告状態。プライオリティ 4

rate-limit	(オプション) ホストにメッセージを送信するためのレート制限 (1 秒当たりのメッセージ数) を設定します。
message_rate	ホストにメッセージを送信するためのレート制限 (1 秒当たりのメッセージ数) (0 ~ 10000)。レート制限を 0 に設定すると、レート制限は無効になります。

デフォルト

ロギング : on
 コンソールのメッセージのプライオリティ : warning
 ディスク ログ ファイルのメッセージのプライオリティ : debug
 ホストのメッセージのプライオリティ : warning
 ログ ファイル : /local1/syslog.txt
 ログ ファイル リサイクル サイズ : 10,000,000 バイト

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

logging コマンドを使用して、システム ログ ファイルの特定のパラメータを設定します。システム ロギングは、内部的に常に有効になっています。デフォルトでは、システム ロギングは、WAAS デバイスで有効になっています。システム ログ ファイルは、SYSFS パーティションの /local1/syslog.txt にあります。このファイルには、認証エントリ、特権レベル、および管理用詳細情報が格納されています。

WAAS では、SCSI ディスクおよび SATA ディスクの単一の障害のあるセクションに関連した、複数の Syslog メッセージをフィルタリングできます。

さまざまなレベルのイベント メッセージを外部 Syslog ホストに送信するよう WAAS デバイスを設定するには、**logging host** オプションを使用します。ロギングは、**logging console priority** オプションを使用すると、さまざまなレベルのメッセージをコンソールに送信するよう設定できます。

no logging disk recycle size コマンドは、ファイル サイズをデフォルト値に設定します。現在のログ ファイル サイズがリサイクル サイズを超えた場合は必ず、ログ ファイルが交代します。ログ ファイルは最大で 5 回循環し、元のログと同じディレクトリに [ログファイル名].[1 ~ 5] として保存されます。交代するログ ファイルは、**logging disk filename** コマンドを使用して設定したファイルです。

リモート Syslog ホストへのシステム ロギングの設定

さまざまなレベルのメッセージを最大 4 つのリモート Syslog ホストに送信するよう、WAAS デバイスを設定できます。次のように **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。

```
WAE(config)# [no] logging host hostname [priority priority-code | port port
|rate-limit limit]
```


説明：

- *hostname* は、リモート Syslog ホストのホスト名または IP アドレスです。最大 4 つまでリモート Syslog ホストを指定します。複数の Syslog ホストを指定するには、複数のコマンドラインを使用します。1 つのコマンドにつき 1 つのホストを指定します。
- *priority-code* は、指定されたリモート Syslog ホストに送信するメッセージの重大度です。デフォルトの *priority-code* は「warning」（レベル 4）です。各 Syslog ホストは、さまざまなレベルのイベント メッセージを受信できます。



(注)

Syslog ホストの冗長性は、WAAS デバイスで複数の Syslog ホストを設定し、設定済みの各 Syslog ホストに対し同一のプライオリティ コードを割り当てること（たとえば、「critical」レベル 2 のプライオリティ コードを、Syslog ホスト 1、Syslog ホスト 2、Syslog ホスト 3 に割り当てる）で達成できます。

- *port* は、WAAS デバイスがメッセージを送信するリモート Syslog ホストの宛先ポートです。デフォルト ポートはポート 514 です。
- *rate-limit* は、リモート Syslog ホストに送信することが許可された 1 秒当たりのメッセージ数を指定します。帯域幅と他のリソース消費を制限するため、リモート Syslog ホストへのメッセージは、レートを制限できます。この限度を超えた場合、指定されたリモート Syslog ホストはメッセージをドロップします。デフォルトのレート制限はありません。デフォルトでは、すべての Syslog メッセージはすべての設定済み Syslog ホストに送信されます。レート制限を超えた場合、どの CLI EXEC シェル ログインでも「Message of the Day (MoTD)」が表示されます。

例

次の例では、WAAS デバイスはプライオリティ コードが「error」（レベル 3）のメッセージをコンソールに送信するよう設定されています。

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

次の例では、WAAS デバイスはプライオリティ コードが「error」（レベル 3）のメッセージをコンソールに送信することを無効にするよう設定されています。

```
WAE(config)# no logging console error
```

次の例では、WAAS デバイスはプライオリティ コードが「error」（レベル 3）のメッセージを、IP アドレスが 172.31.2.160 のリモート Syslog ホストに送信するよう設定されています。

```
WAE(config)# logging host 172.31.2.160 priority error
```

関連コマンド

[clear](#)


[show logging](#)

(config) no

グローバル コンフィギュレーション コマンドを取り消すか、そのデフォルトに設定するには、グローバル コンフィギュレーション コマンドの **no** 形式を使用します。

no command

シンタックスの説明

aaa	AAA の設定を取り消します。
alarm	アラーム パラメータの設定を取り消します。
authentication	ログイン認証および許可の設定を取り消します。
bypass	バイパスの設定を取り消します。
cdp	CDP の設定を取り消します。
clock	時刻クロックの設定を取り消します。
disk	ディスク関連パラメータの設定を取り消します。
exec-timeout	exec timeout の設定を取り消します。
help	command-line interface (CLI; コマンドライン インターフェイス) のサポートの設定を取り消します。
hostname	システムのネットワーク名の設定を取り消します。
inetd	FTP、rcp、および TFTP サービスの設定を取り消します。
interface	サポートされていません。
	
(注) CLI には no interface オプションがありますが、 no コマンドをインターフェイスに適用することはできません。ソフトウェアでは、次のエラー メッセージを表示します。物理インターフェイスの取り外しは、許可されていません。	
ip	IP パラメータの設定を取り消します。
ip access-list	IP アクセス リストの設定を取り消します。
kerberos	kerberos セキュリティ オプションの設定を取り消します。
kernel	カーネル デバッガへのアクセスを無効にします。
line	端末回線設定の設定を取り消します。
logging	システム ロギング (Syslog) の設定を取り消します。
ntp	NTP の設定を取り消します。
port-channel	ポート チャネル グローバル オプションの設定を取り消します。
print-services	WAAS プリント サービスのパラメータの設定を取り消します。
radius-server	RADIUS サーバパラメータの設定を取り消します。
smb-conf	Windows ドメイン <i>smb.conf</i> ファイルの設定を取り消します。
sshd	Secure Shell (SSH; セキュア シェル) サービスのパラメータの設定を取り消します。
ssh-key-generate	SSH ホスト キーの設定を取り消します。
tacacs	TACACS+ パラメータの設定を取り消します。
tcp	グローバル TCP パラメータの設定を取り消します。
telnet enable	Telnet サービスを無効にします。
username	ユーザ名認証の設定を取り消します。

wccp	WCCP を無効にします。
windows-domain	Windows ドメイン サーバ パラメータの設定を取り消します。

デフォルト デフォルトの動作や値はありません。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン **no** コマンドを使用して機能やコマンドを無効にします。デフォルト ゲートウェイの IP アドレスなど、コマンドの特定の引数を無効にする必要がある場合は、コマンドに、**no ip default-gateway ip-address** などの具体的な文字列を指定する必要があります。

例 次の例は、WAAS デバイスで Telnet サービスを無効にします。

```
WAE(config)# no telnet enable
```

(config) ntp

NTP サーバを設定して、システム クロックをタイム サーバによって同期化できるようにするには、**ntp** 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。この機能を無効にするには、このコマンドの **no** 形式を使用します。

```
ntp [authenticate | authentication-key authentication-key [md5 encryption-type] | server {ip-address |
hostname} [ip-addresses | hostnames] | server-with-authentication {ip-address | hostname} key
authentication-key]
```

シンタックスの説明

authenticate	NTP サーバを認証します。
authentication-key	NTP 認証キーを設定します。
<i>authentication-key</i>	NTP 認証キーの値。0 ~ 4294967295 の範囲でなければなりません。
md5	MD5 暗号ハッシュ機能を設定します。
<i>encryption-type</i>	MD5 暗号タイプを 0 に設定する必要があります。
server	WAAS デバイスの NTP サーバ IP アドレスを設定します。
<i>ip-address</i>	NTP サーバ IP アドレス
<i>hostname</i>	NTP サーバのホスト名
<i>ip-addresses</i>	(オプション) クロックの同期化を実現するタイム サーバの IP アドレス (最大 4)
<i>hostnames</i>	(オプション) クロックの同期化を実現するタイム サーバのホスト名 (最大 4)
server-with-authentication	WAAS デバイスの認証 NTP サーバ IP アドレスを設定します。
<i>ip-address</i>	NTP サーバ IP アドレス
<i>hostname</i>	NTP サーバのホスト名
key	NTP 認証キーの値を設定します。
<i>authentication-key</i>	NTP 認証キーの値。0 ~ 4294967295 の範囲でなければなりません。

デフォルト

デフォルトの NTP バージョン番号は 3 です。

コマンドモード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

このコマンドを使用して、WAAS デバイスのクロックを指定の NTP サーバと同期させます。**ntp** コマンドにより、タイムキーピングの目的で NTP サーバを有効にできます。システム クロックを WAAS ソフトウェアのタイム サーバと同期化させる唯一の方法です。

例 次の例は、WAAS デバイスのタイム ソースとして NTP サーバ IP アドレスを指定します。また、この設定の削除も行います。

```
WAE(config)# ntp 172.16.22.44  
WAE(config)# no ntp 172.16.22.44
```

関連コマンド

[clock](#)

[\(config\) clock](#)

[ntpdate](#)

[show clock](#)

[show ntp](#)

(config) policy-engine application classifier

WAE で既存のアプリケーション分類機能を作成または編集するには、**policy-engine application classifier** 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。このコマンドを使用して規則（一致条件ともいわれるもの）を追加または変更し、特定タイプのトラフィックを識別できます。このコマンドを使用して分類機能の一致条件をリストすることもできます。

アプリケーション分類機能または条件を削除するには、このコマンドの **no** 形式を使用します。

```
policy-engine application classifier classifier-name [list |
  match {all | dst {host hostname | ip ip_address | port {eq port | range port1 port2}} |
  src {host hostname | ip ip_address | port {eq port | range port1 port2}}}]
```

シンタックスの説明

classifier-name	分類機能の名前（30 文字以内）。名前は必ずアプリケーション クラスを表す文字で開始します。
list	（オプション）指定された分類機能に格納されている条件をリストします。
match	（オプション）トラフィックの照合基準を指定します。
all	どのタイプのトラフィックも照合します。
dst	宛先ホストの識別基準を指定します。
host hostname	トラフィックの発信元または宛先であるシステムのホスト名を指定します。
ip ip_address	トラフィックの発信元または宛先であるシステムの IP アドレスを指定します。
port	発信元または宛先ホストにより使用されるポートの識別基準を指定します。
eq port	発信元または宛先ポート番号を指定します。
range port1 port2	発信元または宛先ポート番号の範囲を指定します。
src	発信元ホストの識別基準を指定します。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

分類機能を使用するポリシーがある場合、その分類機能を削除すると失敗します。新しいアプリケーション分類機能を作成したり既存のアプリケーション分類機能を追加する場合、WAAS CLI は 1 つまたは複数の条件を指定できる適切なサブモードに入ります。ただし、指定した条件が分類機能の条件リストにすでにある既存の条件を照合する場合は、何も行われません。条件はこのコマンドの **no** 形式を使用して削除できます。新しい分類機能を作成する場合は、最低 1 つの条件を追加する必要があります。



(注)

512 より多いアプリケーション分類機能を作成することはできません。

WAAS ソフトウェアには 150 以上のデフォルトアプリケーションポリシーが付属しており、WAAS システムがネットワーク上の最も一般的なトラフィックの一部を分類、最適化するとき役に立ちます。新しいアプリケーションポリシーを作成する前にデフォルトのポリシーを調べて、それらを適切に変更することを推奨します。通常、新しいポリシーを作成するよりも既存のものを変更したほうが簡単です。WAAS がシステムにバンドルされたポリシーに基づいて最適化またはパススルーす

るデフォルトのアプリケーションおよび分類機能のリストは、『Cisco Wide Area Application Services Configuration Guide』を参照してください。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

(config) policy-engine application map adaptor EPM
(config) policy-engine application map adaptor WAFS transport
(config) policy-engine application map basic delete
(config) policy-engine application map basic disable
(config) policy-engine application map basic insert
(config) policy-engine application map basic list
(config) policy-engine application map basic move
(config) policy-engine application map basic name
(config) policy-engine application map other optimize DRE
(config) policy-engine application map other optimize full
(config) policy-engine application map other pass-through
(config) policy-engine application name

(config) policy-engine application map adaptor EPM

WAE で EndPoint Mapper (EPM) サービスの拡張ポリシー マップ リストを備えたアプリケーション ポリシーを設定するには、**policy-engine application map adaptor EPM** 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。アプリケーション ポリシー設定で EPM サービスを無効にするには、このコマンドの **no** 形式を使用します。

```

policy-engine application map adaptor EPM epm-map {

    delete line-number |

    disable line-number |

    insert {first | last | pos line-number} name app-name {All | classifier classifier-name} [disable]
    action {optimize {DRE {yes | no} compression {LZ | none} | full} | pass-through} |

    list [from line-number [to line-number]] | to line-number [from line-number]] |

    move from line-number to line-number |

    name app-name {All | classifier classifier-name} [disable] action {optimize {DRE {yes | no}
    compression {LZ | none} | full} | pass-through}}

```

シンタックスの説明

<i>epm-map</i>	Messaging Application Programming Interface (MAPI; メッセージング アプリケーション プログラミング インターフェイス) または Universal Unique ID (UUID; ユニバーサルユニーク ID)
delete	行番号で指定されたアプリケーション ポリシー マップを削除します。
<i>line-number</i>	リスト中のアプリケーション ポリシー マップの行番号または位置
disable	行番号で指定されたアプリケーション ポリシー マップを無効にします。
insert	指定された位置に新しいポリシー マップを挿入または追加します。
first	リストの先頭に新しいアプリケーション ポリシー マップを挿入します。
last	リストの最後に新しいアプリケーション ポリシー マップを挿入します。
pos	指定された行番号に新しいアプリケーション ポリシー マップを挿入します。
name	アプリケーションの名前を指定します。
<i>app-name</i>	アプリケーションの名前
All	すべてのトラフィックを指定します。
classifier	アプリケーション トラフィック分類機能の名前を指定します。
<i>classifier-name</i>	アプリケーション トラフィック分類機能の名前
disable	最適化またはパススルーを無効にします。
action	トラフィックを最適化またはパススルーさせるかを指定します。
optimize	一般的な最適化を適用します。
DRE	DRE 最適化を有効または無効にします。
yes	DRE 最適化を有効にします。
no	DRE 最適化を無効にします。
compression	Lempel-Ziv (LZ) 圧縮を適用するか、または圧縮なしにします。
LZ	LZ 圧縮を適用します。
none	圧縮を適用しません。

full	完全な汎用最適化を適用します。
pass-through	最適化なしでトラフィックのパススルーを許可します。
list	指定されたアプリケーション ポリシー マップをリストします。
from	(オプション) リストの最初のアプリケーション ポリシー マップの行番号を指定します。
to	(オプション) リストの最後のアプリケーション ポリシー マップの行番号を指定します。
move	指定されたアプリケーション ポリシー マップをある行から別の行に移動します。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

EndPoint Mapper (EPM) はサーバ ポートを特定のアプリケーションに動的に割り当てるサービスです。常に同じポートを使用する大半のアプリケーションとは違い、EPM サービスに依存するアプリケーションはすべての要求時に別のポートを割り当てることができます。

**(注)**

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

[\(config\) policy-engine application classifier](#)
[\(config\) policy-engine application map adaptor WAFS transport](#)
[\(config\) policy-engine application map basic delete](#)
[\(config\) policy-engine application map basic disable](#)
[\(config\) policy-engine application map basic insert](#)
[\(config\) policy-engine application map basic list](#)
[\(config\) policy-engine application map basic move](#)
[\(config\) policy-engine application map basic name](#)
[\(config\) policy-engine application map other optimize DRE](#)
[\(config\) policy-engine application map other optimize full](#)

(config) policy-engine application map adaptor WAFS transport

Wide Area File Services (WAFS) transport オプションを備えたアプリケーション ポリシーを設定するには、**policy-engine application map adaptor WAFS transport** 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。アプリケーション ポリシー設定で WAFS 転送ポリシー マップを無効にするには、このコマンドの **no** 形式を使用します。

policy-engine application map adaptor WAFS transport {

delete *line-number* |

disable *line-number* |

insert {**first** | **last** | **pos** *line-number*} **name** *app-name* {**All** | **classifier** *classifier-name*} [**disable**]
action {**optimize** {**DRE** {**yes** | **no**} **compression** {**LZ** | **none**} | **full**} | **pass-through**} |

list [**from** *line-number* [**to** *line-number*] | **to** *line-number* [**from** *line-number*]] |

move from *line-number* **to** *line-number* |

name *app-name* {**All** | **classifier** *classifier-name*} [**disable**] **action** {**optimize** {**DRE** {**yes** | **no**}
compression {**LZ** | **none**} | **full**} | **pass-through**}}

シンタックスの説明

delete	行番号で指定されたアプリケーション ポリシー マップを削除します。
<i>line-number</i>	リスト中のアプリケーション ポリシー マップの行番号または位置
disable	行番号で指定されたアプリケーション ポリシー マップを無効にします。
insert	指定された位置に新しいポリシー マップを挿入または追加します。
first	リストの先頭に新しいアプリケーション ポリシー マップを挿入します。
last	リストの最後に新しいアプリケーション ポリシー マップを挿入します。
pos	指定された行番号に新しいアプリケーション ポリシー マップを挿入します。
name	アプリケーションの名前を指定します。
<i>app-name</i>	アプリケーションの名前
All	すべてのトラフィックを指定します。
classifier	アプリケーション トラフィック 分類機能の名前を指定します。
<i>classifier-name</i>	アプリケーション トラフィック 分類機能の名前
disable	最適化またはパススルーを無効にします。
action	トラフィックを最適化またはパススルーさせるかを指定します。
optimize	一般的な最適化を適用します。
DRE	DRE 最適化を有効または無効にします。
yes	DRE 最適化を有効にします。
no	DRE 最適化を無効にします。
compression	Lempel-Ziv (LZ) 圧縮を適用するか、または圧縮なしにします。
LZ	LZ 圧縮を適用します。
none	圧縮を適用しません。
full	完全な汎用最適化を適用します。

pass-through	最適化なしでトラフィックのパススルーを許可します。
list	指定されたアプリケーション ポリシー マップをリストします。
from	(オプション) リストの最初のアプリケーション ポリシー マップの行番号を指定します。
to	(オプション) リストの最後のアプリケーション ポリシー マップの行番号を指定します。
move	指定されたアプリケーション ポリシー マップをある行から別の行に移動します。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

デフォルトでは、WAFS を有効にすると、Edge WAE とコア クラスタ間を進むすべての CIFS トラフィックは加速されます。このコマンドを使用し、エッジおよびコア デバイス間を移動する CIFS トラフィックに対して別のアクション (*optimize* など) を指定します。

**(注)**

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

[\(config\) policy-engine application classifier](#)
[\(config\) policy-engine application map adaptor EPM](#)
[\(config\) policy-engine application map basic delete](#)
[\(config\) policy-engine application map basic disable](#)
[\(config\) policy-engine application map basic insert](#)
[\(config\) policy-engine application map basic list](#)
[\(config\) policy-engine application map basic move](#)
[\(config\) policy-engine application map basic name](#)
[\(config\) policy-engine application map other optimize DRE](#)
[\(config\) policy-engine application map other optimize full](#)
[\(config\) policy-engine application map other pass-through](#)
[\(config\) policy-engine application name](#)

(config) policy-engine application map basic delete

WAE でアプリケーション ポリシー マップのリストから特定の基本（スタティック）アプリケーション ポリシーを削除するには、**policy-engine application map basic delete** 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。

policy-engine application map basic delete pos

シンタックスの説明

pos リスト内のポリシー マップの正確な位置を示す行番号

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

ポリシー マップは一連のアプリケーション ポリシーとそのチェック順序で構成されます。このコマンドは、指定された行番号が現在のポリシー マップを表していない場合は無視されます。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

(config) [policy-engine application classifier](#)
 (config) [policy-engine application map adaptor EPM](#)
 (config) [policy-engine application map adaptor WAFS transport](#)
 (config) [policy-engine application map basic disable](#)
 (config) [policy-engine application map basic insert](#)
 (config) [policy-engine application map basic list](#)
 (config) [policy-engine application map basic move](#)
 (config) [policy-engine application map basic name](#)
 (config) [policy-engine application map other optimize DRE](#)
 (config) [policy-engine application map other optimize full](#)
 (config) [policy-engine application map other pass-through](#)
 (config) [policy-engine application name](#)

(config) policy-engine application map basic disable

WAE でアプリケーション ポリシー マップのリストから特定の基本 (スタティック) アプリケーション ポリシーを無効にするには、**policy-engine application map basic disable** 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。

policy-engine application map basic disable *pos*

シンタックスの説明

pos リスト内のポリシー マップの正確な位置を示す行番号

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

使用上のガイドライン

このコマンドは、指定された行番号が現在のポリシー マップを表していない場合は無視されます。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

[\(config\) policy-engine application classifier](#)

[\(config\) policy-engine application map adaptor EPM](#)

[\(config\) policy-engine application map adaptor WAFS transport](#)

[\(config\) policy-engine application map basic delete](#)

(config) policy-engine application map basic insert

WAE でアプリケーション ポリシー マップのリストに新しい基本 (スタティック) アプリケーション ポリシー マップを挿入するには、**policy-engine application map basic insert** 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。

```
policy-engine application map basic insert {first | last | pos pos} name app-name
```

シンタックスの説明

first	リストの先頭にポリシー マップを挿入します。
last	リストの最後にポリシー マップを挿入します。
pos	リスト中の特定の位置にポリシー マップを挿入します。
<i>pos</i>	ポリシー マップを挿入する行番号
name	すでに定義済みのアプリケーション名を指定します。
<i>app-name</i>	アプリケーションの名前

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

使用上のガイドライン

WAE でアプリケーション ポリシー マップのリストに新しい基本 (スタティック) アプリケーション ポリシー マップを挿入するには、**policy-engine application map basic insert** 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。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

[\(config\) policy-engine application classifier](#)
[\(config\) policy-engine application map adaptor EPM](#)
[\(config\) policy-engine application map adaptor WAFS transport](#)
[\(config\) policy-engine application map basic delete](#)
[\(config\) policy-engine application map basic disable](#)
[\(config\) policy-engine application map basic list](#)
[\(config\) policy-engine application map basic move](#)
[\(config\) policy-engine application map basic name](#)
[\(config\) policy-engine application map other optimize DRE](#)
[\(config\) policy-engine application map other optimize full](#)
[\(config\) policy-engine application map other pass-through](#)
[\(config\) policy-engine application name](#)

(config) policy-engine application map basic list

WAE で基本 (スタティック) アプリケーション ポリシー マップのリストを表示するには、**policy-engine application map basic list** 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。

```
policy-engine application map basic list [from pos [to pos] | to pos]
```

シンタックスの説明

from	(オプション) 指定された位置からリストを開始します。
to	(オプション) 指定された位置でリストを停止します。
pos	リスト内のポリシー マップの正確な位置を示す行番号

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

WAE で基本アプリケーション ポリシー マップのリストを表示するには、**policy-engine application map basic list** 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。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

[\(config\) policy-engine application classifier](#)
[\(config\) policy-engine application map adaptor EPM](#)
[\(config\) policy-engine application map adaptor WAFS transport](#)
[\(config\) policy-engine application map basic delete](#)
[\(config\) policy-engine application map basic disable](#)
[\(config\) policy-engine application map basic insert](#)
[\(config\) policy-engine application map basic move](#)
[\(config\) policy-engine application map basic name](#)
[\(config\) policy-engine application map other optimize DRE](#)
[\(config\) policy-engine application map other optimize full](#)
[\(config\) policy-engine application map other pass-through](#)
[\(config\) policy-engine application name](#)

(config) policy-engine application map basic move

WAE で L3 または L4 パラメータだけに基づいて基本ポリシー マップ リストを持つアプリケーション ポリシーを移動するには、**policy-engine application map basic move** 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。

policy-engine application map basic move from *pos* to *pos*

シンタックスの説明

from	指定された行番号にあるポリシーを移動します。
to	指定された行番号にポリシーを移動します。
pos	リスト内のポリシー マップの正確な位置を示す行番号

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

WAE でレイヤ 3 またはレイヤ 4 パラメータだけに基づいて基本ポリシー マップ リストを持つアプリケーション ポリシーを移動するには、**policy-engine application map basic move** 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。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

例

次の例では、行 10 から行 16 にポリシー マップを移動します。

```
WAE(config)# policy-engine application map basic move from 10 to 16
```

関連コマンド

- [\(config\) policy-engine application classifier](#)
- [\(config\) policy-engine application map adaptor EPM](#)
- [\(config\) policy-engine application map adaptor WAFS transport](#)
- [\(config\) policy-engine application map basic delete](#)
- [\(config\) policy-engine application map basic disable](#)
- [\(config\) policy-engine application map basic insert](#)
- [\(config\) policy-engine application map basic list](#)
- [\(config\) policy-engine application map basic name](#)
- [\(config\) policy-engine application map other optimize DRE](#)
- [\(config\) policy-engine application map other optimize full](#)
- [\(config\) policy-engine application map other pass-through](#)
- [\(config\) policy-engine application name](#)

(config) policy-engine application map basic name

基本ポリシー マップ名を持つアプリケーション ホリシーを設定するには、**policy-engine application map basic name** 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。

```
policy-engine application map basic name app-name classifier classifier-name {[disable] action
  {optimize {DRE {yes | no} compression {LZ | none} | full} | pass-through} [accelerate {cifs |
  MS-port-mapper}]}
```

シンタックスの説明

app-name	アプリケーション名
classifier	アプリケーション トラフィック分類機能の名前を指定します。
classifier-name	分類機能の名前
disable	最適化またはパススルーを無効にします。
action	トラフィックを最適化またはパススルーを許可するかを指定します。
optimize	一般的な最適化を適用します。
DRE	DRE 最適化を有効または無効にします。
yes	DRE 最適化を有効にします。
no	DRE 最適化を無効にします。
compression	圧縮を適用します。
LZ	Lempel-Ziv (LZ) 圧縮を適用します。
none	圧縮を適用しません。
full	完全な汎用最適化を適用します。
pass-through	最適化なしでトラフィックのパススルーを許可します。
accelerate	特殊なアダプタを使用してトラフィックを加速します。
cifs	CIFS アクセラレータを使用してトラフィックを加速します。
MS-port-mapper	Microsoft EndPoint Port Mapper (EPM) を使用してトラフィックを加速します。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

基本ポリシー マップ名を持つアプリケーション ホリシーを設定するには、**policy-engine application map basic name** 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。

WAFS の動的な許可または拒否リストのエントリを表示するには、**show policy-engine application dynamic** コマンドを使用します。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

(config) policy-engine application classifier
(config) policy-engine application map adaptor EPM
(config) policy-engine application map adaptor WAFS transport
(config) policy-engine application map basic delete
(config) policy-engine application map basic disable
(config) policy-engine application map basic insert
(config) policy-engine application map basic list
(config) policy-engine application map basic move
(config) policy-engine application map other optimize DRE
(config) policy-engine application map other optimize full
(config) policy-engine application map other pass-through
(config) policy-engine application name
show policy-engine application dynamic

(config) policy-engine application map other optimize DRE

WAE で分類されていないトラフィックに optimize DRE アクションを設定するには、**policy-engine application map other optimize DRE** 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。

policy-engine application map other optimize DRE {yes | no} compression {LZ | none}

シンタックスの説明

yes	分類されていないトラフィックで optimize DRE アクションを適用します。
no	分類されていないトラフィックで optimize DRE アクションを適用しません。
compression	指定された圧縮を適用します。
LZ	Lempel-Ziv (LZ) 圧縮を適用します。
none	圧縮を適用しません。

コマンドモード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

WAE で分類されていないトラフィックに optimize DRE アクションを設定するには、**policy-engine application map other optimize DRE** 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。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

例

次の例では、圧縮が適用されておらず、分類されていないトラフィックで optimize DRE を設定します。

```
WAE(config)# policy-engine application map other optimize DRE yes compression none
```

関連コマンド

[\(config\) policy-engine application classifier](#)
[\(config\) policy-engine application map adaptor EPM](#)
[\(config\) policy-engine application map adaptor WAFS transport](#)
[\(config\) policy-engine application map basic delete](#)
[\(config\) policy-engine application map basic disable](#)
[\(config\) policy-engine application map basic insert](#)
[\(config\) policy-engine application map basic list](#)
[\(config\) policy-engine application map basic move](#)
[\(config\) policy-engine application map basic name](#)
[\(config\) policy-engine application map other optimize full](#)
[\(config\) policy-engine application map other pass-through](#)
[\(config\) policy-engine application name](#)

