Syslog メッセージ 101001 ～ 199021

この章は、次の項で構成されています。

メッセージ 101001 ～ 109213

この項では、101001 から 109213 までのメッセージについて説明します。

101001

エラーメッセージ `%FTD-1-101001: (Primary) Failover cable OK.`

説明フェールオーバー ケーブルが接続され、正常に機能しています。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

101002

エラーメッセージ `%Threat Defense-1-101002: (Primary) Bad failover cable.`

説明フェールオーバー ケーブルが接続されていますが、正常に機能していません。Primaryは、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション フェールオーバー ケーブルを交換します。

101003、101004

エラーメッセージ `%Threat Defense-1-101003: (Primary) Failover cable not connected (this unit).`

エラーメッセージ `%Threat Defense-1-101004: (Primary) Failover cable not connected (other unit).`

説明フェールオーバー モードがイネーブルになっていますが、フェールオーバー ケーブルがフェールオーバー ペアの一方の装置に接続されていません。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション フェールオーバー ケーブルをフェールオーバー ペアの両方の装置に接続します。

101005

エラーメッセージ `%Threat Defense-1-101005: (Primary) Error reading failover cable status.`

説明フェールオーバー ケーブルが接続されていますが、プライマリ装置が自分のステータスを判断できません。

推奨アクション ケーブルを交換します。

103001

エラーメッセージ `%Threat Defense-1-103001: (Primary) No response from other firewall (reason code = code).`

説明プライマリ装置がフェールオーバー ケーブル経由でセカンダリ装置と通信できません。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。次の表に、フェールオーバーが発生した原因を判断するための原因コードおよび説明を示します。

原因コード	説明
1	ローカル装置が、LAN フェールオーバーが発生した場合はフェールオーバー LAN インターフェイス上で、シリアルフェールオーバーが発生した場合はシリアルフェールオーバーケーブル上で、hello パケットを受信しておらず、ピアがダウンしたと宣言しています。

原因コード	説明
2	インターフェイスが 4 つのフェールオーバー テストのうちのいずれか 1 つを通過させませんでした。4つのテストは、1）Link Up、2）Monitor for Network Traffic、3）ARP、および 4）Broadcast Ping です。
3	シリアル ケーブルでコマンドが送信された後 15 秒以上適切な ACK が受信されません。
4	フェールオーバー LAN インターフェイスがダウンし、他のデータ インターフェイスは、別のインターフェイスのテストに応答していません。また、ローカル装置はピアがダウンしていることを宣言しています。
5	コンフィギュレーション同期化プロセス中に、スタンバイ ピアがダウンしました。
6	複製が完了していません。フェールオーバー ユニットは同期されません。

推奨アクション フェールオーバー ケーブルが正しく接続され、両方の装置が同じハードウェア、ソフトウェア、およびコンフィギュレーションになっていることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

103002

エラーメッセージ `%Threat Defense-1-103002: (Primary) Other firewall network interface interface_number OK.`

説明セカンダリ装置のネットワーク インターフェイスが正常であることをプライマリ装置が検出しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

103003

エラーメッセージ `%Threat Defense-1-103003: (Primary) Other firewall network interface interface_number failed.`

説明セカンダリ装置に不良ネットワーク インターフェイスをプライマリ装置が検出しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション セカンダリ装置のネットワーク接続とネットワーク ハブ接続を確認します。必要に応じて、障害の発生したネットワーク インターフェイスを交換します。

103004

エラーメッセージ `%Threat Defense-1-103004: (Primary) Other firewall reports this firewall failed. Reason: reason-string`

説明プライマリ装置に障害が発生していることを示すメッセージをプライマリ装置がセカンダリ装置から受信しました。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。理由は、次のいずれかになります。

- フェールオーバー コマンド インターフェイスのポーリング パケット失敗がしきい値を超過しました。
- LAN フェールオーバー インターフェイスが失敗しました。
- ピアが Standby Ready 状態への移行に失敗しました。
- コンフィギュレーションの完全なレプリケーションに失敗しました。このファイアウォールのコンフィギュレーションが同期していない可能性があります。
- フェールオーバー メッセージの送信に失敗し、受信使用状態の ACK が受信されません。

推奨アクション プライマリ装置のステータスを確認します。

103005

エラーメッセージ `%Threat Defense-1-103005: (Primary) Other firewall reporting failure. Reason: SSM card failure`

説明 セカンダリ装置がプライマリ装置にSSMカードの障害を報告しました。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。

推奨アクション セカンダリ装置のステータスを確認します。

103006

エラーメッセージ `%Threat Defense-1-103006: (Primary|Secondary) Mate version ver_num is not compatible with ours ver_num`

説明 ローカル装置と異なるバージョンを実行している、HA Hitless Upgrade機能と互換性がないピア装置をSecure Firewall Threat Defenseデバイス が検出しました。

- *ver_num*：バージョン番号

推奨アクション 両方の装置に、同じバージョンまたは互換性のあるバージョンのイメージをインストールします。

103007

エラーメッセージ `%Threat Defense-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num`

説明 ピア装置で実行されているバージョンがローカル装置と異なるが、Hitless Upgradeをサポートしており、ローカル装置と互換性があることをSecure Firewall Threat Defenseデバイス が検出しました。イメージのバージョンが異なるために、システムのパフォーマンスが低下するおそれがあります。また、異なるイメージを長期間実行すると、Secure Firewall Threat Defenseデバイス で安定性の問題が発生する可能性があります。

- **ver_num**：バージョン番号

推奨アクション できるだけ早く、両方の装置に同じバージョンのイメージをインストールします。

103008

エラーメッセージ `%Threat Defense-1-103008: Mate hwdib index is not compatible`

説明 アクティブ装置とスタンバイ装置のインターフェイス数が同じではありません。

推奨アクション ユニット間のインターフェイスの数が同じであることを確認します。場合によって、追加のインターフェイスモジュールを取り付けるか、または別のデバイスを使用する必要があります。物理インターフェイスが一致したら、HAを一時停止してから再開することで、設定の同期を強制します。

104001、104002

エラーメッセージ `%Threat Defense-1-104001: (Primary) Switching to ACTIVE (cause: string).`

エラーメッセージ `%Threat Defense-1-104002: (Primary) Switching to STANDBY (cause: string ).`

説明スタンバイ装置で**failover active** コマンドを入力するか、またはアクティブ装置で**no failover active** コマンドを入力することによって強制的にフェールオーバー ペアの役割が切り替えられました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。string 変数の値は次のとおりです。

- state check
- bad/incomplete config
- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state
- other unit set to active by CLI config command fail active

推奨アクション 手作業による介入が原因でメッセージが表示される場合は、処置は不要です。それ以外の場合は、セカンダリ装置から報告された原因を使用して、ペアの装置両方のステータスを確認します。

104003

エラーメッセージ `%Threat Defense-1-104003: (Primary) Switching to FAILED.`

説明プライマリ装置に障害が発生しました。

推奨アクションプライマリ装置のメッセージを確認して、問題の内容を示す表示がないかどうかを調べます（メッセージ 104001 を参照）。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

104004

エラーメッセージ `%Threat Defense-1-104004: (Primary) Switching to OK.`

説明前に障害になった装置が再び動作していると報告しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105001

エラーメッセージ `%Threat Defense-1-105001: (Primary) Disabling failover.`

説明バージョン 7.x 以降では、このメッセージは、モードのミスマッチ（シングルまたはマルチ）、ライセンスのミスマッチ（暗号化またはコンテキスト）、またはハードウェアの相違（一方の装置には IPS SSM がインストールされ、そのピアには CSC SSM がインストールされている）が原因でフェールオーバーが自動的にディセーブルになったことを示す場合があります。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105002

エラーメッセージ `%Threat Defense-1-105002: (Primary) Enabling failover.`

説明これまでフェールオーバーをディセーブルにしていたコンソールで引数を指定せずに **failover** コマンドが使用されました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105003

エラーメッセージ `%Threat Defense-1-105003: (Primary) Monitoring on interface interface_name waiting`

説明 Secure Firewall Threat Defense デバイスが指定されたネットワーク インターフェイス（フェールオーバー ペアの相手装置とのインターフェイス）をテストしています。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

（注） 実際のステータスの変化と比較すると、syslog のロギングに遅延が生じる可能性があります。この遅延は、インターフェイスモニターリング用に設定されたポーリング時間とホールド時間によるものです。

推奨アクション 不要。Secure Firewall Threat Defense デバイス は、正常動作中に自分のネットワーク インターフェイスを頻繁にモニターします。

105004

エラーメッセージ `%Threat Defense-1-105004: (Primary) Monitoring on interface interface_name normal`

説明指定されたネットワーク インターフェイスのテストが成功しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

（注） 実際のステータスの変化と比較すると、syslog のロギングに遅延が生じる可能性があります。この遅延は、インターフェイスモニターリング用に設定されたポーリング時間とホールド時間によるものです。

推奨アクション 不要。

105005

エラーメッセージ `%Threat Defense-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.`

説明フェールオーバーペアの一方の装置がペアの相手装置と通信できなくなりました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション指定されたインターフェイスに接続されているネットワークが正しく機能していることを確認します。

105006、105007

エラーメッセージ`%Threat Defense-1-105006: (Primary) Link status Up on interface interface_name.`

エラーメッセージ `%Threat Defense-1-105007: (Primary) Link status Down on interface interface_name.`

説明指定されたインターフェイスのリンク ステータスのモニタリング結果が報告されました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション リンク ステータスがダウンである場合は、指定されたインターフェイスに接続されているネットワークが正しく動作していることを確認します。

105008

エラーメッセージ `%FTD-1-105008: (Primary) Testing interface interface_name.`

説明指定されたネットワーク インターフェイスのテストが行われました。このテストは、想定された間隔後にSecure Firewall Threat Defense デバイスがそのインターフェイス上でスタンバイ装置からメッセージを受け取ることができなかった場合に限って実行されます。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105009

エラーメッセージ `%Threat Defense-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.`

説明前のインターフェイス テストの結果（Passed または Failed）が報告されました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション結果が Passed であれば不要です。結果が Failed の場合は、両方のフェールオーバー装置へのネットワーク ケーブル接続、およびネットワーク自体が正しく機能していることをチェックし、スタンバイ装置のステータスを確認します。

105010

エラーメッセージ `%Threat Defense-3-105010: (Primary) Failover message block alloc failed.`

説明ブロック メモリが枯渇しました。これは一時メッセージで、Secure Firewall Threat Defense デバイスは回復する必要があります。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。

推奨アクション show blocks コマンドを使用して、現在のブロック メモリをモニターします。

105011

エラーメッセージ `%Threat Defense-1-105011: (Primary) Failover cable communication failure`

説明フェールオーバー ケーブルがプライマリ装置とセカンダリ装置間の通信を許可していません。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション ケーブルが正しく接続されていることを確認します。

105020

エラーメッセージ `%Threat Defense-1-105020: (Primary) Incomplete/slow config replication`

説明フェールオーバーが発生すると、アクティブな Secure Firewall Threat Defense デバイス はメモリ内の不完全なコンフィギュレーションを検出します。通常、これは複製サービスの中断が原因となっています。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。

推奨アクション Secure Firewall Threat Defense デバイス がフェールオーバーを検出した後、Secure Firewall Threat Defense デバイス は自動的にリブートして、フラッシュ メモリからコンフィギュレーションをロードするか、または別の Secure Firewall Threat Defense デバイス と再同期化します（両方行うこともあります）。フェールオーバーが引き続き発生する場合は、フェールオーバー コンフィギュレーションを調べて、両方の Secure Firewall Threat Defense デバイス 装置が互いに通信できることを確認します。

105021

エラーメッセージ `%Threat Defense-1-105021: (failover_unit ) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name`

説明コンフィギュレーションの同期化中に、他の何らかのプロセスが 5 分を超えてコンフィギュレーションをロックして、フェールオーバープロセスが新しいコンフィギュレーションを適用するのを妨げている場合、スタンバイ装置は自分自身をリロードします。これは、コンフィギュレーション同期化の進行中に、管理者がスタンバイ装置で実行コンフィギュレーションに目を通している場合に発生することがあります。コマンドリファレンスガイドで、特権 EXEC モードの **show running-config** コマンドと、グローバル コンフィギュレーション モードの **pager lines num** コマンドも参照してください。

