



WAE のトラブルシューティング

この章では、WAFS Wide Area Application Engine (WAE) のトラブルシューティングに使用可能なプロセスとユーティリティについて、特に、CLI とより一般的なネットワーキング ツールに重点を置いて説明します。WAFS Central Manager GUI と File Engine Manager GUI は、問題をトラブルシューティングするための数多くの手段を提供しています。これらの GUI を介して使用できるトラブルシューティング機能については、『*WAFS 3.0 User Guide*』を参照してください。CLI を使用すると、1 度に 1 台の WAE をトラブルシューティングできます。GUI を使用すると、1 度に複数の WAE をトラブルシューティングできます。

この章には、次の項があります。

- [トラブルシューティングの概要、13-2 ページ](#)
- [WAE のヘルスの検査、13-2 ページ](#)
- [接続のチェック、13-5 ページ](#)
- [パケットキャプチャ ツールの使用方法、13-7 ページ](#)
- [WAFS debug コマンドを使用したトラブルシューティング、13-9 ページ](#)
- [シスコ スクリプトを使用したトラブルシューティング、13-9 ページ](#)



(注)

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

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

トラブルシューティングの概要

システム問題のトラブルシューティングで重要となるのは、根本的な原因を見つけ出し排除するために、最初におおよその原因を特定し、使用可能なツールの中から適したツールを選択することです。WAFS 環境では、インストールやセットアップ時の問題、ハードウェアの問題、およびソフトウェアの問題の解決に役立つトラブルシューティング ツールが用意されています。WAFS ソフトウェア自体に各種ツールが内蔵されています。その他に、Windows ベースのツール、UNIX ベースのツール、ネットワーク ツールなどもあります。

ヘルス インジケータとログ ファイルの検査、接続の確認、名前解決とブラウジングの確認、統計情報の検査、WAE 動作とネイティブなファイル サーバとの比較、およびクライアント設定の確認を実行し、WAFS WAE の根本的な問題を特定し排除できます。

この章では、基本的なトラブルシューティング情報のみを取り上げます。高度なトラブルシューティング技術については、『Cisco WAFS 3.0 User Guide』を参照してください。

WAE のヘルスの検査

以降で説明するとおり、`show` および `show statistics EXEC` コマンドを使用して、さまざまなログ ファイルを表示することで、WAE がアップし稼働していることを確認できます。

- [show コマンドと show statistics コマンド](#)
- [ログ ファイルの使用方法](#)

show コマンドと show statistics コマンド

表 13-1 に示すとおり、WAFS ソフトウェア自体に、ソフトウェアとハードウェアの各種コンポーネントの動作を分析する上で役立つ多数の `show` コマンドがあります。このコマンドの詳細については、『Cisco WAFS 3.0 Command Reference』を参照してください。

表 13-1 WAFS CLI の show コマンドと show statistics コマンド

show コマンド	show コマンド	show コマンド	show statistics コマンド
aaa accounting	inetd	snmp	icmp
alarms	interface	ssh	ip
arp	inventory	standby	netstat
authentication	ip access-lists	startup-config	radius
bypass	ip routes	sysfs	services
cdp	logging	tacacs	snmp
clock	memory	tcp	tacacs
debugging	ntp	tech-support	tcp
disks	processes	telnet	udp
flash	radius-server	users	wccp
hardware	running-config	version	
hosts	smb-conf	wccp	

たとえば、`show disks details EXEC` コマンドを使用すると、ローカル ディスクが正常に動作していることを確認できます。

```
WAE# show disks details
```

```
Physical disk information:
```

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

```
Mounted filesystems:
```

MOUNT POINT	TYPE	DEVICE	SIZE	INUSE	FREE	USE%
/	root	/dev/root	34MB	28MB	6MB	82%
/swstore	internal	/dev/md1	495MB	212MB	283MB	42%
/state	internal	/dev/md2	4031MB	65MB	3966MB	1%
/disk00-04	WAFSFS	/dev/md4	63035MB	32MB	63003MB	0%
/local/local1	SYSFS	/dev/md5	3967MB	303MB	3664MB	7%
.../local1/spool	PRINTSPOOL	/dev/md6	991MB	16MB	975MB	1%
/sw	internal	/dev/md0	991MB	289MB	702MB	29%

```
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]
.				
.				
.				

ログ ファイルの使用方法

WAFS ソフトウェアによって生成され、管理者にとって役立つ、いくつかのログ ファイルがあります。主要なログ ファイルは、*Manager.log*、*Watchdog.log*、*Utilities.log*、および *syslog.txt* の 4 つです。それらは、*/local/logs/actona/* ディレクトリに含まれています。

これらのログの内容に基づいて、レポートされた問題の日時の前後のエラーや異常を調べることができます。ログ ファイルに含まれるエラーや警告がすべて関係しているとは限りません。フィルタリングが必要となります。

ログ ビュー ツールを使用したトラブルシューティング

`less EXEC` コマンドを使用すると、LESS プログラムを有効化し、表示する WAFS ソフトウェアのログのファイル名を指定できます。`less` コマンドは `more` コマンドによく似ていますが、ファイル内で順方向へ移動できるだけでなく、逆方向へも移動できます。また、LESS プログラムでは、起動する前にファイル全体を読み込む必要がないため、テキスト エディタより迅速にサイズの大きいファイルを起動できます。このコマンドは、ログ ファイルが常駐するディレクトリから実行する必要があります。

次の例では、LESS プログラムを使用した *cups_access_log* ファイルの表示を要求しています。表示を終了するには、q キーを押します。