(config) policy-engine application map other optimize full

分類されていないトラフィックで optimize full アクションを持つアプリケーション ポリシーを設定するには、**policy-engine application map other optimize full** 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。

policy-engine application map other optimize full

シンタックスの説明 このコマンドには引数やキーワードがありません。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator

使用上のガイドライン 分類されていないトラフィックで optimize full アクションを持つアプリケーション ポリシーを設定するには、**policy-engine application map other optimize full** 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。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

- [\(config\) policy-engine application classifier](#)
- [\(config\) policy-engine application map adaptor EPM](#)
- [\(config\) policy-engine application map adaptor WAFS transport](#)
- [\(config\) policy-engine application map basic delete](#)
- [\(config\) policy-engine application map other optimize DRE](#)
- [\(config\) policy-engine application map other pass-through](#)
- [\(config\) policy-engine application name](#)

(config) policy-engine application map other pass-through

WAE で path-through アクションを持つ分類されていないトラフィックでのアプリケーション ポリシーを設定するには、**policy-engine application map other path-through** 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。

policy-engine application map other pass-through

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator

使用上のガイドライン WAE で path-through アクションを持つ分類されていないトラフィックでのアプリケーション ポリシーを設定するには、**policy-engine application map other path-through** 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。



(注) WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

- [\(config\) policy-engine application map basic delete](#)
- [\(config\) policy-engine application map basic disable](#)
- [\(config\) policy-engine application map basic insert](#)
- [\(config\) policy-engine application map basic list](#)
- [\(config\) policy-engine application map basic move](#)
- [\(config\) policy-engine application map basic name](#)
- [\(config\) policy-engine application map basic name](#)
- [\(config\) policy-engine application map other optimize full](#)

(config) policy-engine application name

WAE でアプリケーションに関する一般情報を指定する新しいアプリケーション定義を作成するには、**policy-engine application name** 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。アプリケーション定義を削除するには、このコマンドの **no** 形式を使用します。

policy-engine application name *app-name*

シンタックスの説明

app-name アプリケーションの名前（30 文字以内）。名前にスペースや特殊文字を入れることはできません。

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

使用上のガイドライン

このコマンドを使用して、あとでアプリケーションに関する統計情報を収集するときに利用できる新しいアプリケーション名を作成します。この名前を使用したポリシーがある場合、アプリケーション名の削除は失敗します。正常に削除されると、以前にこのアプリケーションに関連付けられたすべての統計情報はクリアされます。



(注)

アプリケーション名は 256 以内です。



(注)

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

例

次の例は、Payroll アプリケーションのアプリケーション定義を作成する方法を示します。

```
WAE(config)# policy-engine application name Payroll
```

関連コマンド

[\(config\) policy-engine application classifier](#)

[\(config\) policy-engine application map adaptor EPM](#)

[\(config\) policy-engine application map adaptor WAFS transport](#)

[\(config\) policy-engine application map basic delete](#)

[\(config\) policy-engine application map basic disable](#)

[\(config\) policy-engine application map basic insert](#)

[\(config\) policy-engine application map basic list](#)

[\(config\) policy-engine application map basic move](#)

[\(config\) policy-engine application map basic name](#)

[\(config\) policy-engine application map basic name](#)[\(config\) policy-engine application map other optimize DRE](#)[\(config\) policy-engine application map other optimize full](#)[\(config\) policy-engine application map other pass-through](#)

(config) policy-engine config

アプリケーション ポリシーの設定を削除したり、アプリケーション ポリシーの設定を WAE の出荷時の設定に置き換えたりするには、**policy-engine config** 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。

```
policy-engine config {remove-all | restore-predefined}
```

シンタックスの説明

remove-all	アプリケーション ポリシーの設定をすべて同時に削除し、変更された他の設定をリセットします。
restore-predefined	アプリケーション ポリシーの設定（アプリケーション名、分類機能、およびポリシー マップを含む）を出荷時の設定に置き換えます。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

このアクションには次のものが含まれますが、これだけに限定されません。

- 「other」以外のすべてのアプリケーション名を削除する。
- すべての分類機能を削除する。
- すべてのポリシー マップを削除する。
- デフォルト アクションを pass-through にリセットする。

**(注)**

WAAS Central Manager GUI を使用して WAE のアプリケーション ポリシーを一元的に設定することを強く推奨します。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

関連コマンド

[show policy-engine status](#)

(config) port-channel

WAAS デバイスでポート チャネル ロード バランシング オプションを設定するには、**port-channel** 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。ポート チャネルのロード バランシングをデフォルトの方法に設定するには、このコマンドの **no** 形式を使用します。

port-channel load-balance {dst-ip | dst-mac | round-robin}

シンタックスの説明

load-balance	ロード バランシングの方法を設定します。
dst-ip	宛先 IP アドレスによるロード バランシング方法を指定します。
dst-mac	宛先 MAC アドレスによるロード バランシング方法を指定します。
round-robin	ラウンドロビン順次巡回リソース割り当てによるロード バランシング方法を指定します。

デフォルト

ラウンドロビンがデフォルトのロード バランシング方法です。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

port-channel load-balance コマンドは、3つのロード バランシング アルゴリズムのうちの1つを設定し、イーサネット フレーム送信時のインターフェイス選択に柔軟性を提供します。**round-robin** オプションにより、チャネル グループ内で同じネットワーク インターフェイスを均等にバランス良く使用できます。このコマンドはグローバルに有効となるので、チャネル グループを2つ設定している場合は、同一のロード バランシング オプションを使用する必要があります。

例

次の例は、ポート チャネルの宛先 IP ロード バランシングを設定し、続いて無効にします。

```
WAE(config)# port-channel load-balance dst-ip
WAE(config)# no port-channel load-balance
```


(config) primary-interface

WAAS デバイスのプライマリ インターフェイスを設定するには、グローバル コンフィギュレーション モードで **primary-interface** コマンドを使用します。設定されたプライマリ インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
primary-interface {GigabitEthernet 1-2/port | PortChannel 1-2 | Standby group_num}
```

シンタックスの説明

GigabitEthernet	WAAS デバイスのプライマリ インターフェイスとして、ギガビット イーサネット インターフェイスを選択します。
<i>1-2/</i>	ギガビット イーサネットのスロット番号 1 または 2
<i>port</i>	ギガビット イーサネット インターフェイスのポート番号
PortChannel	WAAS デバイスのプライマリ インターフェイスとして、ポート チャネル イーサネット インターフェイスを選択します。
<i>1-2</i>	ポート チャネル番号 1 または 2
Standby	WAAS デバイスのプライマリ インターフェイスとして、スタンバイ グループを選択します。
<i>group_num</i>	スタンバイ グループ番号 (1 ~ 4)

デフォルト

デフォルトのプライマリ インターフェイスは、ギガビット イーサネット 1/0 インターフェイスです。これが設定されていない場合は、リンク ビートが検出された最初の動作可能なインターフェイスが、デフォルトのプライマリ インターフェイスになります。ID 番号の小さいインターフェイスが、最初にポーリングされます (たとえば、ギガビット イーサネット 1/0 が 2/0 より先に確認されます)。ギガビット イーサネット インターフェイスは、ポート チャネル インターフェイスより先にポーリングされます。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

primary-interface グローバル コンフィギュレーション コマンドによって、管理者は WAAS デバイスのプライマリ インターフェイスを指定できます。

プライマリ インターフェイスは、WAAS デバイスを無効にせずに変更できます。プライマリ インターフェイスを変更するには、コマンド文字列を再入力して別のインターフェイスを指定します。



(注)

restore factory-default preserve basic-config コマンドを使用すると、プライマリ インターフェイスの設定は保存されません。**restore factory-default preserve basic-config** コマンドを使用したあとで WAAS デバイスを再度有効にするには、工場出荷時のデフォルトを回復後、プライマリ インターフェイスを再設定するようにしてください。

■ (config) primary-interface

プライマリ インターフェイスをスタンバイ グループに設定しても、スタンバイ機能は有効になりません。関連するスタンバイ インターフェイスは、**interface standby** 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設定する必要があります。

例

次の例は、ギガビットイーサネット スロット 1 ポート 0 を WAAS デバイスのプライマリ インターフェイスとして設定する方法を示します。

```
WAE(config)# primary-interface GigabitEthernet 1/0
```

次の例は、ギガビットイーサネット スロット 2 ポート 0 を WAAS デバイスのプライマリ インターフェイスとして設定する方法を示します。

```
WAE(config)# primary-interface GigabitEthernet 2/0
```

関連コマンド


[\(config\) interface](#)

(config) print-services

WAAS デバイスで設定アクセスが許可された管理者に対して、プリント サービスを有効にし、グループ名を指定するには、**print-services** 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。WAAS デバイスでのプリント サービスを無効にするか、管理グループをクリアするには、このコマンドの **no** 形式を使用します。

```
print-services {enable | admin-group admin-group-name | guest-print enable}
```

シンタックスの説明

enable	WAAS デバイスでのプリント サービスを有効にします。
admin-group	プリント サービス設定権限のある管理者グループを設定します。
<i>admin-group-name</i>	管理グループの名前 (最大 127 文字)。スペースは使用できません。
guest-print enable	ゲストプリント サービスを有効にします。ゲストプリンティングではどのユーザも WAAS プリント サーバに出力できます。
	
(注)	このオプションは application-accelerator デバイス モードだけで利用できます。

デフォルト

デフォルトでは、プリント サービスは無効に設定されており、管理グループは定義されていません (*admin-group-name* がヌル)。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

WAAS プリント サービスは、通常、ブランチ オフィスにある WAE では有効です。WAE は、プリント サーバとして機能し、複数のプリンタへのアクセスのための複数のクライアントから要求を処理します。WAAS プリント サービス機能は、管理者が次のプリント関連タスクを実行できるようにします。

- プリンタ リストからのプリンタの追加、変更、削除
- プリンタのグループの追加、変更、削除 (プリンタ クラスタ)
- プリント ジョブの表示と制御
- 個々のプリンタのステータスの監視
- 診断およびトラブルシューティングの実行
- プリント サーバからのクライアントプリンタ ドライバのインストール
- FTP を使用したログ ファイルのダウンロード
- 印刷割り当ての実施 (スプーリングに対して合計 1 GB)
- どのユーザも WAAS プリント サーバに出力可能

WAAS CLI から WAAS プリント サービスの開始と終了、プリント サービス管理グループの設定、およびプリント スプーラのデバッグができます。WAAS プリント サービスは、Windows プリント サービスの代替手段です。

プリント サービスの開始と終了

print-services enable コマンドを実行すると、次の一連のイベントが発生します。

- ノードマネージャが CUPS プロセス (cupsd) を開始し、*printcap* ファイルにアップデートされたタイムスタンプがないか毎秒確認する。
CUPS は 30 秒以内に起動する必要があります。そうしないとプリント サービスが有効にならず、「CUPS fails to start」メッセージがノードマネージャによってログに記録されます。
- ノードマネージャが Samba (smbd) プロセスを開始する。
Samba を開始できなかった場合は、「Samba fails to start」メッセージがノードマネージャによってログに記録されます。CUPS は終了されません。
- 成功メッセージがノードマネージャによってログに記録される。
- DataServer 値 (cfg/print-services/enable) が 1 に設定される。

プリント サービスの終了は、**no print-services enable** コマンドを使用して行います。このコマンドを入力すると、次の一連のイベントが引き起こされます。

- ノードマネージャが Samba (smbd) プロセスを終了する。
- ノードマネージャが CUPS (cupsd) プロセスを終了する。
- 対応する DataServer 値が 0 に設定される。

プリント サービス管理グループの設定

print-services admin-group コマンドを使用して、特定の Edge WAE の WAAS プリント サービスを制御する管理者のセットを定義できます。このコマンドを入力すると、次のイベントが発生します。

- 指定された管理グループで *smb.conf* ファイルがアップデートされる。
アップデートが失敗し、プリント サービス管理グループを元の値に戻せる場合は、エラーメッセージ「Failed to configure print-services admin group」が表示されます。アップデートが失敗して、プリント サービス管理グループを元の値に戻せない場合は、2つのエラーメッセージ「Failed to configure print-services admin group.」および「Failed to revert back the print-services admin group changes.」が表示されます。
- 指定された管理グループで *cupsd.conf* ファイルがアップデートされる。
アップデートが失敗して、古い設定を元に戻す場合、*smb.conf* ファイルへの変更が復元され、エラーメッセージ「Failed to configure print-services admin group」が表示されます。アップデートが失敗して、古い設定に戻せない場合は、2つのエラーメッセージ「Failed to configure print-services admin group.」および「Failed to revert back the print-services admin group changes.」が表示されます。
- DataServer 値 (cfg/print-services/administrators) が指定された管理グループでアップデートされる。
DataServer 値の設定が失敗した場合、*smb.conf* と *cupsd.conf* の両方の設定が元に戻り、エラーメッセージが表示されます。

プリント サービス管理グループは、**no print-services admin-group** コマンドを使用して削除できます。このコマンドを実行すると、次のイベントが発生します。

- *smb.conf* 設定がクリアされる。
クリアが失敗して古い設定に戻った場合、エラーメッセージ「Failed to configure print-services admin group」が表示されます。クリアが失敗して、古い設定に戻せない場合は、2つのエラーメッセージ「Failed to configure print-services admin group.」および「Failed to revert back the print-services admin group changes.」が表示されます。

- *cupsd.conf* ファイルが管理グループ設定をクリアするよう変更される。
クリアが失敗して古い設定に戻り、*smb.conf* の変更が元に戻った場合、エラー メッセージ「Failed to configure print-services admin group」が表示されます。クリアが失敗して、古い設定に戻せない場合は、2つのエラー メッセージ「Failed to configure print-services admin group.」および「Failed to revert back the print-services admin group changes.」が表示されます。
- 対応する DataServer 値がクリアされる。
DataServer 値のクリアが失敗した場合、*smb.conf* と *cupsd.conf* の両方の設定が元に戻り、エラー メッセージが表示されます。

この変更を有効にするには、手動で Samba および CUPS プロセスを再開する必要があります。

例

次の例は、WAAS デバイスでのプリント サービスを有効にします。

```
WAE(config)# print-services enable
```

次の例では、*printAdmins* という名前のプリント サービス管理グループを追加します。

```
WAE(config)# print-services admin-group printAdmins
The new print-services administrator group is configured successfully. Please restart
print services for the change to take effect.
WAE(config)# no print-services enable
WAE(config)# print-services enable
```

次の例は、WAAS デバイスからプリント サービスの管理グループを削除します。

```
WAE(config)# no print-services admin-group printAdmins
The print-services administrator group is removed successfully. Please restart print
services for the change to take effect.
WAE(config)# no print-services enable
WAE(config)# print-services enable
```

関連コマンド

[debug](#)

[show print-services](#)

[show running-config](#)

[show startup-config](#)

(config) radius-server

WAAS デバイスで一連の RADIUS 認証サーバ設定を設定するには、グローバル コンフィギュレーション モードで **radius-server** コマンドを使用します。RADIUS 認証サーバ設定を無効にするには、このコマンドの **no** 形式を使用します。

```
radius-server {host hostname | hostipaddr [primary] | key keyword | retransmit retries | timeout seconds}
```

シンタックスの説明

host	RADIUS サーバを指定します。最大 5 つのサーバを指定できます。
<i>hostname</i>	RADIUS サーバのホスト名
<i>hostipaddr</i>	RADIUS サーバの IP アドレス
primary	(オプション) サーバをプライマリ サーバとして設定します。
key	RADIUS サーバで共有する暗号キーを指定します。
<i>keyword</i>	共有キーのテキスト (最大 15 文字)
retransmit	アクティブなサーバへの送信試行回数を指定します。
<i>retries</i>	トランザクションの送信試行回数 (1 ~ 3)。デフォルトは 2 です。
timeout	RADIUS サーバが応答を待機する時間を指定します。指定できる範囲は 1 ~ 20 秒です。
<i>seconds</i>	秒単位の待機時間 (1 ~ 20)。デフォルトは 5 秒です。

デフォルト

retransmit *retries* : 2 2

timeout *seconds* : 5

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

RADIUS は、NAS が使用するクライアント / サーバ認証および許可アクセス プロトコルで、ネットワーク デバイスにアクセスしようとするユーザを認証します。NAS はクライアントとして機能し、ユーザ情報を複数の RADIUS サーバに渡します。NAS は、複数の RADIUS サーバから受信した応答に基づいて、ユーザのネットワーク アクセスを許可または拒否します。RADIUS は、RADIUS クライアントとサーバ間の転送に UDP を使用します。

クライアントとサーバに RADIUS キーを設定できます。クライアントにキーを設定する場合、RADIUS サーバに設定したキーと同じである必要があります。RADIUS クライアントとサーバは、送信されるすべての RADIUS パケットを、そのキーを使用して暗号化します。RADIUS キーを設定しなければ、パケットは暗号化されません。キー自体はネットワークで送信されません。



(注)

RADIUS プロトコルの動作の詳細は、RFC 2138 の『*Remote Authentication Dial In User Service (RADIUS)*』を参照してください。

RADIUS 認証は、通常、管理者が最初に WAAS デバイスにログインし、モニタリング、設定、またはトラブルシューティングの目的で WAE を設定するときに発生します。

RADIUS 認証はデフォルトで無効に設定されています。RADIUS 認証と他の認証方式は同時に有効にできます。最初に使用する方法を指定することもできます（「(config) authentication」コマンドを参照）。

例

次の例は、RADIUS サーバを指定し、RADIUS キーを指定し、再送信のデフォルトを受け入れます。設定は、**show radius-server** コマンドで確認できます。

```
WAE(config)# radius-server host 172.16.90.121
WAE(config)# radius-server key myradiuskey
WAE# show radius-server
Radius Configuration:
-----
Radius Authentication is on
  Timeout          = 5
  Retransmit       = 3
  Key               = ****
  Servers
  -----
```

関連コマンド

[show radius-server](#)

(config) smb-conf

WAAS デバイスの Samba コンフィギュレーション ファイル *smb.conf* のパラメータを手動で設定するには、**smb-conf** 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。パラメータをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

smb-conf section {global | print\$ | printers} name attr-name value attr-value [service print]

シンタックスの説明

global	global プリント パラメータの 1 つを指定します。
print\$	print\$ パラメータの 1 つを指定します。
printers	printers パラメータの 1 つを指定します。
name	手動で設定するパラメータの名前を指定されたセクションに指定します。
<i>attr-name</i>	最大 80 文字のパラメータ名
value	パラメータの値を指定します。
<i>attr-value</i>	最大 255 文字のパラメータ名
service print	(オプション) プリント サービス用 Samba コンフィギュレーション ファイルをアップデートします。このオプションを指定しないと、 smb-conf コマンドは Windows 認証に使用する Samba コンフィギュレーション ファイルをアップデートします。

名前やデフォルト値など global、print\$ および printers パラメータの詳細については、[表 3-101](#) を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

smb.conf ファイルには、さまざまなプリント関連パラメータが含まれています。*global* パラメータは、サーバ全体に適用されます。残りすべてのセクションおよび共有に対するデフォルト設定を定義するサービス レベルのパラメータは、このパラメータセットに含まれています。これにより、繰り返し同じ値を設定する必要がなくなります。このようなグローバルに設定された共有設定を上書きし、個々のセクションや共有に対して他の値を指定できます。*print\$* パラメータは、プリンタに適用されます。*printers* パラメータは、共有に適用されます。これらのパラメータにより、最小限の設定ですべてのプリンタを共有できるようになります。これらのパラメータは、デフォルトですべてのプリンタに適用されます。

[表 3-101](#) で、プリント関連パラメータを説明します。

表 3-101 プリント関連パラメータ

パラメータ名	デフォルト値	パラメータの説明
global パラメータ		
idmap uid	70000-200000	UNIX ユーザを NT ユーザ SID にマップするために割り当てられたユーザ ID の範囲
idmap gid	70000-200000	UNIX グループを NT グループ SID にマップするために割り当てられたグループ ID の範囲
winbind enum users	no	MSRPC を使用しているドメイン ユーザは列挙しません。
winbind enum groups	no	MSRPC を使用しているドメイン グループは列挙しません。
winbind cache time	10	ドメイン ユーザまたはグループ情報が、期限切れするまでキャッシュ内に残存する時間
winbind use default domain	yes	ユーザとグループにデフォルトのドメインを使用します。
printcap name	cups	CUPS を使用して利用可能なプリンタ名を決定します。
load printers	yes	すべての利用可能なプリンタ共有を自動的に作成します。
printing	cups	CUPS 互換のプリント コマンドを使用します。
cups options	raw	プリント 出力のフォーマットを raw に設定します。
force printername	yes	CUPS GUI で指定された同じプリンタ名を強制的に Samba でのプリンタ名として使用します。
lpq cache time	0	lpq コマンドの結果に対するキャッシュ時間を制御します。
log file	/local/local1/errorlog/samba.log	プリント関連のエラーがログに記録されている場所
max log size	50	ログファイルに収容できるエラーの最大数。エラーが 50 を超えると、新しいエラーを記録するために、最も古いエラーを削除します。
socket options	TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192	クライアントとの接続を調整できるようにオペレーティングシステムのネットワーク レイヤ上のコントロールを設定します。このオプションは通常、ローカルネットワークの最適なパフォーマンスを達成するため Samba サーバの調整に使用します。
smb ports	50139	Samba サーバ上の利用可能なポート
local master	no	<i>nmbd</i> をサブネット上のローカル マスター ブラウザに設定します。
domain master	no	<i>nmbd</i> を指定されたワークグループのドメイン マスター ブラウザに設定します。
preferred master	no	<i>nmbd</i> をそのワークグループの優先マスター ブラウザに設定します。
dns proxy	no	DNS プロキシは有効になっていません。
template homedir	/local/local1/	File Engine または WAE のホーム ディレクトリ
template shell	/admin-shell	管理シェルのディレクトリ
comment	Comment:	クライアントがサーバにクエリーを送信する際に表示されるプリント サーバ (または共有) の任意の記述。 windows-domain comment コマンドで設定することもできます。

表 3-101 プリント関連パラメータ (続き)

パラメータ名	デフォルト値	パラメータの説明
netbios name	MYFILEENGINE	プリント サービスをホスティングする Samba サーバの名前。 windows-domain netbios-name コマンドで設定することもできます。
realm	CISCO	Active Directory ドメイン名。必ず大文字にします。 windows-domain realm コマンドで設定することもできます。
wins server	10.10.10.1	プリント サービスへのユーザ アクセスの認証に使用した Windows ドメイン サーバの IP アドレス。 windows-domain wins-server コマンドで設定することもできます。
password server	10.10.10.10	ユーザの認証に使用したパスワード サーバのオプションの IP アドレス。 windows-domain password-server コマンドで設定することもできます。
security	domain	認証に Windows ドメイン サーバを使用します。 windows-domain security コマンドで設定することもできます。
client schannel	no	Windows ドメイン サーバ認証に使用するセキュア チャネル インジケータ
ldap ssl	on	Samba が LDAP サーバに接続するとき SSL を使用するかどうか定義します。デフォルトでは LDAP サーバ接続時に常に SSL を使用します。「off」に設定した場合、ディレクトリ サーバのクエリー時に SSL は使用されません。「start_tls」に設定した場合、ディレクトリ サーバとの通信には LDAPv3 StartTLS 拡張動作 (RFC2830) が使用されます。
print\$ パラメータ		
path	/state/samba/printers	プリンタ リストの場所
guest ok	yes	プリンタに接続するのにパスワードは不要です。
browseable	yes	プリンタのリストにそのプリンタが表示されるようにします。
read only	yes	ユーザがプリンタ リストを作成または変更しないようにします。
write list	root	プリンタ管理者 (root ユーザ) がプリンタ リストを変更できるようにします。
printers パラメータ		
path	/local/local1/spool/samba.log	着信ファイルがプリント用にスプールされる場所
browseable	no	printable が yes の場合は、常に no に設定します。これにより、利用可能な共有リストでプリンタ共有が非表示になります。
guest ok	yes	プリンタのサービスに接続するのにパスワードは不要です。
writable	no	ユーザが、プリント サービス ディレクトリのファイルを作成または変更しないようにします。

表 3-101 プリント関連パラメータ (続き)

パラメータ名	デフォルト値	パラメータの説明
printable	yes	接続したクライアントが、スプールファイルを開き、書き込み、プリントのパスパラメータで指定したディレクトリに送信できるようにします。Samba がプリンタ共有とファイル共有を区別するために使用します。no に設定した場合、プリントは許可されません。
printer admin	root	プリンタ管理者 (root ユーザ) はドライバの追加とプリンタプロパティの設定ができます。

例 次の例は、Samba エラー ログ ファイルの最大サイズを 50 エラーから 70 エラーに変更する方法を示します。

```
WAE# smb-conf global max log size 75
```

次の例は、レルムをデフォルトの CISCO から MYCOMPANYNAME に変更する方法を示します。

```
WAE# smb-conf global realm MYCOMPANYNAME
```

次の例は、LDAP サーバ署名を有効にし、続いて無効にする方法を示します。

```
WAE# smb-conf global name "ldap ssl" value "start_tls"
```

関連コマンド

[show smb-conf](#)

[windows-domain](#)

[\(config\) windows-domain](#)

(config) snmp-server access-list

WAAS デバイスで標準アクセス コントロール リストを設定して、SNMP エージェントを介してアクセスできるようにするには、**snmp-server access-list** 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。標準アクセス コントロール リストを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server access-list {num | name}
```

シンタックスの説明

<i>num</i>	標準アクセス リストの番号 (1 ~ 99)
<i>name</i>	標準アクセス リストの名前 (最大 30 文字)

デフォルト

デフォルトの動作や値はありません。

コマンドモード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

snmp-server access-list number グローバル コンフィギュレーション コマンドは、Access Control List (ACL; アクセス コントロール リスト) を設定して SNMP エージェントがアクセスできるようにします。*number* 変数は 1 ~ 99 の範囲の数値で、標準アクセス コントロール リストを示します。SNMP は、着信パケットを、アクセス コントロール リストでチェックしてから、受け入れるかまたはドロップするかします。

例

次の例では、SNMP エージェントは、パケットを ACL 12 でチェックしてから、受け入れまたはドロップできます。

```
WAE(config)# snmp-server access-list 12
```



(注)

最初に **ip access-list standard** 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、アクセス リスト 12 を作成する必要があります。

関連コマンド

[\(config\) ip access-list](#)
[show running-config](#)

(config) snmp-server community

WAAS デバイスで SNMP エージェントを有効にして、コミュニティ アクセス スtring を設定し、SNMP エージェントにアクセスできるようにするには、**snmp-server community** 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。SNMP エージェントを無効にして以前設定したコミュニティ String 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 community string [group groupname | rw]
```

シンタックスの説明

String	パスワードのように機能し、SNMP エージェントのアクセスを許可するコミュニティ String。最大 64 文字まで使用できます。
group	(オプション) コミュニティ String が所属するグループを指定します。
groupname	グループの名前。最大 64 文字まで使用できます。
rw	(オプション) このコミュニティ String への読み取りと書き込みアクセスを可能にします。

デフォルト

SNMP エージェントは無効化されており、コミュニティ String は設定されていません。設定されると、SNMP コミュニティ String はデフォルトですべてのオブジェクトに対する読み取り専用アクセスを許可します。

使用上のガイドライン

SNMP コミュニティ String は、WAE 上で SNMP エージェントにアクセスする際、認証のパスワードとして使用されます。認証を受けるため、WAAS デバイスに送信される SNMP メッセージの Community Name フィールドは、WAAS デバイスで定義された SNMP コミュニティ String に一致する必要があります。

WAAS デバイスの SNMP エージェントは、WAAS デバイスで SNMP コミュニティ String が定義されると有効になります。作成できる SNMP コミュニティの最大数は 10 です。

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維持します。



ヒント 認証を受けるためには、WAAS デバイスに送信される SNMP メッセージの「Community Name」フィールドは必ず、ここで定義されるコミュニティ String と一致せねばなりません。

MIB サブツリーの一部分に対してだけアクセスを許可するコミュニティ String を設定できます。このコマンドの旧バージョンとの下位互換性を維持するため、デフォルトの読み取りグループまたはデフォルトの書き込みグループは (コマンドラインに **rw** オプションが指定されている場合)、グループ名が指定されないときは、コミュニティ String に関連付けられます。このデフォルト グループは両方とも、ユーザには非表示で、コンフィギュレーション ファイルや **show snmp group EXEC** コマンドに表示されませんが、SNMP エージェントの初期化中に作成されます。

コマンド モード

グローバル コンフィギュレーション

■ (config) snmp-server community

デバイス モード application-accelerator
 replication-accelerator
 central-manager

例 次の例は、SNMP エージェントを有効にし、コミュニティ ストリング comaccess を SNMP に割り当てます。

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

次の例は、SNMP エージェントを無効にし、定義済みのコミュニティ ストリングを削除します。

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

関連コマンド (config) snmp-server community
 (config) snmp-server contact
 (config) snmp-server enable traps
 (config) snmp-server group
 (config) snmp-server host
 (config) snmp-server location
 (config) snmp-server mib persist event
 (config) snmp-server notify inform
 (config) snmp-server trap-source
 (config) snmp-server user
 (config) snmp-server view
 snmp trigger

(config) snmp-server contact

WAAS デバイスでシステム サーバ担当者 (sysContact) 文字列を設定するには、**snmp-server contact** 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。システム担当者情報を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *line*

シンタックスの説明

contact	MIB-II オブジェクト <i>sysContact</i> のテキストを指定します。
<i>line</i>	この管理対象ノードの担当者の ID

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

デフォルト

システム担当者文字列は設定されていません。

使用上のガイドライン

システム担当者文字列は、MIB-II システム グループ *sysContact* オブジェクトに保存されている値です。

例

次の例は、システム担当者文字列を設定し、続いて削除します。