推奨アクションスタンバイ装置が最初にブートし、アクティブ装置とのフェールオーバー接続を確立している間は、スタンバイ装置でコンフィギュレーションを表示または修正しないでください。

105022

エラーメッセージ `%FTD-1-105022: (host) Config replication failed with reason = (reason)`

説明 高可用性レプリケーションが失敗すると、このメッセージが生成されます。それぞれの説明は次のとおりです。

- *host*：現在のフェールオーバーユニット、つまりプライマリまたはセカンダリを示します。
- *reason*：フェールオーバー コンフィギュレーション レプリケーション終了のタイムアウト期限の理由。
  - CFG_SYNC_TIMEOUT：アクティブからスタンバイへの設定の複製時に 60 秒のタイマーが経過したため、デバイスの再起動が開始されます。
  - CFG_PROGRESSION_TIMEOUT：高可用性構成の複製を管理する 6 時間のタイマーが経過しました。

推奨アクション なし。

105031

エラーメッセージ `%Threat Defense-1-105031: Failover LAN interface is up`

説明 LAN フェールオーバー インターフェイス リンクがアップしています。

推奨アクション 不要。

105032

エラーメッセージ `%Threat Defense-1-105032: LAN Failover interface is down`

説明 LAN フェールオーバー インターフェイス リンクがダウンしています。

推奨アクション LAN のフェールオーバー インターフェイスの接続を確認します。速度または二重通信の設定が正しいことを確認します。

105033

エラーメッセージ `%Threat Defense-1-105033: LAN FO cmd Iface down and up again`

説明 フェールオーバーの LAN インターフェイスがダウンしました。

推奨アクション フェールオーバー リンクを確認します。通信の問題の可能性があります。

105034

エラーメッセージ `%Threat Defense-1-105034: Receive a LAN_FAILOVER_UP message from peer.`

説明 ピアがブートされて、初期コンタクト メッセージが送信されました。

推奨アクション 不要。

105035

エラーメッセージ `%Threat Defense-1-105035: Receive a LAN failover interface down msg from peer.`

説明ピア LAN フェールオーバー インターフェイス リンクがダウンしています。装置がスタンバイ モードになっている場合、アクティブ モードに切り替わります。

推奨アクション ピア LAN のフェールオーバー インターフェイスの接続を確認します。

105036

エラーメッセージ `%Threat Defense-1-105036: dropped a LAN Failover command message.`

説明 Secure Firewall Threat Defense デバイス は無応答の LAN フェールオーバー コマンド メッセージを廃棄しました。これは LAN フェールオーバー インターフェイスに接続障害が存在することを示します。

推奨アクション LAN インターフェイス ケーブルが接続されていることを確認します。

105037

エラーメッセージ `%Threat Defense-1-105037: The primary and standby units are switching back and forth as the active unit.`

説明プライマリ装置およびスタンバイ装置がアクティブ装置として交互に切り替わっています。これは、LAN フェールオーバー接続障害またはソフトウェアのバグが存在することを示します。

推奨アクション LAN インターフェイス ケーブルが接続されていることを確認します。

105038

エラーメッセージ `%Threat Defense-1-105038: (Primary) Interface count mismatch`

説明フェールオーバーが発生すると、アクティブな Secure Firewall Threat Defense デバイス はメモリ内の不完全なコンフィギュレーションを検出します。通常、これは複製サービスの中断が原因となっています。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション Secure Firewall Threat Defense デバイス によってフェールオーバーが検出されると、Secure Firewall Threat Defense デバイス は自動的にリブートして、フラッシュ メモリからコンフィギュレーションをロードするか、または別の Secure Firewall Threat Defense デバイスと再同期化します（両方行うこともあります）。フェールオーバーが引き続き発生する場合は、フェールオーバー コンフィギュレーションを調べて、両方の Secure Firewall Threat Defense デバイス 装置が互いに通信できることを確認します。

105039

エラーメッセージ `%Threat Defense-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.`

説明 フェールオーバーは最初にプライマリおよびセカンダリの Secure Firewall Threat Defense デバイス で設定されているインターフェイスの数が同じであることを確認します。このメッセージは、セカンダリのSecure Firewall Threat Defense デバイスで設定されているインターフェイスの数をプライマリのSecure Firewall Threat Defense デバイスが確認できないことを示します。このメッセージは、プライマリ Secure Firewall Threat Defense デバイス がフェールオーバー インターフェイス経由でセカンダリ Secure Firewall Threat Defense デバイス と通信できないことを示します。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション プライマリおよびセカンダリの Secure Firewall Threat Defense デバイス のフェールオーバー LAN、インターフェイス設定、ステータスを確認します。セカンダリの Secure Firewall Threat Defense デバイス が Secure Firewall Threat Defense デバイス アプリケーションを実行しており、フェールオーバーがイネーブルであることを確認します。

105040

エラーメッセージ `%Threat Defense-1-105040: (Primary) Mate failover version is not compatible.`

説明 プライマリおよびセカンダリの Secure Firewall Threat Defense デバイス は、フェールオーバー ペアとして動作するために同じフェールオーバー ソフトウェアのバージョンを実行する必要があります。このメッセージは、セカンダリのSecure Firewall Threat Defense デバイス フェールオーバー ソフトウェアのバージョンがプライマリのSecure Firewall Threat Defense デバイスと互換性がないことを示します。フェールオーバーがプライマリのSecure Firewall Threat Defense デバイスでディセーブルになっています。Primary は、セカンダリの Secure Firewall Threat Defense デバイス の場合は Secondary と示されることもあります。

推奨アクション フェールオーバーをイネーブルにするために、プライマリおよびセカンダリの Secure Firewall Threat Defense デバイス 間で一致したソフトウェア バージョンを使用します。

105041

エラーメッセージ `%Threat Defense-1-105041: cmd failed during sync`

説明 アクティブ装置とスタンバイ装置のインターフェイス数が同じではないため、nameif コマンドの複製に失敗しました。

推奨アクション ユニット間のインターフェイスの数が同じであることを確認します。場合によって、追加のインターフェイス モジュールを取り付けるか、または別のデバイスを使用する必要があります。物理インターフェイスが一致したら、HA を一時停止してから再開することで、設定の同期を強制します。

105042

エラーメッセージ `%Threat Defense-1-105042: (Primary) Failover interface OK`

説明 フェールオーバーメッセージを送信するインターフェイスは、フェールオーバーリンクの物理ステータスがダウンしている場合、またはフェールオーバーピア間の L2 接続が失われ、その結果 ARP パケットがドロップされる場合にダウンする可能性があります。このメッセージは、L2 ARP 接続を復元した後に生成されます。

推奨アクション 不要。

105043

エラーメッセージ `%Threat Defense-1-105043: (Primary) Failover interface failed`

説明 この Syslog は、フェールオーバーリンクの物理ステータスがダウンしている場合、またはフェールオーバーピア間の L2 接続が失われた場合に生成されます。切断すると、ユニット間の ARP パケットが失われます。

推奨処置

- フェールオーバーリンクの物理ステータスを確認し、物理ステータスと動作ステータスが機能していることを確認します。
- ARP パケットがフェールオーバーペア間のフェールオーバーリンクの中継パスを通過することを確認します。

105044

エラーメッセージ `%Threat Defense-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.`

説明動作モード（シングルまたはマルチ）がフェールオーバー ピア間で一致しない場合、フェールオーバーはディセーブルになります。

推奨アクション 同じ動作モードになるようにフェールオーバー ピアを設定してから、フェールオーバーを再度イネーブルにします。

105045

エラーメッセージ `%Threat Defense-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).`

説明フィーチャ ライセンスがフェールオーバー ピア間で一致しない場合、フェールオーバーはディセーブルになります。

推奨アクション 同じフィーチャ ライセンスになるようにフェールオーバー ピアを設定してから、フェールオーバーを再度イネーブルにします。

105046

エラーメッセージ `%Threat Defense-1-105046: (Primary|Secondary) Mate has a different chassis`

説明 2つのフェールオーバー装置が異なるタイプのシャーシを持っています。たとえば、一方が 3 スロットのシャーシを持ち、もう一方が 6 スロットのシャーシを持つ場合です。

推奨アクション 2 つのフェールオーバー装置が同じであることを確認します。

105047

エラーメッセージ `%Threat Defense-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2`

説明 2つのフェールオーバー装置は、対応するスロットに異なるタイプのカードが実装されています。

推奨アクション フェールオーバー装置のカード コンフィギュレーションが同じであることを確認します。

105048

エラーメッセージ `%Threat Defense-1-105048: (unit ) Mate's service module (application ) is different from mine (application )`

説明 アクティブ装置とスタンバイ装置のサービスモジュールで異なるアプリケーションが動作していることをフェールオーバー プロセスが検出しました。異なるサービス モジュールが使用されている場合、2 つのフェールオーバー装置は互換性がありません。

- **unit**：プライマリまたはセカンダリ
- **application**：アプリケーションの名前（たとえば、InterScan Security Card）

推奨アクション フェールオーバーを再度イネーブルにする前に、両方の装置が同じサービス モジュールを装備していることを確認します。

105050

エラーメッセージ `%Threat Defense-3-105050: ASAv ethernet interface mismatch`

説明 スタンバイ装置のイーサネット インターフェイスの数がアクティブ装置のイーサネット インターフェイスの数より少ないです。

推奨アクション インターフェイスの数が同じ Secure Firewall Threat Defense デバイス を互いにペアにしてください。装置のインターフェイスの数が同じであることを確認します。場合によって、追加のインターフェイス モジュールを取り付けるか、または別のデバイスを使用する必要があります。物理インターフェイスが一致したら、HA を一時停止してから再開することで、設定の同期を強制します。

106001

エラーメッセージ `%Threat Defense-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`

説明内部アドレスへの接続の試行が、指定されたトラフィック タイプに定義されたセキュリティ ポリシーによって拒否されました。表示される IP アドレスは、NAT によって表示される IP アドレスではなく実際の IP アドレスです。表示される tcp_flags 値は、接続が拒否されたときに存在していた TCP ヘッダーのフラグに対応します。たとえば、Secure Firewall Threat Defense デバイスに接続状態が存在しない TCP パケットが到着し、それが廃棄された場合です。このパケットの tcp_flags は FIN および ACK です。

tcp_flags を次に示します。

- ACK：肯定応答番号が受信されました。
- FIN：データが送信されました。
- PSH：受信者がデータをアプリケーションに渡しました。
- RST：接続がリセットされました。
- SYN：シーケンス番号が接続を開始するために同期化されました。
- URG：緊急ポインタが有効であると宣言されました。

推奨アクション 不要。

106002

エラーメッセージ `%Threat Defense-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address`

説明指定された接続は、**outbound deny** コマンドが原因で失敗しました。**protocol** 変数は ICMP、TCP、または UDP になります。

推奨アクション show outbound コマンドを使用して、発信リストを確認します。

106006

エラーメッセージ `%Threat Defense-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.`

説明着信 UDP パケットが、指定されたトラフィック タイプに定義されているセキュリティ ポリシーによって拒否されました。

推奨アクション 不要。

106007

エラーメッセージ `%Threat Defense-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.`

説明 DNS クエリーまたは応答を含む UDP パケットが拒否されました。

推奨アクション 内部ポート番号が 53 の場合、内部ホストはキャッシング ネーム サーバーとして設定されていると考えられます。**access-list** コマンド文を追加して、UDP ポート 53 のトラフィックおよび内部ホストの変換エントリを許可します。外部ポート番号が 53 の場合、DNS サーバーの応答が遅かったため、クエリーには別のサーバーが応答したと考えられます。

106010

エラーメッセージ `%Threat Defense-3-106010: Deny inbound protocol src [interface_name : source_address/source_port ] [([idfw_user | FQDN_string ], sg_info )] dst [interface_name : dest_address /dest_port ][([idfw_user | FQDN_string ], sg_info )]`