```
WAE# less cups_access_log
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 150
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 136
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 76
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 170
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 165
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 174
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 216
localhost - - [22/Mar/2005:01:10:24 +0200] "POST / HTTP/1.1" 200 277
/local/local1/logs/cups_access_log (END)
WAE#
```

接続のチェック

以降で説明するとおり、ネットワーク内の WAE の接続をチェックできます。

- [Telnet クライアントを使用したトラブルシューティング](#)
- [Ping を使用したトラブルシューティング](#)
- [Traceroute を使用したトラブルシューティング](#)

Telnet クライアントを使用したトラブルシューティング

WAFS は、宛先ポートを指定できる Telnet クライアントをサポートしています。Telnet クライアントを使用して、問題のある WAE へ Telnet を試みることで、接続をテストできます。この機能をサポートするために、telnet EXEC コマンドが追加されました。

```
WAE# telnet ?  
      Hostname or A.B.C.D Remote host or IP address
```

Ping を使用したトラブルシューティング

基本的な LAN および WAN ネットワークの接続問題を診断するためにエコー 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} [PING options]
```

このコマンドは、WAE と次のその他のコンポーネント間の接続をテストするために使用できます。

- ネイティブ ファイル サーバ
- Core File Engine として動作する WAE
- Edge File Engine として動作する WAE
- クライアント

ping EXEC コマンドの機能は、コマンド引数としてすべての標準の ping オプションをサポートします (標準の ping オプションの詳細については、Linux man ページを参照してください)。

```
WAE# ping ?  
      LINE Destination Host or IP Address (or PING options)
```

ping EXEC コマンドに *hostname* 引数を指定して入力するには、事前に必ず DNS 機能を WAE に設定しておいてください。応答しないホストを強制的にタイムアウトにしたり、ループの繰り返しを排除したりするには、Ctrl-C キーを押します。

次の例では、IP アドレス 192.168.131.189 のネイティブ ファイル サーバに WAFS CLI から ping を実行しています。

```
WAE# ping 192.168.131.189  
PING 192.168.131.189 (192.168.131.189) from 10.1.1.21 : 56(84) bytes of data.  
64 bytes from 192.168.131.189: icmp_seq=0 ttl=249 time=613 usec  
64 bytes from 192.168.131.189: icmp_seq=1 ttl=249 time=485 usec  
64 bytes from 192.168.131.189: icmp_seq=2 ttl=249 time=494 usec  
64 bytes from 192.168.131.189: icmp_seq=3 ttl=249 time=510 usec  
64 bytes from 192.168.131.189: icmp_seq=4 ttl=249 time=493 usec  
  
--- 192.168.131.189 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
```

Traceroute を使用したトラブルシューティング

traceroute は、ほとんどのオペレーティング システムで広く使用されているユーティリティです。ping と同様に、ネットワークの接続状態を判断する上で有用なツールです。ping コマンドを使用すると、ユーザは 2 つのエンド システム間の接続が存在するかどうかを確認できます。traceroute はこれと同様に機能しますが、2 つのシステム間の中間ルータの一覧も表示します。したがって、ユーザは、あるシステムから別のシステムにパケットが移動できるルートを確認できます。