```
WAE(config)# snmp-server contact Dial System Operator at beeper # 27345
```

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

関連コマンド

[\(config\) snmp-server community](#)
[\(config\) snmp-server enable traps](#)
[\(config\) snmp-server group](#)
[\(config\) snmp-server host](#)
[\(config\) snmp-server location](#)
[\(config\) snmp-server mib persist event](#)
[\(config\) snmp-server notify inform](#)
[\(config\) snmp-server trap-source](#)
[\(config\) snmp-server user](#)
[\(config\) snmp-server view](#)
[snmp trigger](#)

(config) snmp-server enable traps

WAAS デバイスが SNMP トラップを送信できるようにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用します。すべての SNMP トラップまたは SNMP 認証トラップだけを無効にする場合は、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps [alarm [clear-critical | clear-major | clear-minor | raise-critical |
raise-major | raise-minor] | config | content-engine [disk-fail | disk-read | disk-write |
overload-bypass | transaction-log] | entity | event | snmp [authentication | cold-start] | wafs [cslog
| eslog | mgrlog]]
```

シンタックスの説明

alarm	(オプション) WAAS アラーム トラップを有効にします。
clear-critical	(オプション) clear-critical アラーム トラップを有効にします。
clear-major	(オプション) clear-major アラーム トラップを有効にします。
clear-minor	(オプション) clear-minor アラーム トラップを有効にします。
raise-critical	(オプション) raise-critical アラーム トラップを有効にします。
raise-major	(オプション) raise-major アラーム トラップを有効にします。
raise-minor	(オプション) raise-minor アラーム トラップを有効にします。
config	(オプション) CiscoConfigManEvent トラップを有効にします。
content-engine	(オプション) SNMP WAAS トラップを有効にします。
disk-fail	(オプション) ディスク障害エラー トラップを有効にします。
disk-read	(オプション) ディスク読み取りエラー トラップを有効にします。
disk-write	(オプション) ディスク書き込みエラー トラップを有効にします。
overload-bypass	(オプション) WCCP 過負荷バイパス エラー トラップを有効にします。
transaction-log	(オプション) トランザクション ログ書き込みエラー トラップを有効にします。
entity	(オプション) SNMP エンティティ トラップを有効にします。
event	(オプション) Event MIB トラップを有効にします。
snmp	(オプション) SNMP 固有トラップを有効にします。
authentication	(オプション) 認証トラップを有効にします。
cold-start	(オプション) コールドスタート トラップを有効にします。
wafs	(オプション) すべての WAFS 固有トラップを有効にします。
cslog	(オプション) CS ログ トラップを有効にします。
eslog	(オプション) ES ログ トラップを有効にします。
mgrlog	(オプション) Manager ログ トラップを有効にします。

デフォルト

このコマンドはデフォルトで無効に設定されています。どのトラップも有効になっていません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

特定のアラーム条件に対して SNMP トラップを生成するように WAAS デバイスを設定できます。次の事項に基づいて、WAAS デバイスに SNMP アラーム トラップ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、マイナー）
- 動作（アラームの発生またはクリア）

WAAS ソフトウェア リリースでは、CISCO-CONTENT-ENGINE-MIB で次の 6 つの汎用アラーム トラップが利用できます。

アラーム トラップの名前	重大度	動作
cceAlarmCriticalRaised	クリティカル	発生
cceAlarmCriticalCleared	クリティカル	クリア
cceAlarmMajorRaised	メジャー	発生
cceAlarmMajorCleared	メジャー	クリア
cceAlarmMinorRaised	マイナー	発生
cceAlarmMinorCleared	マイナー	クリア

**(注)**

デフォルトでは、この 6 つの汎用アラーム トラップは無効に設定されています。

この 6 つの汎用アラーム トラップは、SNMP と Node Health Manager の統合をもたらします。6 つの汎用アラーム トラップのそれぞれが、WAAS CLI を使用して有効または無効にできます。

トラップを設定するには、**snmp-server enable traps** コマンドを実行する必要があります。**snmp-server enable traps** コマンドを実行しないと、トラップは送信されません。

snmp-server enable traps コマンドは、**snmp-server host** コマンドと一緒に使用します。**snmp-server host** コマンドを使用して、SNMP トラップを受信するホストを 1 つまたは複数、指定します。トラップを送信するには、**snmp-server host** コマンドを使用して少なくとも 1 つホストを設定する必要があります。

トラップを受信するホストについては、**snmp-server enable traps** コマンドと **snmp-server host** コマンドの両方を、そのホストに対して有効にしておく必要があります。

また、SNMP は、**snmp-server community** コマンドで有効にしておく必要があります。

MIB-II SNMP 認証トラップの送信を無効にするには、**no snmp-server enable traps snmp authentication** コマンドを入力します。

例

次の例は、コミュニティ スtring public を使用して、WAAS デバイスがホスト 172.31.2.160 にすべてのトラップを送信できるようにします。

```
WAE(config)# snmp-server enable traps
WAE(config)# snmp-server host 172.31.2.160 public
```

次の例では、すべてのトラップを無効にします。

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

■ (config) snmp-server enable traps

関連コマンド

(config) snmp-server community
(config) snmp-server contact
(config) snmp-server group
(config) snmp-server host
(config) snmp-server location
(config) snmp-server mib persist event
(config) snmp-server notify inform
(config) snmp-server trap-source
(config) snmp-server user
(config) snmp-server view
snmp trigger

(config) snmp-server group

WAAS デバイスのユーザ セキュリティ モデル グループを定義するには、**snmp-server group** 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。指定したグループを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server 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]}}
```

シンタックスの説明

name	SNMP グループの名前。最大 64 文字まで使用できます。
v1	Version 1 セキュリティ モデルを使用するグループを指定します。
notify	(オプション) 通知、インフォーム、トラップの指定を可能にするグループの通知ビューを指定します。
name	通知ビューの名前。最大 64 文字まで使用できます。
read	(オプション) エージェントのコンテンツの表示だけを可能にするグループの読み取りビューを指定します。
name	読み取りビューの名前。最大 64 文字まで使用できます。
write	(オプション) データ入力とエージェントのコンテンツの設定を可能にするグループの書き込みビューを指定します。
name	書き込みビューの名前。最大 64 文字まで使用できます。
v2c	Version 2c セキュリティ モデルを使用するグループを指定します。
v3	ユーザ セキュリティ モデル (SNMPv3) を使用するグループを指定します。
auth	AuthNoPriv セキュリティ レベルを使用するグループを指定します。
noauth	noAuthNoPriv セキュリティ レベルを使用するグループを指定します。
priv	AuthPriv セキュリティ レベルを使用するグループを指定します。

デフォルト

デフォルトでは、ユーザ セキュリティ モデル グループは定義されていません。

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

作成できる SNMP グループの最大数は 10 です。

Version 1 (**v1**) セキュリティ モデル、Version 2c (**v2c**) セキュリティ モデル、またはユーザ セキュリティ モデル (**v3** または SNMPv3) の 3 つの SNMP セキュリティ モデル グループのいずれか 1 つを選択します。オプションで、選択した特定のセキュリティ モデルについて、グループの通知、読み取り、または書き込みビューを指定します。**v3** オプションを使用すると、**auth** (AuthNoPriv セキュリティ レベル)、**noauth** (noAuthNoPriv セキュリティ レベル)、または **priv** (AuthPriv セキュリティ レベル) のいずれか 1 つを使用してグループを指定できます。

■ (config) snmp-server group

例 次の例は、SNMP Version 1 セキュリティ モデルおよび通知にビュー名 *mymib* を使用するユーザ セキュリティ グループ *acme* を定義します。

```
WAE(config)# snmp-server group acme v1 notify mymib
```

関連コマンド

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server host

(config) snmp-server location

(config) snmp-server mib persist event

(config) snmp-server notify inform

(config) snmp-server trap-source

(config) snmp-server user

(config) snmp-server view

snmp trigger

(config) snmp-server host

ホスト SNMP トラップ操作の受信者を指定するには、**snmp-server 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。指定したホストを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server host {hostname|ip-address} communitystring [v2c [retry number] [timeout seconds]] | [v3
  {auth [retry number] [timeout seconds] | noauth [retry number] [timeout seconds] | priv [retry
  number] [timeout seconds]]]
```

シンタックスの説明

<i>hostname</i>	WAAE デバイスからの SNMP トラップ メッセージで送信される SNMP トラップ ホストのホスト名
<i>ip-address</i>	WAAS デバイスからの SNMP トラップ メッセージで送信される SNMP トラップ ホストの IP アドレス
<i>communitystring</i>	WAE からの SNMP トラップ メッセージで送信されるパスワード形式のコミュニティ ストリング。最大 64 文字まで入力できます。
v2c	(オプション) Version 2c セキュリティ モデルを指定します。
retry	(オプション) インフォーム要求の再試行回数を設定します (デフォルトは 2 回です)。
<i>number</i>	インフォーム要求の再試行回数 (1 ~ 10)
timeout	(オプション) インフォーム要求のタイムアウトを設定します (1 ~ 1000) (デフォルトは 15 秒です)。
<i>seconds</i>	タイムアウトの値 (秒単位)
v3	(オプション) ユーザ セキュリティ モデル (SNMPv3) を指定します。
auth	AuthNoPriv セキュリティ レベルを使用する通知を送信します。
noauth	noAuthNoPriv セキュリティ レベルを使用する通知を送信します。
priv	AuthPriv セキュリティ レベルを使用する通知を送信します。

デフォルト

このコマンドはデフォルトで無効に設定されています。どのトラップも送信されません。有効にした場合、トラップの送信に使用される SNMP プロトコルのデフォルトのバージョンは、SNMP Version 1 です。

retry number : 2 リトライ

timeout : 15 秒

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

snmp-server host コマンドを実行しないと、トラップは送信されません。WAAS デバイスが SNMP トラップを送信するように設定するには、少なくとも 1 度 **snmp-server host** コマンドを実行する必要があります。複数のホストを有効にするには、各ホストに対して別に **snmp-server host** コマンドを発行する必要があります。**snmp-server host** コマンドの最大数は 4 です。

■ (config) snmp-server host

同じホストに対して複数の **snmp-server host** コマンドが発行される場合は、直前のコマンドのコミュニティストリングが使用されます。

snmp-server host コマンドは、**snmp-server enable traps** コマンドと一緒に使用して SNMP トラップを有効にします。

また、SNMP は、**snmp-server community** コマンドで有効にしておく必要があります。

例

次の例は、RFC 1157 で規定された SNMP トラップを、IP アドレス 172.16.2.160 で指定されたホストに送信します。コミュニティストリングは **comaccess** です。

```
WAE(config)# snmp-server enable traps
WAE(config)# snmp-server host 172.16.2.160 comaccess
```

次の例は、SNMP トラップ受信者リストからホスト 172.16.2.160 を削除します。

```
WAE(config)# no snmp-server host 172.16.2.160
```

関連コマンド

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server location

(config) snmp-server mib persist event

(config) snmp-server notify inform

(config) snmp-server trap-source

(config) snmp-server user

(config) snmp-server view

snmp trigger

(config) snmp-server location

WAAS デバイスで SNMP システム位置文字列を設定するには、**snmp-server location** 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。位置文字列を削除するには、このコマンドの **no** 形式を使用します。

snmp-server location *line*

シンタックスの説明

location	MIB-II オブジェクト <i>sysLocation</i> のテキストを指定します。
<i>line</i>	このノードの物理的な位置を記述する文字列

デフォルト

システム位置文字列は設定されていません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

システム位置文字列は、MIB-II システム グループ システム位置オブジェクトに保存されている値です。システム位置文字列は、**show snmp EXEC** コマンドで確認できます。

例

次の例はシステム位置文字列を示します。

```
WAE(config)# snmp-server location Building 3/Room 214
```

関連コマンド

[\(config\) snmp-server community](#)
[\(config\) snmp-server contact](#)
[\(config\) snmp-server enable traps](#)
[\(config\) snmp-server group](#)
[\(config\) snmp-server host](#)
[\(config\) snmp-server mib persist event](#)
[\(config\) snmp-server notify inform](#)
[\(config\) snmp-server trap-source](#)
[\(config\) snmp-server user](#)
[\(config\) snmp-server view](#)
[snmp trigger](#)

(config) snmp-server mib persist event

SNMP Event MIB の永続性を設定するには、**snmp-server mib persist event** グローバル コンフィギュレーション コマンドを使用します。Event MIB を無効にするには、このコマンドの **no** 形式を使用します。

snmp-server mib persist event

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン Event MIB は、WAAS ソフトウェアによってサポートされている MIB 変数に対してしきい値を設定し、そのしきい値を永続的にディスクに保存できます。

WAAS ソフトウェアの SNMP の実装では、次に示す MIB をサポートします。

- ACTONA-ACTASTORE-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CDP-MIB
- CISCO-CONTENT-ENGINE-MIB (一部)
- CISCO-ENTITY-ASSET-MIB
- CISCO-SMI
- CISCO-TC
- ENTITY-MIB
- EVENT-MIB
- HOST-RESOURCES-MIB
- MIB-II
- SNMP-COMMUNITY-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMPv2
- SNMP-VACM-MIB



(注)

WAAS ソフトウェアでは、SNMP および Node Health Manager 統合の CISCO-CONTENT-ENGINE-MIB に 6 つの汎用アラーム トラップがあります。

WAAS ソフトウェアでは、IP ACL を使用して WAAS デバイスでの SNMP アクセスを制御できます。

WAE への MIB ファイルのダウンロード

次のシスコ FTP サイトから、WAAS ソフトウェア稼働の WAAS デバイスによってサポートされているすべての MIB の MIB ファイルをダウンロードできます。

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

各 MIB で定義されている MIB オブジェクトは、上記の FTP サイトにある MIB ファイル内に記述されているため、ここでは説明しません。

例

次の例は Event MIB の永続性を設定します。

```
WAE(config)# snmp-server mib persist event
```

関連コマンド

[\(config\) snmp-server community](#)

[\(config\) snmp-server contact](#)

[\(config\) snmp-server enable traps](#)

[\(config\) snmp-server group](#)

[\(config\) snmp-server host](#)

[\(config\) snmp-server location](#)

[\(config\) snmp-server notify inform](#)

[\(config\) snmp-server trap-source](#)

[\(config\) snmp-server user](#)

[\(config\) snmp-server view](#)

[snmp trigger](#)

(config) snmp-server notify inform

WAAS デバイスで SNMP 通知インフォーム要求を設定するには、**snmp-server notify inform** 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。設定をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

snmp-server notify inform

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト **snmp-server notify inform** コマンドを発行しない場合、デフォルトは SNMP トラップ要求です。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

例 次の例は、デフォルトの SNMP トラップに対して SNMP 通知インフォーム要求を設定します。
WAE(config)# **snmp-server notify inform**

関連コマンド

- [\(config\) snmp-server community](#)
- [\(config\) snmp-server contact](#)
- [\(config\) snmp-server enable traps](#)
- [\(config\) snmp-server group](#)
- [\(config\) snmp-server host](#)
- [\(config\) snmp-server location](#)
- [\(config\) snmp-server mib persist event](#)
- [\(config\) snmp-server trap-source](#)
- [\(config\) snmp-server user](#)
- [\(config\) snmp-server view](#)
- [snmp trigger](#)

(config) snmp-server trap-source

WAAS デバイスから SNMP トラップ メッセージを送信するのに使用されるネットワーク インターフェイスを設定するには、**snmp-server trap-source** 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。設定されたトラップソースを削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server trap-source {GigabitEthernet 1-2/port | PortChannel 1-2 | Standby group_num}
```

シンタックスの説明

GigabitEthernet	SNMP トラップ メッセージを送信するためのトラップ ソースとして、ギガビット イーサネット インターフェイスの IP を選択します。
<i>1-2/</i>	ギガビット イーサネットのスロット番号 1 または 2
<i>port</i>	ギガビット イーサネット インターフェイスのポート番号
PortChannel	SNMP トラップ メッセージを送信するためのトラップ ソースとして、ポート チャネル インターフェイスの IP を選択します。
<i>1-2</i>	ポート チャネル番号 1 または 2
Standby	SNMP トラップ メッセージを送信するためのトラップ ソースとして、ギガビット イーサネット インターフェイスの IP を選択します。
<i>group_num</i>	スタンバイ グループ番号 (1 ~ 4)

デフォルト

プライマリ インターフェイスの IP は、SNMP トラップを送信するためのデフォルト トラップ ソースとして使用されます。プライマリ インターフェイスが設定されていない場合は、WAAS デバイスのローカル IP アドレスがトラップ ソースとして使用されます。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

snmp-server trap-source 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、SNMP トラップ メッセージ内でトラップソースとして含まれる IP アドレスを持つインターフェイスを指定できます。トラップソース インターフェイスを変更するには、異なるネットワーク インターフェイスを使用してコマンドを再入力します。

WAAS デバイス上に設定済みのトラップソース インターフェイスがない場合、WAAS デバイスの現在のプライマリ インターフェイスの IP アドレスが使用されます。プライマリ インターフェイスが設定されていない場合は、WAAS デバイスのローカル IP アドレスがトラップ ソースとして使用されます。

例

次の例は、ギガビット イーサネット スロット 1 ポート 0 を WAAS デバイスの SNMP トラップソース インターフェイスとして設定する方法を示します。

```
WAE(config)# snmp-server trap-source GigabitEthernet 1/0
```

■ (config) snmp-server trap-source

次の例は、ギガビットイーサネット スロット 2 ポート 0 を WAAS デバイスの SNMP トラップソース インターフェイスとして設定する方法を示します。

```
WAE(config)# snmp-server trap-source GigabitEthernet 2/0
```

関連コマンド

(config) snmp-server community

(config) snmp-server contact

(config) snmp-server enable traps

(config) snmp-server group

(config) snmp-server host

(config) snmp-server location

(config) snmp-server mib persist event

(config) snmp-server notify inform

(config) snmp-server user

(config) snmp-server view

snmp trigger

(config) snmp-server user

SNMP サーバにアクセスできるユーザを定義するには、**snmp-server user** グローバル コンフィギュレーション コマンドを使用します。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]}]]
```

シンタックスの説明

<i>name</i>	SNMP ユーザの名前。文字、数字、ダッシュ、および下線を使用できますが、空白は使用できません。これは、WAAS デバイスの SNMP エージェントと通信する SNMP ホスト上のユーザの名前です。最大 64 文字まで入力できます。
<i>group</i>	SNMP ユーザが所属するグループの名前。最大 64 文字まで入力できます。
auth	(オプション) ユーザ認証パラメータを設定します。
md5	HMAC MD5 認証アルゴリズムを設定します。
<i>password</i>	HMAC-MD5 ユーザ認証パスワード
priv	(オプション) パケットの認証パラメータを設定します。
<i>password</i>	HMAC-MD5 ユーザプライベートパスワード。最大 256 文字まで入力できます。
sha	HMAC-SHA 認証アルゴリズムを設定します。
<i>password</i>	HMAC-SHA 認証パスワード。最大 256 文字まで入力できます。
remote	(オプション) ユーザが所属するリモート SNMP エンティティのエンジン ID を指定します。
<i>octetstring</i>	最低限 1 人の SNMP ユーザに対する、リモート SNMP エンティティ用のグローバルに一意の ID (たとえば、SNMP ネットワーク管理ステーション)



ヒント

SNMPv3 インフォーム メッセージを送信するには、リモート SNMP ID オプションを持った最低限 1 人の SNMPv3 ユーザが、WAAS デバイスに設定されている必要があります。SNMP ID はオクテット文字列形式で入力します。たとえば、リモート SNMP エンティティの IP アドレスが 192.147.142.129 である場合、オクテット文字列は 00:00:63:00:00:00:a1:c0:93:8e:81 になります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

WAAS デバイス用に SNMP ユーザを定義する場合、次の点に注意してください。

- SNMPv3 プロトコルを SNMP 要求用に使用する場合は、WAAS デバイスが SNMP を介してアクセスされるため、最低限 1 つの SNMPv3 ユーザ アカウントを WAAS デバイス上に設定する必要があります。

(config) snmp-server user

- SNMPv1 または SNMPv2c セキュリティ モデルで定義されたグループは、SNMP ユーザと関連付けしてはなりません。コミュニティ ストリングとのみ、関連付けてください。

例

次の例では、WAAS デバイスに SNMPv3 ユーザ アカウントを作成します。SNMPv3 ユーザは *acme* という名前で、*admin* というグループに所属しています。この SNMP ユーザ アカウントは認証パスワードなしで設定されているため、WAAS デバイス上の SNMP エージェントはこのユーザからの SNMP 要求に対する認証を実行しません。

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

関連コマンド

[\(config\) snmp-server community](#)

[\(config\) snmp-server contact](#)

[\(config\) snmp-server enable traps](#)

[\(config\) snmp-server group](#)

[\(config\) snmp-server host](#)

[\(config\) snmp-server location](#)

[\(config\) snmp-server mib persist event](#)

[\(config\) snmp-server notify inform](#)

[\(config\) snmp-server trap-source](#)

[\(config\) snmp-server view](#)

[snmp trigger](#)

(config) snmp-server view

WAAS デバイスの SNMPv2 MIB ビューを定義するには、**snmp-server view** 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。MIB ビューの定義を削除するには、このコマンドの **no** 形式を使用します。

```
snmp-server view viewname MIBfamily {excluded | included}
```

シンタックスの説明

<i>viewname</i>	このビュー サブツリー ファミリの名前。最大 64 文字まで入力できます。
<i>MIBfamily</i>	MIB のサブツリーを識別するオブジェクトの ID。最大 64 文字まで入力できます。
excluded	ビューから MIB ファミリを除外します。
included	ビューに MIB ファミリを入れます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

例

次の例は SNMPv2 MIB ビューを定義します。

```
WAE(config)# snmp-server view fileview ciscoFileEngineMIB included
```

関連コマンド



[\(config\) snmp-server community](#)
[\(config\) snmp-server contact](#)
[\(config\) snmp-server enable traps](#)
[\(config\) snmp-server group](#)
[\(config\) snmp-server host](#)
[\(config\) snmp-server location](#)
[\(config\) snmp-server mib persist event](#)
[\(config\) snmp-server notify inform](#)
[\(config\) snmp-server trap-source](#)
[\(config\) snmp-server user](#)
[snmp trigger](#)

(config) sshd

WAAS デバイスで SSH デーモンを有効にするには、グローバル コンフィギュレーション モードで **sshd** コマンドを使用します。WAAS デバイスで SSH デーモンを無効にするには、このコマンドの **no** 形式を使用します。

```
sshd {allow-non-admin-users | enable | password-guesses number | timeout seconds |
      version {1 | 2}}
```

シンタックスの説明

allow-non-admin-users	非管理ユーザが選択したデバイス（またはデバイス グループ）に SSH アクセスできるようにします。デフォルトでは、このオプションは無効に設定されています。
	 (注) 非管理ユーザとは非スーパーユーザ管理者です。非スーパーユーザ管理者はログイン アカウントが特権レベル 0 であるため、WAAS デバイスには制限されたアクセスしかできません。スーパーユーザ管理者は最高レベルの特権（特権レベル 15）のログイン アカウントを持っているため、WAAS デバイスに完全にアクセスできます。
enable	WAAS デバイス上で SSH デーモンを有効にします。
password-guesses	接続当たりの許容パスワード推測数を指定します。
<i>number</i>	許容される不正パスワード推測の最大数（1 ～ 99）（デフォルトは 3 秒です）。
timeout	クライアントとサーバ間のネゴシエーション（認証）フェーズの間、タイムアウトするまでに SSH セッションがアクティブな秒数を設定します。
	 (注) WAAS デバイスに SSH 接続を確立し、ログインプロンプトで要求されたときにユーザ名を入力しなかった場合、正常なログイン後でも、猶予期間が期限切れしていれば、WAAS デバイスによって接続が打ち切られます。
<i>seconds</i>	秒単位の SSH ログイン猶予期間の値（1 ～ 99999）（デフォルトは 300 秒です）。
version	その SSH バージョンが WAAS デバイスでサポートされるように設定します。
1	SSH バージョン 1 を WAAS デバイスでサポートするように指定します。
2	SSH バージョン 2 を WAAS デバイスでサポートするように指定します。

デフォルト

デフォルトでは、WAAS デバイスの SSH デーモンは無効に設定されています。**sshd enable** コマンドを使用して WAAS デバイスで SSH デーモンを有効にした場合、次のデフォルト設定が使用されます。

password-guesses number : 3 つの推測

timeout seconds : 300 秒

version : SSH バージョン 1 および 2 の両方が有効

コマンドモード グローバル コンフィギュレーション

デバイスモード application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

SSH は、安全で暗号化されたチャネルを介して WAAS デバイスにログインアクセスできるようにします。SSH は、サーバとクライアント プログラムで構成されます。Telnet と同様、クライアント プログラムを使用して SSH サーバが稼働するマシンにリモートでログインできますが、クライアントとサーバ間を転送されるメッセージが暗号化される点が Telnet と異なります。SSH の機能には、ユーザ認証、メッセージの暗号化、およびメッセージ認証があります。

sshd コマンドを有効にする前に、**ssh-key-generate** コマンドを使用して秘密および公開のホストキーを作成します。クライアント プログラムは、このキーを使用してサーバの ID を確認します。

sshd password-guesses コマンドでは SSH サーバ側から許容パスワード推測数を指定しますが、SSH ログインセッションの実際のパスワード推測数は、SSH サーバおよび SSH クライアントの許容パスワード推測数を組み合わせたもので決まります。SSH サーバ側で推測数 3 を超えて許容している場合でも、一部の SSH クライアントは、許容パスワード推測数を 3 (場合によっては 1) に制限します。

sshd password-guesses を入力する際、許容パスワード推測数 n を入力すると、特定の SSH クライアントはこの数値を $n+1$ として解釈します。たとえば、特定のデバイスに対してコマンド **sshd password-guesses 2** を発行して推測数を 2 に設定すると、一部の SSH クライアントの SSH セッションは推測数 3 回を許可します。

SSH バージョン 1 およびバージョン 2 の両方を有効にできます。また 1 つのバージョンを有効にし、もう一方のバージョンを無効にすることもできます。**sshd enable** 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、SSH デーモンを有効にすると、SSH バージョン 1 および SSH バージョン 2 の両方のサポートが有効になります。WAAS デバイスに SSH の一方のバージョンだけ (たとえば SSH バージョン 2) をサポートさせるには、もう一方のバージョンを無効にする必要があります。たとえば、SSH バージョン 1 を無効にするには、**no sshd version 1** コマンドを入力します。

WAAS デバイスで SSH デーモンが現在有効になっている場合、デバイスで少なくとも 1 つの SSH バージョンを有効にする必要があります。SSH の両方のバージョンを無効にする前に、**no sshd enable** コマンドを入力して WAAS デバイス上の SSH デーモンを無効にする必要があります。SSH デーモンを無効にする前に SSH の両方のバージョンを無効にしようとする、SSH の両方のバージョンを無効にする前に SSH デーモンを無効にするよう要求する次のメッセージがコンソールに表示されます。

```
WAE(config)# no sshd version 1
WAE(config)# no sshd version 2
Atleast SSHv1 or SSHv2 must be enabled with sshd enabled.
Disable sshd to disable both SSHv1 and SSHv2.
Did not update ssh version support. Please retry.
```

WAAS デバイスで SSH バージョン 1 および SSH バージョン 2 の両方のサポートが有効な場合、**show running-config EXEC** コマンドの出力には SSHD 設定が表示されません。

SSH の一方のバージョンのサポートを無効にした場合、**show running-config EXEC** コマンドの出力には次の行が表示されます。

```
no sshd version version_number
```

**(注)**

Telnet デーモンは今までもおり WAAS デバイスで利用できます。SSH は Telnet に取って代わるものではありません。

例

次の例は、WAAS デバイスで Secure Shell デーモンを有効にして設定します。

```
WAE(config)# sshd enable
WAE(config)# sshd password-guesses 4
WAE(config)# sshd timeout 20
```

次の例は、WAAS デバイスの SSH バージョン 1 のサポートを無効にします。

```
WAE(config)# no sshd version 1
```

関連コマンド[\(config\) ssh-key-generate](#)