説明 着信接続は、セキュリティ ポリシーによって拒否されました。

推奨アクション トラフィックを許可する必要がある場合は、セキュリティ ポリシーを修正します。このメッセージが繰り返し表示される場合は、リモート ピアの管理者にお問い合わせください。

106011

エラーメッセージ `%Threat Defense-3-106011: Deny inbound (No xlate) protocol src Interface:IP/port dst Interface-nameif:IP/port`

説明 このメッセージは、Web ブラウザ経由でインターネットにアクセスしている内部ユーザーがいる場合、通常のトラフィック条件で表示されます。接続がリセットされた場合は常に、Secure Firewall Threat Defense デバイス が接続リセットを受信した後にその接続の端にあるホストがパケットを送信すると、このメッセージが表示されます。これは通常、無視してかまいません。

推奨アクション **no logging message 106011** コマンドを入力して、このメッセージが syslog サーバーに記録されないようにします。

106012

エラーメッセージ `%Threat Defense-6-106012: Deny IP from IP_address to IP_address , IP options hex.`

説明 IP パケットが IP オプションとともに表示されました。IP オプションはセキュリティ リスクと見なされるので、パケットは廃棄されました。

推奨アクション リモート ホスト システムの管理者に問い合わせて、問題を判別します。ローカル サイトを確認して、あいまいなソース ルーティングや厳密なソース ルーティングがないかどうかを調べます。

106013

エラーメッセージ `%Threat Defense-2-106013: Dropping echo request from IP_address to PAT address IP_address`

説明 Secure Firewall Threat Defense デバイス は、PAT グローバル アドレスに対応する宛先アドレスを持つ着信 ICMP エコー要求パケットを廃棄しました。着信パケットは、そのパケットを受信するべき PAT ホストを指定できないので廃棄されます。

推奨アクション 不要。

106014

エラーメッセージ `%Threat Defense-3-106014: Deny inbound icmp src interface_name : IP_address [([idfw_user | FQDN_string ], sg_info )] dst interface_name : IP_address [([idfw_user | FQDN_string ], sg_info )] (type dec , code dec )`

説明 Secure Firewall Threat Defense デバイス は、着信 ICMP パケット アクセスをすべて拒否しました。デフォルトで、ICMP パケットはすべて、特に許可されている場合を除き、アクセスを拒否されます。

推奨アクション 不要。

106015

エラーメッセージ `%Threat Defense-6-106015: Deny TCP (no connection) from IP_address /port to IP_address /port flags tcp_flags on interface interface_name.`

説明 Secure Firewall Threat Defense デバイス は、関連付けられている接続が Secure Firewall Threat Defense 接続テーブルにない TCP パケットを廃棄しました。Secure Firewall Threat Defense デバイス は、新しい接続の確立要求を示す SYN フラグをパケットで探します。SYN フラグがセットされておらず、既存の接続がない場合、Secure Firewall Threat Defense デバイス はそのパケットを廃棄します。

推奨アクション Secure Firewall Threat Defense デバイス がこれらの無効な TCP パケットを大量に受信する場合を除き、不要です。大量に受信する場合は、パケットを送信元までトレースして、これらのパケットが送信された原因を判別します。

106016

エラーメッセージ `%Threat Defense-2-106016: Deny IP spoof from (IP_address ) to IP_address on interface interface_name.`

説明宛先 IP アドレスが 0.0.0.0 で、宛先 MAC アドレスが Secure Firewall Threat Defense インターフェイスのアドレスのパケットが Secure Firewall Threat Defense インターフェイスに到着しました。また、このメッセージは、Secure Firewall Threat Defense デバイス が無効な送信元アドレス（たとえば、次に示すアドレスなどの無効アドレス）を持つパケットを廃棄した場合にも生成されます。

- ループバック ネットワーク（127.0.0.0）
- ブロードキャスト（limited、net-directed、subnet-directed、および all-subnets-directed）
- 宛先ホスト（land.c）

スプーフィング パケット検出をさらに強化するには、**icmp** コマンドを使用して、内部ネットワークに属する送信元アドレスを持つパケットを廃棄するように Secure Firewall Threat Defense デバイス を設定します。現在、**access-list** コマンドは推奨されておらず、正しく動作することも保証されていません。

推奨アクション外部ユーザーが保護されているネットワークを危険にさらそうとしていないかどうかを判別します。設定に誤りのあるクライアントをチェックします。

106017

エラーメッセージ `%Threat Defense-2-106017: Deny IP due to Land Attack from IP_address to IP_address`

説明 IP 送信元アドレスと IP 宛先が同一で、かつ宛先ポートと送信元ポートが同一のパケットを Secure Firewall Threat Defense デバイス が受信しました。このメッセージは、システムの攻撃を目的としてスプーフィングされたパケットを示します。この攻撃は、Land 攻撃と呼ばれます。

推奨アクションこのメッセージが引き続き表示される場合は、攻撃が進行中である可能性があります。パケットは、攻撃の起点を決定するのに十分な情報を提供しません。

106018

エラーメッセージ `%Threat Defense-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address`

説明ローカル ホスト（inside_address）から外部ホスト（outside_address）への発信 ICMP パケット（指定された ICMP のパケット）が発信 ACL リストによって拒否されました。

推奨アクション 不要。

106020

エラーメッセージ `%Threat Defense-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address`

説明 Secure Firewall Threat Defense デバイス が、小さなオフセットまたはフラグメントの重複が含まれる teardrop シグニチャを持つ IP パケットを廃棄しました。これは、Secure Firewall Threat Defense デバイス または侵入検知システムを欺く敵対イベントです。

推奨アクション リモート ピアの管理者に連絡するか、またはセキュリティ ポリシーに従ってこの問題の危険度を高くします。

106021

エラーメッセージ `%Threat Defense-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`

説明攻撃が進行中です。インバウンド接続上の IP アドレスのスプーフィングが試みられています。逆ルート ルックアップとも呼ばれる Unicast RPF は、ルートによって表される送信元アドレスを持たないパケットを検出し、そのパケットをSecure Firewall Threat Defense デバイスへの攻撃の一部であると想定します。

このメッセージは、ip verify reverse-path コマンドで Unicast RPF をイネーブルにしている場合に表示されます。この機能は、インターフェイスに入力されるパケットについて動作します。外側で設定されている場合、Secure Firewall Threat Defense デバイスは、外部から到達するパケットを確認します。

Secure Firewall Threat Defense デバイスは、source_address に基づいてルートを検索します。エントリが検出されず、ルートが定義されない場合は、このメッセージが表示され、接続は廃棄されます。

ルートがある場合、Secure Firewall Threat Defense デバイスは対応するインターフェイスを確認します。パケットが別のインターフェイスに到達している場合、スプーフィングであるか、または宛先への複数パスが存在する非対称ルーティング環境であるかのどちらかです。Secure Firewall Threat Defense デバイスは、非対称ルーティングをサポートしていません。

Secure Firewall Threat Defense デバイス は内部インターフェイスに設定されている場合、スタティック ルート コマンド文または RIP をチェックします。source_address が見つからない場合、内部ユーザーはアドレスをスプーフィングしています。

推奨アクション攻撃が進行中であっても、この機能がイネーブルになっていれば、ユーザーによる処置は不要です。Secure Firewall Threat Defense デバイス により、攻撃が阻止されます。

106022

エラーメッセージ `%Threat Defense-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`

説明接続と一致するパケットが、その接続が開始されたインターフェイスとは異なるインターフェイスに到着しました。また、ip verify reverse-path コマンドが設定されていません。

たとえば、ユーザーが内部インターフェイスで接続を開始したが、Secure Firewall Threat Defense デバイスが境界インターフェイスに到着する同じ接続を検出する場合、Secure Firewall Threat Defense デバイスは宛先へのパスを複数持っていることになります。これは非対称ルーティングと呼ばれ、Secure Firewall Threat Defense デバイスではサポートされていません。

攻撃者は、Secure Firewall Threat Defense デバイスに侵入する方法として、1 つの接続から別の接続にパケットを付加しようと試みることもあります。どちらの場合も、Secure Firewall Threat Defense デバイス はこのメッセージを表示して、接続を廃棄します。

推奨アクション ルーティングが非対称でないことを確認します。

106023

エラーメッセージ `%Threat Defense-4-106023: Deny protocol src [interface_name :source_address /source_port ] [([idfw_user |FQDN_string ], sg_info )] dst interface_name`

:*dest_address /dest_port* [([*idfw_user* |*FQDN_string*], *sg_info*)] [type {*string* }, code {*code* }] by *access_group acl_ID* [0x8ed66b60, 0xf8852875]

説明 ACL により実 IP パケットが拒否されました。このメッセージは、ACL に対して **log** オプションをイネーブルにしていない場合でも表示されます。IP アドレスは、NAT によって表示される値ではなく実際の IP アドレスです。一致するものが見つかった場合、IP アドレスに対応するユーザー ID 情報と FQDN 情報の両方が出力されます。Secure Firewall Threat Defense デバイス は、識別情報（ドメイン\ユーザー）または FQDN（ユーザー名が使用できない場合）のいずれかをログに記録します。識別情報または FQDN が使用可能な場合、Secure Firewall Threat Defense デバイス は、この情報を送信元と宛先の両方のログに記録します。

推奨アクション 同じ送信元アドレスからのメッセージが引き続き表示される場合は、フットプリンティングまたはポート スキャンが行われている可能性があります。リモート ホストの管理者にお問い合わせください。

106024

エラーメッセージ `%Threat Defense-2-106024: Access rules memory exhausted`

説明 アクセス リストのコンパイル プロセスで、メモリが不足しています。最後の正常なアクセス リスト以降に追加されたコンフィギュレーション情報はすべて、Secure Firewall Threat Defense デバイス から削除されました。最新のコンパイル済みアクセス リストのセットが引き続き使用されます。

推奨アクション Access Lists、AAA、ICMP、SSH、Telnet、および他の規則タイプは、アクセス リストの規則タイプとして格納され、コンパイルされます。これらの規則タイプの一部を削除して、他の規則タイプを追加できるようにします。

106025、106026

エラーメッセージ `%Threat Defense-6-106025: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol`

エラーメッセージ `%Threat Defense-6-106026: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol`

説明 マルチコンテキスト モードのパケットのセキュリティ コンテキストを判定できません。どちらのメッセージも、ルータまたはトランスペアレント モードで廃棄される IP パケットに対して生成されることがあります。

推奨アクション 不要。

106027

エラーメッセージ `%Threat Defense-4-106027:acl_ID: Deny src [source address] dst [destination address] by access-group "access-list name"`

説明 ACL により非 IP パケットが拒否されました。このメッセージは、たとえ拡張 ACL に対して log オプションがイネーブルになっていない場合でも表示されます。

推奨アクション同じ送信元アドレスからのメッセージが引き続き表示される場合は、フットプリンティングまたはポート スキャンが行われようとしていることを示している可能性があります。リモート ホストの管理者にお問い合わせください。

106100

エラーメッセージ`%Threat Defense-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name /source_address (source_port ) (idfw_user , sg_info ) interface_name /dest_address (dest_port ) (idfw_user , sg_info ) hit-cnt number ({first hit | number -second interval}) hash codes`

説明最初の出現か、またはある期間の合計出現数を示します。このメッセージは、拒否されたパケットだけを記録して、ヒット数も設定可能なレベルも含まないメッセージ 106023 よりも多くの情報を提供します。

アクセス リストの行に *log* 引数が含まれている場合、非同期パケットが Secure Firewall Threat Defense デバイスに到達し、アクセス リストによって評価されることによって、このメッセージ ID がトリガーされる可能性があると想定されます。たとえば、Secure Firewall Threat Defense デバイス で（接続テーブルに TCP 接続が存在しない）ACK パケットを受信した場合、Secure Firewall Threat Defense デバイス によってメッセージ 106100 が生成される可能性があります。このメッセージは、パケットは許可されたが、一致する接続が存在しないために後で正しく廃棄されることを示します。

