インターネット ゲートキーパー（Linux ゲートウェイ） - エラー ログ

この記事の情報は、F-Secure インターネットゲートキーパーバージョン4.10 以降を対象としています。

山括弧 <> はメッセージによって内容が異なるフィールドを示しています。山括弧は参考用でメッセージに表示されません。

エラーメッセージの内容

メッセージ

CRITICAL [<場所>] bind=Address already in use(98) (addr=<アドレス>, port=<ポート>). # Please check whether other service(mail/web server,etc...) is already running on port <ポート>.

説明

設定したポートとアドレスに接続できないため、サービスを開始できません。bind() の Linux システム コールで指定したポートが利用されます。このエラーは指定したポートが使用中で、bind() が失敗するときに表示されます。

解決策

ポートを使用している他のサービスを確認して、サービスを必要に応じて停止してください。サービスが必要な場合、本製品が使用しているポートを別のものに設定してください。“netstat –anp” (診断情報は "system/netstat_anp.txt") を実行すると各ポートが使用しているプロセスを確認できます。

メッセージ

WARNING [<場所>] Maximum connections: warning: Client connections reached maximum connections(<最大値>). More request will be blocked/rejected. If there is many warnings, please increase 'Maximum Connections' settings(pre_spawn value of virusgw.ini) of this service. (<暫定値> will be good value as start line).

説明

接続できるクライアントの上限に達したときにログされます。上限に達した場合、処理を続けるためにクライアントの接続数を下げる必要があります。

接続数の上限に達した場合、バックログ (Linux listen() システム コールのバックログ) は 5 に設定され、最大 6 つの TCP 接続を “ESTABLISHED” (確立) の状態に設定することが可能です。上限に達したときの接続要求に対しては “SYN_RECV” の接続状態が指定されます。また、Linux による TCP 接続は処理されません。

接続数の上限はアクセス ログにある内部プロセス ID (“PROXY-STAT:[サービス タイプ]:[内部プロセス ID]:..") から確認できます。内部プロセス ID (識別子は 0 で始まる) は番号が低いほど優先度が高くなります。そのため、[内部プロセス ID]+1) は対象となるプロセスの開始時の同時接続数に適用されます。

ポート番号の ESTABLISH ステータスは netstat コマンドで確認できます:

```
# netstat -anp | grep :9080 | grep ESTABLISHED | wc -l
```

(ポート 9080 は例です)

解決策

- **状況:** 表示されるメッセージの数が少なく (たとえば、1 時間ごとに)、製品が正常に動作し、増加している接続数は一時的なことと思われます。**解決策:** 設定を変更する必要はありません。
- **状況:** デフォルトではスキャンのタイムアウト値は 90 秒に設定されています。これを無効 (0 に設定)、またはより大きい値に設定すると、特定のファイルに対するスキャンの時間が長くなり、接続数の上限に達する原因にもなります。
  解決策: タイムアウト値をデフォルトの 90 秒に戻してください。
- **状況:** 製品とサーバまたはクライアントの間にネットワークの問題がある場合、接続数の上限に達する可能性があります。
  解決策: ネットワークの問題を解消してください。

- **状況:** 上記以外の場合 (複数のエラーがログされる、スキャンのタイムアウト値が変更されていない、ネットワークの問題はない) でサーバにアクセスできない場合、接続数が上限を超えている可能性があります。
- **解決策:** 接続数の上限を必要に応じて上げてください。クライアントの接続数が判断できない場合、次の暫定値でシステムを検証してください: HTTP 200、SMTP 50、POP 50、FTP 10。システムの検証後、設定を必要に応じて変更してください。通常の環境では接続数の上限を 2000 より下に設定することが適切です。

接続数の上限を上げた場合、接続数をより多く許可できる代わりに追加のメモリが必要となります。1 つの接続に 500 KB ほど使用されます。

メッセージ

WARNING [<場所>] getaddrinfo failed. admin_mx_host=[<ホスト名>] admin_mx_port=[<ホストのポート>] gai_strerror=[<エラー内容>]

説明

ウイルスまたはスパム検出時に管理者へ通知する設定の SMTP サーバ (/opt/f-secure/fsigk/conf/fsigk.ini の “admin_mx_host”) に接続できません。