(config) ssh-key-generate

WAAS デバイスの SSH ホスト キーを生成するには、**ssh-key-generate** 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。SSH キーを削除するには、このコマンドの **no** 形式を使用します。

```
ssh-key-generate [key-length length]
```

シンタックスの説明

key-length	(オプション) SSH キーの長さを設定します。
length	SSH キー作成のビット数 (512 ~ 2048)

デフォルト

key-length length : 1024 ビット

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

sshd enable コマンドを入力にする前に、**ssh-key-generate** コマンドを入力して秘密および公開のホスト キーを作成します。クライアント プログラムは、このキーを使用してサーバの ID を確認します。

SSH クライアントを使用して WAAS デバイスにログインすると、デバイス上で稼働する SSH デーモンの公開鍵がクライアント マシンのホーム ディレクトリにある `known_hosts` ファイルに記録されます。その後、**key-length** コマンド オプションでビット数を指定してホスト キーを再生成した場合、`known_hosts` ファイルにある WAAS デバイスに関連付けられた古い公開鍵のエントリを削除してから、SSH クライアント プログラムを実行して WAAS デバイスにログインする必要があります。古いエントリの削除後、クライアント プログラムを実行すると、`known_hosts` ファイルが WAAS デバイスの新しい SSH 公開鍵でアップデートされます。

例

次の例は、WAAS デバイスで SSH 公開鍵を作成し、その後 SSH デーモンを有効にします。

```
WAE(config)# ssh-key-generate
Ssh host key generated successfully
Saving the host key to box ...
Host key saved successfully
WAE(config)# sshd enable
Starting ssh daemon ...
Ssh daemon started successfully
```

関連コマンド

(config) [sshd](#)

(config) tacacs

WAAS デバイスで TACACS+ サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **tacacs** コマンドを使用します。個々のオプションを無効にするには、このコマンドの **no** 形式を使用します。

```
tacacs {host {hostname | ip-address} [primary] | key keyword | password ascii | retransmit retries |
        timeout seconds}
```

シンタックスの説明

host	サーバアドレスを指定します。
<i>hostname</i>	TACACS+ サーバのホスト名
<i>ip-address</i>	TACACS+ サーバの IP アドレス
primary	(オプション) サーバをプライマリ サーバとして設定します。
key	セキュリティワードを設定します。
<i>keyword</i>	キーワード。空の文字列がデフォルトです。
password ascii	TACACS+ パスワードタイプとして ASCII を指定します。
retransmit	サーバに要求が再送信される回数を設定します。
<i>retries</i>	許容される試行数 (1 ~ 3)。デフォルトは 2 回です。
timeout	サーバへの要求がタイムアウトするまで待機する秒数を設定します。
<i>seconds</i>	秒単位でのタイムアウト (1 ~ 20)。デフォルトは 5 秒です。

デフォルト

keyword : なし (空の文字列)

timeout seconds : 5 秒

retries : 2

password : デフォルトのパスワードタイプは PAP

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

WAAS デバイスで 1 つのプライマリ TACACS+ サーバと、2 つのバックアップ TACACS+ サーバを設定できます。認証は最初にプライマリ サーバで試行され、次に設定された順序でその他のサーバで試行されます。プライマリ サーバとは、別のサーバが **tacacs host hostname primary** コマンドで明示的にプライマリとして指定されていないかぎり、最初に設定されたサーバです。

TACACS+ は、指定されたサービスに基づいて、標準ポート (ポート 49) を通信に使用します。**tacacs** コマンドを使用すると、TACACS+ キー、再送信回数、サーバのホスト名または IP アドレス、およびタイムアウトを設定できます。

TACACS+ サーバでのユーザ認証を有効にするには、**authentication** 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 ([**(config) authentication**] コマンドを参照)。

また、TACACS+ リモート データベースは、管理ユーザのログインおよび設定権限を管理できます。**tacacs host** コマンドにより、リモート データベースのアクセスに必要なネットワーク パラメータを設定できます。

TACACS+ キーは **tacacs key** コマンドを使用して指定します。このキーはサーバに送信するパケットの暗号化に使用します。このキーは、サーバデーモンで指定したのと同じである必要があります。キーの最大文字数は、印字可能 ASCII 文字（タブは除く）で 99 文字を超えてはなりません。空のキー文字列がデフォルトです。先頭のスペースはすべて無視されます。キー文字列の内部とキーの終わりのスペースは無視されません。キー内にスペースがある場合でも二重引用符は不要です。ただし、引用符自体がキーの一部である場合を除きます。

tacacs timeout は、WAAS デバイスが特定の TACACS+ サーバへの要求に関して タイムアウトを宣言するまで待機する秒数です。指定できる範囲は 1 ~ 20 秒で、5 秒がデフォルトです。WAAS デバイスが、次の TACACS+ サーバを試行するまでに、リトライタイムアウトのサイクルを繰り返す回数は、**tacacs retransmit** コマンドによって指定します。デフォルトは 2 回の試行です。

ログインの失敗は 3 回まで許可されています。TACACS+ のログインは、TACACS+ サーバの数や設定されたタイムアウトおよびリトライの数によっては、ローカルのログインより時間がかかる場合があります。

tacacs password ascii コマンドを使用して、TACACS+ のパスワード タイプを ASCII として指定します。デフォルトのパスワード タイプは Password Authentication Protocol (PAP; パスワード認証プロトコル) です。**no tacacs password ascii** コマンドを使用して ASCII パスワード タイプが無効にされると、パスワード タイプは再度 PAP にリセットされます。

TACACS+ クライアントは、ユーザ認証について別の要求をサーバに送付できます。クライアントは、PAP パスワード タイプで要求を TACACS+ に送付できます。この状況では、認証パケットにはユーザ名とユーザのパスワードの両方が含まれています。サーバは、適切に設定されたユーザのアカウントを備えている必要があります。

あるいは、クライアントは、別の方法として ASCII パスワード タイプで要求を TACACS+ に送付できます。この状況では、認証パケットにはユーザ名だけが含まれ、サーバの応答を待機します。サーバがユーザのアカウントが存在することを確認すると、クライアントはそのユーザのパスワードで別の Continue 要求を送付します。認証サーバは、どちらのタイプのパスワードもサポートするため、適切に設定されたユーザのアカウントを備えている必要があります。

例

次の例は、暗号化パケットで使用されるキーを設定します。

```
WAE(config)# tacacs key human789
```

次の例は、spearhead という名前のホストを、プライマリ TACACS+ サーバとして設定します。

```
WAE(config)# tacacs host spearhead primary
```

次の例は、TACACS+ サーバのタイムアウト インターバルを設定します。

```
WAE(config)# tacacs timeout 10
```

次の例では、タイムアウト後の、認証要求のリトライ（再送信）の回数を設定します。

```
WAE(config)# tacacs retransmit 5
```

次の例では、パスワードタイプがデフォルトで PAP であることが示されます。

```
WAE# show tacacs
Login Authentication for Console/Telnet Session: enabled (secondary)
Configuration Authentication for Console/Telnet Session: enabled (secondary)

TACACS+ Configuration:
-----
TACACS+ Authentication is off
Key          = *****
Timeout      = 5
Retransmit   = 2
Password type: pap

Server                               Status
-----
10.107.192.148                        primary
10.107.192.168
10.77.140.77
```

tacacs password ascii コマンドを使用して、パスワードタイプを ASCII に設定できます。次に、**show tacacs** コマンドでその変更を確認できます。

```
WAE(config)# tacacs password ascii
WAE(config)# exit
WAE# show tacacs
Login Authentication for Console/Telnet Session: enabled (secondary)
Configuration Authentication for Console/Telnet Session: enabled (secondary)

TACACS+ Configuration:
-----
TACACS+ Authentication is off
Key          = *****
Timeout      = 5
Retransmit   = 2
Password type: ascii

Server                               Status
-----
10.107.192.148                        primary
10.107.192.168
10.77.140.77
```

関連コマンド

[\(config\) authentication](#)

[show authentication](#)

[show statistics authentication](#)

[show statistics tacacs](#)

[show tacacs](#)

(config) tcp

WAAS デバイスで TCP パラメータを設定するには、**tcp** 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。TCP パラメータを無効にするには、このコマンドの **no** 形式を使用します。

tcp cwnd-base *segments*

tcp ecn enable

tcp increase-xmit-timer-value *value*

tcp init-ss-threshold *value*



tcp keepalive-probe-cnt *count*

tcp keepalive-probe-interval *seconds*

tcp keepalive-timeout *seconds*

tcp memory-limit low-water-mark *low high-water-mark-pressure* *high high-water-mark-absolute*
absolute

シンタックスの説明

cwnd-base	初期送信輻輳ウィンドウをセグメント単位で設定します。
<i>segments</i>	初期送信輻輳ウィンドウセグメント (1 ~ 10)
ecn enable	TCP 明示的輻輳通知を有効にします。
increase-xmit-timer-value	TCP アルゴリズムによって決定された基準値を 1 ~ 3 倍することで、再送信タイマーの長さを修正するのに使用する係数 (1 ~ 3) を指定します。
	 (注) この係数を修正する場合は注意してください。TCP が低速の信頼性の高い接続で使用される場合は、スループットを向上させられます。ただし、信頼性のないパケット配信環境では変更しないでください。
<i>value</i>	再送信係数 (1 ~ 3)
init-ss-threshold	初期スロースタートしきい値を設定します。
<i>value</i>	スロースタートしきい値
keepalive-probe-cnt	WAAS デバイスがアイドル接続を開いたままにする時間の長さを指定します。
<i>count</i>	プローブ カウント数 (1 ~ 10)
keepalive-probe-interval	WAAS デバイスが接続をリトライする回数を指定します。
<i>seconds</i>	秒単位のキープアライブ プローブ インターバル (1 ~ 300)
keepalive-timeout	WAAS デバイスが接続を切断するまで開いたままにする時間の長さを指定します。
<i>seconds</i>	秒単位でのキープアライブ タイムアウト (1 ~ 3600)
memory-limit	システムの TCP メモリ使用限度 (すべての接続の送信および受信バッファ使用を含む) を指定します。
	 注意 TCP バッファ オーバーフローを防止するため、手順が確かでないかぎりデフォルト値を変更しないでください。

low-water-mark	これより低いと TCP がメモリ プレッシャ モードから出て通常のメモリ割り当てモードに入るメモリ使用限度 (MB 単位) を指定します。
<i>low</i>	MB 単位のメモリ使用状況 (4 ~ 600)
high-water-mark-pressure	これより高いと TCP が通常のメモリ割り当てモードを出てメモリ プレッシャ モードに入るメモリ使用限度 (MB 単位) を指定します。
<i>high</i>	MB 単位のメモリ使用状況 (5 ~ 610)
high-water-mark-absolute	TCP のメモリ使用状況 (MB 単位) の絶対ハード限界を指定します。
<i>absolute</i>	MB 単位のメモリ使用状況 (6 ~ 620)

デフォルト

tcp cwnd-base : 2 2

tcp increase-xmit-timer-value : 1 1

tcp init-ss-threshold : 2 セグメント

tcp keepalive-probe-interval : 4 4

tcp keepalive-probe-interval : 75 秒

tcp keepalive-timeout : 90 秒

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

TCP スタック パラメータを微調整して、キャッシュのパフォーマンスおよび TCP エンドツーエンドでの HTTP ストリームのスループットを最大化できます。キャッシュのパフォーマンスとスループットの最大化のための関連 TCP パラメータには、タイムアウト時間、クライアントとサーバの受信および送信バッファ サイズ、TCP ウィンドウのスケーリング動作を調整する機能が含まれています。

**(注)**

TCP パラメータに伴う複雑性のため、このパラメータの調整には細心の注意を払ってください。ほぼすべての環境では、デフォルトの TCP 設定で十分です。TCP 設定の微調整は、経験が豊富で、TCP 運用の詳細事項を完全に理解しているネットワーク管理者を対象としています。詳細については、『Cisco Wide Area Application Services Configuration Guide』を参照してください。

tcp keepalive-probe-cnt 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、WAAS デバイスが接続を閉じるまでにデバイスへの接続を試行する回数を指定します。回数は 1 ~ 10 の範囲で指定でき、デフォルトは 4 回の試行です。

WAAS デバイスが TCP キープアライブを送出する頻度は、**tcp keepalive-probe-interval** 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指定します。インターバルは 1 ~ 120 秒の範囲で指定できます。デフォルトは 75 秒です。

WAAS デバイスが失敗をログに記録するまで応答を待機する（デバイスが応答しない）期間を、**tcp keepalive-timeout** 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指定します。タイムアウトは 1 ～ 120 秒の範囲で指定できます。デフォルトは 90 秒です。

例

次の例は、TCP の明示的輻輳通知を有効にします。

```
WAE(config)# tcp ecn enable
```

次の例は、最低水準メモリ使用を 100 MB、最高水準メモリ使用を 450 MB および絶対最高水準メモリ使用を 500 MB に指定します。

```
WAE(config)# tcp memory-limit low-water-mark 100 high-water-mark-pressure 450  
high-water-mark-absolute 500
```

関連コマンド

[clear](#)

[show statistics tcp](#)

[show tcp](#)

(config) telnet enable

WAAS デバイスで Telnet を有効にするには、**telnet enable** 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。

telnet enable

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトでは、Telnet サービスは WAAS デバイスで有効になっています。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン WAAS デバイスでの Telnet セッションの開始にはターミナル エミュレーション ソフトウェアを使用します。

WAAS デバイス上でデバイス ネットワーク設定を定義するには Telnet セッションの代わりにコンソール接続を使用する必要があります。ただし、コンソール接続を使用してデバイス ネットワーク設定を定義した後は、Telnet セッションを使用して以降の設定作業を実行できます。



(注) クライアントとデバイス間で転送されるメッセージは暗号化されません。

例 次の例は、WAAS デバイスで Telnet の使用を有効にします。

```
WAE(config)# telnet enable
```

関連コマンド [telnet](#)
[show telnet](#)

(config) tfo auto-discovery

セットアップ オプション付きの TCP パケットを受信できないオリジン サーバ（ファイアウォールの背後にあるサーバなど）を自動的に検出し、指定した時間（分数）、サーバの IP アドレスをブラックリストに追加するように WAE を設定するには、**tfo auto-discovery blacklist** 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。TFO 自動ディスカバリを無効にするには、このコマンドの **no** 形式を使用します。

tfo auto-discovery [blacklist] {enable | hold-time *minutes*}

シンタックスの説明

enable	TFO 自動ディスカバリ機能をアクティブ化します。
blacklist enable	TFO 自動ディスカバリ ブラックリスト機能をアクティブ化します。
blacklist hold-time	ブラックリストに追加されたサーバのアドレスをキャッシュで保持する最大時間を指定します。
<i>minutes</i>	サーバのブラックリスト エントリを保持する分数。範囲は 1 ～ 10080 分です。デフォルトは 60 分です。

デフォルト

デフォルトの TFO 自動検出ブラックリストの保持時間は、60 分です。

コマンドモード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

TFO 自動ディスカバリ機能のブラックリストの保持時間を調整するには、**tfo auto-discovery blacklist hold-time** コマンドを使用します。自動ディスカバリを使用すると、WAE は、オプション付きの TCP パケットを受信できないオリジン サーバ（ファイアウォールの背後にあるサーバなど）を追跡し、ブラックリストに追加されたサーバにオプション付きの TCP パケットを送信しないことを学習します。サーバの IP アドレスがブラックリストに追加されると、設定された時間（分数）、そのアドレスがブラックリストに保持されます。保持時間が満了すると、後続の接続が再び TCP オプションを追加しようとするので、WAE はサーバがこれらのオプションを受信できるかどうかを再決定します。ネットワーク パケットの損失によってサーバが誤ってブラックリストに追加されることがあるので、定期的に TCP オプションを再送信することは実用的です。

関連コマンド

[show statistics tfo](#)

[show tfo status](#)

(config) tfo optimize

Traffic Flow Optimization (TFO) 用に WAE を設定するには、**tfo optimize** 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。TFO 最適化を無効にするには、このコマンドの **no** 形式を使用します。

tfo optimize {DRE {yes | no} compression {LZ | none} | full}

シンタックスの説明

DRE	Data Redundancy Elimination (DRE) を行う、または行わない TFO 最適化を設定します。
yes	DRE を有効にします。
no	DRE を無効にします。
compression	一般的な圧縮を行う、または行わない TFO 最適化を設定します。
LZ	Lempel-Ziv (LZ) 圧縮を行う TFO 最適化を設定します。
none	圧縮を行う TFO 最適化を設定します。
full	DRE および LZ 圧縮を行う TFO 最適化を設定します。このキーワードを使用することは、 tfo optimize DRE yes compression LZ コマンドを指定することと同じことです。

デフォルト

WAAS デバイスのデフォルトの TFO 最適化は **tfo optimize full** です。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

関連コマンド

[show statistics tfo](#)

[show tfo bufpool](#)

[show tfo status](#)

(config) tfo tcp keepalive

Traffic Flow Optimization (TFO) 最適化用 WAE で TCP キープアライブを設定するには、**tfo tcp keepalive** 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。

tfo tcp keepalive

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト キープアライブはデフォルトで無効に設定されています。

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator

使用上のガイドライン このコマンドは TFO 最適化ソケット (2 つのピア WAE 間の接続) 上の TCP キープアライブを有効にします。

関連コマンド

- [\(config\) tfo tcp optimized-mss](#)
- [\(config\) tfo tcp optimized-receive-buffer](#)
- [\(config\) tfo tcp optimized-send-buffer](#)
- [\(config\) tfo tcp original-mss](#)
- [\(config\) tfo tcp original-receive-buffer](#)
- [\(config\) tfo tcp original-send-buffer](#)

(config) tfo tcp optimized-mss

Traffic Flow Optimization (TFO) 最適化用 WAE で最適化側の TCP 最大セグメント サイズを設定するには、**tfo tcp optimized-mss** 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。

tfo tcp optimized-mss *segment-size*

シンタックスの説明

segment-size セグメント サイズ (512 ~ 1460)

デフォルト

セグメント サイズのデフォルト値は 1432 バイトです。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

このコマンドは TFO 最適化ソケット (2 つのピア WAE 間の接続) 上の TCP 最大セグメント サイズを設定します。

関連コマンド

[\(config\) tfo tcp keepalive](#)
[\(config\) tfo tcp optimized-receive-buffer](#)
[\(config\) tfo tcp optimized-send-buffer](#)
[\(config\) tfo tcp original-mss](#)
[\(config\) tfo tcp original-receive-buffer](#)
[\(config\) tfo tcp original-send-buffer](#)

(config) tfo tcp optimized-receive-buffer

Traffic Flow Optimization (TFO) 最適化用 WAE で最適化側の受信バッファを設定するには、**tfo tcp optimized-receive-buffer** 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。

```
tfo tcp optimized-receive-buffer buffer-size
```

シンタックスの説明	<i>buffer-size</i>	キロバイトの受信バッファ サイズ
-----------	--------------------	------------------

デフォルト	3232 KB
-------	---------

コマンド モード	グローバル コンフィギュレーション
----------	-------------------

デバイス モード	application-accelerator
----------	-------------------------

使用上のガイドライン	<p>このコマンドは TFO 最適化ソケット (2 つのピア WAE 間の接続) 上の TCP 受信バッファ サイズを設定します。帯域遅延積 (BDP) の高いリンクでは、デフォルトより大きい値を使用すべきです。バッファは BDP 以上が必要です。BDP は 帯域幅 (ビット / 秒) * 遅延 (秒) に相当します。たとえば、ラウンドトリップ遅延が 150 ms (0.15 秒) の 45 Mbps リンクの場合、BDP は 45 Mbps * 0.15 秒 = 6.75 Mb、すなわち 0.844 MB (844 KB) です。この場合、バッファ サイズは 1024 KB に設定できます。</p>
------------	--

関連コマンド	<p>(config) tfo tcp keepalive</p> <p>(config) tfo tcp optimized-mss</p> <p>(config) tfo tcp optimized-send-buffer</p> <p>(config) tfo tcp original-mss</p> <p>(config) tfo tcp original-receive-buffer</p> <p>(config) tfo tcp original-send-buffer</p>
--------	---

(config) tfo tcp optimized-send-buffer

Traffic Flow Optimization (TFO) 最適化用 WAE で最適化側の送信バッファを設定するには、**tfo tcp optimized-send-buffer** 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。

tfo tcp optimized-send-buffer *buffer-size*

シンタックスの説明	<i>buffer-size</i> キロバイトの送信バッファ サイズ
デフォルト	32 KB
コマンド モード	グローバル コンフィギュレーション
デバイス モード	application-accelerator
使用上のガイドライン	<p>このコマンドは TFO 最適化ソケット (2 つのピア WAE 間の接続) 上の TCP 送信バッファ サイズを設定します。帯域遅延積 (BDP) の高いリンクでは、デフォルトより大きい値を使用すべきです。バッファは BDP 以上が必要です。BDP は 帯域幅 (ビット / 秒) * 遅延 (秒) に相当します。たとえば、ラウンドトリップ遅延が 150 ms (0.15 秒) の 45 Mbps リンクの場合、BDP は 45 Mbps * 0.15 秒 = 6.75 Mb、すなわち 0.844 MB (844 KB) です。この場合、バッファ サイズは 1024 KB に設定できます。</p>
関連コマンド	<p>(config) tfo tcp keepalive</p> <p>(config) tfo tcp optimized-mss</p> <p>(config) tfo tcp optimized-receive-buffer</p> <p>(config) tfo tcp original-mss</p> <p>(config) tfo tcp original-receive-buffer</p> <p>(config) tfo tcp original-send-buffer</p>

(config) tfo tcp original-mss

Traffic Flow Optimization (TFO) 最適化用 WAE で非最適化側の TCP 最大セグメントサイズを設定するには、**tfo tcp original-mss** 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。

tfo tcp original-mss *segment-size*

シンタックスの説明

segment-size セグメント サイズ (512 ~ 1460)

デフォルト

1432 バイト

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

このコマンドは TFO 非最適化ソケット (WAE とクライアント間または WAE とサーバ間の接続) 上の TCP 最大セグメントサイズを設定します。

関連コマンド

[\(config\) tfo tcp keepalive](#)

[\(config\) tfo tcp optimized-mss](#)

[\(config\) tfo tcp optimized-receive-buffer](#)

[\(config\) tfo tcp optimized-send-buffer](#)

[\(config\) tfo tcp original-receive-buffer](#)

[\(config\) tfo tcp original-send-buffer](#)

(config) tfo tcp original-receive-buffer

Traffic Flow Optimization (TFO) 最適化用 WAE で非最適化側の受信バッファを設定するには、**tfo tcp original-receive-buffer** 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。

```
tfo tcp original-receive-buffer buffer-size
```

シンタックスの説明	<i>buffer-size</i> キロバイトの受信バッファ サイズ
デフォルト	32 KB
コマンド モード	グローバル コンフィギュレーション
デバイス モード	application-accelerator
使用上のガイドライン	このコマンドは TFO 非最適化ソケット (WAE とクライアント間または WAE とサーバ間の接続) 上の TCP 受信バッファ サイズを設定します。
関連コマンド	<p>(config) tfo tcp keepalive</p> <p>(config) tfo tcp optimized-mss</p> <p>(config) tfo tcp optimized-receive-buffer</p> <p>(config) tfo tcp optimized-send-buffer</p> <p>(config) tfo tcp original-mss</p> <p>(config) tfo tcp original-send-buffer</p>

(config) tfo tcp original-send-buffer

Traffic Flow Optimization (TFO) 最適化用 WAE で非最適化側の送信バッファを設定するには、**tfo tcp original-send-buffer** 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。

```
tfo tcp original-send-buffer buffer-size
```

シンタックスの説明

<i>buffer-size</i>	キロバイトの送信バッファ サイズ
--------------------	------------------

デフォルト

32 KB

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

このコマンドは TFO 非最適化ソケット (WAE とクライアント間または WAE とサーバ間の接続) 上の TCP 送信バッファ サイズを設定します。

関連コマンド

- [\(config\) tfo tcp keepalive](#)
- [\(config\) tfo tcp optimized-mss](#)
- [\(config\) tfo tcp optimized-receive-buffer](#)
- [\(config\) tfo tcp optimized-send-buffer](#)
- [\(config\) tfo tcp original-mss](#)
- [\(config\) tfo tcp original-receive-buffer](#)

(config) transaction-logs

WAE でトランザクション ログキングを設定して有効にするには、**transaction-logs** 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。トランザクション ログキング オプションを無効にするには、このコマンドの **no** 形式を使用します。

transaction-logs tfo enable

transaction-logs tfo logging {enable | facility parameter | host {hostname | ip-address} [port port-num] [rate-limit number-message-per-sec]}

transaction-logs tfo archive interval seconds

transaction-logs tfo archive interval every-day {at hour:minute | every hours}

transaction-logs tfo archive interval every-hour {at minute | every minutes}

transaction-logs tfo archive interval every-week [on weekdays at hour:minute]

transaction-logs tfo archive max-file-size filesize

transaction-logs export compress

transaction-logs export enable

transaction-logs export ftp-server {hostname | servipaddr} login passw directory

transaction-logs export interval minutes

transaction-logs export interval every-day {at hour:minute | every hours}

transaction-logs export interval every-hour {at minute | every minutes}

transaction-logs export interval every-week [on weekdays at hour:minute]

transaction-logs export sftp-server {hostname | servipaddr} login passw directory

シンタックスの説明

tfo	TFO トランザクション ログ機能を指定します。
enable	TFO トランザクション ログ機能を有効にします。
logging	ログキング TFO トランザクションをリモート Syslog ホストに指定します。
enable	リモート Syslog ホストへのログキング TFO トランザクションを有効にします。
facility	適切なトランザクション ログ ファシリティを指定します。 このドロップダウン リストは初期値「Do not set」に設定されます。この設定は Syslog ホストに送信されるファシリティが Syslog メッセージを送信するローカル ホスト上のファシリティになることを示します。たとえば、リアルタイム トランザクション ログ メッセージを送信するトランザクション ログキング モジュールの場合、ファシリティは「user」ファシリティです。

<i>parameter</i>	次のいずれかのファシリティを指定します。 auth 許可システム daemon システム デーモン kern カーネル local0 ローカル使用 local1 ローカル使用 local2 ローカル使用 local3 ローカル使用 local4 ローカル使用 local5 ローカル使用 local6 ローカル使用 local7 ローカル使用 mail メール システム news USENET ニュース syslog Syslog 自身 user ユーザ プロセス uucp UUCP システム
host	リモート Syslog サーバを設定します。
<i>hostname</i>	トランザクション ログを送信するリモート Syslog サーバのホスト名または IP アドレス。デフォルトではリモート Syslog サーバは指定されていません。
<i>ip-address</i>	リモート Syslog サーバの IP アドレス
port	(オプション) Syslog サーバのトランザクション ログ メッセージ送信時に使用するポートを設定します。
<i>port-num</i>	WAE がトランザクション ログ ファイルを送信するリモート Syslog ホストの宛先ポート。デフォルトのポート番号は 514 です。このポートはシステム ロギングの Well-known ポートです。
rate-limit	(オプション) トランザクション ロガーが許可されたリモート Syslog サーバへのメッセージ送信レートを設定します。
<i>number-message-per-sec</i>	リモート Syslog ホストに送信することが許可された 1 秒当たりのメッセージ数。帯域幅と他のリソース消費を制限するため、リモート Syslog ホストへのメッセージは、レートを制限できます。 この限度を超えた場合、指定されたリモート Syslog ホストはメッセージをドロップします。デフォルトのレート制限はありません (rate-limit は 0 に設定)。デフォルトでは、すべての Syslog メッセージはすべての設定済み Syslog ホストに送信されます。指定できる範囲は 1 ~ 10,000 メッセージ/秒です。
archive	アーカイブ パラメータを設定します。
interval	アーカイブ ファイルを保存する頻度を決定します。
<i>seconds</i>	秒単位でのアーカイブ頻度 (120 ~ 604800)
every-day	1 日以内のの間隔でアーカイブします。
at	毎日アーカイブする現地時間を指定します。
<i>hour:minute</i>	現地時間でのアーカイブ時刻 (hh:mm)
every	時間単位で間隔を指定します。間隔は午前 0 時から開始します。