メッセージの値は次のとおりです。

- permitted | denied | est-allowed：これらの値は、パケットが ACL によって許可されたか拒否されたかを指摘します。値が est-allowed の場合、パケットは ACL によって拒否されましたが、すでに確立されているセッションで許可されました（たとえば、内部ユーザーがインターネットへのアクセスを許可され、通常は ACL によって拒否される応答パケットが許可されます）。
- *protocol*：TCP、UDP、ICMP、または IP プロトコル番号。
- *interface_name*：ログ フローの送信元または宛先のインターフェイス名。VLAN インターフェイスがサポートされています。
- *source_address*：ログ フローの送信元 IP アドレス。IP アドレスは、NAT によって表示される値ではなく実際の IP アドレスです。
- *dest_address*：ログ フローの宛先 IP アドレス。IP アドレスは、NAT によって表示される値ではなく実際の IP アドレスです。
- *source_port*：ログ フローの送信元ポート（TCP または UDP）。ICMP の場合、送信元ポートの後の数字は、メッセージ タイプです。
- *idfw_user*：Secure Firewall Threat Defense デバイス が当該 IP アドレスのユーザー名を見つけた場合に既存の syslog に追加される、ドメイン名を含むユーザー識別用ユーザー名。
- *sg_info*：Secure Firewall Threat Defense デバイス によって当該 IP アドレスのセキュリティ グループ タグが検出された場合に syslog に追加されるセキュリティ グループ タグ。セキュリティ グループ名は、セキュリティ グループ タグがあればそれとともに表示されます。
- *dest_port*：ログ フローの宛先ポート（TCP または UDP）。ICMP の場合、宛先ポートの後の数字は ICMP メッセージ コードです。これは一部のメッセージ タイプに使用可能です。

タイプ 8 の場合、これは常に 0 です。ICMP メッセージ タイプのリストについては、次の URL を参照してください。http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml

- hit-cnt *number*：設定した期間に、このフローが ACL エントリによって許可または拒否された回数。Secure Firewall Threat Defense デバイス がこのフローに対して最初のメッセージを生成するときの値は 1 です。
- first hit：このフローに対して生成された最初のメッセージ。
- *number*-second interval：ヒット数を累算する対象期間。この期間は、**access-list** コマンドで **interval** オプションを使用して設定します。
- hash codes：オブジェクト グループ ACE および構成要素の通常の ACE には、必ず 2 が表示されます。値は、パケットがヒットする ACE 上で決定されます。これらのハッシュ コードを表示するには **show-access list** コマンドを入力します。

推奨アクション 不要。

106101

エラーメッセージ `%Threat Defense-1-106101 Number of cached deny-flows for ACL log has reached limit (number ).`

説明 ACL **deny** 文（**access-list** *id* **deny** コマンド）に **log** オプションを設定してあり、トラフィック フローが ACL 文と一致する場合、Secure Firewall Threat Defense デバイス はフロー情報をキャッシュします。このメッセージは、Secure Firewall Threat Defense デバイスでキャッシュされる一致フローの数がユーザーが設定した制限（**access-list deny-flow-max** コマンドを使用）を超えたことを示します。このメッセージは、サービス拒絶（DoS）攻撃の結果生成される可能性があります。

- *number*：**access-list deny-flow-max** コマンドを使用して設定された制限

推奨アクション 不要。

106102

エラーメッセージ `%Threat Defense-6-106102: access-list acl_ID {permitted|denied} protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number {first hit|number -second interval} hash codes`

説明 VPN フィルタを通じて適用されるアクセス リストによってパケットが許可または拒否されました。このメッセージは、メッセージ 106100 に相当する VPN/AAA フィルタのメッセージです。

推奨アクション 不要。

106103

エラーメッセージ `%Threat Defense-4-106103: access-list acl_ID denied protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number first hit hash codes`

説明 VPN フィルタを通じて適用されるアクセス リストによってパケットが拒否されました。このメッセージは、メッセージ 106023 に相当する VPN/AAA フィルタのメッセージです。

推奨アクション 不要。

107001

エラーメッセージ `%Threat Defense-1-107001: RIP auth failed from IP_address : version=number, type=string, mode=string, sequence=number on interface interface_name`

説明 Secure Firewall Threat Defense デバイス は不正な認証を持つ RIP 応答メッセージを受信しました。このメッセージは、ルータまたはSecure Firewall Threat Defense デバイスの設定の誤り、またはSecure Firewall Threat Defense デバイスのルーティング テーブルへの攻撃の失敗が原因となることもあります。

推奨アクション このメッセージは攻撃の可能性を示しているため、モニターする必要があります。このメッセージに示されている送信元 IP アドレスを熟知していない場合は、信頼できるエンティティ間でRIP認証キーを交換します。攻撃者が既存のキーを判別しようと試みている可能性もあります。

109011

エラーメッセージ `%Threat Defense-2-109011: Authen Session Start: user 'user ', sid number`

説明認証セッションがホストと Secure Firewall Threat Defense デバイス の間で開始されましたが、まだ完了していません。

推奨アクション 不要。

109012

エラーメッセージ `%Threat Defense-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds`

説明認証キャッシュがタイムアウトになっています。ユーザーは、次の接続で再認証が必要になります。timeout uauth コマンドを使用して、このタイマーのタイムアウト時間を変更できます。

推奨アクション 不要。

109013

エラーメッセージ `%Threat Defense-3-109013: User must authenticate before using this service`

説明ユーザーは、サービスを使用する前に認証を受ける必要があります。

推奨アクション サービスを使用する前に FTP、Telnet、または HTTP を使用して認証します。

109016

エラーメッセージ `%Threat Defense-3-109016: Can't find authorization ACL acl_ID for user 'user '`

説明このユーザーの AAA サーバーで指定された ACL が、Secure Firewall Threat Defense デバイスに存在しません。このエラーは、Secure Firewall Threat Defense デバイスを設定する前に AAA サーバーを設定した場合に発生することがあります。AAA サーバーでベンダー固有の属性（VSA）が次の値のいずれかになっている可能性があります。

- acl=acl_ID
- shell:acl=acl_ID
- ACS:CiscoSecured-Defined-ACL=acl_ID

推奨アクション Secure Firewall Threat Defense デバイス に ACL を追加し、AAA サーバーで指定したものと同じ名前を必ず使用します。

109018

エラーメッセージ `%Threat Defense-3-109018: Downloaded ACL acl_ID is empty`

説明ダウンロードされた認可に ACE がありません。この状況は、属性文字列 *ip:inacl#* のつづりの誤り、または access-list コマンドの省略が原因となっている可能性があります。

```
junk:junk# 1=permit tcp any any eq junk ip:inacl#1=”
```

推奨アクション 指摘されたエラーのある ACL コンポーネントを AAA サーバー上で修正します。

109019

エラーメッセージ `%Threat Defense-3-109019: Downloaded ACL acl_ID has parsing error; ACE string`

説明ダウンロードした認可の属性文字列 ip:inacl#NNN= のシーケンス番号 NNN を解析中にエラーが発生しました。= の欠落、数字以外の文字やスペース以外の文字が # と = の間にある、NNN が 999999999 より大きい、などの原因が考えられます。

```
ip:inacl# 1 permit tcp any any
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 1000000000=permit tcp any any
```

推奨アクション 指摘されたエラーのある ACL コンポーネントを AAA サーバー上で修正します。

109020

エラーメッセージ `%Threat Defense-3-109020: Downloaded ACL has config error; ACE`

説明ダウンロードされた認可のコンポーネントの 1 つにコンフィギュレーション エラーがあります。要素のテキスト全体がメッセージに含まれています。このメッセージは通常、無効な access-list コマンド文が原因となっています。

推奨アクション 指摘されたエラーのある ACL コンポーネントを AAA サーバー上で修正します。

109026

エラーメッセージ `%Threat Defense-3-109026: [aaa protocol ] Invalid reply digest received; shared server key may be mismatched.`

説明 AAA サーバーからの応答を検証できません。設定されたサーバー キーが誤っている可能性があります。このメッセージは、RADIUS サーバーまたは TACACS+ サーバーとのトランザクション中に生成されることがあります。

aaa-server コマンドを使用して設定されたサーバー キーが正しいことを確認します。

109027

エラーメッセージ `%Threat Defense-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address , User = user`

説明 AAA サーバーからの応答を検証できません。設定されたサーバー キーが誤っている可能性があります。このメッセージは、RADIUS サーバーまたは TACACS+ サーバーとのトランザクション中に表示されることがあります。server_IP_address は、関連する AAA サーバーの IP アドレスです。user は、接続に関連付けられているユーザー名です。

推奨アクション aaa-server コマンドを使用して設定されたサーバー キーが正しいことを確認します。

109029

エラーメッセージ `%Threat Defense-5-109029: Parsing downloaded ACL: string`

説明ユーザー認証中に RADIUS サーバーからダウンロードされたアクセス リストを解析している間に構文エラーが発生しました。

- *string*：アクセス リストの正しい解析を妨げた構文エラーを詳述するエラー メッセージ

推奨アクションこのメッセージに提示されている情報を使用して、RADIUS サーバー コンフィギュレーション内のアクセス リスト定義にある構文エラーを特定し、訂正します。

109030

エラーメッセージ `%Threat Defense-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source |dest netmask netmask .`

説明 RADIUS サーバーで設定されたダイナミック ACL が、ワイルドカード ネットマスクを自動的に検出するメカニズムによって変換されませんでした。問題は、ネットマスクがワイルド

カードであるか、通常のネットマスクであるかをこのメカニズムが判別できないために発生します。

- **access_list**：変換できないアクセス リスト
- **source**：送信元 IP アドレス
- **dest**：宛先 IP アドレス
- **netmask**：宛先アドレスまたは送信元アドレスに対する 10 進数表記のサブネット マスク

推奨アクション RADIUS サーバーのアクセス リスト ネットマスクを確認して、ワイルドカードコンフィギュレーションがないかどうかを調べます。ネットマスクをワイルドカードにする予定の場合、およびそのサーバーのアクセス リスト ネットマスクすべてがワイルドカードである場合、AAA サーバーの **acl-netmask-convert** に wildcard 設定を使用します。それ以外の場合は、ネットマスクを通常のネットマスクまたはホールを含まないワイルドカードネットマスクに変更します（つまり、ネットマスクは連続する 2 進数の 1 を提示します。たとえば、00000000.00000000.00011111.11111111 または 16 進数の 0.0.31.255 のようになります）。マスクを通常にする予定の場合、およびそのサーバーのすべてのアクセス リスト ネットマスクが通常である場合、AAA サーバーの **acl-netmask-convert** に normal 設定を使用します。

109032

エラーメッセージ `%Threat Defense-3-109032: Unable to install ACL access_list , downloaded for user username ; Error in ACE: ace .`

説明 Secure Firewall Threat Defense デバイス は、ユーザー接続に適用するアクセス コントロール リストを RADIUS サーバーから受信しましたが、リストのエントリに構文エラーが含まれています。エラーが含まれるリストを使用すると、セキュリティ ポリシー違反になる可能性があるため、Secure Firewall Threat Defense デバイス はユーザーを認証できませんでした。

- *access_list*：**show access-list** コマンドの出力に表示されるダイナミック アクセス リストに割り当てられている名前
- *username*：その接続がこのアクセス リストの制御を受けるユーザーの名前
- *ace*：エラーが検出されたときに処理されていたアクセス リストのエントリ

推奨アクション RADIUS サーバーのコンフィギュレーションのアクセス リスト定義を訂正します。

109033

エラーメッセージ `%Threat Defense-4-109033: Authentication failed for admin user user from src_IP . Interactive challenge processing is not supported for protocol connections`

説明管理接続の認証中に AAA チャレンジ処理がトリガーされましたが、Secure Firewall Threat Defense デバイス はそのクライアント アプリケーションでの対話型チャレンジ処理を開始できません。このような場合は、認証試行が拒否され、接続が拒否されます。

- *user*：認証対象のユーザーの名前
- *src_IP*：クライアント ホストの IP アドレス。
- *protocol*：クライアント接続プロトコル（SSH v1 または管理 HTTP）

推奨アクションこれらの接続タイプに対してチャレンジ処理が発生しないように AAA を再設定します。これは、通常、RSA SecurID サーバー、またはRADIUS経由のトークンベースAAAサーバーに対して、これらの接続タイプの認証を避けることを意味します。

109034

エラーメッセージ `%Threat Defense-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port . Interactive challenge processing is not supported for protocol connections`