解決策

SMTP サーバのホスト名を確認してください。

メッセージ

WARNING [<場所>] connect=<エラー メッセージ>(<エラー コード>) cannot connect to admin mail server[<ホスト名>:<ホストのポート>]

説明

ウイルスまたはスパム検出時に管理者へ通知する設定の SMTP サーバ (/opt/f-secure/fsigk/conf/fsigk.ini の “admin_mx_host” と “admin_mx_port”) に接続できましたが、エラーが発生しました。

解決策

SMTP サーバのホスト名とポート番号を確認してください。

メッセージ

WARNING [<場所>] smtp error: Send command line: buf=[<応答行>] (expected <応答行>)

説明

ウイルスまたはスパム検出時に管理者への通知に使用される SMTP の応答メッセージがエラーを返しました。

送信コマンドが SMTP の接続ステータスを示します。"HELO/MAIL FROM/RCPT TO/DATA/QUIT" (各コマンドが送信された場合)、"GREETING" (接続が開始された場合) または "DATA END" (データが送信された場合) のいずれかを選択できます。

解決策

設定した SMTP サーバにメールを送信できるか [応答行] を確認してください。

メッセージ

CRITICAL [<場所>] semget=<エラー メッセージ>(<エラー コード>) semget failure. Childnum(pre_spawn=<Maximum value>) may be large. If needed, maximum semaphore number(SEMMNI) can be increased by adding a line like 'kernel.sem=250 128000 32 512' in '/etc/sysctl.conf' and running 'sysctl -p'.

説明

セマフォが確保できないため、サービスを開始できません。

解決策

サービス プロセス (fsigk_xxx) を中断した場合 (“kill -KILL” コマンドを使用してなど)、セマフォが解放されていなく、システム プロセスに残っているときにエラーが発生する可能性があります。その場合、サーバ (オペレーティング システム) を再起動してください。使用中のセマフォは “/proc/sysvipc/sem” から確認できます。

接続数の上限が高く設定されている場合、セマフォがより多く必要となるため、エラーが発生する可能性が高くなります。接続数の上限は 2000 より下に設定し、絶対に必要な場合を除いて 2000 以上に設定しないでください。通常の環境では接続数の上限を 2000 より下に設定することが適切です。

本製品はプロセスの数に応じてセマフォを必要とします。接続数の上限を上げたり、他のプロセスが多くのセマフォを使用とする場合、オペレーティング システムが使用できるセマフォの数を上げる必要があります。次の方法でセマフォの数を上げることができます。

1. 次の行を /etc/sysctl.conf に追加します:
   kernel.sem=250 128000 32 512
2. 次のコマンドを実行します:
   # sysctl -p
3. 次のコマンドでセマフォの数が設定されたことを確認します:
   # cat /proc/sys/kernel/sem
   250 128000 32 512

メッセージ

WARNING [<場所>] sendfile timeout: No data can be sent for 120 seconds. There may be a temporary network problem between receiver. / URL=[<URL>], n=<カウント>, written=<カウント>, filelen=<カウント>, writesize=<カウント>

説明

120 秒以内にデータが送信されていないことでセッションが切断されたときにログされます。

解決策

ネットワークに問題があるか確認してください。

IGK サーバの NIC にてパケットがドロップされている可能性があります。パケットがドロップされている場合、バッファ拡張による対処をご検討ください。
現在のバッファサイズは「ethtool -g　[devname]」で確認することができます。

メッセージ

WARNING [<場所>] Too large header (><バイト制限>) ignored. URL=[<URL>]

説明

HTTP レスポンス ヘッダが大きい (17 KB 以上) 場合に表示されます。サービスは正常に動作しています。

解決策

特定の URL またはブラウザで問題が発生するか確認してください。

メッセージ

CRITICAL [<場所>] not enough diskspace in temporary directory [<ディレクトリ名>]. (<カウント> kB free?)(ret=<リターン コード>)

説明

一時ディレクトリの空き容量が 5 MB 未満の場合に表示されます。サービスは開始されません。

解決策

一時ディレクトリの空き容量を増やしてください。

メッセージ

CRITICAL [<場所>] Realtime virus scan seems to be enabled. Please stop realtime virus scan, or exclude scanning for temporary directory(<ディレクトリ名>)