<i>hours</i>	毎日のファイル アーカイブの時間数 1 1 時間ごと 12 12 時間ごと 2 2 時間ごと 24 24 時間ごと 3 3 時間ごと 4 4 時間ごと 6 6 時間ごと 8 8 時間ごと
every-hour	1 時間以内の間隔でアーカイブを指定します。
at	毎時アーカイブする時刻を設定します。
<i>minute</i>	毎時アーカイブの分 (0 ~ 59)
every	毎時アーカイブの間隔を 0 分で始まる分単位で指定します。
<i>minutes</i>	毎時アーカイブの分数 10 10 分ごと 15 15 分ごと 2 2 分ごと 20 20 分ごと 30 30 分ごと 5 5 分ごと
every-week	週 1 回以上の間隔でアーカイブします。
on	(オプション) アーカイブを実行する曜日を設定します。
<i>weekdays</i>	アーカイブを実行する曜日。1 つまたは複数の曜日を指定できます。 Fri 毎金曜日 Mon 毎月曜日 Sat 毎土曜日 Sun 毎日曜日 Thu 毎木曜日 Tue 毎火曜日 Wed 毎水曜日
at	(オプション) アーカイブを実行する各日の現地時間を設定します。
<i>hour:minute</i>	現地時間でのアーカイブ時刻 (hh:mm)
max-file-size	ローカル ディスクに保存するアーカイブ ファイルの最大サイズを KB 単位で指定します。
<i>filesize</i>	KB 単位の最大アーカイブ ファイル サイズ (1000 ~ 2000000)。この値はローカル ディスクに保存するアーカイブ ファイルの最大サイズです。
export	ファイル エクスポート パラメータを設定します。FTP エクスポート機能は最大 4 つのサーバをサポートできます。各サーバでそのサーバに有効なユーザ名、パスワードおよびディレクトリを設定する必要があります。
compress	外部 FTP サーバへエクスポートする前に、zip フォーマットへのアーカイブ ファイルの圧縮を有効にします。
enable	指定された間隔でログ ファイルのエクスポートを有効にします。
ftp-server	FTP サーバがエクスポートされたアーカイブ ファイルを受信できるように設定します。

<i>hostname</i>	ターゲット FTP サーバのホスト名
<i>servipaddr</i>	ターゲット FTP サーバの IP アドレス
<i>login</i>	ターゲット FTP サーバのユーザ ログイン
<i>passw</i>	ターゲット FTP サーバのユーザ パスワード
<i>directory</i>	エクスポート ファイルの FTP サーバ上のターゲット ディレクトリ パス
interval	FTP サーバにデータを移動することで作業ログがクリアされるインターバルを指定します。
<i>minutes</i>	ファイルをエクスポートする間隔の分数 (1 ~ 10080)
every-day	1 日以内の間隔でエクスポートを指定します。
at	毎日エクスポートする現地時間を指定します。
<i>hour:minute</i>	現地時間でのエクスポート時刻 (hh:mm)
every	毎日のエクスポートの間隔を時間単位で指定します。
<i>hours</i>	毎日のエクスポートの時間数 1 1 時間ごと 12 12 時間ごと 2 2 時間ごと 24 24 時間ごと 3 3 時間ごと 4 4 時間ごと 6 6 時間ごと 8 8 時間ごと
every-hour	1 時間以内の間隔でエクスポートを指定します。
at	毎日エクスポートする時刻を指定します。
<i>minute</i>	毎時エクスポートの分 (0 ~ 59)
every	間隔を 0 分で始まる分数で指定します。
<i>minutes</i>	毎時エクスポートの分数 10 10 分ごと 15 15 分ごと 2 2 分ごと 20 20 分ごと 30 30 分ごと 5 5 分ごと
every-week	週 1 回以上のインターバルでエクスポートを指定します。
on	(オプション) エクスポートを実行する曜日を指定します。
<i>weekdays</i>	エクスポートを実行する曜日。1 つまたは複数の曜日を指定できます。 Fri 毎金曜日 Mon 毎月曜日 Sat 毎土曜日 Sun 毎日曜日 Thu 毎木曜日 Tue 毎火曜日 Wed 毎水曜日
at	(オプション) 週一度のエクスポートを実行する時刻を指定します。
<i>hour:minute</i>	現地時間でのエクスポートを実行する時刻 (hh:mm)

sftp-server	Secure File Transfer Protocol (SFTP; セキュア ファイル転送プロトコル) がエクスポートされたアーカイブファイルを受信できるように設定します。
<i>hostname</i>	ターゲット SFTP サーバのホスト名
<i>servipaddr</i>	ターゲット SFTP サーバの IP アドレス
<i>login</i>	ターゲット SFTP サーバのユーザ ログイン (40 文字以内)
<i>passw</i>	ターゲット SFTP サーバのユーザ パスワード (40 文字以内)
<i>directory</i>	エクスポート ファイルの SFTP サーバ上のターゲット ディレクトリパス

デフォルト

archive : 無効
enable : 無効
export compress : 無効
export : 無効
archive interval : 毎日、1 時間ごと
archive max-file-size : 2,000,000 KB
exportinterval : 毎日、1 時間ごと
logging port port-num : 514

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

Sysfs のマウント場所に応じて、トランザクションはローカル ディスクの次のいずれかのファイルの作業ログにロギングされます。

- /local1/logs/working.log
- /local2/logs/working.log

トランザクション ロギングを有効にした場合、アーカイブ ログヘデータを移動することで作業ログをクリアする間隔を指定できます。アーカイブ ログ ファイルは Sysfs をマウントした場所に応じてローカル ディスクのディレクトリ /local1/logs/ または /local2/logs/ に保存されます。

複数のアーカイブ ファイルが保存されるため、ファイル名にはファイル アーカイブ時のタイムスタンプが含まれます。ファイルは FTP/SFTP サーバにエクスポートできるので、ファイル名にはこの WAE の IP アドレスも含まれます。

アーカイブ ファイル名は次のフォーマットを使用します。

celog_IPADDRESS_YYYYMMDD_HHMMSS.txt.

トランザクション ログは認証エラーなど特定のエラーについてリアルタイムでモニタリングできます。リモート Syslog サーバに HTTP トランザクション ログ メッセージを送信して、HTTP 要求認証の失敗がないリモート Syslog サーバをリアルタイムでモニタリングできます。このリアルタイム トランザクション ログ機能により、HTTP 要求認証エラーなどの特定のエラーがないかトランザクション ログをリアルタイムで監視できます。ローカル ファイル システムへの既存のトランザクション ロギングは変わりません。

このため、転送プロトコルとして UDP を使用してリモート Syslog サーバにトランザクション ログメッセージを送信するように WAE を設定する必要があります。UDP は信頼できない転送プロトコルであるためリモート Syslog ホストへのメッセージ転送は信用できず、リモート Syslog サーバで受信した Syslog メッセージを監視する必要があります。トランザクション ロギング モジュールがリモート Syslog サーバにメッセージ送信できるレートを制限できます。Syslog メッセージのフォーマットは標準 Syslog メッセージフォーマットで、トランザクション ログメッセージが Syslog メッセージのペイロードです。

リモート Syslog サーバへのリアルタイム トランザクション ロギングはトランザクション ログ エントリとしてメッセージ ペイロードを持つ標準 Syslog メッセージを使用します。このタイプのリアルタイム トランザクション ログ メッセージ用に新しい Syslog エラー ID が定義されています。トランザクション ログメッセージをリアルタイムで1つのリモート Syslog ホストに送信するよう、WAE を設定できます。リモート Syslog ホストへのトランザクション ログ エントリのメッセージフォーマットはトランザクション ログ ファイルと同じで、シスコ標準 Syslog ヘッダー情報が先頭に付きます。

以下は、トランザクション ロギング モジュール (WAE) からリモート Syslog ホストに送信されるリアルタイムの Syslog メッセージのフォーマット例です。

```
fac-pri Apr 22 20:10:46 ce-host cache:%CE-TRNSLG-6-460012:translog formatted msg
```

次にメッセージの各フィールドを説明します。

- *fac-pri* は 0 ~ 1023 (0x0000 ~ 0x03FF) までの 32 ビット 10 進数として符号化された (標準 Syslog フォーマットと同様) トランザクション ログ メッセージのファシリティ パラメータおよびプライオリティを示します。最下位 3 ビットはプライオリティ (0 ~ 7) を示し、次の最下位 7 ビットはファシリティ (0 ~ 127) を示します。

リアルタイム トランザクション ログメッセージがリモート Syslog ホストにロギングされるときにトランザクション ログ モジュールが使用するファシリティ パラメータは *user* です。トランザクション ロギングに別のファシリティ パラメータを指定しないかぎり、同じファシリティがリモート Syslog ホストに送信されます。リアルタイム トランザクション ログメッセージのプライオリティ フィールドは常に LOG_INFO に設定されます。

上記の例で *fac-pri* のデフォルト値は 14 (0x000E) で、ファシリティ = user (LOG_USER (1)) およびプライオリティ = LOG_INFO (6) です。

- メッセージの次のフィールドは日付です。フォーマットは上記の例に示したとおりです。
- *ce-host* はメッセージを送信する WAE のホスト名または IP です。
- *cache* はメッセージを送信する WAE 上のプロセスの名前です。
- %CE-TRNSLG-6-460012 は WAE でのリアルタイム トランザクション ログメッセージのシスコ標準フォーマットの Syslog ヘッダーです。この識別情報はプライオリティ レベル 6、すなわち情報メッセージを示します。



(注) WAAS システムの Syslog メッセージはトランザクション ロギング用に設定されたリモート Syslog ホストとの通信エラーを報告します。これら Syslog メッセージのエラーメッセージ範囲は %CE-TRNSLG-6-460013 から %CE-TRNSLG-3-460016 までです。最後のエラーメッセージ (%CE-TRNSLG-3-460016) はレベル「6」(情報レベルメッセージ)ではなくレベル「3」(エラーレベルメッセージ)を示します。情報レベルメッセージはレート制限のためメッセージがドロップされたときに報告され、ドロップされたメッセージ数が報告されます。これら Syslog メッセージについての詳細は、『Cisco WAAS System Messages Reference』を参照してください。

- *translog formatted msg* はトランザクション ログ ファイルに出力されるトランザクション ログメッセージです。



(注) リアルタイム Syslog メッセージの合計の長さは 1024 文字です。実際のトランザクション ログ エントリがこの限度を超えると、切り捨てられます。

リモート Syslog サーバがこのメッセージをファイルにロギングするとき、フォーマットは次のようになります。

```
Apr 22 20:10:46 ce-host cache:%CE-TRNSLG-6-460012:translog formatted msg
```

ここで `ce-host` はリアルタイム トランザクション ログ メッセージをリモート Syslog サーバに送信する WAE のホスト名です。

トランザクション ログのホスト設定のコンフィギュレーションは、リアルタイム トランザクション ログのメッセージのプライオリティ レベルを指定する必要がない以外、Syslog メッセージのコンフィギュレーション設定と同じです。すべてのメッセージはプライオリティ レベル 6 (LOG_INFO) と関連付けられます。メッセージをプライオリティ レベルに基づいてフィルタリングする必要はありません。

関連コマンド

[clear](#)

[show transaction-logging](#)

[transaction-log](#)

(config) username

WAAS デバイスでユーザ名認証を設定するには、**username** 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。

```
username name {passwd | print-admin-passwd | privilege {0 | 15}}
```

シンタックスの説明

name	ユーザ名
passwd	ユーザのパスワードをインタラクティブに指定します。パスワードの入力が要求されたあと、再度確認のためにパスワードの入力を要求されます。
print-admin-passwd	ユーザのプリント管理パスワードをインタラクティブに設定します。パスワードの入力が要求されたあと、再度確認のためにパスワードの入力を要求されます。
privilege	ユーザの特権レベルを設定します。
0	標準ユーザのユーザ特権レベルを指定します。
15	スーパーユーザのユーザ特権レベルを指定します。

デフォルト

デフォルトの管理者アカウント：

- ユーザ名：admin
- パスワード：デフォルト
- 特権：スーパーユーザ (15)

コマンドモード

グローバル コンフィギュレーション

デバイスモード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

システム管理者はコンソール ポートまたは WAE Device Manger GUI を介して、Core または Edge WAE として稼働している WAAS デバイスにログインできます。管理者はコンソール ポートまたは WAAS Central Manager GUI を介して WAAS Central Manager にログインできます。

システム管理者が認証および許可の設定の前に WAAS デバイスにログインする場合は、定義済みスーパーユーザ アカウント（定義済みユーザ名は *admin*、定義済みパスワードは *default*）を使用して WAAS デバイスにアクセスできます。この定義済みスーパーユーザ アカウントを使用して WAAS デバイスにログインした場合、WAAS システム内のすべての WAAS サービスおよびエンティティのアクセスが許可されます。

最初に WAAS デバイスを設定した後、各 WAAS デバイスの定義済みスーパーユーザ アカウントのパスワード（定義済みユーザ名は *admin*、パスワードは *default*、特権レベルはスーパーユーザ（特権レベル 15））をただちにを変更することを強く推奨します。

■ (config) username

このスーパーユーザ アカウントの定義済みパスワードを WAAS デバイスで変更しなかった場合、このスーパーユーザ アカウントを使用して WAAS CLI にログインするたびに次のメッセージが表示されます。

```
Device is configured with a (well known) default username/password
for ease of initial configuration. This default username/password
should be changed in order to avoid unwanted access to the device.
```

```
System Initialization Finished.
waas-cm#
```

このスーパーユーザ アカウントの定義済みパスワードを WAAS Central Manager で変更しなかった場合、このスーパーユーザ アカウントを使用して WAAS Central Manager GUI にログインするたびにダイアログボックスも表示されます。



(注) 可能な場合は、WAAS CLI の代わりに WAAS Central Manager GUI を使用して WAAS デバイスのユーザのパスワードおよび特権レベルを設定することを強く推奨します。WAAS Central Manager GUI を使用して WAAS Central Manager に登録されている単一 WAE または WAE グループ上のユーザを一元的に設定および管理方法については、『*Cisco Wide Area Application Services Configuration Guide*』を参照してください。

username グローバル コンフィギュレーション コマンドにより、既存ユーザアカウントのパスワードおよび特権レベルを変更できます。定義済みスーパーアカウントのパスワードを個々のデバイスで変更するには、**username** グローバル コンフィギュレーション コマンドの **passwd** オプションを使用します。

```
waas-cm(config)# username admin passwd
```

たとえば、WAAS Central Manager waas-cm のスーパーユーザ アカウントの定義済みパスワードを次のように mysecret に変更します。

```
waas-cm# config
waas-cm(config)# username admin passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
New UNIX password: mysecret (Note that the text is not displayed)
Retype new UNIX password: mysecret
waas-cm(config)# exit
```

ユーザ認証

ユーザのアクセスは認証レベルで制御されます。すべての WAAS CLI 要求などの WAAS デバイスに着信するすべての HTTP 要求について、認証レベルは指定されたユーザ名およびパスワードで認識できます。CLI で設定されたパラメータに基づいて、要求を受け入れるか拒否するかの決定がなされます。この決定は、ローカル認証を確認するか、リモート認証サーバにクエリーを送信することで行われます。認証レベルは許可レベルとは切り離され、認証レベルでロールやドメインの概念はありません。

ローカル CLI 認証を使用すると、すべての設定済みユーザは、**show running-config** コマンドを入力すると表示できます。

ユーザ許可

ドメインとロールは、許可レベルで WAAS デバイスによって適用されます。要求は、許可レベルによって検討される前に、認証レベルによって受け入れられる必要があります。許可レベルでは、WAAS Cntral Manager GUI およびドメイン設定の指定されたロールに基づいて、リソースへのアクセスを規制します。

認証メカニズムに関係なく、すべてのユーザ許可設定は GUI で参照できます。

例

次の例は、パスワードと特権レベルを再設定する方法を示します。

```
WAE# show user username abeddoe
Uid          : 2003
Username     : abeddoe
Password     : *****
Privilege    : normal user
```

```
WAE# show user username bwhidney
Uid          : 2002
Username     : bwhidney
Password     : *****
Privilege    : normal user
```

```
WAE(config)# username bwhidney passwd
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
New UNIX password: newpassword (Note that the text is not displayed)
Retype new UNIX password: newpassword
```

```
WAE(config)# username abeddoe privilege 15
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
```

```
WAE# show user username abeddoe
Uid          : 2003
Username     : abeddoe
Password     : *****
Privilege    : super user
Configured in : Local database
```

```
WAE# show user username bwhidney
Uid          : 2002
Username     : bwhidney
Password     : *****
Privilege    : normal user
Configured in : Local database
```

関連コマンド

[show user](#)

(config) wccp access-list

WAE で着信 WCCP GRE カプセル化トラフィックの IP アクセス リストを設定するには、**wccp access-list** 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。

```
wccp access-list {acl-number | ext-acl-number | acl-name}
```

シンタックスの説明

<i>acl-number</i>	標準 IP アクセス リストの番号 (1 ~ 99)
<i>ext-acl-number</i>	拡張 IP アクセス リストの番号 (100 ~ 199)
<i>acl-name</i>	アクセス リストの名前 (最大 30 文字)

デフォルト

WCCP アクセス リストはデフォルトでは設定されていません。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

wccp access-list number グローバル コンフィギュレーション コマンドは、Access Control List (ACL; アクセス コントロール リスト) を設定して WCCP アプリケーションにアクセスできるようにします。*number* 変数は、1 ~ 99 の範囲の数値で標準アクセス コントロール リストを示し、100 ~ 199 の範囲の数値で拡張アクセス コントロール リストを示します。WCCP は、着信パケットを、指定されたアクセス コントロール リストでチェックしてから、受け入れるか、またはドロップするかします。

WAE で標準 IP ACL を使用して WAE での WCCP アクセスを制御する方法の詳細な説明については、『*Cisco Wide Area Application Services Configuration Guide*』を参照してください。



(注)

WCCP は IPv4 ネットワークでのみ動作します。

例

次の例は、IP アクセス リスト番号 10 を着信 WCCP トラフィックに適用するように WAE を設定します。

```
WAE(config)# wccp access-list 10
```

次に、WAE での **show ip access-list EXEC** コマンドによる出力例を示します。WAE ではいくつかの WCCP アクセス リストが設定されています。

```
WAE(config)# show ip access-list
Space available:
  40 access lists
  489 access list conditions

Standard IP access list 10
  1 deny 10.1.1.1
  2 deny any
    (implicit deny any: 0 matches)
  total invocations: 0
Standard IP access list 98
  1 permit any
    (implicit deny any: 0 matches)
  total invocations: 0
Extended IP access list 100
  1 permit icmp any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 101
  1 permit ip any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 102
  1 permit icmp 0.0.1.1 255.255.0.0 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 111
  1 permit gre 0.1.1.1 255.0.0.0 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 112
  1 permit ip any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list 113
  1 permit gre 0.1.1.1 255.0.0.0 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list ext_acl_2
  1 permit gre any any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Extended IP access list extended_ip_acl
  1 permit tcp any eq 2 any eq exec
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0

Interface access list references:
PortChannel    2    inbound    extended_ip_acl
PortChannel    2    outbound   101

Application access list references:
snmp-server                standard    2
  UDP ports: none (List Not Defined)
WCCP                       either      10
  Any IP Protocol
```

次に、WCCP アクセス リストが WAE に定義されているときの、**show wccp gre EXEC** コマンドによる出力例を示します。

```
WAE# show wccp gre
Transparent GRE packets received:          366
Transparent non-GRE packets received:      0
Transparent non-GRE packets passed through: 0
Total packets accepted:                    337
Invalid packets received:                  0
Packets received with invalid service:     0
Packets received on a disabled service:    0
Packets received too small:                0
Packets dropped due to zero TTL:            0
Packets dropped due to bad buckets:         0
Packets dropped due to no redirect address: 0
Packets dropped due to loopback redirect:   0
Connections bypassed due to load:          0
Packets sent back to router:               0
Packets sent to another CE:                0
GRE fragments redirected:                  0
Packets failed GRE encapsulation:          0
Packets dropped due to invalid fwd method:  0
Packets dropped due to insufficient memory: 0
Packets bypassed, no conn at all:          0
Packets bypassed, no pending connection:   0
Packets due to clean wccp shutdown:        0
Packets bypassed due to bypass-list lookup: 0
Packets received with client IP addresses: 0
Conditionally Accepted connections:        0
Conditionally Bypassed connections:        0
L2 Bypass packets destined for loopback:   0
Packets w/WCCP GRE received too small:    0
Packets dropped due to IP access-list deny: 29
L2 Packets fragmented for bypass:          0
```

関連コマンド

[\(config\) egress-method](#)

[show ip access-list](#)

[show wccp](#)

(config) wccp flow-redirect enable

WAE で WCCP フロー リダイレクションを有効にするには、**wccp flow-redirect** 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。フロー リダイレクションを無効にするには、このコマンドの **no** 形式を使用します。

wccp flow-redirect enable

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト 有効

コマンド モード グローバル コンフィギュレーション

デバイス モード application-accelerator

使用上のガイドライン WCCP フロー保護は、WAE が新たにオンラインになるか、サービス グループから削除されたときに、既存のフローが切断されないように保証するメカニズムです。透過的なトラフィック代行受信またはリダイレクションが最初に始まると、WCCP フロー保護は、以前から存在する確立された HTTP フローが継続できるようにすることで、既存の HTTP フローが切断されないように保証します。また、WCCP フロー保護は、新しい WAE が既存の WAE グループに加入したときに、クラスター内の以前から存在する WAE によって処理されていた既存のフローが引き続きそれぞれの既存のフローを受信できるように保証します。

WCCP フロー保護が使用するメカニズムは、フロー単位の状態情報を中央で集中的に管理することによる利益のすべてをもたらします。フロー単位の状態情報をスイッチング レイヤに管理した場合のオーバーヘッドやスケーリングの問題、冗長性や復元力の問題（たとえば、非対称トラフィックフロー）などは一切発生しません。

wccp flow-redirect 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、WCCP フロー保護を実装します。フロー保護は、WAE の最初の起動時または新しいトラフィックが割り当てられたとき、TCP フローを過剰に受信しないだけでなく、損傷のない状態に保持するように設計されています。この機能は、WAE がそれぞれの容量に応じて負荷を担うスロースタート メカニズムも備えています。



(注) バイパスが有効になると、クライアント自身は発信元の Web サーバに到達しようとします。すべてのバイパス オプションを無効にして不要なネットワーク負荷をなくす必要があります。

WCCP は IPv4 ネットワークでのみ動作します。

例 次の例は、WAE での WCCP フロー保護を有効にする方法を示します。

```
WAE(config)# wccp flow-redirect enable
```

(config) wccp router-list

ルータ リストを WCCP Version 2 用に設定するには、**wccp router-list** 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。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wccp router-list number ip-address

シンタックスの説明

<i>number</i>	ルータ リストの番号 (1 ~ 8)
<i>ip-address</i>	リストに追加するルータの IP アドレス

デフォルト

無効

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

WAE への WCCP Version 2 サービス設定の一環として、WCCP Version 2 対応ルータのリストを作成します。このルータは、WAE 用の CIFS キャッシュサービスをサポートするものです。

各ルータ リストには、最大 8 つまでルータを指定できます。ルータ リストを 8 つと、各リストにつき最大 32 の IP アドレスを追加できます。



(注)

ip wccp 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、ルータ リストに含まれている各ルータで WCCP を有効にする必要があります。

WCCP は IPv4 ネットワークでのみ動作します。

例

次の例では、ルータ リスト番号 7 を作成します。ここには、単一のルータが含まれています (IP アドレスが 192.168.68.98 の WCCP Version 2 対応ルータ)。

```
WAE(config)# wccp router-list 7 192.168.68.98
```

次の例は、上の例で作成したルータ リスト番号 7 を削除します。

```
WAE(config)# no wccp router-list 7 192.168.68.98
```

次の例は、ルータ リストを作成し (ルータ リスト 1)、それからルータ リスト 1 の WCCP Version 2 対応ルータからのリダイレクトされた TCP トラフィックを受け入れるよう WAE を設定する方法を示します。

```
WAE(config)# wccp router-list 1 10.10.10.2
WAE(config)# wccp tcp-promiscuous router-list 1
WAE(config)# wccp version 2
```

関連コマンド

(config) [wccp version](#)

(config) wccp shutdown

WAE が WCCP のクリーン シャットダウンを実行する最大時間間隔を設定するには、**wccp shutdown** 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。クリーン シャットダウンを無効にするには、このコマンドの **no** 形式を使用します。

```
wccp shutdown {max-wait seconds}
```

シンタックスの説明

max-wait	クリーン シャットダウン時間間隔を設定します。
seconds	秒単位での時間 (0 ~ 86400)。デフォルトは 120 秒です。

デフォルト

クリーン シャットダウン前の最大時間間隔は、デフォルトで 120 秒です。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

TCP 接続の切断を防ぐため、WAE は、**reload** または **wccp version** コマンドの発行後、WCCP のクリーン シャットダウンを実行します。WAE は、すべての接続が処理されるか、または設定した **max-wait** インターバルが経過するまで、リブートしません。

クリーン シャットダウン中、WAE は処理中のフローについては引き続きサービスを提供する一方で、新しいフローのバイパスを開始します。フローの数が 0 になると、WAE は、リード WAE に自分のパケットを他の WAE へ再割り当てさせることで、自分自身はクラスタから脱退します。WAE が損傷するか、WCCP をクリーン シャットダウンせずにリブートされた場合には、依然として TCP 接続が切断される可能性があります。クリーン シャットダウンは、進行中に打ち切られることがあります。

WAE の特定ポートの個々の WCCP サービスはシャットダウンできません。WAE 上で WCCP をシャットダウンする必要があります。WAE 上で WCCP をシャットダウンすると、WAE はその WCCP 構成設定およびサービス プロキシ型要求 (たとえば、FWAE がクライアントブラウザから直接受信する HTTP 要求) を保存します。



(注)

WCCP は IPv4 ネットワークでのみ動作します。

例

次の例は、1000 秒待機するように WAE を設定する方法を示します。

```
WAE(config)# wccp shutdown max-wait 1000
```

次の例は、**no wccp version 2** コマンドを入力して WAE 上の WCCP Version 2 をシャットダウンする方法を示します。この場合、**no wccp version 2** コマンドを実行すると、WAE は 1000 秒待機してから WCCP Version 2 をシャットダウンします。

```
WAE(config)# no wccp version 2
```

■ (config) wccp shutdown

カウントダウン メッセージが表示され、WAE の WCCP がシャットダウンされるまでの残りの秒数が示されます。

```
Waiting (999 seconds) for WCCP shutdown. Press ^C to skip shutdown
```

The clean shutdown can be aborted while in progress by simultaneously pressing ^C after the countdown message appears.