説明ネットワーク接続の認証中にAAAチャレンジ処理がトリガーされましたが、Secure Firewall Threat Defense デバイス はそのクライアント アプリケーションでの対話型チャレンジ処理を開始できません。このような場合は、認証試行が拒否され、接続が拒否されます。

- *user*：認証対象のユーザーの名前
- *src_IP/port*：クライアント ホストの IP アドレスおよびポート。
- *dst_IP/port*：クライアントが接続しようとしているサーバーの IP アドレスおよびポート。
- *protocol*：クライアント接続プロトコル（たとえば、FTP）

推奨アクションこれらの接続タイプに対してチャレンジ処理が発生しないように AAA を再設定します。これは、通常、RSA SecurID サーバー、またはRADIUS経由のトークンベースAAAサーバーに対して、これらの接続タイプの認証を避けることを意味します。

109035

エラーメッセージ `%Threat Defense-3-109035: Exceeded maximum number (<max_num>) of DAP attribute instances for user <user>`

説明このログは、RADIUS サーバーから受信した DAP 属性の数が、指定されたユーザーの接続の認証中に許可されている最大数を超えた場合に生成されます。

推奨アクション DAP 属性のコンフィギュレーションを変更してログで指定されている許可最大数以下に DAP 属性の数を削減し、指定したユーザーが接続できるようにします。

109036

エラーメッセージ `%Threat Defense-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username .`

説明 LDAP 応答メッセージに、1000 を超える値を持つ属性が含まれています。

- *attribute_name*：LDAP 属性名
- *username*：ログイン時のユーザー名

推奨アクション 不要。

109037

エラーメッセージ `%Threat Defense-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username .`

説明 Secure Firewall Threat Defense デバイス では、AAA サーバーから同じ属性の複数の値を受信することがサポートされています。AAA サーバーから同じ属性に関して 5000 を超える値を含む応答が送信されてきた場合、Secure Firewall Threat Defense デバイス ではこの応答メッセージを形式誤りとして処理し、認証を拒否します。このような状況は、特殊なテストツールを使用するラボ環境でだけ確認されています。実際の実稼働ネットワークで発生する可能性はまずありません。

- *attribute_name*：LDAP 属性名
- *username*：ログイン時のユーザー名

推奨アクション プロトコル スニファ（WireShark など）を使用して Secure Firewall Threat Defense デバイス と AAA サーバー間の認証トラフィックを取り込み、トレース ファイルを Cisco TAC に転送して分析を依頼してください。

109038

エラーメッセージ `%Threat Defense-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name`

説明 AAA サブシステムが AAA サーバーからの属性を内部表現へと解析しようとして失敗しました。

- *string-from-server*：AAA サーバーから受信した文字列。40 文字に切り捨てられます。
- *type*：指定された属性のタイプ

推奨アクション 属性が AAA サーバー上に正しく生成されていることを確認します。詳細については、**debug ldap** コマンドおよび **debug radius** コマンドを使用します。

109039

エラーメッセージ `%Threat Defense-5-109039: AAA Authentication:Dropping an unsupported IPv6/IP46/IP64 packet from lifc :laddr to fifc :faddr`

説明 NAT によって IPv6 アドレスに変換される IPv6 アドレスまたは IPv4 アドレスを含むパケットには、AAA の認証または承認が必要です。AAA の認証および承認は IPv6 アドレスをサポートしません。パケットはドロップされます。

- *lifc*：入力インターフェイス
- *laddr*：送信元 IP アドレス
- *fifc*：出力インターフェイス
- *faddr*：NAT 変換後の宛先 IP アドレス（存在する場合）

推奨アクション 不要。

109100

エラーメッセージ `%Threat Defense-6-109100: Received CoA update from coa-source-ip for user username , with session ID: audit-session-id , changing authorization attributes`

説明 Secure Firewall Threat Defense デバイス は、セッション ID *audit-session-id* を持つユーザー *username* の *coa-source-ip* からの CoA ポリシー更新要求を正常に処理しました。この Syslog メッセージは、認可変更ポリシーの更新を Secure Firewall Threat Defense デバイス が受け取り、検証および適用した後に生成されます。エラーがない場合、認可変更を受け取って処理するときに生成されるのはこの Syslog メッセージのみです。

- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109101

エラーメッセージ `%Threat Defense-6-109101: Received CoA disconnect request from coa-source-ip for user username , with audit-session-id: audit-session-id`

説明 Secure Firewall Threat Defense デバイス は、アクティブな VPN セッションに対して正しくフォーマットされた Disconnect-Request を受信し、接続を正常に終了しました。

- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109102

エラーメッセージ `%Threat Defense-4-109102: Received CoA action-type from coa-source-ip , but cannot find named session audit-session-id`

説明 Secure Firewall Threat Defense デバイス は有効な認可変更要求を受信しましたが、要求で指定されたセッション ID が Secure Firewall Threat Defense デバイス 上のアクティブなセッションと一致しません。これは、ユーザーがすでに閉じたセッション上の認可変更をサーバーが発行しようとした結果である可能性があります。

- *action-type*：要求された認可変更アクション（update または disconnect）
- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109103

エラーメッセージ `%Threat Defense-3-109103: CoA action-type from coa-source-ip failed for user username , with session ID: audit-session-id .`

説明 Secure Firewall Threat Defense デバイス は正しくフォーマットされた認可変更要求を受信しましたが、正常に処理できませんでした。

- *action-type*：要求された認可変更アクション（update または disconnect）
- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 関連する VPN サブシステムのログを調査し、更新された属性を提供できなかった理由、またはセッションを終了できなかった理由を判断します。

109104

エラーメッセージ `%Threat Defense-3-109104: CoA action-type from coa-source-ip failed for user username , session ID: audit-session-id . Action not supported.`

説明 Secure Firewall Threat Defense デバイス は認可変更を正しい形式で受け取りましたが、指定されたアクションが Secure Firewall Threat Defense デバイス でサポートされていないために処理しませんでした。

- *action-type*：要求された認可変更アクション（update または disconnect）
- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109105

エラーメッセージ `%FTD-3-109105: Failed to determine the egress interface for locally generated traffic destined to <protocol> <IP>:<port>.`

説明 インターフェイスが BVI であれば、ルートが存在しない場合、Secure Firewall Threat Defense デバイス は syslog をログに記録する必要があります。デフォルト ルートが存在し、正しいインターフェイスにパケットをルーティングしない場合は追跡できなくなります。 Secure Firewall Threat Defense の場合は、データインターフェイスの次にまず管理ルートが検索されます。このためデフォルトルートが異なる宛先にパケットをルーティングする場合は、追跡が難しくなります。

推奨アクション 正しい宛先のデフォルト ルートを追加するか、スタティック ルートを追加することを強くお勧めします。

109201

エラーメッセージ `%FTD-5-109201: UAUTH Session session, User username, Assigned IP IP Address, Succeeded adding entry.`

説明 VPN ユーザーが正常に追加されると、このメッセージが生成されます。

推奨アクションなし。

109202

エラーメッセージ `%Threat Defense-6-109202: UAUTH Session session, User username, Assigned IP IP Address, Succeeded incrementing entry use.`

説明 VPN ユーザーアカウントはすでに存在し、参照カウントは正常に増分されました。

推奨アクションなし。

109203

エラーメッセージ `%Threat Defense-3-109203: UAUTH Session session, User username, Assigned IP IP Address, Failed adding entry.`

説明 このメッセージは、デバイスが新しく作成されたユーザーエントリに ACL ルールを適用できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109204

エラーメッセージ `%Threat Defense-5-109204: UAUTH Session session, User username, Assigned IP IP Address, Succeeded applying filter.`

説明 このメッセージは、デバイスが新しく作成されたユーザーエントリに ACL ルールを適用できなかった場合に生成されます。

推奨アクションなし。

109205

エラーメッセージ `%Threat Defense-3-109205: UAUTH Session session, User username, Assigned IP IP Address, Failed applying filter.`

説明 このメッセージは、ユーザーエントリがすでに存在し、インターフェイス上のセッションに新しいルールを適用できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109206

エラーメッセージ %Threat Defense-3-109206: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Removing stale entry added *hours* ago.

説明 このメッセージは、デバイスがコリジョンのためにユーザーエントリの追加に失敗し、古いエントリを削除した場合に生成されます。

推奨アクション 再接続を試みます。

109207

エラーメッセージ %Threat Defense-5-109207: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded updating entry.

説明 このメッセージは、デバイスがインターフェイス上のユーザーのルールを正常に適用したときに生成されます。

推奨アクションなし。

109208

エラーメッセージ %Threat Defense-3-109208: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating entry - no entry.

説明 このメッセージは、デバイスがユーザーエントリを新しいルールで更新できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109209

エラーメッセージ %Threat Defense-3-109209: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating filter for entry.

説明 このメッセージは、デバイスがコリジョンのためにユーザーエントリのルールを更新できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109210

エラーメッセージ %Threat Defense-5-109210: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.

説明 このメッセージは、トンネルの切断中にデバイスがユーザーのルールを正常に削除した場合に生成されます。

推奨アクションなし。

109211

エラーメッセージ `%Threat Defense-6-109211: UAUTH Session session, User username, Assigned IP IP Address, Successfully removed the rules for user during tunnel torn down.`

説明 このメッセージは、トンネルの削除後に参照カウントが正常に減少した場合に生成されます。

推奨アクションなし。

109212

エラーメッセージ `%Threat Defense-3-109212: UAUTH Session session, User username, Assigned IP IP Address, Failed removing entry.`

説明 このメッセージは、無効なアドレスまたは不正なエントリが原因でデバイスの削除に失敗した場合に生成されます。

推奨アクション 再度接続の切断を試みます。

109213

エラーメッセージ `%Threat Defense-3-109213: UAUTH Session session, User username, Assigned IP IP Address, Failed removing entry.`

説明 このメッセージは、ユーザーエントリのコリジョンが原因でデバイスの削除に失敗した場合に生成されます。

推奨アクション 再度接続の切断を試みます。

メッセージ 110002 ～ 113045

この項では、110002 ～ 113045 のメッセージについて説明します。

110002

エラーメッセージ `%Threat Defense-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port`

説明パケットの送信に使用するインターフェイスを Secure Firewall Threat Defense デバイス が検出しようとしたときに、エラーが発生しました。

- *protocol*：パケットのプロトコル
- *src interface*：パケットの送信元インターフェイス
- *src IP*：パケットの送信元 IP アドレス
- *src port*：送信元ポート番号
- *dest IP*：パケットの宛先 IP アドレス
- *dest port*：宛先ポート番号

推奨アクション エラー メッセージ、設定、およびエラーの原因となったイベントの詳細をコピーし、Cisco TAC にお問い合わせください。

110003

エラーメッセージ `%Threat Defense-6-110003: Routing failed to locate next-hop for protocol from src interface :src IP/src port to dest interface :dest IP/dest port`

説明インターフェイス ルーティング テーブル上のネクスト ホップを Secure Firewall Threat Defense デバイス が検出しようとしたときに、エラーが発生しました。

- *protocol*：パケットのプロトコル
- *src interface*：パケットの送信元インターフェイス
- *src IP*：パケットの送信元 IP アドレス
- *src port*：送信元ポート番号
- *dest IP*：パケットの宛先 IP アドレス
- *dest port*：宛先ポート番号

推奨アクション エラー メッセージ、設定、およびエラーの原因となったイベントの詳細をコピーし、Cisco TAC にお問い合わせください。デバッグ時にルーティング テーブルの詳細を表示するには、**show asp table routing** コマンドを使用します。

110004

エラーメッセージ `%Threat Defense-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone /parent_outside_ifc :outside_addr /outside_port (mapped_addr /mapped_port) to inside_zone /parent_inside_ifc :inside_addr /inside_port (mapped_addr /mapped_port)`

説明出力インターフェイスでフローが変更されました。

推奨アクション 不要。

111001

エラーメッセージ `%Threat Defense-5-111001: Begin configuration: IP_address writing to device`

説明コンフィギュレーションをデバイス（フロッピーディスク、フラッシュ メモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末のいずれか）に格納する **write** コマンドを入力しました。**IP_address** は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111002