説明

アンチウイルス ソフトウェアの検出時および一時ディレクトリにリアルタイム ウイルス保護が有効の場合に表示されます。サービスは開始されません。

解決策

リアルタイム ウイルス保護を完全に無効にしてください。または一時ディレクトリを対して無効にしてください。

メッセージ

WARNING [<場所>] [<検出時のアクション>]:smtp error:[<送信コマンド名>]: buf=[<応答行>]

説明

ウイルスまたはスパム検出時に送信者/受信者への通知に使用される SMTP の応答メッセージがエラーを返しました。

[ウィルス検出時の動作] のオプションが「ブロック」、「削除後、受信者へ通知」、「削除」に設定されています。

送信コマンドが SMTP の接続ステータスを示します。"RSET/MAIL FROM/RCPT TO/DATA/QUIT" (各コマンドが送信された場合)、または "DATA END" (データが送信された場合) のいずれかを選択できます。

解決策

設定した SMTP サーバにメールを送信できるか [応答行] を確認してください。

メッセージ

WARNING [<場所>] NOOP command reply error [<応答行>]

説明

NOOP コマンドが FTP サーバに送信され、200 以外が返された場合に表示されます。

解決策

FTP サーバが接続されていない、または NOOP コマンドに応答していないか確認してください。

メッセージ

CRITICAL/WARNING [<場所>] System call=Too many open files in system(23) <エラー メッセージ>

説明

開いているファイルが多すぎることを示します。システムで開けるファイルの上限に達したときにメッセージが表示されます。

次の方法で /proc/sys/fs/file-nr が処理したファイルの数を確認できます。

cat /proc/sys/fs/file-nr

[ファイル ハンドラ数] [使用中のファイル ハンドラ] [ファイル ハンドラの上限]

(例: # cat /proc/sys/fs/file-nr
1864 504 52403)

解決策

“lsof” コマンドなどを使用して、ファイル ハンドラを多く使用しているプロセスがあるか確認してください。

システムに問題がなく、ファイル ハンドラの数が上限に近づいている場合、“/proc/sys/fs/file-max” を次のように変更することでファイル ハンドラの数を上げられます。

1. sysctl.conf (ファイル ハンドラ数の上限が 65535 に変更されます) に次の行を追加します:

   fs.file-max = 65535
2. 変更を適用するために次のコマンドを実行してください:

   sysctl -p

メッセージ

CRITICAL/WARNING [<場所>] open=No such file or directory(2) <エラー メッセージ>

説明

本製品で使用される一時ファイルが開けない場合に表示されます。

解決策

一時ファイルがコマンドまたは別のプログラムによって削除されたか確認してください。

メッセージ

CRITICAL [<場所>] Cannot find tproxy(version2) interface. Tproxy kernel patch is required. Please apply the tproxy patch and check that "/proc/net/tproxy" exists. Please see document for "transparent_tproxy" settings for details.

説明

TPROXY の使用設定 (ソース IP が使用され、transparent_tproxy=yes") が行われ、tproxy パッチが動作していないときに表示されます。

解決策

tproxy パッチがカーネルに適用されていない可能性があります。/proc/net/tproxy が存在するか確認してください。

Turbolinux 10 Server を使用している場合、次のことに注意してください:
- kernel-2.6.8-5 以降を使用する必要があります。“uname -a” コマンドを使用して、カーネルのバージョンが 2.6.8-5 以降であることを確認してください。カーネルが古い場合、Turbolinux10 のカーネルをアップデートしてください。

iptable_tproxy モジュールを実装する必要があります。“iptable_tproxy” モジュールが “lsmod” コマンドの結果に含まれているか確認してください。含まれていない場合、次の方法でモジュールを含めてください:

1. /etc/sysconfig/iptables-config で、iptables が iptable_tproxy を読み込むように IPTABLES_MODULES の行を次のように変更します:
   IPTABLES_MODULES="iptable_tproxy"
2. iptables を再起動します:
   # /etc/rc.d/init.d/iptables restart
3. /proc/net/tproxy が存在するか確認します。
4. インターネット ゲートウェイを再起動します。

tproxy(version1) を使用している場合、"transparent_tproxy_version=1" を設定ファイルに追加し、サービスを再起動してください。tproxy version1 は今後未対応になる可能性がありますので version2 の使用を推奨します。