関連コマンド

[\(config\) wccp flow-redirect enable](#)

[\(config\) wccp version](#)

(config) wccp tcp-promiscuous

WAE で Web Cache Coordination Protocol (WCCP) Version 2 TCP 混合モード サービス (WCCP Version 2 サービス 61 および 62) を設定するには、**wccp tcp-promiscuous** 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。

```
wccp tcp-promiscuous {mask {dst-ip-mask mask | src-ip-mask mask} | router-list-num number
[assign-method-strict | hash-destination-ip | hash-source-ip | l2-redirect | l2-return | mask-assign
| password password | weight weight]}
```

シンタックスの説明

mask	WAE 割り当てに使用するマスクを指定します。
dst-ip-mask	パケットの宛先 IP アドレスの照合に使用する IP アドレス マスクを 16 進数 (たとえば 0xFE000000) で指定します。範囲は 0x00000000 ~ 0xFE000000 です。デフォルトは 0x00000000 です。
src-ip-mask	パケットの発信元 IP アドレスの照合に使用する IP アドレス マスクを 16 進数 (たとえば 0xFE000000) で指定します。範囲は 0x00000000 ~ 0xFE000000 です。デフォルトは 0x00001741 です。
mask	16 進表記のマスク (0x00000000 ~ 0xFE000000)
router-list-num	TCP 混合モード サービスと関連付ける WCCP ルータ リストの番号を指定します。
number	TCP 混合モード サービスと関連付ける WCCP ルータ リスト (1 ~ 8) の番号 (これら WCCP Version 2 対応ルータは TCP トラフィックを WAE に透過的にリダイレクトします)。
assign-method-strict	(オプション) 設定された割り当て方式だけを使用することを指定します。
hash-destination-ip	(オプション) 宛先 IP アドレスのロード バランシング ハッシュ方法を指定します。 hash-destination-ip オプションと hash-source-ip オプションの両方を指定できます。
hash-source-ip	(オプション) 送信元 IP アドレスのロード バランシング ハッシュ方法を指定します。これは、デフォルトです。
l2-redirect	(オプション) パケット転送にレイヤ 2 リダイレクションを使用することを指定します。WAE にデバイスとのレイヤ 2 接続があり、デバイスがレイヤ 2 ダイレクション用に設定されている場合、レイヤ 2 ダイレクションは WAE が WCCP Version 2 対応スイッチまたはルータから透過的にリダイレクトされたトラフィックを受信することを許可します。
l2-return	(オプション) パケット リターンにレイヤ 2 リライティングを使用することを指定します。
mask-assign	(オプション) WAE 割り当てにマスク方式を使用することを指定します。
password	(オプション) クラスタ内の WAE 間のセキュア トラフィックおよび指定されたサービスのルータに使用するパスワードを指定します。クラスタ内の残りすべての WAE とルータは、同じパスワードで有効にしてください。
password	WCCP サービス パスワード。パスワードは 8 文字以内にしてください。

weight	(オプション) 重量比率を使用することを指定します。重量はロードバランシング目的でデバイスにリダイレクトされる総負荷の比率を表します (たとえば、重量 30 の WAE は総負荷の 30% を受信します)。
<i>weight</i>	重量比率。重量値は 0 ~ 100% の範囲です。デフォルトでは重量は割り当てられおらず、トラフィック負荷は サービス グループ内の WAE に均等に分散されます。

コマンドモード グローバル コンフィギュレーション

デバイスモード application-accelerator

使用上のガイドライン WCCP はクライアント要求を処理のため WAE に透過的にリダイレクトするメカニズムを提供します。基本 WCCP を設定するには、データセンター内のルータと Core WAE、およびブランチオフィスのルータと Edge WAE で WCCP サービスを有効にする必要があります。利用可能なすべての WCCP 機能またはサービスを設定して WAE を立ち上げ、稼働させる必要はありません。

この WCCP サービスは、ルータおよび WAE で WCCP Version 2 が実行している必要があります。

TCP 混合モード サービスは、すべての TCP トラフィックを代行受信してローカル WAE にリダイレクトする WCCP サービスです。

指定された WCCP Version 2 ルータにより WAE に透過的にリダイレクトされる TCP トラフィックに対して WAE が混合モード TCP デバイスとして機能できるようにするため、WAE は WCCP Version 2 サービス 61 および 62 を使用します。WCCP サービス 61 および 62 は、WAAS CLI の WAE 上で標準名「tcp-promiscuous」で表されます。

WCCP 代行受信された接続の出力方式を設定するには、**egress-method** 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。



(注) WCCP は IPv4 ネットワークでのみ動作します。

例 次の例は、**wccp tcp-promiscuous router-list-num** コマンドを使用して TCP 混合モードサービスをオンにし、このサービスをルータ リストと関連付ける方法を示します。

```
WAE # wccp tcp-promiscuous router-list-num 1
WCCP configuration for TCP Promiscuous service 61 succeeded.
WCCP configuration for TCP Promiscuous succeeded.
Please remember to configure WCCP service 61 and 62 on the corresponding router.
```

関連コマンド

- (config) egress-method
- (config) wccp router-list
- show wccp

(config) wccp version

WAE が使用するべき WCCP のバージョンを指定するには、**wccp version** 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。現在実行しているバージョンを無効にするには、このコマンドの **no** 形式を使用します。

```
wccp version {2}
```

シンタックスの説明

2 WCCP Version 2 を使用するように WAE を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

グローバル コンフィギュレーション

デバイス モード

application-accelerator

使用上のガイドライン

Web トラフィック (ポート 80) をサポートしているのは WCCP Version 1 だけなので、WCCP Version 1 ではなく WCCP Version 2 を使用するように WAE を設定する必要があります。

reload または **no wccp version 2** コマンドの入力後、WAE によりクリーン シャットダウンが実行されます。クリーン シャットダウンは、TCP 接続の切断を防止します。

次の一連のイベントは、WAE と、WCCP Version 2 を実行するよう設定されたルータ間の相互作用について詳しく説明します。

1. 各 WAE はルータ リストで設定されている (**(config) wccp router-list** コマンドを参照)。
2. 各 WAE はその存在と、通信が確立しているすべてのルータのリストを通知する。ルータは、グループ内の WAE のビュー (リスト) で応答する。

ルータと WAE は相互に認識するようになり、管理プロトコルを使用して WCCP サービス グループを形成します。WAE も定期的に「Here I am」のメッセージをルータに送信して、ルータが WAE を再度検出できるようにします。ビューを正しく示すため、プロトコルにはサービス グループ内のルータのリストをメッセージの一部として入れる必要があります。

3. WAE クラスタ内のすべての WAE でビューの整合がとれると、ある WAE がリード WAE として指定される。WAE のグループがある場合、すべてのルータによって認識され、最低位の IP アドレスを持つ WAE がリード WAE になります。

このリード WAE の役割は、WAE のグループ内の WAE 全体にトラフィックを割り当てる方法を決定することです。リード WAE は、このクラスタ内の WAE にパケットをリダイレクトするとき WCCP 対応ルータが守るべきポリシーを設定します。割り当て情報は、指定された WAE からサービス グループ全体に渡され、サービス グループのルータがパケットを正しくリダイレクトし、サービス グループの各 WAE がそのロードを正しく管理できるようにします。



(注)

WCCP は IPv4 ネットワークでのみ動作します。

例

次の例は、WAE で WCCP Version 2 を有効にする方法を示します。

```
WAE(config)# wccp version 2
```

関連コマンド (config) wccp tcp-promiscuous
(config) wccp router-list

(config) windows-domain

WAAS デバイスで Windows ドメイン サーバ オプションを設定するには、**windows-domain** 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。

```
windows-domain {administrative group {normal-user | super-user} groupname | comment string |
netbios-name name | password-server {hostname | ipaddress} | realm kerberos-realm | wins-server
{hostname | ipaddress} | workgroup name | security ADS}
```

シンタックスの説明

administrative	管理オプションを設定します。
group	管理グループ名を設定します。
normal-user	標準ユーザ（特権 0）の管理グループ名を設定します。
super-user	スーパーユーザ（特権 15）の管理グループ名を設定します。
<i>groupname</i>	管理グループの名前
comment	Windows ドメイン サーバのコメントを指定します。
<i>string</i>	テキスト文字列
netbios-name	WAE の NetBIOS 名を指定します。これは、Edge FE がプリント サービスに対する可用性を通知するときに提供される名前です。
<i>name</i>	NetBIOS 名
password-server	クライアントのパスワードの確認に使用するパスワード サーバを指定します。
<i>hostname</i>	パスワード サーバのホスト名
<i>ipaddress</i>	パスワード サーバの IP アドレス
realm	認証に使用する Kerberos レルムを指定します。このレルムは NT 4 ドメインの Active Directory Service (ADS; Active Directory サービス) として使用されます。この引数は Kerberos ADS モードを使用しているときだけ有効です。
<i>kerberos-realm</i>	Kerberos レルムの IP アドレスまたは名前（大文字） Kerberos レルムは通常、Kerberos サーバまたは Active Directory ドメインの DNS 名に設定されます。デフォルト値はヌル文字列です。 例：kerberos-realm = MYBOX.MYCOMPANY.COM
wins-server	Windows Internet Naming Service (WINS) サーバを指定します。
<i>hostname</i>	WINS サーバのホスト名
<i>ipaddress</i>	WINS サーバの IP アドレス
workgroup	WAAS デバイスが所属するワーク グループ（またはドメイン）を指定します。
<i>name</i>	ワーク グループまたはドメインの名前
security	Kerberos 認証を設定します。
ADS	Active Directory Service を指定します。

デフォルト Windows ドメイン オプションはデフォルトで無効です。

コマンドモード グローバル コンフィギュレーション

デバイスモード application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン このグローバル コンフィギュレーション コマンドを使用して、WAAS デバイスの Windows ドメイン サーバパラメータを設定します。

Kerberos 認証を有効にした場合、デフォルトの **realm** は DOMAIN.COM で、**security** は ADS です。Kerberos 認証を無効にした場合、**security** はドメインです。

例 次の例は、*myFileEngine* の NetBIOS 名で、*ABD* ドメインに *10.10.24.1* で、Edge FE 用の Windows ドメイン サーバを設定する方法を示します。また、パスワードサーバも識別します。

```
WAE(config)# windows-domain wins-server 10.10.24.1
WAE(config)# windows-domain password-server 10.10.100.4
WAE(config)# windows-domain netbios-name myFileEngine
WAE(config)# windows-domain workgroup ABC
```

次の例は、**kerberos** コマンドを使用して Kerberos 認証を有効にした場合の Windows ドメイン サーバの設定方法を示します。

```
WAE(config)# windows-domain realm ABC.COM
WAE(config)# windows security ADS

===== checking new config using testparm =====

Load smb config files from /state/actona/conf/smb.conf
Processing section "[print$]"
Processing section "[printers]"
Loaded services file OK.

WAE(config)# exit
WAE# show windows-domain
  Login Authentication for Console/Telnet Session: enabled

Windows domain Configuration:
-----
  Workgroup:
  Comment: Comment:
  Net BIOS: MYFILEENGINE
  Realm: ABC
  WINS Server: 10.10.10.1
  Password Server: 10.10.10.10
  Security: ADS
```

関連コマンド [\(config\) kerberos](#)

[show windows-domain](#)

[windows-domain](#)

インターフェイス コンフィギュレーション モード コマンド

インターフェイス コンフィギュレーション モードは、特定インターフェイスでの WAAS ソフトウェア機能構成の設定、表示、テストに使用します。このモードを開始するには、グローバル コンフィギュレーション モードから **interface** コマンドを入力します。次の例は、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
WAE# configure
WAE(config)# interface ?
  GigabitEthernet  Select a gigabit ethernet interface to configure
  InlineGroup       Select an inline group interface to configure
  PortChannel        Ethernet Channel of interfaces
  Standby            Standby groups
WAE(config)# interface gigabitethernet ?
  <1-2>/ GigabitEthernet slot/port
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)#
```

インターフェイス コンフィギュレーション モードを終了するには、**exit** を入力してグローバル コンフィギュレーション モードに戻ります。

```
WAE(config-if)# exit
WAE(config)#
```

(config-if) autosense

インターフェイスでの自動検知を有効にするには、**autosense** インターフェイス コンフィギュレーション コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

autosense

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト 自動検知はデフォルトで有効です。

コマンド モード インターフェイス コンフィギュレーション

デバイス モード application-accelerator

replication-accelerator

central-manager

使用上のガイドライン シスコ ルータのイーサネット インターフェイスは、デュプレックス設定をネゴシエーションしません。WAAS デバイスをクロスケーブルで直接ルータに接続した場合は、WAAS デバイス インターフェイスを手動でルータのインターフェイス設定と一致するように設定する必要があります。**autosense** を無効にしてからイーサネット インターフェイスを設定してください。**autosense** が有効なときは、手動の設定は上書きされます。自動検知を起動するには WAAS デバイスをリブートする必要があります。

例 次の例はギガビット イーサネット ポート 1/0 での自動検知を無効にします。

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# no autosense
```

次の例はギガビット イーサネット ポート 1/0 での自動検知を再度有効にします。

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# autosense
WAE(config-if)# exit
WAE(config)# exit
WAE# reload
```

関連コマンド (config) interface

show interface

show running-config

show startup-config

(config-if) bandwidth

ネットワーク インターフェイスでのリンク速度を設定するには、**bandwidth** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
bandwidth {10 | 100 | 1000}
```

シンタックスの説明

10	リンク速度を 10 Mbps に設定します。
100	リンク速度を 100 Mbps に設定します。
1000	リンク速度を 1000 Mbps に設定します。このオプションはすべてのポートで利用できるわけではなく、自動検知と同じです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

WAAS デバイス上のネットワーク インターフェイスのリンク速度を設定する場合に、**bandwidth** インターフェイス コンフィギュレーション コマンドを使用します。速度は、Mbps 単位で指定します。速度が 1000 Mbps に設定された場合、WAAS ソフトウェアでは自動的に自動検知を有効にします。

Gigabit over Copper インターフェイスがアップまたはダウンしている場合、ギガビット イーサネット インターフェイス設定（自動検知、リンク速度、およびデュプレックス設定）を設定できます。インターフェイスがアップしている場合は、特定のインターフェイス設定に適用されます。インターフェイスがダウンしている場合は、指定された設定は保存され、インターフェイスが起動したときに適用されます。たとえば、現在ダウンしている Gigabit over Copper インターフェイスに対して次の任意のコマンドを指定した場合、インターフェイスの起動時に自動的にこの設定が適用されます。

```
WAE(config-if)# bandwidth 10
WAE(config-if)# bandwidth 100
WAE(config-if)# bandwidth 1000
WAE(config-if)# autosense
WAE(config-if)# half-duplex
WAE(config-if)# full-duplex
```



(注)

WAE またはルータ、スイッチ、もしくはその他のデバイス上で半二重接続を使用しないことを強く推奨します。半二重を使用すると、パフォーマンスを改善するシステムの機能が妨げられるため、適切ではありません。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を再度チェックし、全二重が設定されていることを確認します。

例

次の例は、インターフェイスの帯域幅を 1000 Mbps に設定する方法を示します。

```
WAE(config-if)# bandwidth 1000
```

次の例は、インターフェイスに対してデフォルトの帯域幅の値を元に戻す方法を示します。

```
WAE(config-if)# no bandwidth
```

関連コマンド

[\(config-if\) autosense](#)

[\(config\) interface](#)

(config-if) cdp

すべてのインターフェイス上ではなく、WAAS デバイスの特定のインターフェイス上で Cisco Discovery Protocol (CDP; シスコ検出プロトコル) を有効にするには、インターフェイス コンフィギュレーション モードで **cdp** コマンドを使用します。

```
cdp {enable}
```

シンタックスの説明

enable	特定のインターフェイスで CDP を有効にします。
---------------	---------------------------

デフォルト

デフォルトの動作や値はありません。

コマンドモード

インターフェイス コンフィギュレーション

デバイスモード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

グローバル コンフィギュレーション モードで **cdp enable** コマンドを使用すると、WAAS デバイスのすべてのインターフェイス上でグローバルに CDP を有効にします。インターフェイスごとに CDP の動作を制御するには、インターフェイス コンフィギュレーション モードで **cdp enable** コマンドを使用します。



(注)

インターフェイス レベルで CDP を有効にすると、グローバル制御を上書きします。ただし、特定のインターフェイスで CDP を有効にする前に、WAAS デバイスで CDP をグローバルに有効にする必要があります。そうしないと、コマンド出力に次のメッセージが表示されます。

```
WAE(config-if)# cdp enable
Cannot enable CDP on this interface, CDP Global is disabled
```

例

次の例では、WAAS デバイスのギガビット イーサネット インターフェイス (スロット 1/ポート 0) で CDP を有効にします。

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

関連コマンド

[\(config\) cdp](#)

[show cdp](#)

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config-if) exit

インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

exit

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード すべてのモード

デバイス モード application-accelerator
replication-accelerator
central-manager

例 次の例は、インターフェイス コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

```
WAE(config-if)# exit  
WAE(config)#
```

(config-if) failover timeout

障害が発生してからトラフィックを別のポートに移行するまでのインライン インターフェイスの最大時間を設定するには、**failover timeout** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

failover timeout {1 | 3 | 5}

シンタックスの説明

1	フェールオーバーまでの秒数を指定します。
3	フェールオーバーまでの秒数を指定します。
5	フェールオーバーまでの秒数を指定します。

デフォルト

デフォルトは 1 秒です。

コマンド モード

インターフェイス コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

failover timeout コマンドは、inlineGroup インターフェイスで使用されます。このコマンドは、電力の停止やカーネル クラッシュなどの障害が発生してから **fail-to-wire** モードの動作に移行するまでのインライン インターフェイスの最大時間を秒数で設定します。たとえば、タイムアウトを 3 秒に設定すると、WAE の電力が停止したり、カーネル クラッシュに陥ったりした場合に、最大 3 秒間トラフィックがドロップします。この時間を経過すると、グループ インターフェイスの両ポートで受信されたすべてのトラフィックがグループの他のポートから送信されます。デフォルトのタイムアウトは 1 秒です。

例

次の例では、スロット 1 に設置されたアダプタのインライン グループ 0 のフェールオーバー時間の制限値を 5 秒に設定してから、この設定を削除します。

```
(config)# interface inlineGroup 1/0
(config-if)# failover timeout 5
(config-if)# no failover timeout 5
```

関連コマンド

[\(config\) interface](#)
[\(config-if\) inline](#)
[\(config-if\) shutdown](#)

(config-if) full-duplex

WAAS デバイスでインターフェイスを全二重動作に設定するには、**full-duplex** インターフェイス コンフィギュレーション コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

full-duplex

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード インターフェイス コンフィギュレーション

デバイス モード application-accelerator

replication-accelerator

central-manager

使用上のガイドライン この EXEC コマンドを使用して、インターフェイスを全二重動作に設定します。全二重では、データは、インターフェイスまたはケーブルを介して同時に双方向に移動できます。半二重設定では、指定した時間には必ず、データが一方方向にのみ移動することを保証します。全二重は高速ですが、このモードではインターフェイスが効率的に動作できないことがあります。データの衝突やネットワーク エラーが多すぎる場合は、全二重ではなく半二重にインターフェイスを設定してください。



(注) WAE またはルータ、スイッチ、もしくはその他のデバイス上で半二重接続を使用しないことを強く推奨します。半二重を使用すると、パフォーマンスを改善するシステムの機能が妨げられるため、適切ではありません。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を再度チェックし、全二重が設定されていることを確認します。

例 次の例は、スロット 1/ポート 0 のギガビット イーサネット インターフェイスを全二重動作に設定します。

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# full-duplex
```

The following example disables full-duplex operation:

```
WAE(config-if)# no full-duplex
```

関連コマンド [\(config-if\) half-duplex](#)

[\(config\) interface](#)

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config-if) half-duplex

WAAS デバイスでインターフェイスを半二重動作に設定するには、**half-duplex** インターフェイス コンフィギュレーション コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

half-duplex

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード インターフェイス コンフィギュレーション

デバイス モード application-accelerator

replication-accelerator

central-manager

使用上のガイドライン このインターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを半二重動作に設定します。全二重では、データは、インターフェイスまたはケーブルを介して同時に双方向に移動できます。半二重設定では、指定した時間には必ず、データが一方向にのみ移動することを保証します。全二重は高速ですが、このモードではインターフェイスが効率的に動作できないことがあります。データの衝突やネットワーク エラーが多すぎる場合は、全二重ではなく半二重にインターフェイスを設定してください。



(注) WAE またはルータ、スイッチ、もしくはその他のデバイス上で半二重接続を使用しないことを強く推奨します。半二重を使用すると、パフォーマンスを改善するシステムの機能が妨げられるため、適切ではありません。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を再度チェックし、全二重が設定されていることを確認します。

例 次の例は、スロット 1/ ポート 0 のギガビット イーサネット インターフェイスを半二重動作に設定します。

```
WAE# configure
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# half-duplex
```

次の例では、半二重動作を無効にします。

```
WAE(config-if)# no half-duplex
```

関連コマンド [\(config-if\) full-duplex](#)

[\(config\) interface](#)

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config-if) inline

inlineGroup インターフェイスでのインライン代行受信を有効にするには、**inline** インターフェイス コンフィギュレーション コマンドを使用します。インライン代行受信を無効にするには、このコマンドの **no** 形式を使用します。

```
inline [vlan {all | native | vlan_list}]
```

シンタックスの説明

vlan	(オプション) VLAN リストのパラメータを変更します。
all	すべてのタグ付きパケットとタグなしパケットにコマンドを適用します。
native	タグなしパケットを指定します。
vlan_list	このインターフェイス上で許可または制限する VLAN ID のリストです。カンマ (,) を使用してリストのエントリを区切ります。ハイフン (-) を使用して VLAN ID の範囲を指定します。有効な範囲は 0 ~ 4095 です。

デフォルト

WAE インライン ネットワーク アダプタを設置している場合、すべての VLAN でデフォルトは有効です。

コマンド モード

インターフェイス コンフィギュレーション

デバイス モード

application-accelerator
 replication-accelerator
 central-manager

使用上のガイドライン

inline コマンドは、inlineGroup インターフェイスで使用されます。このコマンドはインライン代行受信を有効または無効にします。VLAN リストを省略すると、すべての VLAN タグ付きパケットまたはタグなしパケットにコマンドが適用されます。指定された VLAN セットにインライン機能を制限できます。

VLAN リストを「all」、カンマ区切りの VLAN ID のリスト、または VLAN ID の範囲にすることができます。タグなしパケットを指定するために、特別な VLAN ID である「native」を加えることができます。



(注) インライン検査がアクティブの場合、すべての VLAN のインライン機能を明示的に無効にするまで WCCP を設定できません。反対に、WCCP を無効にするまでインライングループのインライン代行受信を有効にできません。

例

次の例は、スロット 1 に設置されているアダプタの inlineGroup 0 のポートで受信された任意の VLAN ID を持つすべてのタグなしパケットとタグ付きパケットのインライン代行受信を有効にする方法を示します。

```
(config)# interface inlineGroup 1/0
(config-if)# inline
(config-if)# exit
```

■ (config-if) inline

次の例は、VLAN ID 5 または 10 ~ 15 の VLAN ID を含む、802.1Q カプセル化パケットの同一ポートでのインライン代行受信を無効にする方法を示します。2 つの VLAN が所定の順序で組み合わされている場合、スロット 1 のグループ 0 のポートで受信されるすべてのパケット (VLAN 5、10、11、12、13、14、および 15 を除く) で代行受信が行われます。

```
(config)# interface inlineGroup 1/0
(config-if)# no inline vlan 5,10-15
(config-if)# exit
```

次の例は、スロット 2 のグループ 1 のポートですべてのタグなしトラフィックおよび VLAN 0 ~ 100 のみのトラフィックのインライン代行受信を有効にする方法を示します。

```
(config)# interface inlineGroup 2/1
(config-if)# no inline vlan 101-4095
(config-if)# exit
```

次の例は、スロット 2 のグループ 1 のポートで VLAN 395 のみのトラフィックのインライン代行受信を有効にする方法を示します。デフォルトの動作では、すべての VLAN でトラフィックの代行受信が有効になっているため、まずすべての VLAN で代行受信を無効にし、それから有効にする VLAN のみ有効に設定します。

```
(config)# interface inlineGroup 2/1
(config-if)# no inline vlan all
(config-if)# inline vlan 395
(config-if)# exit
```

関連コマンド

[show interface](#)

(config-if) ip

IP アドレスまたはサブネットマスクを設定したり、WAAS デバイスのインターフェイス上の DHCP から IP アドレスをネゴシエーションしたりするには、**ip** インターフェイス コンフィギュレーション コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

```
ip address {ip-address ip-subnet [secondary] | dhcp [client-id id [hostname name] | hostname name [client-id id]}
```

シンタックスの説明

address	インターフェイスの IP アドレスを設定します。
<i>ip-address</i>	IP アドレス
<i>ip-subnet</i>	IP サブネットマスク
secondary	(オプション) この IP アドレスをセカンダリ アドレスにします。
dhcp	DHCP でネゴシエーションした IP アドレスを設定します。
client-id	(オプション) クライアント ID を指定します。
<i>id</i>	クライアントの識別情報
hostname	(オプション) ホスト名を指定します。
<i>name</i>	ホスト名

デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション

デバイス モード

application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

このコマンドを使用して、WAAS デバイスのネットワーク インターフェイスの IP アドレス、サブネットマスク、DHCP IP アドレス ネゴシエーションの設定や変更を行います。IP アドレスへの変更は、すぐに有効となります。

ip address インターフェイス コンフィギュレーション コマンドにより、次のように指定されたインターフェイスのセカンダリ IP アドレスの設定が可能になります。

```
WAE(config-if)# ip address ip_address netmask [secondary]
```

各インターフェイスについて最大 4 つのセカンダリ IP アドレスを指定できます。同一 IP アドレスは複数のインターフェイスに割り当てできません。セカンダリ IP アドレスは、プライマリ IP アドレスが設定されている場合にのみ、アクティブになります。次のコマンドはプライマリ IP アドレスを設定します。

```
WAE(config-if)# ip address ip_address netmask
```

セカンダリ IP アドレスは、インターフェイスがシャットダウンすると無効になり、インターフェイスが起動すると有効になります。

特定の IP アドレスを無効にするには、このコマンドの **no** 形式を使用します。

```
WAE(config-if)# no ip address ip_address netmask
```



(注)

同一のサブネットで、2つのインターフェイスが IP アドレスを持つことはできません。

再利用可能な IP アドレスを DHCP からネゴシエーションするには、**ip-address dhcp** コマンドを使用します。

例

次の例は、IP アドレスが 10.10.10.10、ネットマスクが 255.0.0.0 のポート チャネル インターフェイスを設定する方法を示します。

```
WAE# configure
WAE(config)# interface PortChannel 2
WAE(config-if)# ip address 10.10.10.10 255.0.0.0
```

次の例では、インターフェイスに設定された IP アドレスを削除します。

```
WAE(config-if)# no ip address
```

次の例では、インターフェイスを DHCP 対応として有効にします。

```
WAE(config-if)# ip address dhcp
```

次の例では、DHCP サーバに送信する、WAAS デバイスのクライアント ID とホスト名を設定します。

```
WAE(config-if)# ip address dhcp client-id myclient hostname myhost
```

関連コマンド

[\(config\) interface](#)

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config-if) ip access-group

定義済みアクセス リストを適用することによって、WAAS デバイスの特定のインターフェイスでの接続を制御するには、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用します。アクセス リストを無効にするには、このコマンドの **no** 形式を使用します。

```
ip access-group {acl-name | acl-num} {in | out}
```

シンタックスの説明

<i>acl-name</i>	最大 30 文字の英数字の ID で、文字で始まります。現在のインターフェイスに適用する ACL を識別します。
<i>acl-num</i>	現在のインターフェイスに適用するアクセス リストを識別する数値の ID。有効な範囲は、標準のアクセス リストでは 1 ~ 99、拡張アクセス リストでは 100 ~ 199 です。
in	指定されたアクセス リストを現在のインターフェイスの着信パケットに適用します。
out	指定されたアクセス リストを現在のインターフェイスの発信パケットに適用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション

デバイス モード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイス上のアクセス リストをアクティブにします。各インターフェイスについて、発信アクセス リストと着信アクセス リストをそれぞれ 1 つずつ使用できます。

ip access-group コマンドを入力する前に、アクセス リストを適用するインターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。**ip access-list** コマンドを使用して、適用するアクセス リストを定義します。

例

次の例では、インターフェイス ギガビット イーサネット 1/2 のアウトバウンド トラフィックに対して、**acl-out** という名前のアクセス リストを適用します。

```
WAE(config)# interface GigabitEthernet 1/2  
WAE(config-if)# ip access-group acl-out out
```

関連コマンド

clear
(config) ip access-list
show ip access-list

(config-if) mtu

インターフェイスの最大伝送ユニット (Maximum Transmission Unit; MTU) パケットサイズを設定するには、**mtu** インターフェイス コンフィギュレーション コマンドを使用します。MTU パケットサイズをリセットするには、このコマンドの **no** 形式を使用します。

```
mtu mtusize
```

シンタックスの説明

<i>mtusize</i>	MTU パケット サイズ (バイト単位で 88 ~ 1500)
----------------	---------------------------------

デフォルト

デフォルトの動作や値はありません。

コマンドモード

インターフェイス コンフィギュレーション

デバイスモード

application-accelerator
replication-accelerator
central-manager

使用上のガイドライン

MTU は、特定のデータ リンク接続を使用して転送できる IP データグラムの最大サイズです。**mtu** コマンドを使用して、最大パケット サイズ (バイト単位) を設定します。

例

次の例では、MTU を 1500 バイトに設定し、その後、その設定を削除します。

```
WAE(config-if)# mtu 1500
WAE(config-if)# no mtu 1500
```

関連コマンド

[show interface](#)
[show running-config](#)
[show startup-config](#)

(config-if) no

ギガビットイーサネットインターフェイスコンフィギュレーションコマンドを無効にするか、そのデフォルトを設定するには、ギガビットイーサネットインターフェイスコンフィギュレーションモードで次の **no** コマンドを使用します。

```
no [autosense | bandwidth {10 | 100 | 1000} | cdp enable | channel-group {1 | 2} | description text |
full-duplex | half-duplex | ip {access-group {acl-num | acl_name} {in | out} | address {ip_address
netmask [secondary]} | dhcp {client-id id hostname name | hostname name client-id id}} | mtu
mtusize | shutdown | standby grpnumber [priority priority]]
```

InlineGroup インターフェイスコンフィギュレーションコマンドを無効にするか、そのデフォルトを設定するには、InlineGroup インターフェイスコンフィギュレーションモードで、次の **no** コマンドを使用します。

```
no [autosense | bandwidth {10 | 100 | 1000} | failover timeout {1 | 3 | 5} | full-duplex | half-duplex |
inline [vlan {all | native | vlan_list}] | shutdown]
```

PortChannel インターフェイスコンフィギュレーションコマンドを無効にするか、そのデフォルトを設定するには、PortChannel インターフェイスコンフィギュレーションモードで、次の **no** コマンドを使用します。

```
no [description text | ip {access-group {acl-num | acl_name} {in | out} | address ip-address netmask} |
shutdown]
```

シンタックスの説明

コマンドのオプションは一貫していません。構文の詳細については、「(config) interface」コマンドを参照してください。

コマンドのデフォルト設定

デフォルトの動作や値はありません。

コマンドモード

インターフェイス コンフィギュレーション

デバイスモード

application-accelerator

replication-accelerator

central-manager

■ (config-if) no

使用上のガイドライン

no インターフェイス コンフィギュレーション コマンドのコマンド オプションは、現在のインターフェイス コンフィギュレーション モードによって異なります。たとえば、ギガビット インターフェイス コンフィギュレーション モードの場合、no コマンドには 11 個のオプションがあります。