エラーメッセージ `%Threat Defense-5-111002: Begin configuration: IP_address reading from device`

説明コンフィギュレーションをデバイス（フロッピーディスク、フラッシュ メモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末のいずれか）から読み取る **read** コマンドを入力しました。**IP_address** は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111003

エラーメッセージ `%Threat Defense-5-111003: IP_address Erase configuration`

説明コンソールで **write erase** コマンドを入力してフラッシュ メモリの内容を消去しました。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクションコンフィギュレーションを消去した後、Secure Firewall Threat Defense デバイスを再設定して新しいコンフィギュレーションを保存します。または、フロッピーディスクまたはネットワークの他の場所にある TFTP サーバーに以前保存してあるコンフィギュレーションから情報を復元できます。

111004

エラーメッセージ `%Threat Defense-5-111004: IP_address end configuration: {FAILED|OK}`

説明 config floppy/memory/ network コマンドまたは **write floppy/memory/network/standby** コマンドを入力しました。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクションメッセージが OK で終われば不要です。このメッセージでエラーが表示された場合は、問題を解決します。たとえば、フロッピーディスクに書き込む場合は、フロッピーディスクが書き込み禁止になっていないことを確認します。TFTP サーバーに書き込む場合は、サーバーが動作していることを確認します。

111005

エラーメッセージ `%Threat Defense-5-111005: IP_address end configuration: OK`

説明コンフィギュレーション モードを終了しました。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111007

エラーメッセージ `%Threat Defense-5-111007: Begin configuration: IP_address reading from device.`

説明 **reload** コマンドまたは **configure** コマンドを入力してコンフィギュレーションを読み込みました。deviceテキストは、フロッピーディスク、メモリ、ネット、スタンバイ、または端末になります。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111008

エラーメッセージ `%Threat Defense-5-111008: User user executed the command string`

説明ユーザーが **show** コマンド以外の任意のコマンドを入力しました。

推奨アクション 不要。

111009

エラーメッセージ `%Threat Defense-7-111009:User user executed cmd:string`

説明ユーザーにより、コンフィギュレーションが変更されないコマンドが入力されました。このメッセージは、**show** コマンドに限り表示されます。

推奨アクション 不要。

111010

エラーメッセージ `%Threat Defense-5-111010: User username , running application-name from IP ip addr , executed cmd`

説明ユーザーが設定変更を行いました。

- *username*：設定変更を行ったユーザー
- *application-name*：ユーザーが実行しているアプリケーション
- *ip addr*：管理ステーションの IP アドレス
- *cmd*：ユーザーが実行したコマンド

推奨アクション 不要。

111111

エラーメッセージ `% Threat Defense-1-111111 error_message`

説明システム エラーまたはインフラストラクチャ エラーが発生しました。

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

112001

エラーメッセージ `%Threat Defense-2-112001: (string :dec ) Clear complete.`

説明モジュール コンフィギュレーションを消去する要求が完了しました。ソース ファイルおよび行番号が特定されます。

推奨アクション 不要。

113001

エラーメッセージ `%Threat Defense-3-113001: Unable to open AAA session. Session limit [limit ] reached.`

説明 AAA リソースが使用できないために、IPSec トンネルまたは WebVPN 接続で AAA 動作を実行できません。**limit** 値は、同時 AAA トランザクションの最大数を示します。

推奨アクション 可能であれば、AAA リソースの要求を減らします。

113003

エラーメッセージ `%Threat Defense-6-113003: AAA group policy for user user is being set to policy_name .`

説明トンネル グループに関連付けられているグループ ポリシーが、ユーザー固有のポリシー *policy_name* で上書きされます。*policy_name* は、LOCAL 認証の設定時に **username** コマンドを使用して指定されており、RADIUS 認証の設定時に RADIUS CLASS 属性で返されます。

推奨アクション 不要。

113004

エラーメッセージ `%Threat Defense-6-113004: AAA user aaa_type Successful: server = server_IP_address , User = user`

説明 IPSec または WebVPN 接続に対する AAA 操作が正常に完了しました。AAA タイプは、認証、許可、またはアカウンティングです。**server_IP_address** は、関連する AAA サーバーの IP アドレスです。**user** は、接続に関連付けられているユーザー名です。

推奨アクション 不要。

113005

エラーメッセージ `%Threat Defense-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr : user = *****: user IP = ip_addr`

説明接続で AAA 認証に失敗しました。ユーザー名は無効な場合や不明な場合は表示されませんが、有効な場合または **no logging hide username** コマンドが設定されている場合は表示されます。

推奨アクション 認証を再試行してください。

113005

エラーメッセージ `%Threat Defense-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr : user = *****: user IP = ip_addr`

説明接続で AAA 認証に失敗しました。ユーザー名は無効な場合や不明な場合は表示されませんが、有効な場合または **no logging hide username** コマンドが設定されている場合は表示されます。

推奨アクション 認証を再試行してください。

113006

エラーメッセージ `%Threat Defense-6-113006: User user locked out on exceeding number successive failed authentication attempts`

説明ローカルに設定されているユーザーがロックアウトされています。このメッセージは、このユーザーについて認証失敗が連続して設定回数だけ発生したときに現れ、今後このユーザーが認証を受けようとしても、管理者が **clear aaa local user lockout** コマンドを使用してユーザーをアンロックするまでは、すべて拒否されることを示します。**user** は現在ロックされているユーザーであり、**number** は **aaa local authentication attempts max-fail** コマンドを使用して設定されている連続失敗しきい値です。

推奨アクション clear_aaa_local_user_lockout コマンドを使用してユーザーをアンロックするか、許容される連続認証失敗の最大数を調整します。

113007

エラーメッセージ `%Threat Defense-6-113007: User user unlocked by administrator`

説明ローカルに設定されたユーザーが、**aaa local authentication attempts max-fail** コマンドを使用して設定された連続認証失敗の最大数を超えたためロックアウトされた後、表示されている管理者によってアンロックされました。

推奨アクション 不要。

113008

エラーメッセージ `%Threat Defense-6-113008: AAA transaction status ACCEPT: user = user`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが正常に完了しました。user は、接続に関連付けられているユーザー名です。

推奨アクション 不要。

113009

エラーメッセージ `%Threat Defense-6-113009: AAA retrieved default group policy policy for user user`

説明 IPSec 接続または WebVPN 接続の認証または認可が行われました。**tunnel-group** コマンドまたは **webvpn** コマンドで指定されたグループ ポリシーの属性が取得されました。

推奨アクション 不要。

113010

エラーメッセージ `%Threat Defense-6-113010: AAA challenge received for user user from server server_IP_address`

説明 SecurID サーバーを使用した IPSec 接続の認証が行われました。ユーザーは、認証に先立って詳細情報を入力するよう求められます。

- **user**：接続に関連付けられているユーザー名
- **server _IP_address**：関連する AAA サーバーの IP アドレス

推奨アクション 不要。

113011

エラーメッセージ `%Threat Defense-6-113011: AAA retrieved user specific group policy policy for user user`

説明 IPSec 接続または WebVPN 接続の認証または認可が行われました。**tunnel-group** コマンドまたは **webvpn** コマンドで指定されたグループ ポリシーの属性が取得されました。

推奨アクション 不要。

113012

エラーメッセージ `%Threat Defense-6-113012: AAA user authentication Successful: local database: user = user`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーが、ローカル ユーザー データベースに正常に認証されました。

- **user**：接続に関連付けられているユーザー名

推奨アクション 不要。

113013

エラーメッセージ `%Threat Defense-6-113013: AAA unable to complete the request Error: reason = reason : user = user`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。

- **reason**：理由の詳細
- **user**：接続に関連付けられているユーザー名

推奨アクション 不要。

113014

エラーメッセージ `%Threat Defense-6-113014: AAA authentication server not accessible: server = server_IP_address : user = user`

説明デバイスが、IPSec 接続または WebVPN 接続に関連付けられている AAA トランザクション中に設定済み AAA サーバーと通信できませんでした。このため、ユーザーが接続しようとしたとき、**aaa-server** グループに設定されているバックアップ サーバーおよびそのサーバーのアベイラビリティ次第で、接続に失敗する場合も、失敗しない場合もあります。ユーザー名は無効な場合や不明な場合は表示されませんが、有効な場合または **no logging hide username** コマンドが設定されている場合は表示されます。

推奨アクション 設定済みの AAA サーバーとの接続を確認します。

113015

エラーメッセージ `%Threat Defense-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user: user IP = xxx.xxx.xxx.xxx`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーのローカル ユーザー データベースへの認証要求が拒否されました。ユーザー名は無効な場合や不明な場合は表示されませんが、有効な場合または **no logging hide username** コマンドが設定されている場合は表示されます。

- **reason**：要求が拒否された理由の詳細
- **user**：接続に関連付けられているユーザー名
- **user_ip**：認証または認証要求を開始したユーザーの IP アドレス<915CLI>

推奨アクション 不要。

113016

エラーメッセージ `%Threat Defense-6-113016: AAA credentials rejected: reason = reason : server = server_IP_address : user = user<915CLI>: user IP = xxx.xxx.xxx.xxx`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。ユーザー名は無効な場合や不明な場合は表示されませんが、有効な場合または **no logging hide username** コマンドが設定されている場合は表示されます。

- **reason**：要求が拒否された理由の詳細

- **server_IP_address**：関連する AAA サーバーの IP アドレス
- **user**：接続に関連付けられているユーザー名
- *<915CLI>user_ip*：認証または認証要求を開始したユーザーの IP アドレス

推奨アクション 不要。

113017

エラーメッセージ `%Threat Defense-6-113017: AAA credentials rejected: reason = reason : local database: user = user: user IP = xxx.xxx.xxx.xxx`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。このイベントが表示されるのは、AAA トランザクションが外部 AAA サーバーではなくローカル ユーザー データベースと行われる場合だけです。

- **reason**：要求が拒否された理由の詳細
- **user**：接続に関連付けられているユーザー名
- **user_ip**：認証または認証要求を開始したユーザーの IP アドレス

推奨アクション 不要。

113018

エラーメッセージ `%Threat Defense-3-113018: User: user , Unsupported downloaded ACL Entry: ACL_entry , Action: action`

説明サポートされていないフォーマットの ACL エントリが認証サーバーからダウンロードされました。メッセージの値は次のとおりです。

- **user**：ログインを試行しているユーザー
- **ACL_entry**：認証サーバーからダウンロードされたサポートされていない ACL エントリ
- **action**：サポートされていない ACL エントリに対して実行するアクション

推奨アクション 認証サーバーの ACL エントリは、サポートされている ACL エントリ フォーマットに適合するように管理者が変更する必要があります。

113019

エラーメッセージ `%Threat Defense-4-113019: Group = group , Username = username , IP = peer_address , Session disconnected. Session Type: type , Duration: duration , Bytes xmt: count , Bytes rcv: count , Reason: reason`

説明最大アイドル ユーザーが切断されたタイミングとその理由を示します。

- **group**：グループ名
- **username**：ユーザー名
- **IP**：ピア アドレス
- **Session Type**：セッション タイプ（たとえば IPSec または UDP）

- **duration**：接続期間（時間、分、および秒）
- **Bytes xmt**：送信されたバイト数
- *Bytes rcv*：受信されたバイト数
- **reason**：切断原因

ユーザーから要求された

搬送が失われた

サービスが失われた

アイドル タイムアウト

最大時間を超過した

管理者がリセットした

管理者がリブートした

管理者がシャットダウンした

ポート エラー

NAS エラー

NAS 要求

NAS リブート

ポートの不要化

接続が切り替えられた。同一ユーザーによる同時ログイン許容数を超えたことを示します。この問題を解決するには、同時ログイン数を増やすか、ユーザーに対して特定のユーザー名とパスワードで 1 回だけログインを許可するようにします。