ホスト名または IP アドレスのどちらかがわかっている場合は、traceroute EXEC コマンドを使用して、リモート ホストへのルートを検索できます。たとえば、コア サーバへの接続を確認するために、このコマンドを使用できます。

```
WAE# traceroute coreserver
traceroute to 192.168.71.113 (192.168.71.113), 30 hops max, 38 byte packets
***
***
***
10  p3-3.paloalto-cr2.bbnplanet.net (4.0.26.13)  3.219 ms  2.001 ms  2.097 ms
11  p7-1.paloalto-nbr2.bbnplanet.net (4.0.6.77)  3.133 ms  1.949 ms  2.076 ms
12  p4-0.paloalto-nbr1.bbnplanet.net (4.0.5.65)  2.755 ms  2.204 ms  2.037 ms
13  p1-0.paix-bi2.bbnplanet.net (4.0.6.98)  2.928 ms  2.146 ms  2.334 ms
14  p1-0.xpaix17-level3.bbnplanet.net (4.0.1.70)  3.397 ms  3.631 ms  3.081 ms
15  gige10-0.ipcolo4.SanJose1.Level3.net (64.159.2.42)  3.334 ms  2.999 ms  2.388 ms
16  cust-int.level3.net (64.152.69.18)  3.871 ms  3.031 ms  *
17  ge-3-3-0.msrl.pao.yahoo.com (192.168.101.42)  3.695 ms  ge-2-3-0.msrl.pao.yahoo.com
    (192.168.101.46)  6.998 ms  *
18  vl16.bas1.scd.yahoo.com (66.218.64.146)  6.282 ms  5.091 ms  5.162 ms
19  w2.rc.scd.yahoo.com (66.218.71.113)  6.028 ms  5.782 ms  5.544 ms
```

パケットキャプチャ ツール の 使用 方法

ネットワークレベルのツールを使用して、パケットがネットワークを經由している途中で、そのパケットを代行受信し分析することができます。このようなツールのうち 2 つのツールを以降で説明します。

- [TCPdump を使用したトラブルシューティング](#)
- [Tethereal を使用したトラブルシューティング](#)

TCPdump を使用したトラブルシューティング

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キャプチャできるユーティリティです。したがって、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役立ちます。

通常のネットワーク動作時には、ネットワーク インターフェイス宛てのパケットのみが代行受信され、TCP/IP プロトコル レイヤ スタックの上位レイヤへ渡されます。インターフェイス宛てで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る受信対象でないパケットも、代行受信され、プロトコル スタックの上位レイヤへ渡されます。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ことで動作します。TCPdump は無償の libpcap (パケット キャプチャ ライブラリ) を使用します。

TCPdump ツールを有効化するには、`tcpdump EXEC` コマンドを使用します。次の例は、WAFS `tcpdump` コマンドで使用可能なオプションを示しています。

```
WAE# tcpdump -h
tcpdump version 3.8.1 (jlemon)
libpcap version 0.8
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [-C file_size ]
               [-E algo:secret ] [-F file ] [-i interface ] [-r file ]
               [-s snaplen ] [-T type ] [-w file ] [-y datalinktype ]
               [ expression ]
WAE#
```

Tethereal を使用したトラブルシューティング

Tethereal は、ネットワーク トラフィック アナライザ ツール Ethernet のコマンドライン バージョンです。TCPdump と同様に、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 トラフィック分析のほかにも、Tethereal は、パケットをデコードするためのファシリティを提供しています。

Tetherreal ツールを有効化するには、**tetherreal** EXEC コマンドを使用します。次の例は、WAFS **tetherreal** コマンドで使用可能なオプションを示しています。

```
FileEgine#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 ] [ -DlNpqSVx ] [ -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
```

WAFS debug コマンドを使用したトラブルシューティング

WAE では、複数のデバッグ モードがサポートされています。各モードは、**debug EXEC** コマンドを使用して切り替えることができます。これらのモードでは、設定エラーからプリント スプーラの問題に至るまでさまざまな問題をトラブルシューティングできます。**debug** コマンドは、Cisco TAC の指示があった場合にだけ使用することをお勧めします。

```
WAE#debug ?
aaa           Accounting debug command
all           Enable or Disable all debugging
authentication Authentication debug commands
buf           Buffer manager debug commands
cdp           CDP debug commands
cli           CLI debug commands
dataserver    Dataserver debug commands
dhcp          dhcp debug commands
ftp-over-http FTP-over-HTTP debug commands
logging       LOG debug commands
ntp           NTP debug commands
print-spooler Print Spooler debug commands
stats         Statistics debug commands
wccp         WCCP information
<cr>
```

シスコ スクリプトを使用したトラブルシューティング

トラブルシューティングを目的に、シスコが提供しているスクリプトを実行できます。また、**script EXEC** コマンドを使用して、シスコが提供するスクリプトのエラーをチェックできます。スクリプトは、個々のお客様が必要に応じて使用できるように開発されています。汎用目的のスクリプトはありません。

script EXEC コマンドは、これらのタスクを処理する **script** ユーティリティを開きます。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、**script** ユーティリティは、ユーザの標準ターミナルからの入力を読み込むことができます。



(注)

script ユーティリティは、シスコが提供しているスクリプトのみを実行します。シスコのシグニチャがないスクリプト 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。

次の例では、スクリプト ファイル *test_script.pl* 内のエラーをチェックしています。

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