```
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# no ?
  autosense      Interface autosense
  bandwidth      Interface bandwidth
  cdp            Cisco Discovery Protocol Interface Config commands
  channel-group  Configure EtherChannel group
  description    Interface specific description
  full-duplex    Interface fullduplex
  half-duplex    Interface halfduplex
  ip            Interface Internet Protocol Config commands
  mtu           Set the interface Maximum Transmission Unit (MTU)
  shutdown      Shutdown the specific interface
  standby       Standby interface config commands
WAE(config-if)# no
```

ただし、スタンバイ インターフェイス コンフィギュレーション モードの場合は、no コマンドのオプションは 4 個しかありません。

```
WAE(config)# interface standby 4
WAE(config-if)# no ?
  description  Standby interface description
  errors       Set the maximum number of errors allowed on this interface
  ip          Set the IP address of a standby group
  shutdown    Shutdown this interface
WAE(config-if)# no
```

例

次の例では、スロット 2、ポート 0 のギガビット インターフェイスがインターフェイス帯域幅を自動検知しないように設定します。

```
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# no autosense
```

関連コマンド

[\(config\) interface](#)

[show interface](#)

[show running-config](#)

[show startup-config](#)

(config-if) shutdown

WAAS デバイスの特定のハードウェア インターフェイスをシャットダウンするには、**shutdown** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスを稼働状態に戻すには、このコマンドの **no** 形式を使用します。

shutdown

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード インターフェイス コンフィギュレーション

デバイス モード application-accelerator
replication-accelerator
central-manager

使用上のガイドライン 代替構文は、「[\(config\) interface](#)」コマンドを参照してください。

例 次の例では、WAAS デバイスのギガビット イーサネット インターフェイスをシャットダウンします。

```
WAE# configure
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# shutdown
```

関連コマンド [\(config\) interface](#)

[show interface](#)

[show running-config](#)


[show startup-config](#)

(config-if) standby

WAAS デバイスのインターフェイスが別のインターフェイスをバックアップするように設定するには、インターフェイス コンフィギュレーション モードで **standby** コマンドを使用します。このコマンドの **no** 形式を使用すると、インターフェイスのデフォルト設定に戻ります

```
standby group_number {description text | errors max-errors | ip ip-address netmask | priority
priority_level | shutdown}
```

シンタックスの説明

group_number	スタンバイ グループ番号 (1 ~ 4)
description	(オプション) 指定されたインターフェイスの説明を設定します。
text	指定されたインターフェイスの説明。説明のテキストの長さは最大 240 文字です。
errors	インターフェイスがシャットダウンし、スタンバイ インターフェイスが起動するまでに、アクティブなインターフェイスで許容されるエラーの最大数を設定します。このオプションはデフォルトで無効に設定されています。
max-errors	エラーの最大数 (0 ~ 4294967295)
ip	指定されたスタンバイ グループ (Standby Group 1、2、3、4 のいずれか) の IP アドレスを設定します。
ip-address	指定されたスタンバイ グループ (Standby Group 1、2、3、4 のいずれか) の IP アドレス。スタンバイ グループのグループ IP アドレスとネットマスクは、メンバインターフェイスのすべてに対して設定する必要があります。
netmask	指定されたスタンバイ グループ (Standby Group 1、2、3、4 のいずれか) の ネットマスク
priority	スタンバイ グループ内のメンバ インターフェイスのプライオリティを設定します。メンバインターフェイスのプライオリティは、実行時に変更できません。この変更後、最高のプライオリティを持つメンバ インターフェイスが、新しいアクティブ インターフェイスになります (デフォルトの動作は、プライオリティの高いインターフェイスが存在する場合に、現在アクティブなインターフェイスをプリエンプトすることです)。
priority_level	各メンバ インターフェイスには、プライオリティの数値が割り当てられます。最も高いプライオリティ数値を持つメンバインターフェイスが、そのスタンバイ グループのアクティブ インターフェイスになります。アクティブ インターフェイスだけがグループ IP アドレスを使用できます。 プライオリティの数値なしで priority オプションを指定した場合、デフォルト値の 100 が使用されます。
shutdown	(オプション) 指定されたスタンバイ グループ (Standby Group 1、2、3、4 のいずれか) をシャットダウンします。スタンバイ グループのグループ IP アドレスを設定していなくても、スタンバイ グループをシャットダウンできます。
	
(注)	スタンバイ グループをシャットダウンすると、このスタンバイ グループによって以前に生成されたアラームがすべてクリアされます。

デフォルト

デフォルトではスタンバイ インターフェイスはありません。**errors** オプションはデフォルトで無効に設定されています。

コマンドモード インターフェイス コンフィギュレーション

デバイスモード application-accelerator

replication-accelerator

central-manager

使用上のガイドライン

複数のインターフェイスを、WAAS デバイスの別のインターフェイスのバックアップ インターフェイス (スタンバイ インターフェイス) として機能するように設定できます。この機能を「スタンバイ インターフェイスのサポート」と呼びます。スタンバイ グループは、インターフェイスの論理グループであり、この機能を実装するために使用します。アクティブなネットワーク インターフェイスに障害が発生 (原因はケーブルの問題、レイヤ 2 スイッチの障害、高いエラー数、またはその他の障害) し、そのインターフェイスがスタンバイ グループの一部である場合は、スタンバイ インターフェイスがアクティブになり、障害が発生したインターフェイスのロードを引き取ります。

スタンバイ グループには最低限 2 つのインターフェイスが必要です。スタンバイ グループの一部であるインターフェイスは、「メンバ インターフェイス」と呼ばれます。スタンバイ グループの作成後、どのインターフェイスをこの論理グループに割り当てるかを定義します。メンバ インターフェイスの定義の一環として、スタンバイ グループ内の各メンバ インターフェイスのプライオリティを指定します。最も高いプライオリティを割り当てられたメンバ インターフェイスが、その特定スタンバイ グループのアクティブ インターフェイスになります。アクティブ インターフェイスに障害が発生した場合は、スタンバイ グループ内で次にプライオリティの高い動作可能なメンバがアップされます。その特定のスタンバイ グループのすべてのメンバ インターフェイスがダウンし、そのあとにメンバ インターフェイスの 1 つがアップした場合、WAAS ソフトウェアはこの状況を検出し、アップしたメンバ インターフェイスの上にスタンバイ グループを持ってきます。

スタンバイ グループ内のメンバ インターフェイスの障害またはフェールオーバーは、アラームとトラップを発生させます (WAAS デバイスでアラームとトラップが有効になっている場合)。アラームはスタンバイ グループのメンバ インターフェイス間でフェールオーバーが発生すると送出されます。具体的には、メンバ インターフェイスに障害が発生したときに、マイナー アラームが送出され、このアラームは、インターフェイスのフェールオーバーが正常に終了すると、自動的にクリアされます。メジャー アラームは、スタンバイ グループがダウンすると (つまり、スタンバイ グループのメンバ インターフェイスが起動しない) 送出されます。



(注)

物理インターフェイスは複数のスタンバイ グループに所属できます。したがって、1 つのインターフェイスは複数のスタンバイ グループのスタンバイ インターフェイスとして機能できます。

スタンバイ インターフェイスを設定するには、インターフェイスを論理的にスタンバイ グループに割り当てます。次の規則により、スタンバイ グループの関係を定義します。

- 各スタンバイ グループに一意のスタンバイ IP アドレスを割り当て、スタンバイ グループのすべてのメンバ インターフェイスで共有する。スタンバイ グループの IP アドレスはメンバ インターフェイス間で共有されますが、スタンバイ グループのアクティブ インターフェイスだけが常にこの共有 IP アドレスを使用します。この共有 IP アドレスは、アクティブ インターフェイスのエイリアスとして設定されます。
- 信頼性向上のため、メンバ インターフェイスのデプレックスおよび速度設定値を設定する。
- スタンバイ グループのすべてのメンバ インターフェイスに障害が発生し、1 つが回復した場合、WAAS ソフトウェアは、動作可能なメンバ インターフェイスの上にスタンバイ グループを持ってくる。

- 物理インターフェイスがポート チャネル グループのメンバである場合は、スタンバイ グループに参加できない。同様に、物理インターフェイスがスタンバイ グループのメンバである場合は、ポート チャネル グループに参加できない。
- スタンバイ グループは2つ以上のインターフェイスで構成される。
- WAAS デバイスでのスタンバイ グループの最大数は4である。



(注)

インターフェイス IP アドレスおよびスタンバイ グループ IP アドレスは、動作の信頼性を確保するため別のサブネット上にある必要があります。ダミーの IP アドレスをプライベートアドレス領域で使用してインターフェイスのプライマリ IP アドレスとして機能させ、実際の WAAS デバイスの IP アドレスを使用して別のサブネットのスタンバイ グループ IP アドレスとして機能させ、この要求を満たすことができます。ダミーの IP アドレスを使用した場合、このインターフェイス IP アドレスはインターフェイス起動の代替手段としてしか機能しません。たとえば、WAAS デバイスのインターフェイスは初期化のため、インターフェイスの IP アドレスが必要です。必ず、**ip route** コマンドではなく、**ip default-gateway** 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、インターフェイスのデフォルト ゲートウェイを設定してください。

- スタンバイ グループの各インターフェイスに、プライオリティを割り当てる。スタンバイ グループで最も高いプライオリティを持つ動作可能なインターフェイスが、アクティブ インターフェイスになります。アクティブ インターフェイスだけがグループ IP アドレスを使用できます。
- スタンバイ グループ内インターフェイスのプライオリティは、実行時に変更できる。この変更後、最高のプライオリティを持つメンバインターフェイスが、新しいアクティブ インターフェイスになります（デフォルトの動作は、プライオリティの高いインターフェイスが存在する場合に、現在アクティブなインターフェイスをプリエンプトすることです）。
- インターフェイスをシャットダウンし、スタンバイ インターフェイスを起動するまでにアクティブ インターフェイス上で許容されるエラーの最大数は、**errors** オプションで設定する。これはデフォルトでは、無効に設定されています。



ヒント

インターフェイスが複数のスタンバイ グループに所属する場合、ロード バランシングの向上のため、各スタンバイグループのインターフェイスに異なるプライオリティを設定できます。たとえば、インターフェイス ギガビット イーサネット 1/0 およびギガビット イーサネット 2/0 は、ともにスタンバイ グループ 1 とスタンバイ グループ 2 にあります。ギガビット イーサネット 1/0 をスタンバイ グループ 1 で最高のプライオリティに設定し、ギガビット イーサネット 2/0 をスタンバイ グループ 2 で最高のプライオリティに設定した場合、スタンバイ グループ 1 はギガビット イーサネット 1/0 をアクティブ インターフェイスとして使用し、スタンバイ グループ 2 ではギガビット イーサネット 2/0 をアクティブ インターフェイスとして使用します。この設定により、各インターフェイスは、どちらかに障害が発生した場合、もう 1 つのインターフェイスでバックアップできます。



(注)

ポート チャネルとは異なり、スタンバイ グループはグループ レベルで IP ACL をサポートしません。ただし、スタンバイ グループのメンバインターフェイスがインターフェイス レベルで IP ACL をサポートするように設定できます。たとえば、個別に **Standby Group 1** の 2 つのメンバインターフェイスを設定（ギガビット イーサネット スロット 1/ ポート 0 インターフェイスとギガビット イーサネット スロット 2/ ポート 0 インターフェイス）して、**ACL1** という名前の IP ACL をサポートできますが、**Standby Group 1** が **ACL1** をサポートするようには設定できません。

例 次の例は、2つのギガビットイーサネットインターフェイスが、インターフェイス 1/0 をアクティブインターフェイスとして、同じスタンバイグループのメンバになるように設定します。

```
WAE(config-if)# interface gigabitEthernet 1/0 standby 1 ip 10.16.10.10 255.255.254.0
WAE(config-if)# interface gigabitEthernet 2/0 standby 1 ip 10.16.10.10 255.255.254.0
WAE(config-if)# interface gigabitEthernet 1/0 standby 1 priority 300
WAE(config-if)# interface gigabitEthernet 2/0 standby 1 priority 200
WAE(config-if)# interface gigabitEthernet 1/0 standby 1 errors 10000
WAE(config-if)# interface gigabitEthernet 2/0 standby 1 errors 10000
```

次の例では、**show standby EXEC** コマンドを入力して、スタンバイグループの設定に関する情報を表示します。次のコマンド出力例では、1つのスタンバイグループ (Standby Group 1) がこの WAAS デバイスに対して設定されています。コマンド出力では、どのメンバインターフェイスがアクティブなインターフェイスであるかも示しています。この場合、アクティブなインターフェイスはギガビットイーサネットスロット 1/ポート 0 インターフェイスです。

```
WAE# show standby
Standby Group: 1
  Description: This a backup for Gigabit Ethernet 2/0.
  IP address: 10.16.10.10, netmask: 255.0.0.0
  Member interfaces: none
  Active interface: Gigabit Ethernet 1/0
  Maximum errors allowed on the active interface: 500
```



(注) 特定のスタンバイグループ設定に関する情報を表示するには、**show interface standby group_number EXEC** コマンドを入力します。

次の例では、スタンバイグループ Standby Group 1 を作成します。

```
WAE# configure
WAE(config)# interface standby 1
WAE(config-if)#
```

次の例では、Standby Group 1 にグループ IP アドレス 10.10.10.10 とネットマスク 255.0.0.0 を割り当てます。グループ IP アドレスは、スタンバイグループがシャットダウンされているかどうかに関係なく設定できます。

```
WAE(config-if)# ip address 10.10.10.10 255.0.0.0
WAE(config-if)# errors 500
```

次の例は、2つのギガビットイーサネットインターフェイスを Standby Group 1 に追加して、これらのメンバインターフェイスそれぞれにグループ内のプライオリティを割り当てる方法を示します。

- a. 最初にギガビットイーサネットインターフェイス (スロット 1/ポート 0) を Standby Group 1 に追加し、プライオリティ 150 を割り当てます。

```
WAE(config)# interface gigabitEthernet 1/0
WAE(config-if)# standby 1 priority 150
```

- b. 次に、2番めのギガビットイーサネットインターフェイス (スロット 2/ポート 0) を Standby Group 1 に追加し、プライオリティ 100 (デフォルト値) を割り当てます。

```
WAE(config)# interface gigabitEthernet 2/0
WAE(config-if)# standby 1
WAE(config-if)# exit
WAE(config)#
```

(config-if) standby

GigabitEthernet 0/0 に、グループ内の全メンバー インターフェイスの中で最高のプライオリティが割り当てられているため（プライオリティの数値が 150）、起動時にはそのグループのアクティブ インターフェイスとして選択されます。

次の例は、**standby** コマンドの **no** 形式を使用して、GigabitEthernet スロット 1/ ポート 0 インターフェイスを Standby Group 1 から削除します。

```
WAE(config)# interface gigabitEthernet 1/0
WAE(config-if)# no standby 1
WAE(config-if)# exit
WAE(config)#
```

次の例は、Standby Group 1 をシャットダウンする方法を示しています。スタンバイ グループをシャットダウンすると、このスタンバイ グループによってそれ以前に生成されたアラームはすべてクリアされます。

```
WAE(config)# interface standby 1
WAE(config-if)# exit
WAE(config)# exit
```

次の例は、Standby Group 1 を削除する方法を示します。

```
WAE(config)# interface standby 1
WAE(config-if)# no ip address 10.10.10.10 255.0.0.0
Please remove member interface(s) from this standby group first.
WAE(config)# interface GigabitEthernet 2/0
WAE(config-if)# no standby 1
WAE(config-if)# exit
WAE(config)# interface standby 1
WAE(config-if)# no ip address 10.10.10.10 255.0.0.0
WAE(config-if)# exit
WAE(config)# no interface standby 1
WAE(config)# exit
```

関連コマンド

[\(config\) interface](#)

[show interface](#)

[show running-config](#)

[show standby](#)

[show startup-config](#)

標準 ACL コンフィギュレーション モード コマンド

グローバル コンフィギュレーション モードから、標準 ACL コンフィギュレーション モードおよび拡張 ACL コンフィギュレーション モードを開始できます。

- 標準アクセス リストを使用するには、グローバル コンフィギュレーション モードのプロンプトから **ip access-list standard** コマンドを入力します。CLI がコンフィギュレーション モードを開始すると、それ以降に入力するコマンドはすべて、現在のアクセス リストに適用されます。
- 拡張アクセス リストを使用するには、グローバル コンフィギュレーション モードのプロンプトから **ip access-list extended** コマンドを入力します。CLI がコンフィギュレーション モードを開始すると、それ以降に入力するコマンドはすべて、現在のアクセス リストに適用されます。

ACL コンフィギュレーション モードを終了するには、**exit** を入力してグローバル コンフィギュレーション モードに戻ります。

```
WAE(config-std-nacl)# exit
WAE(config)#
```

グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。

(config) ip access-list standard

インターフェイスまたはアプリケーションへのアクセスを制御するために WAAS デバイスの標準アクセス リストを作成および変更するには、**ip access-list standard** 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。標準アクセス リストを無効にするには、このコマンドの **no** 形式を使用します。

```
ip access-list standard {acl-name | acl-num}
```

シンタックスの説明

standard	標準 ACL コンフィギュレーション モードを有効にします。CLI が標準 ACL コンフィギュレーション モードを開始すると、それ以降に入力するコマンドはすべて、現在の標準アクセス リストに適用されます。(config-std-nacl) プロンプトが表示されます。 WAE(config-std-nacl)#
acl-name	ACL コンフィギュレーション モードから入力されたすべてのコマンドが適用するアクセス リスト。最大 30 文字の英数字文字列を使用し、文字で始まります。
acl-num	アクセス リスト コンフィギュレーション モードから入力されたすべてのコマンドが適用するアクセス リスト。数値識別情報を使用します。標準アクセス リストの有効な範囲は、1 ~ 99 です。

デフォルト

アクセス リストは、少なくとも 1 つの **permit** エントリが設定されていないかぎり、すべてのパケットをドロップします。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
central-manager

使用上のガイドライン

アクセス リストは、WAAS デバイスの特定のアプリケーションまたはインターフェイスへのアクセスを制御するために使用してください。アクセス コントロール リストは、パケットの種類を指定する複数のエントリで構成され、WAAS デバイスはこのパケットをドロップするかさらに処理するため受け入れます。WAAS デバイスは、アクセス リストに出現する順序で各エントリを適用します。この順序はデフォルトでは、エントリが設定された順序です。



(注)

ルータに定義されている IP ACL は、WAE に定義されている IP ACL より優先されます。WAE に定義されている IP ACL は、WAE に定義されている WAAS アプリケーション定義ポリシーより優先されます。

ACL コンフィギュレーション モード内では、編集コマンド (**list**、**delete**、**move**) を使用して、現在の条件エントリを表示したり、特定のエントリを削除したり、エントリの評価順序を変更したりできます。グローバル コンフィギュレーション モードに戻るには、ACL コンフィギュレーション モードプロンプトで **exit** を入力します。

エントリを作成するには、**deny** または **permit** キーワードを使用して、WAAS デバイスにドロップさせる、またはさらに処理するために受け入れさせるパケットのタイプを指定します。デフォルトでは、アクセス リストはすべてを拒否します。アクセス リストが暗黙の **deny any** エントリで終了しているためです。したがって、少なくとも 1 つの **permit** エントリを指定して、有効なアクセス リストを作成する必要があります。

アクセス リストを作成した後、**access-group** コマンドを使用してアクセス リストをアクセス グループに組み入れることができます。このコマンドはアクセス リストの適用方法を決定します。アクセス リストは、当該のコマンドを使用すれば特定のアプリケーションにも適用できます。存在しないアクセス リストの参照は、**permit any** 条件文と同等です。

標準アクセス リストを作成するには、**ip access-list standard** 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。新しいまたは既存のアクセス リストは、文字または数字で始まる、最大 30 文字の長さの名前を付けて識別します。標準アクセス リストを識別するために番号を使用する場合、番号の範囲は 1 ~ 99 です。



(注)

SNMP サーバまたは TFTP ゲートウェイ / サーバのアクセスには標準アクセス リストを使用する必要があります。ただし、WCCP アプリケーションへのアクセスには、標準アクセス リストまたは拡張アクセス リストのどちらでも使用できます。

通常は、標準アクセス リストを使用して、特定の IP アドレスを持つホスト、または特定のネットワークのホストからの接続を許可します。特定のホストからの接続を許可するには、**permit host source-ip** オプションを使用し、**source-ip** には指定されたホストの IP アドレスを指定します。

特定のネットワークからの接続を許可するには、**permit host source-ip wildcard** オプションを使用します。**source-ip** には、ネットワーク ID または指定したいネットワークのホストの IP アドレスを指定します。**wildcard** には、マスクをドット区切り 10 進表記で指定します。これはサブネット マスクとは逆で、0 は照合が必要な位置を示し、1 は無視する位置を示します。たとえば、ワイルドカード 0.0.0.255 により、送信元 IP アドレスの最後の 8 ビットは無視されます。したがって、**permit 192.168.1.0 0.0.0.255** のエントリにより、192.168.1.0 ネットワークの任意のホストからのアクセスが許可されます。

標準アクセス リストを識別すると、CLI により標準 ACL コンフィギュレーション モードが開始され、以降のコマンドはすべて、指定されたアクセス リストに適用されます。

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# exit
```

例

次の例では、WAAS デバイスで、送信元 IP アドレス 192.168.1.0 からのパケットをすべて許可し、さらに処理するための標準アクセス リストを作成します。

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# permit 192.168.1.0 any
WAE(config-std-nacl)# exit
```

次のコマンドは、インターフェイスのアクセス リストをアクティブにします。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl in
WAE(config-if)# exit
```

次の例は、**show running-configuration** コマンドを実行したときに、この設定がどう表示されるかを示します。

```
...
!  
interface GigabitEthernet 1/0  
 ip address 10.1.1.50 255.255.0.0  
 ip access-group teststdacl in  
 exit  
. . .  
ip access-list standard teststdacl  
 permit 192.168.1.0 any  
 exit  
. . .
```

関連コマンド

clear

show ip access-list

(config-if) ip access-group

(config-std-nacl) deny

(config-std-nacl) delete

(config-std-nacl) list

(config-std-nacl) move

(config-std-nacl) permit

(config-std-nacl) delete

標準 IP ACL から行を削除するには、**delete** コマンドを使用します。

```
delete line-num
```

シンタックスの説明

<i>line-num</i>	アクセスリストの指定された行番号にあるエントリ
-----------------	-------------------------

コマンドモード

標準 ACL コンフィギュレーションモード

デバイスモード

application-accelerator

central-manager

例

次の例では、標準 IP ACL の teststdacl から行 10 を削除します。

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# delete 10
```

関連コマンド

[\(config-std-nacl\) deny](#)

[\(config-std-nacl\) delete](#)

[\(config-std-nacl\) list](#)

[\(config-std-nacl\) move](#)

[\(config-std-nacl\) permit](#)

(config-std-nacl) deny


WAAS デバイスにドロップさせるパケットのタイプを指定する行を標準アクセスリストに追加するには、**deny** コマンドを使用します。

```
[insert line-num] deny {source-ip [wildcard] | host source-ip | any}
```

標準 IP ACL を無効にするには、次の構文を使用します。

```
no deny {source-ip [wildcard] | host source-ip | any}
```

シンタックスの説明

insert	(オプション) 指定された行番号のあとに続く条件を、アクセス リストに挿入します。
<i>line-num</i>	アクセス リストの指定された行番号にあるエントリ
deny	指定された条件に一致するパケットをドロップさせます。
<i>source-ip</i>	送信元 IP アドレス。パケットの送信元となるネットワークまたはホストの番号で、4 桁のドット区切り 10 進表記の 32 ビット数を使用します (たとえば、0.0.0.0)。
<i>wildcard</i>	(オプション) 上記 source-ip アドレスの各部分に対して照合される、4 桁のドット区切り 10 進表記で表わされたワイルドカード。0 は照合するビット、1 は無視するビットを示します。
	 (注) 標準 IP ACL の場合、 ip access-list コマンドの <i>wildcard</i> パラメータは常にオプションです。標準 IP ACL で host キーワードを指定した場合、 <i>wildcard</i> パラメータは認められません。
host	後続の IP アドレスを照合します。
any	任意の IP アドレスを照合します。

デフォルト

アクセス リストは、少なくとも 1 つの **permit** エントリが設定されていないかぎり、すべてのパケットをドロップします。

コマンド モード

標準 ACL コンフィギュレーション モード

デバイス モード

application-accelerator

central-manager

使用上のガイドライン

エントリを作成するには、**deny** または **permit** キーワードを使用して、WAAS デバイスにドロップさせる、またはさらに処理するために受け入れさせるパケットのタイプを指定します。デフォルトでは、アクセス リストはすべてを拒否します。アクセス リストが暗黙の **deny any** エントリで終了しているためです。したがって、少なくとも 1 つの **permit** エントリを指定して、有効なアクセス リストを作成する必要があります。

通常は、標準アクセス リストを使用して、特定の IP アドレスを持つホスト、または特定のネットワークのホストからの接続を許可します。特定のホストからの接続を許可するには、**permit host source-ip** オプションを使用し、*source-ip* には指定されたホストの IP アドレスを指定します。

特定のネットワークからの接続を許可するには、**permit host source-ip wildcard** オプションを使用します。*source-ip* には、ネットワーク ID または指定したいネットワークのホストの IP アドレスを指定します。*wildcard* には、マスクをドット区切り 10 進表記で指定します。これはサブネットマスクとは逆で、0 は照合が必要な位置を示し、1 は無視する位置を示します。たとえば、ワイルドカード 0.0.0.255 により、送信元 IP アドレスの最後の 8 ビットは無視されます。したがって、**permit 192.168.1.0 0.0.0.255** のエントリにより、192.168.1.0 ネットワークの任意のホストからのアクセスが許可されます。

例

次の例では、処理するために送信元 IP アドレス 192.168.1.0 からのパケットをすべて拒否する標準アクセスリストを作成します。

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# deny 192.168.1.0 any
WAE(config-std-nacl)# exit
```

次のコマンドは、インターフェイスの標準アクセスリストをアクティブにします。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl in
WAE(config-if)# exit
```

次の例は、**show running-configuration** コマンドを実行したときに、この設定がどう表示されるかを示します。

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group teststdacl in
 exit
...
ip access-list standard example
 deny 192.168.1.0 any
 exit
...