ポートが中断された

使用できないサービス

コールバック

ユーザー エラー

ホストが要求した

SA が期限切れ

IKE の削除

帯域幅の管理エラー

証明書が期限切れ

フェーズ 2 の不一致

ファイアウォールの不一致

ピア アドレスの変更

ACL 解析エラー

フェーズ 2 エラー

設定エラー

ピアの再接続

内部エラー

クリプト マップ ポリシーが見つからない

L2TP 開始

VLAN マッピング エラー

NAC ポリシー エラー

ダイナミック アクセス ポリシーの終了

サポートされていないクライアント タイプ

不明

推奨アクション理由に問題が示されていない限り、処置は不要です。

113020

エラーメッセージ `%Threat Defense-3-113020: Kerberos error: Clock skew with server` *`ip_address`* `greater than 300 seconds`

説明 Kerberos サーバー経由の IPSec または WebVPN のユーザーの認証が、Secure Firewall Threat Defense デバイス のクロックとそのサーバーのクロックが 5 分（300 秒）以上ずれているために失敗しました。この失敗が起こったときは、接続しようとしても拒否されます。

- *ip_address*：Kerberos サーバーの IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス サーバーと Kerberos サーバーのクロックを同期させます。

113021

エラーメッセージ `%Threat Defense-3-113021 : Attempted console login failed. User` *`username`* `did NOT have appropriate Admin Rights.`

説明ユーザーが管理コンソールにアクセスしようとしましたが、拒否されました。

- *username*：ユーザーが入力したユーザー名

推奨アクション 新しく追加された admin 権限ユーザーの場合は、そのユーザーのサービス タイプ（LOCAL または RADIUS 認証サーバー）が次のようなアクセスを許可するように設定されていることを確認します。

- nas-prompt：コンソールへのログインおよび要求されたレベルの EXEC 特権を許可しますが、イネーブル（コンフィギュレーション修正）アクセスは許可しません。
- admin：すべてのアクセスを許可します。コマンド特権によって制約できます。

上記以外のユーザーの場合は、そのユーザーが管理コンソールへの不適切なアクセスを試みています。実行されるアクションは、このような問題に関する社内のポリシーに適合している必要があります。

113022

エラーメッセージ `%Threat Defense-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED`

説明 Secure Firewall Threat Defense デバイス が AAA サーバーに認証、許可、またはアカウンティングの要求を試みましたが、設定されているタイムアウト期間内に応答を受信しませんでした。この AAA サーバーには失敗のマークが付けられます。この AAA サーバーは、サービスから削除されました。

- *protocol*：次のいずれかのタイプの認証プロトコル

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr*：AAA サーバーの IP アドレス
- *tag*：サーバー グループ名

推奨アクション AAA サーバーがオンラインで、Secure Firewall Threat Defense デバイス からアクセスできることを確認します。

113023

エラーメッセージ `%Threat Defense-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE`

説明以前失敗のマークを付けられた AAA サーバーが、Secure Firewall Threat Defense デバイスによって再びアクティブにされました。AAA 要求の処理に、この AAA サーバーを使用できるようになりました。

- *protocol*：次のいずれかのタイプの認証プロトコル

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr*：AAA サーバーの IP アドレス
- *tag*：サーバー グループ名

推奨アクション 不要。

113024

エラーメッセージ `%Threat Defense-5-113024: Group tg : Authenticating type connection from ip with username, user_name , from client certificate`

説明ユーザー名の事前入力機能によって、AAA 用にクライアント証明書から抽出されたユーザー名で元のユーザー名が上書きされました。

- *tg*：トンネル グループ
- *type*：接続のタイプ（SSL クライアントまたはクライアントレス）
- *ip*：接続しているユーザーの IP アドレス
- *user_name*：AAA 用にクライアント証明書から抽出された名前

推奨アクション 不要。

113025

エラーメッセージ `%Threat Defense-5-113025: Group tg : fields  Could not authenticate connection type connection from ip`

説明証明書からユーザー名を正常に抽出できませんでした。

- *tg*：トンネル グループ
- *fields*：検索対象の DN フィールド
- *connection type*：接続のタイプ（SSL クライアントまたはクライアントレス）
- *ip*：接続しているユーザーの IP アドレス

推奨アクション 管理者は、**authentication aaa certificate**、**ssl certificate-authentication**、および **authorization-dn-attributes** の各キーワードが正しく設定されていることを確認する必要があります。

113026

エラーメッセージ `%Threat Defense-4-113026: Error error while executing Lua script for group tunnel group`

説明 AAA 用にクライアント証明書からユーザー名を抽出中に、エラーが発生しました。このメッセージは、username-from-certificate use-script オプションが有効な場合にだけ生成されます。

- *error*：Lua 環境から返されたエラー文字列
- *tunnel group*：証明書からユーザー名を抽出しようとしたトンネル グループ

推奨アクション username-from-certificate use-script オプションで使用されているスクリプトにエラーがないかどうかを調べます。

113027

エラーメッセージ `%Threat Defense-2-113027: Error activating tunnel-group scripts`

説明スクリプト ファイルを正常にロードできません。username-from-certificate use-script オプションを使用するトンネル グループが正しく動作していません。

推奨アクション 管理者は、ASDM を使用して、スクリプト ファイルにエラーがないかどうかを確認する必要があります。**debug aaa** コマンドを使用して詳細なエラー メッセージを取得すると役立ちます。

113028

エラーメッセージ `%Threat Defense-7-113028: Extraction of username from VPN client certificate has` *`string`*`. [Request` *`num`* `]`

説明証明書のユーザー名の処理要求は、実行中であるか、終了しました。

- *num*：要求の ID（ファイバへのポインタの値）。単調に増加する番号です。
- *string*：次のいずれかのステータス メッセージ。
  - 「been requested（要求済み）」
  - 「started（開始）」
  - 「finished with error（エラーで終了）」
  - 「finished successfully（正常に終了）」
  - 「completed（完了）」

推奨アクション 不要。

113029

エラーメッセージ `%Threat Defense-4-113029: Group` *`group`* `User` *`user`* `IP` *`ipaddr`* `Session could not be established: session limit of` *`num`* `reached`

説明現在のセッション数が最大セッション ロードを超過しているため、ユーザー セッションを確立できません。

推奨アクション可能であれば、設定されている制限を増加し、ロード バランス クラスタを増やします。

113030

エラーメッセージ `%Threat Defense-4-113030: Group` *`group`* `User` *`user`* `IP` *`ipaddr`* `User ACL` *`acl`* `from AAA doesn't exist on the device, terminating connection.`

説明指定された ACL が Secure Firewall Threat Defense デバイス 上で見つかりませんでした。

- **group**：グループの名前
- **user**：ユーザーの名前

- **ipaddr**：IP アドレス
- **acl**：ACL 名

推奨アクション コンフィギュレーションを変更して、指定された ACL を追加するか、ACL の名前を修正します。

113031

エラーメッセージ `%Threat Defense-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.`

説明 適用される ACL のタイプが誤っています。**vpn-filter** コマンドによって、IPv6 ACL が IPv4 ACL として設定されています。

- *group*：ユーザーのグループ ポリシー名
- *user*：ユーザー名
- *ipaddr*：ユーザーのパブリック（割り当てられていない）IP アドレス
- *filter*：VPN フィルタの名前

推奨アクション Secure Firewall Threat Defense デバイス の VPN フィルタと IPv6 VPN フィルタの設定、および AAA（RADIUS）サーバーのフィルタ パラメータを検証します。正しいタイプの ACL が指定されていることを確認します。

113032

エラーメッセージ `%Threat Defense-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.`

説明 適用する ACL のタイプが誤っています。**ipv6-vpn-filter** コマンドによって、IPv4 ACL が IPv6 ACL として設定されています。

- *group*：ユーザーのグループ ポリシー名
- *user*：ユーザー名
- *ipaddr*：ユーザーのパブリック（割り当てられていない）IP アドレス
- *filter*：VPN フィルタの名前

推奨アクション Secure Firewall Threat Defense デバイス の VPN フィルタと IPv6 VPN フィルタの設定、および AAA（RADIUS）サーバーのフィルタ パラメータを検証します。正しいタイプの ACL が指定されていることを確認します。

113033

エラーメッセージ `%Threat Defense-6-113033: Group group User user IP ipaddr AnyConnect session not allowed. ACL parse error.`

説明 関連する ACL が解析していないため、このグループ内の指定されたユーザーの WebVPN セッションが許可されません。このエラーが修正されるまで、ユーザーが WebVPN を介してログインすることは許可されません。

- *group*：ユーザーのグループ ポリシー名
- *user*：ユーザー名
- *ipaddr*：ユーザーのパブリック（割り当てられていない）IP アドレス

推奨アクション WebVPN ACL を修正します。

113034

エラーメッセージ `%Threat Defense-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.`

説明 Cisco AV-PAIR ACL が使用されたため、指摘された ACL が使用されませんでした。

- **group**：グループの名前
- **user**：ユーザーの名前
- **ipaddr**：IP アドレス
- **acl**：ACL 名

推奨アクション 使用する適切な ACL を決定し、設定を修正します。

113035

エラーメッセージ `%Threat Defense-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.`

説明ユーザーがAnyConnectクライアントを使用してログインしました。SVCサービスがグローバルにイネーブルになっていないか、またはSVCイメージが無効か破損しています。セッション接続が終了されました。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *iaddrp*：接続を試行しているユーザーの IP アドレス

推奨アクション **svc-enable** コマンドを使用して、SVC をグローバルにイネーブルにします。**svc image** コマンドを使用して新しいイメージをリロードすることで、SVC イメージの整合性とバージョンを検証します。

113036

エラーメッセージ `%Threat Defense-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.`

説明指摘されたパラメータの値が不良です。値は非常に長い可能性があるため、表示されません。

- **group**：グループの名前
- **user**：ユーザーの名前
- **ipadddr**：IP アドレス
- **name**：パラメータの名前

推奨アクション 設定を変更し、指定したパラメータを修正します。

113037

エラーメッセージ `%Threat Defense-6-113037: Reboot pending, new sessions disabled. Denied user login.`

説明Secure Firewall Threat Defense デバイス がリブート処理中のため、ユーザーが WebVPN にログインできません。

推奨アクション 不要。

113038

エラーメッセージ `%Threat Defense-4-113038: Group group User user IP ipaddr Unable to create AnyConnect parent session.`

説明リソースの問題のため、指定されたグループ内のユーザーに対して AnyConnect セッションが作成されませんでした。たとえば、ユーザーが最大ログイン制限に達した可能性があります。

- **group**：グループの名前
- **user**：ユーザーの名前
- **ipadddr**：IP アドレス

推奨アクション 不要。

113039

エラーメッセージ `%Threat Defense-6-113039: Group group User user IP ipaddr AnyConnect parent session started.`

説明指摘された IP アドレスにおける このグループ内のユーザーに対して AnyConnect セッションが開始されました。ユーザーが AnyConnect ログイン ページを介してログインすると、AnyConnect セッションが開始されます。

- **group**：グループの名前
- **user**：ユーザーの名前
- **ipadddr**：IP アドレス

推奨アクション 不要。

113040

エラーメッセージ `%Threat Defense-4-113040: Terminating the VPN connection attempt from attempted group . Reason: This connection is group locked to locked group.`

説明 接続が試行されるトンネル グループは、グループ ロックに設定されているトンネル グループと同じではありません。

- *attempted group*：接続が着信するトンネル グループ
- *locked group*：接続がロックまたは制限されているトンネル グループ

推奨アクション グループ ポリシーまたはユーザー属性のグループロック値を確認します。

113041

エラーメッセージ `%Threat Defense-4-113041: Redirect ACL configured for assigned IP does not exist on the device.`

説明 リダイレクト URL がインストールされ、ACL が ISE から受信されたが、リダイレクト ACL が Secure Firewall Threat Defense デバイス に存在しない場合にエラーが発生しました。

- *assigned-ip*：クライアントに割り当てられる IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス にリダイレクト ACL を設定します。

113042

エラーメッセージ `%Threat Defense-4-113042: CoA: Non-HTTP connection from src_if :src_ip /src_port to dest_if :dest_ip /dest_port for user username at client_IP denied by redirect filter; only HTTP connections are supported for redirection.`

説明 CoA 機能の場合、リダイレクト ACL フィルタは、リダイレクト処理中に一致する非 HTTP トラフィックをドロップし、終了したトラフィック フローに関する情報を提供します。