メッセージ

WARNING [<場所>] vsc_start() error

説明

ウイルス定義ファイルまたはスキャン エンジンのライブラリを読み込みできません。

解決策

ウイルス定義ファイルまたはスキャン エンジンのファイルが削除された場合、次のコマンドでインストールを上書きしてください:

rpm パッケージ:
rpm -Uvh --force fsigk-xxx-0.i386.rpm

deb パッケージ:
dpkg –r fsigk
dpkg –i fsigk-xxx_all.deb

SELinux を使用している場合、/var/log/messages にエラーがあってポリシーがプロセスの読み込みを拒否しているか確認してください。また、SELinux を無効にしてエラーが発生するか確認してください。/etc/sysconfig/selinux で "SELINUX=disabled" を変更することで SELinux を無効にできます。無効にした後、サーバを再起動してください。

メッセージ

WARNING [<場所>] child(<インデックス>) stopped.(sig=17[SIGCHLD], si_code=3[CLD_DUMPED],status=<チャイルドのステータス>, childid=<ID>, cur_pid=<処理 ID>,pid=<チャイルド プロセス ID>

WARNING [<場所>] core dumped(child proxy process). Please send core file(core or core.xxx) on the installation directory and diag.tar.gz to support center. (child=<インデックス>,sig=17[SIGCHLD], si_code=3[CLD_DUMPED],status=<チャイルドのステータス>(<ステータス文字列>),childid=<ID>,cur_pid=<処理 ID>,pid=<チャイルド プロセス ID>)

WARNING [<場所>] Error recovery: restarting service...

説明

プロキシ プロセスが異常終了 (core dump) したことを示します。また、サービスが再起動しました。エラー メッセージは 3 つ続けて表示されます。

解決策

サービスの再起動と復元が自動的に行われます。再起動中はサービスが停止されます (約 10 秒)。

メッセージが表示される場合、製品に問題がある可能性が高いです。F-Secure にサポートを依頼する場合、インストール ディレクトリ (/opt/f-secure/fsigk/) にある “core” で始まるファイルをすべて F-Secure に送ってください。

製品の最新版を使用していない場合、最新版にアップデートしてください。

メッセージ

WARNING [<場所>] accept=Connection reset by peer(104) main/accept_loop/accept(s=<Id>)

説明

このメッセージはカーネル 2.2 を使用している環境で接続後にすぐに切断した場合に表示される可能性があります。メッセージが表示されても本製品は正常に動作します。

解決策

カーネル 2.2 は未対応になりました。可能な場合、ディストリビューションをアップデートしてください。

メッセージ

CRITICAL [<場所>] LICENSE_ERROR#ret=-1#msg=License Expired

説明

体験版のライセンスが切れたことを示します。

解決策

ライセンスを購入し、製品のアクティベーションを行うためにライセンス キーコードを入力してください。

メッセージ

WARNING [<場所>] Commtouch database error: Initial database update may be on going. Wait a moment. (dlopen(./databases/commtouchunix.0/libfsasd-lnx32.so) failed.
dlerror(): ./databases/commtouchunix.0/libfsasd-lnx32.so: cannot open shared object file: No such file or directory)

WARNING [<場所>] Commtouch database error: Initial database update may be on going. Wait a moment. (FsasFunctionsInitialize failed.)

説明

commtouch のスパム スキャン エンジンにデータベースが存在しないことを示します

解決策

データベースのダウンロードが完了するまで待ちます。

メッセージ

WARNING [<場所>] fsas_open_session(./fsasd-socket) failed.

説明

'fsasd' プロセスが実行していないことを示します。

解決策

fsasd サービスを開始するために "/etc/init.d/rc.fsigk_fsasd start" または "/etc/init.d/rc.virusgw_fsasd start" を実行してください。

メッセージ

WARNING [<場所>] fsav_open_session: Cannot connect to fsavd's socket(./fsavd-socket-0). fsavd may be not running. Please run 'rc.fsigk_fsavd restart' to restart fsavd.

説明

スキャン エンジン (fsavd) のソケット (./fsavd-socket-0) に接続できません。スキャン エンジン (fsavd) が実行されていない可能性があります。

解決策

スキャン エンジン (fsavd) は Web コンソールから実行された場合、自動的に開始されます。プロキシ サービスをコマンドラインから実行した場合、スキャン エンジン (fsavd) を事前に開始する必要があります。“/opt/f-secure/fsigk/rc.fsigk_fsavd restart” コマンドでスキャン エンジンを再起動できます。