```

関連コマンド

[\(config-std-nacl\) delete](#)

[\(config-std-nacl\) list](#)

[\(config-std-nacl\) move](#)

[\(config-std-nacl\) permit](#)

(config-std-nacl) exit

標準 ACL コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

exit

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード すべてのモード

デバイス モード application-accelerator
central-manager

例 次の例では、標準 ACL コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

```
WAE(config-std-nacl)# exit  
WAE(config)#
```


(config-std-nacl) list

標準 IP ACL 内の指定したエントリのリストを表示させるには、**list** コマンドを使用します。

```
list [start-line-num [end-line-num]]
```

シンタックスの説明

<i>start-line-num</i>	(オプション) リスト開始行の番号
<i>end-line-num</i>	(オプション) リストの最終行の番号

コマンドモード

標準 ACL コンフィギュレーション モード

デバイス モード

application-accelerator
central-manager

例

次の例では、標準 IP ACL 内の指定したエントリのリストを表示します。

```
WAE(config)# ip access-list standard teststdacl  
WAE(config-std-nacl)# list 25 50
```

関連コマンド

[\(config-std-nacl\) delete](#)
[\(config-std-nacl\) move](#)

(config-std-nacl) move

標準 IP ACL 内の新しい位置に行を移動するには、**move** コマンドを使用します。

```
move old-line-num new-line-num
```

シンタックスの説明

<i>old-line-num</i>	移動するエントリの行番号
<i>new-line-num</i>	エントリの新しい位置。既存のエントリは、アクセスリストの後方に移動します。

コマンドモード

標準 ACL コンフィギュレーションモード

デバイスモード

application-accelerator

central-manager

例

次の例では、標準 IP ACL 内の新しい位置に行を移動します。

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# move 25 30
```

関連コマンド

[\(config-std-nacl\) delete](#)

[\(config-std-nacl\) list](#)

(config-std-nacl) permit


さらに処理するために WAAS デバイスに受け入れさせるパケットのタイプを指定する行を標準アクセスリストに追加するには、**permit** コマンドを使用します。

```
[insert line-num] permit {source-ip [wildcard] | host source-ip | any}
```

標準 IP ACL を無効にするには、次の構文を使用します。

```
no permit {source-ip [wildcard] | host source-ip | any}
```

シンタックスの説明

insert	(オプション) 指定された行番号のあとに続く条件を、アクセス リストに挿入します。
line-num	アクセス リストの指定された行番号にあるエントリ
source-ip	送信元 IP アドレス。パケットの送信元となるネットワークまたはホストの番号で、4 桁のドット区切り 10 進表記の 32 ビット数を使用します (たとえば、0.0.0.0)。
wildcard	(オプション) 上記 source-ip アドレスの各部分に対して照合される、4 桁のドット区切り 10 進表記で表わされたワイルドカード。0 は照合するビット、1 は無視するビットを示します。
	
(注)	標準 IP ACL の場合、 ip access-list コマンドの wildcard パラメータは常にオプションです。標準 IP ACL で host キーワードを指定した場合、 wildcard パラメータは認められません。
host	後続の IP アドレスを照合します。
any	任意の IP アドレスを照合します。

デフォルト

アクセス リストは、少なくとも 1 つの **permit** エントリが設定されていないかぎり、すべてのパケットをドロップします。

コマンド モード

標準 ACL コンフィギュレーション モード

デバイス モード

application-accelerator

central-manager

使用上のガイドライン

エントリを作成するには、**deny** または **permit** キーワードを使用して、WAAS デバイスにドロップさせる、またはさらに処理するために受け入れさせるパケットのタイプを指定します。デフォルトでは、アクセス リストはすべてを拒否します。アクセス リストが暗黙の **deny any** エントリで終了しているためです。したがって、少なくとも 1 つの **permit** エントリを指定して、有効なアクセス リストを作成する必要があります。

通常は、標準アクセス リストを使用して、特定の IP アドレスを持つホスト、または特定のネットワークのホストからの接続を許可します。特定のホストからの接続を許可するには、**permit host source-ip** オプションを使用し、**source-ip** には指定されたホストの IP アドレスを指定します。

特定のネットワークからの接続を許可するには、**permit host source-ip wildcard** オプションを使用します。**source-ip** には、ネットワーク ID または指定したいネットワークのホストの IP アドレスを指定します。**wildcard** には、マスクをドット区切り 10 進表記で指定します。これはサブネット マス

(config-std-nacl) permit

クとは逆で、0 は照合が必要な位置を示し、1 は無視する位置を示します。たとえば、ワイルドカード 0.0.0.255 により、送信元 IP アドレスの最後の 8 ビットは無視されます。したがって、**permit 192.168.1.0 0.0.0.255** のエントリにより、192.168.1.0 ネットワークの任意のホストからのアクセスが許可されます。

例

次の例では、さらに処理するために送信元 IP アドレス 192.168.1.0 からのパケットをすべて許可する標準アクセス リストを作成します。

```
WAE(config)# ip access-list standard teststdacl
WAE(config-std-nacl)# permit 192.168.1.0 any
WAE(config-std-nacl)# exit
```

次のコマンドは、インターフェイスの標準アクセス リストをアクティブにします。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group teststdacl in
WAE(config-if)# exit
```

次の例は、**show running-configuration** コマンドを実行したときに、この設定がどう表示されるかを示します。

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group teststdacl in
 exit
. . .
ip access-list standard example
 permit 192.168.1.0 any
 exit
. . .
```

関連コマンド

[\(config-std-nacl\) delete](#)

[\(config-std-nacl\) deny](#)

[\(config-std-nacl\) list](#)

[\(config-std-nacl\) move](#)

拡張 ACL コンフィギュレーション モード コマンド

インターフェイスまたはアプリケーションへのアクセスを制御するために WAAS デバイスの拡張アクセス リストを作成および変更するには、**ip access-list extended** 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。拡張アクセス リストを無効にするには、このコマンドの **no** 形式を使用します。

```
ip access-list extended {acl-name | acl-num}
```

シンタックスの説明

extended	拡張 ACL コンフィギュレーション モードを有効にします。CLI は、拡張 ACL コンフィギュレーション モードを開始します。このモードでは、以降のすべてのコマンドが現在の拡張アクセス リストに適用されます。次の (config-ext-nacl) プロンプトが表示されます。 WAE(config-ext-nacl)#
acl-name	ACL コンフィギュレーション モードから入力されたすべてのコマンドが適用するアクセス リスト。最大 30 文字の英数字文字列を使用し、文字で始まります。
acl-num	アクセス リスト コンフィギュレーション モードから入力されたすべてのコマンドが適用するアクセス リスト。数値識別情報を使用します。拡張アクセス リストの有効な範囲は、100 ~ 199 です。

デフォルト

アクセス リストは、少なくとも 1 つの **permit** エントリが設定されていないかぎり、すべてのパケットをドロップします。

コマンド モード

グローバル コンフィギュレーション

デバイス モード

application-accelerator
central-manager

使用上のガイドライン

アクセス リストは、WAAS デバイスの特定のアプリケーションまたはインターフェイスへのアクセスを制御するために使用してください。Access Control List (ACL; アクセス コントロール リスト) は、パケットの種類を指定する複数のエントリで構成され、WAAS デバイスはこのパケットをドロップするかさらに処理するため受け入れます。WAAS デバイスは、アクセス リストに出現する順序で各エントリを適用します。この順序はデフォルトでは、エントリが設定された順序です。

次に、WAAS デバイスを使用している環境での ACL の使用方法の例を示します。

- WAAS デバイスは顧客宅内にあり、サービス プロバイダーによって管理され、サービス プロバイダーは管理のためにだけデバイスを保護します。
- WAAS デバイスは企業のどこにでも導入できます。ルータやスイッチと同様、管理者は、IT ソース サブネットへの、Telnet、SSH、および WAAS GUI アクセスを制限しようとしています。

- 強化外部インターフェイスを持つアプリケーション層プロキシファイアウォールでは、ポートは公開されていません。(強化とは、主に安全上の理由から、どのポートがアクセス可能かをインターフェイスが慎重に制限するという事です。外部インターフェイスでは、多様な種類のセキュリティ攻撃が考えられます)。WAE の外部アドレスはインターネット グローバルで、内部アドレスは非公開です。内部インターフェイスには ACL があり、デバイスへの、Telnet、SSH、および WAAS GUI アクセスを制限します。
- WCCP を使用する WAAS デバイスは、ファイアウォールとインターネット ルータ、またはインターネット ルータから離れたサブネットとの間に位置します。WAAS デバイスとルータはともに ACL を備えている必要があります。



(注)

ルータに定義されている ACL は、WAE に定義されている ACL より優先されます。WAE に定義されている ACL は、WAE に定義されている WAAS アプリケーション定義ポリシーより優先されます。

ACL コンフィギュレーション モード内では、編集コマンド (**list**、**delete**、**move**) を使用して、現在の条件エントリを表示したり、特定のエントリを削除したり、エントリの評価順序を変更したりできます。グローバル コンフィギュレーション モードに戻るには、ACL コンフィギュレーション モードプロンプトで **exit** を入力します。

エントリを作成するには、**deny** または **permit** キーワードを使用して、WAAS デバイスにドロップさせる、またはさらに処理するために受け入れさせるパケットのタイプを指定します。デフォルトでは、アクセス リストはすべてを拒否します。アクセス リストが暗黙の **deny any** エントリで終了しているためです。したがって、少なくとも 1 つの **permit** エントリを指定して、有効なアクセス リストを作成する必要があります。

アクセス リストを作成した後、**access-group** コマンドを使用してアクセス リストをアクセス グループに組み入れることができます。このコマンドはアクセス リストの適用方法を決定します。アクセス リストは、当該のコマンドを使用すれば特定のアプリケーションにも適用できます。存在しないアクセス リストの参照は、**permit any** 条件文と同等です。

拡張アクセス リストを作成するには、**ip access-list extended** 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。新しいまたは既存のアクセス リストは、文字または数字で始まる、最大 30 文字の長さの名前を付けて識別します。拡張アクセス リストを識別するために番号を使用する場合、番号の範囲は 100 ~ 199 です。



(注)

SNMP サーバまたは TFTP ゲートウェイ / サーバのアクセスには標準アクセス リストを使用する必要があります。ただし、WCCP アプリケーションへのアクセスには、標準アクセス リストまたは拡張アクセス リストのどちらでも使用できます。

特定のホストからの接続を許可するには、**permit host source-ip** オプションを使用し、**source-ip** には指定されたホストの IP アドレスを指定します。

特定のネットワークからの接続を許可するには、**permit host source-ip wildcard** オプションを使用します。**source-ip** には、ネットワーク ID または指定したいネットワークのホストの IP アドレスを指定します。**wildcard** には、マスクをドット区切り 10 進表記で指定します。これはサブネット マスクとは逆で、0 は照合が必要な位置を示し、1 は無視する位置を示します。たとえば、ワイルドカード 0.0.0.255 により、送信元 IP アドレスの最後の 8 ビットは無視されます。したがって、**permit 192.168.1.0 0.0.0.255** のエントリにより、192.168.1.0 ネットワークの任意のホストからのアクセスが許可されます。

拡張アクセス リストを識別すると、CLI により拡張 ACL コンフィギュレーション モードが開始され、以降のコマンドはすべて、指定されたアクセス リストに適用されます。

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)#
```

例

次のコマンドは、WAAS デバイスでアクセス リストを作成します。このアクセス リストを作成することで、WAAS デバイスにリダイレクトされるすべての Web トラフィックを受け入れ、SSH を使用したホスト管理アクセスを制限します。

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# permit tcp any any eq www
WAE(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

次のコマンドは、インターフェイスのアクセス リストをアクティブにします。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group testextacl in
WAE(config-if)# exit
```

次の例は、**show running-configuration** コマンドを実行したときに、この設定がどう表示されるかを示します。

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group testextacl in
 exit
...
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
...

```

関連コマンド

clear

show ip access-list

(config-if) ip access-group

(config-ext-nacl) deny

(config-ext-nacl) delete

(config-ext-nacl) list

(config-ext-nacl) move

(config-ext-nacl) permit

(config-ext-nacl) delete

拡張 ACL から行を削除するには、**delete** コマンドを使用します。

delete *line-num*

シンタックスの説明

line-num アクセスリストの指定された行番号にあるエントリ

コマンドモード

拡張 ACL コンフィギュレーションモード

デバイスモード

application-accelerator

central-manager

例

次の例では、拡張 ACL の testextacl から行 10 を削除します。

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# delete 10
```

関連コマンド

[\(config-ext-nacl\) list](#)

[\(config-ext-nacl\) move](#)

(config-ext-nacl) deny

WAAS デバイスにドロップさせるパケットのタイプを指定する行を拡張アクセスリストに追加するには、**deny** コマンドを使用します。拡張 ACL に条件を追加する際、オプションは選択したプロトコルによって異なるので注意してください。

IP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] deny {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
```

```
no deny {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
```

TCP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] deny tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

```
no deny tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

UDP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] deny udp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

```
no deny udp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```


ICMP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] deny icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any} [icmp-type [code] | icmp-msg]
```

```
no deny icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any} [icmp-type [code] | icmp-msg]
```

シンタックスの説明

insert	(オプション) アクセス リストの指定された行番号に、指定された条件を挿入します。
<i>line-num</i>	アクセス リストの指定された行番号に、エントリを挿入します。
gre	Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) プロトコルを使用してパケットを照合します。
icmp	ICMP パケットを照合します。
tcp	TCP プロトコルを使用してパケットを照合します。
udp	UDP プロトコルを使用してパケットを照合します。
ip	すべての IP パケットを照合します。
<i>proto-num</i>	(オプション) IP プロトコル番号
<i>source-ip</i>	送信元 IP アドレス。パケットの送信元となるネットワークまたはホストの番号で、4 桁のドット区切り 10 進表記の 32 ビット数を使用します (たとえば、0.0.0.0)。

<i>wildcard</i>	(オプション) 上記 <i>source-ip</i> アドレスの各部分に対して照合される、4 桁のドット区切り 10 進表記で表わされたワイルドカード。0 は照合するビット、1 は無視するビットを示します。
	 (注) 拡張 IP ACL の場合、 ip access-list コマンドの <i>wildcard</i> パラメータは常にオプションです。拡張 IP ACL で host キーワードを指定した場合、 <i>wildcard</i> パラメータは認められません。
host	後続の IP アドレスを照合します。
any	任意の IP アドレスを照合します。
<i>dest-ip</i>	宛先 IP アドレス。パケットの送信先となるネットワークまたはホストの番号で、4 桁のドット区切り 10 進表記の 32 ビット数を使用します (たとえば、0.0.0.0)。
<i>operator</i>	(オプション) 指定されたポートで使用するオペレータ。 lt はより少ない、 gt はより多い、 is は同等、 eq は同等である、 neq は同等でない、および range は範囲内を表します。
<i>port</i>	(オプション) ポート。数値 (0 ~ 65535) またはキーワードを使用します。 range には、2 つのポート番号が必要です。UDP および TCP のキーワードのリストについては、「使用上のガイドライン」セクションを参照してください。
established	(オプション) 確認応答ビットまたはリセット ビットが設定された TCP パケットを照合します。
<i>icmp-type</i>	(オプション) ICMP メッセージタイプ (0 ~ 255) で照合します。
<i>code</i>	(オプション) <i>icmp-type</i> とともに使用して、さらに ICMP コードタイプ (0 ~ 255) で照合します。
<i>icmp-msg</i>	(オプション) 「使用上のガイドライン」セクションのキーワードで示すように、ICMP メッセージタイプとコードタイプの組み合わせで照合します。

デフォルト

アクセス リストは、少なくとも 1 つの **permit** エントリが設定されていないかぎり、すべてのパケットをドロップします。

コマンド モード

拡張 ACL コンフィギュレーション モード

デバイス モード

application-accelerator

central-manager

使用上のガイドライン

エントリを作成するには、**deny** または **permit** キーワードを使用して、WAAS デバイスにドロップさせる、またはさらに処理するために受け入れさせるパケットのタイプを指定します。デフォルトでは、アクセス リストはすべてを拒否します。アクセス リストが暗黙の **deny any** エントリで終了しているためです。したがって、少なくとも 1 つの **permit** エントリを指定して、有効なアクセス リストを作成する必要があります。

特定のホストからの接続を許可するには、**permit host source-ip** オプションを使用し、*source-ip* には指定されたホストの IP アドレスを指定します。

特定のネットワークからの接続を許可するには、**permit host source-ip wildcard** オプションを使用します。*source-ip* には、ネットワーク ID または指定したいネットワークのホストの IP アドレスを指定します。*wildcard* には、マスクをドット区切り 10 進表記で指定します。これはサブネット マス

クとは逆で、0 は照合が必要な位置を示し、1 は無視する位置を示します。たとえば、ワイルドカード 0.0.0.255 により、送信元 IP アドレスの最後の 8 ビットは無視されます。したがって、**permit 192.168.1.0 0.0.0.255** のエントリにより、192.168.1.0 ネットワークの任意のホストからのアクセスが許可されます。

拡張 IP ACL の場合、**host** キーワードが指定されていないときは、**wildcard** パラメータは必須です。

拡張アクセス リストは、宛先 IP アドレスまたはプロトコル タイプに基づく接続を制御するために使用します。この条件を送信元 IP アドレスに関する情報と結合して、より限定的な条件を作成できます。

表 3-102 に、拡張アクセス リストで使用できる UDP キーワードをリストします。

表 3-102 拡張アクセス リストの UDP キーワード

CLI UDP キーワード	説明	UDP ポート番号
bootpc	Bootstrap Protocol (BOOTP; ブートストラップ プロトコル) クライアント	68
bootps	BOOTP サーバ	67
domain	Domain Name System (DNS; ドメイン ネーム システム)	53
mms	Microsoft Media Server	1755
netbios-dgm	NetBIOS データグラム サービス	138
netbios-ns	NetBIOS ネーム サービス	137
netbios-ss	NetBIOS セッション サービス	139
nfs	Network File System (NFS; ネットワーク ファイル システム) サービス	2049
ntp	Network Time Protocol (NTP; ネットワーク タイム プロトコル)	123
snmp	Simple Network Management Protocol (SNMP; 簡易 ネットワーク管理プロトコル)	161
snmptrap	SNMP トラップ	162
tacacs	TACACS	49
tftp	Trivial File Transfer Protocol (TFTP)	69
wccp	Web Cache Communication Protocol (WCCP)	2048

表 3-103 に、拡張アクセス リストで使用できる TCP キーワードをリストします。

表 3-103 拡張アクセス リストの TCP キーワード

CLI TCP キーワード	説明	TCP ポート番号
domain	Domain Name System (DNS; ドメイン ネーム システム)	53
exec	Exec (rcp)	512
ftp	File Transfer Protocol (FTP; ファイル転送プロトコル)	21
ftp-data	FTP データ接続 (ほとんど使用されない)	20
https	Secure HTTP	443
mms	Microsoft Media Server	1755
nfs	Network File System service (NFS; ネットワーク ファイル システム) サービス	2049
ssh	Secure Shell (SSH; セキュア シェル) ログイン	22
tacacs	TACACS	49
telnet	Telnet	23
www	WWW (HTTP)	80

表 3-104 に、特定の ICMP メッセージ タイプおよびコードの照合に使用できるキーワードをリストします。

表 3-104 ICMP メッセージのキーワード

administratively-prohibited	alternate-address	conversion-error
dod-host-prohibited	dod-net-prohibited	echo
echo-reply	general-parameter-problem	host-isolated
host-precedence-unreachable	host-redirect	host-tos-redirect
host-tos-unreachable	host-unknown	host-unreachable
information-reply	information-request	mask-reply
mask-request	mobile-redirect	net-redirect
net-tos-redirect	net-tos-unreachable	net-unreachable
network-unknown	no-room-for-option	option-missing
packet-too-big	parameter-problem	port-unreachable
precedence-unreachable	protocol-unreachable	reassembly-timeout
redirect	router-advertisement	router-solicitation
source-quench	source-route-failed	time-exceeded
timestamp-reply	timestamp-request	traceroute
ttl-exceeded	unreachable	

例 次の例は、WAAS デバイスでアクセス リストを作成する方法を示します。このアクセス リストを作成することで、WAAS デバイスにリダイレクトされるすべての Web トラフィックを受け入れ、SSH を使用したホスト管理アクセスを制限します。

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# permit tcp any any eq www
WAE(config-ext-nacl)# deny tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

次の例は、インターフェイスのアクセス リストをアクティブにする方法を示します。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group extended testextacl in
WAE(config-if)# exit
```

次の例は、**show running-configuration** コマンドを実行したときに、この設定がどう表示されるかを示します。

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group extended testextacl in
 exit
...
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
...

```

関連コマンド

[\(config-ext-nacl\) delete](#)

[\(config-ext-nacl\) list](#)

[\(config-ext-nacl\) move](#)

[\(config-ext-nacl\) permit](#)

(config-ext-nacl) exit

拡張 ACL コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

exit

シンタックスの説明 このコマンドには引数やキーワードがありません。

デフォルト デフォルトの動作や値はありません。

コマンド モード すべてのモード

デバイス モード application-accelerator
central-manager

例 次の例では、拡張 ACL コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

```
WAE(config-ext-nacl)# exit  
WAE(config)#
```

(config-ext-nacl) list

拡張 ACL 内の指定したエントリのリストを表示させるには、**list** コマンドを使用します。

```
list [start-line-num [end-line-num]]
```

シンタックスの説明

<i>start-line-num</i>	(オプション) リスト開始行の番号
<i>end-line-num</i>	(オプション) リストの最終行の番号

コマンドモード

拡張 ACL コンフィギュレーション モード

デバイス モード

application-accelerator
central-manager

例

次の例は、拡張 ACL 内の指定したエントリのリストを表示する方法を示します。

```
WAE(config)# ip access-list extended testextacl  
WAE(config-ext-nacl)# list 25 50
```

関連コマンド

[\(config-ext-nacl\) delete](#)
[\(config-ext-nacl\) move](#)

(config-ext-nacl) move

拡張 ACL 内の新しい位置に行を移動するには、**move** コマンドを使用します。

```
move old-line-num new-line-num
```

シンタックスの説明

<i>old-line-num</i>	移動するエントリの行番号
<i>new-line-num</i>	エントリの新しい位置。既存のエントリは、アクセスリストの後方に移動します。

コマンドモード

拡張 ACL コンフィギュレーションモード

デバイスモード

application-accelerator

central-manager

例

次の例は、拡張 ACL 内の新しい位置に行を移動する方法を示します。

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# move 25 30
```

関連コマンド

[\(config-ext-nacl\) delete](#)

[\(config-ext-nacl\) list](#)

(config-ext-nacl) permit

さらに処理するために WAAS デバイスに受け入れさせるパケットのタイプを指定する行を拡張アクセスリストに追加するには、**permit** コマンドを使用します。拡張 ACL に条件を追加する際、オプションは選択したプロトコルによって異なるので注意してください。

IP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] permit {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
```

```
no permit {gre | icmp | tcp | udp | ip | proto-num} {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any}
```

TCP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] permit tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

```
no permit tcp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]] [established]
```

UDP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] permit udp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```

```
no permit udp {source-ip [wildcard] | host source-ip | any} [operator port [port]] {dest-ip [wildcard] | host dest-ip | any} [operator port [port]]
```


ICMP の場合、次の構文を使用して条件を追加します。

```
[insert line-num] permit icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any} [icmp-type [code] | icmp-msg]
```

```
no permit icmp {source-ip [wildcard] | host source-ip | any} {dest-ip [wildcard] | host dest-ip | any} [icmp-type [code] | icmp-msg]
```

シンタックスの説明

insert	(オプション) アクセス リストの指定された行番号に、指定された条件を挿入します。
<i>line-num</i>	アクセス リストの指定された行番号に、エントリを挿入します。
gre	Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) プロトコルを使用してパケットを照合します。
icmp	ICMP パケットを照合します。
tcp	TCP プロトコルを使用してパケットを照合します。
udp	UDP プロトコルを使用してパケットを照合します。
ip	すべての IP パケットを照合します。
<i>proto-num</i>	(オプション) IP プロトコル番号
<i>source-ip</i>	送信元 IP アドレス。パケットの送信元となるネットワークまたはホストの番号で、4 桁のドット区切り 10 進表記の 32 ビット数を使用します (たとえば、0.0.0.0)。

<i>wildcard</i>	(オプション) 上記 <i>source-ip</i> アドレスの各部分に対して照合される、4 桁のドット区切り 10 進表記で表わされたワイルドカード。0 は照合するビット、1 は無視するビットを示します。
	 (注) 拡張 IP ACL の場合、 ip access-list コマンドの <i>wildcard</i> パラメータは常にオプションです。拡張 IP ACL で host キーワードを指定した場合、 <i>wildcard</i> パラメータは認められません。
host	後続の IP アドレスを照合します。
any	任意の IP アドレスを照合します。
<i>dest-ip</i>	宛先 IP アドレス。パケットの送信先となるネットワークまたはホストの番号で、4 桁のドット区切り 10 進表記の 32 ビット数を使用します (たとえば、0.0.0.0)。
<i>operator</i>	(オプション) 指定されたポートで使用するオペレータ。 lt はより少ない、 gt はより多い、 is は同等、 eq は同等である、 neq は同等でない、および range は範囲内を表します。
<i>port</i>	(オプション) ポート。数値 (0 ~ 65535) またはキーワードを使用します。 range には、2 つのポート番号が必要です。UDP および TCP のキーワードのリストについては、「使用上のガイドライン」セクションを参照してください。
established	(オプション) 確認応答ビットまたはリセット ビットが設定された TCP パケットを照合します。
<i>icmp-type</i>	(オプション) ICMP メッセージタイプ (0 ~ 255) で照合します。
<i>code</i>	(オプション) <i>icmp-type</i> とともに使用して、さらに ICMP コードタイプ (0 ~ 255) で照合します。
<i>icmp-msg</i>	(オプション) 「使用上のガイドライン」セクションのキーワードで示すように、ICMP メッセージタイプとコードタイプの組み合わせで照合します。

デフォルト

アクセス リストは、少なくとも 1 つの **permit** エントリが設定されていないかぎり、すべてのパケットをドロップします。

コマンド モード

拡張 ACL コンフィギュレーション モード

デバイス モード

application-accelerator

central-manager

使用上のガイドライン

エントリを作成するには、**deny** または **permit** キーワードを使用して、WAAS デバイスにドロップさせる、またはさらに処理するために受け入れさせるパケットのタイプを指定します。デフォルトでは、アクセス リストはすべてを拒否します。アクセス リストが暗黙の **deny any** エントリで終了しているためです。したがって、少なくとも 1 つの **permit** エントリを指定して、有効なアクセス リストを作成する必要があります。

特定のホストからの接続を許可するには、**permit host source-ip** オプションを使用し、*source-ip* には指定されたホストの IP アドレスを指定します。

特定のネットワークからの接続を許可するには、**permit host source-ip wildcard** オプションを使用します。*source-ip* には、ネットワーク ID または指定したいネットワークのホストの IP アドレスを指定します。*wildcard* には、マスクをドット区切り 10 進表記で指定します。これはサブネット マス

クとは逆で、0 は照合が必要な位置を示し、1 は無視する位置を示します。たとえば、ワイルドカード 0.0.0.255 により、送信元 IP アドレスの最後の 8 ビットは無視されます。したがって、**permit 192.168.1.0 0.0.0.255** のエントリにより、192.168.1.0 ネットワークの任意のホストからのアクセスが許可されます。

拡張 IP ACL の場合、**host** キーワードが指定されていないときは、**wildcard** パラメータは必須です。

拡張アクセス リストは、宛先 IP アドレスまたはプロトコル タイプに基づく接続を制御するために使用します。この条件を送信元 IP アドレスに関する情報と結合して、より限定的な条件を作成できます。

表 3-105 に、拡張アクセス リストで使用できる UDP キーワードをリストします。

表 3-105 拡張アクセス リストの UDP キーワード

CLI UDP キーワード	説明	UDP ポート番号
bootpc	Bootstrap Protocol (BOOTP; ブートストラップ プロトコル) クライアント	68
bootps	BOOTP サーバ	67
domain	Domain Name System (DNS; ドメイン ネーム システム)	53
mms	Microsoft Media Server	1755
netbios-dgm	NetBIOS データグラム サービス	138
netbios-ns	NetBIOS ネーム サービス	137
netbios-ss	NetBIOS セッション サービス	139
nfs	Network File System (NFS; ネットワーク ファイル システム) サービス	2049
ntp	Network Time Protocol (NTP; ネットワーク タイム プロトコル)	123
snmp	Simple Network Management Protocol (SNMP; 簡易 ネットワーク管理プロトコル)	161
snmptrap	SNMP トラップ	162
tacacs	TACACS	49
tftp	Trivial File Transfer Protocol (TFTP)	69
wccp	Web Cache Communication Protocol (WCCP)	2048

表 3-106 に、拡張アクセス リストで使用できる TCP キーワードをリストします。

表 3-106 拡張アクセス リストの TCP キーワード

CLI TCP キーワード	説明	TCP ポート番号
domain	Domain Name System (DNS; ドメイン ネーム システム)	53
exec	Exec (rcp)	512
ftp	File Transfer Protocol (FTP; ファイル転送プロトコル)	21
ftp-data	FTP データ接続 (ほとんど使用されない)	20
https	Secure HTTP	443
mms	Microsoft Media Server	1755
nfs	Network File System (NFS; ネットワーク ファイル システム) サービス	2049
ssh	Secure Shell (SSH; セキュア シェル) ログイン	22
tacacs	TACACS	49
telnet	Telnet	23
www	WWW (HTTP)	80

表 3-107 に、特定の ICMP メッセージタイプおよびコードの照合に使用できるキーワードをリストします。

表 3-107 ICMP メッセージのキーワード

administratively-prohibited	alternate-address	conversion-error
dod-host-prohibited	dod-net-prohibited	echo
echo-reply	general-parameter-problem	host-isolated
host-precedence-unreachable	host-redirect	host-tos-redirect
host-tos-unreachable	host-unknown	host-unreachable
information-reply	information-request	mask-reply
mask-request	mobile-redirect	net-redirect
net-tos-redirect	net-tos-unreachable	net-unreachable
network-unknown	no-room-for-option	option-missing
packet-too-big	parameter-problem	port-unreachable
precedence-unreachable	protocol-unreachable	reassembly-timeout
redirect	router-advertisement	router-solicitation
source-quench	source-route-failed	time-exceeded
timestamp-reply	timestamp-request	traceroute
ttl-exceeded	unreachable	

例 次の例は、WAAS デバイスでアクセス リストを作成する方法を示します。このアクセス リストを作成することで、WAAS デバイスにリダイレクトされるすべての Web トラフィックを受け入れ、SSH を使用したホスト管理アクセスを制限します。

```
WAE(config)# ip access-list extended testextacl
WAE(config-ext-nacl)# permit tcp any any eq www
WAE(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

次の例は、インターフェイスのアクセス リストをアクティブにする方法を示します。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group example in
WAE(config-if)# exit
```

次の例は、**show running-configuration** コマンドを実行したときに、この設定がどう表示されるかを示します。

```
...
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group testextacl in
 exit
...
ip access-list extended testextacl
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
...

```

関連コマンド

[\(config-ext-nacl\) delete](#)

[\(config-ext-nacl\) deny](#)

[\(config-ext-nacl\) list](#)

[\(config-ext-nacl\) move](#)

■ (config-ext-nacl) permit