- *src_if*、*src_ip*、*src_port*：フローの送信元インターフェイス、IP アドレス、ポート
- *dest_if*、*dest_ip*、*dest_port*：フローの宛先インターフェイス、IP アドレス、ポート
- *username*：ユーザーの名前
- *client_IP*：クライアントの IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス のリダイレクト ACL の設定を検証します。リダイレクトするトラフィックに正しく一致し、通過を許可するフローが間違ってブロックされることがないように適正なフィルタを使用してください。

メッセージ 114001 ～ 199027

この項では、114001 から 199027 までのメッセージについて説明します。

114001

エラーメッセージ `%Threat Defense-1-114001: Failed to initialize 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードを初期化できませんでした。

- *syslog_id*：メッセージ識別子

- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114002

エラーメッセージ `%Threat Defense-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードの SFP コネクタを初期化できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。

3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114003

エラーメッセージ `%Threat Defense-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードにキャッシュされたコマンドを実行できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114004

エラーメッセージ `%Threat Defense-6-114004: 4GE SSM I/O Initialization start.`

説明 4GE SSM I/O の初期化が開始されていることがユーザーに通知されました。

- >*syslog_id*：メッセージ識別子

推奨アクション 不要。

114005

エラーメッセージ `%Threat Defense-6-114005: 4GE SSM I/O Initialization end.`

説明 4GE SSM I/O の初期化が終了したことがユーザーに通知されました。

- >*syslog_id*：メッセージ識別子

推奨アクション 不要。

114006

エラーメッセージ `%Threat Defense-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのポート統計情報を取得できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114007

エラーメッセージ `%Threat Defense-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの現在のモジュール ステータス レジスタ情報を取得できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114008

エラーメッセージ `%Threat Defense-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのために、Up 状態へのリンク移行が 4GE SSM I/O カードで検出された後に Secure Firewall Threat Defense デバイスがポートをイネーブルにできませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114009

エラーメッセージ `%Threat Defense-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト アドレスを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114010

エラーメッセージ `%Threat Defense-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト ハードウェア アドレスを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR
- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114011

エラーメッセージ `%Threat Defense-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト アドレスを削除できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114012

エラーメッセージ `%Threat Defense-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト ハードウェア アドレスを削除できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114013

エラーメッセージ `%Threat Defense-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの MAC アドレス テーブルを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114014

エラーメッセージ `%Threat Defense-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの MAC アドレスを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114015

エラーメッセージ `%Threat Defense-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの個々のモードまたは無差別モードを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114016

エラーメッセージ `%Threat Defense-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト モードを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114017

エラーメッセージ `%Threat Defense-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string ).`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのために Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードのリンク ステータスを取得できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション：次のステップを実行します。

1. システム管理者に通知します。
2. イベントに関連付けられているメッセージとエラーを記録して確認します。
3. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
4. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
5. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114018

エラーメッセージ `%Threat Defense-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのポート速度を設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114019

エラーメッセージ `%Threat Defense-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのメディア タイプを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114020

エラーメッセージ `%Threat Defense-3-114020: Port link speed is unknown in 4GE SSM I/O card.`

説明 Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードのポート リンク速度を検出できません。

推奨アクション：次のステップを実行します。

1. イベントに関連付けられているメッセージを記録して確認します。
2. 4GE SSM I/O カードをリセットし、ソフトウェアがイベントから自動的に回復するかどうかを観察します。
3. ソフトウェアが自動的に回復しない場合は、デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114021

エラーメッセージ `%Threat Defense-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to` *`error`* `.`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのために Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードのマルチキャスト アドレス テーブルを設定できませんでした。

- **error**：スイッチ アクセス エラー（10 進数のエラー コード）または I2C シリアル バス エラー。考えられる I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション：次のステップを実行します。

1. イベントに関連付けられているメッセージを記録して確認します。
2. Secure Firewall Threat Defense デバイスのリブートを試みます。
3. ソフトウェアが自動的に回復しない場合は、デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114022

エラーメッセージ `%Threat Defense-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string`

説明スイッチ アクセス エラーが原因で Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードでブロードキャスト トラフィックを渡すことができませんでした。

- *error_string*：10 進エラー コードであるスイッチ アクセス エラー

推奨アクション：次のステップを実行します。

1. イベントが含まれているメッセージとエラーを記録します。
2. ssm4ge_dump ファイルをコンパクト フラッシュから取得し、Cisco TAC に送信します。
3. 手順 1 および 2 で収集した情報を Cisco TAC に連絡します。

（注） 4GE SSM が自動的にリセットされ回復します。

114023

エラーメッセージ `%Threat Defense-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to error_string .`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーが原因で、4GE SSM I/O カードで MAC テーブルをキャッシュまたはフラッシュできませんでした。このメッセージが表示されるのは稀です。

- **error_string**：I2C シリアル バス エラー（可能な値については、2 番めの項目を参照）またはスイッチ アクセス エラー（10 進エラー コード）。
- I2C シリアル バス エラーは次のとおりです。

I2C_BUS_TRANSACTION_ERROR

I2C_CHKSUM_ERROR

I2C_TIMEOUT_ERROR

I2C_BUS_COLLISION_ERROR

I2C_HOST_BUSY_ERROR

I2C_UNPOPULATED_ERROR

I2C_SMBUS_UNSUPPORT

I2C_BYTE_COUNT_ERROR

I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントが含まれている syslog メッセージとエラーを記録します。
2. Secure Firewall Threat Defense デバイス のソフトウェア リブートを試みます。
3. Secure Firewall Threat Defense デバイス の電源を一度切ってから再投入します。

（注） 電源を切った後、必ず数秒待ってから電源を入れます。手順 1 ～ 3 を完了した後、問題が解決しない場合は、Cisco TAC に連絡して、手順 1 の情報を提供します。Secure Firewall Threat Defense デバイス の RMA が必要になる場合があります。

115000

エラーメッセージ `%Threat Defense-2-115000: Critical assertion in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

説明重要なアサーションが失敗しました。このメッセージは、チェック ビルドでの開発時にだけ使用され、実稼働ビルドでは使用されません。

- **process name**：プロセスの名前
- *fiber name*：ファイバの名前
- *component name*：指定したコンポーネントの名前
- *subcomponent name*：指定したサブコンポーネントの名前
- *filename*：指定したファイルの名前
- *line number*：指定した行の行番号
- *condition*：指摘された状態

推奨アクション優先度の高い障害を記録として残し、アサーションの原因を調査し、問題を修正する必要があります。

115001

エラーメッセージ `%Threat Defense-3-115001: Error in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

説明エラー アサーションが失敗しました。このメッセージは、チェック ビルドでの開発時にだけ使用され、実稼働ビルドでは使用されません。

- **process name**：プロセスの名前
- *fiber name*：ファイバの名前
- *component name*：指定したコンポーネントの名前
- *subcomponent name*：指定したサブコンポーネントの名前
- *filename*：指定したファイルの名前
- *line number*：指定した行の行番号
- *condition*：指摘された状態

推奨アクション障害を記録として残し、アサーションの原因を調査し、問題を修正する必要があります。

115002

エラーメッセージ `%Threat Defense-4-115002: Warning in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

説明警告アサーションが失敗しました。このメッセージは、チェック ビルドでの開発時にだけ使用され、実稼働ビルドでは使用されません。

- **process name**：プロセスの名前
- *fiber name*：ファイバの名前
- *component name*：指定したコンポーネントの名前
- *subcomponent name*：指定したサブコンポーネントの名前
- *filename*：指定したファイルの名前
- *line number*：指定した行の行番号
- *condition*：指摘された状態

推奨アクションアサーションの原因を調査し、問題が見つかった場合は、障害を記録として残し、問題を修正する必要があります。

199001

エラーメッセージ `%Threat Defense-5-199001: Reload command executed from Telnet (remote IP_address ).`

説明 reload コマンドで Secure Firewall Threat Defense デバイス のリブートを開始するホストのアドレスが記録されました。

推奨アクション 不要。

199002

エラーメッセージ `%Threat Defense-6-199002: startup completed. Beginning operation.`

説明 Secure Firewall Threat Defense デバイス が、その初期ブートおよびフラッシュ メモリ読み取りシーケンスを完了し、正常動作を開始する準備が整いました。

（注） このメッセージは、no logging message コマンドを使用してもブロックできません。

推奨アクション 不要。

199003

エラーメッセージ `%Threat Defense-6-199003: Reducing link MTU dec .`

説明 Secure Firewall Threat Defense デバイス が、内部ネットワークよりも大きい MTU を使用している外部ネットワークからパケットを受信しました。その後Secure Firewall Threat Defense デバイスは、適切な MTU をネゴシエートするため、ICMP メッセージをその外部ホストに送信しました。ログ メッセージには、ICMP メッセージのシーケンス番号が含まれています。

推奨アクション 不要。

199005

エラーメッセージ `%Threat Defense-6-199005: Startup begin`

説明 Secure Firewall Threat Defense デバイス が開始されました。

推奨アクション 不要。

199010

エラーメッセージ `%Threat Defense-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0`

説明システムは重大なエラーから回復しました。

推奨アクション Cisco TAC にお問い合わせください。

199011

エラーメッセージ `%Threat Defense-2-199011: Close on bad channel in process/fiber process/fiber , channel ID p , channel state s process/fiber  name of the process/fiber that caused the bad channel close operation.`

説明予期しないチャネル クローズ状態が検出されました。

- **p**：チャネル ID
- *process/fiber*：不正なチャネル クローズ動作の原因となったプロセス/ファイバの名前
- **s**：チャネル状態

推奨アクション Cisco TAC にお問い合わせください。その際はログ ファイルを添付してください。

199012

エラーメッセージ `%FTD-1-1199012: Stack overflow during new_stack_call in process/fiber` *`process/fiber`* `, call target` *`f`* `, stack size` *`s`* `,` *`process/fiber`* `name of the process/fiber that caused the stack overflow`

説明 スタックオーバーフロー状態が検出されました。

- **f**：new_stack_call のターゲット
- *process/fiber*：スタックオーバーフローの原因となったプロセス/ファイバの名前
- **s**：new_stack_call で指定されている新しいスタック サイズ

推奨アクション Cisco TAC にお問い合わせください。その際はログファイルを添付してください。

199013

エラーメッセージ `%Threat Defense-1-199013:` *`syslog`*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：アラート syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199014

エラーメッセージ `%Threat Defense-2-199014:` *`syslog`*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：重大な syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199015

エラーメッセージ `%Threat Defense-3-199015:` *`syslog`*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：エラー syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199016

エラーメッセージ `%Threat Defense-4-199016:` *syslog*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：警告 syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199017

エラーメッセージ `%Threat Defense-5-199017: syslog`

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：通知 syslog が外部プロセスから verbatim を渡しました

推奨アクション 不要。

199018

エラーメッセージ `%Threat Defense-6-199018: syslog`

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：情報 syslog が外部プロセスから verbatim を渡しました

推奨アクション 不要。

199019

エラーメッセージ `%Threat Defense-7-199019: syslog`

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：デバッグ syslog が外部プロセスから verbatim を渡しました

推奨アクション 不要。

199020

エラーメッセージ `%Threat Defense-2-199020: System memory utilization has reached X %. System will reload if memory usage reaches the configured trigger level of Y %.`

説明システム メモリの使用率がシステム メモリのウォッチドッグ機能の設定値の 80% に達しました。

推奨アクション トラフィック負荷を軽減し、トラフィック インスペクションを削除し、ACL エントリの数を減らすなどして、システム メモリの使用率を減らしてください。メモリ リークが疑われる場合は、Cisco TAC にお問い合わせください。

199021

エラーメッセージ `%Threat Defense-1-199021: System memory utilization has reached the configured watchdog trigger level of Y %. System will now reload`

説明 システム メモリの使用率がシステム メモリのウォッチドッグ機能の設定値の 100% に達しました。システムは自動的にリロードされます。

推奨アクション トラフィック負荷を軽減し、トラフィック インスペクションを削除し、ACL エントリの数を減らすなどして、システム メモリの使用率を減らしてください。メモリ リークが疑われる場合は、Cisco TAC にお問い合わせください。

199021

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。