Syslog メッセージ 602101 ～ 622102

この章は、次の項で構成されています。

メッセージ 602101 ～ 609002

この項では、602101 から 609002 までのメッセージについて説明します。

602101

エラーメッセージ `%Threat Defense-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address , src_addr=source_address , prot=protocol`

説明 Secure Firewall Threat Defense デバイス が ICMP 宛先到達不能メッセージを送信し、フラグメンテーションが必要です。

推奨アクション データが正しく送信されることを確認します。

602103

エラーメッセージ `%FTD-6-602103: IPSEC: Received an ICMP Destination Unreachable from src_addr with suggested PMTU of rcvd_mtu; PMTU updated for SA with peer peer_addr, SPI spi, tunnel name username, old PMTU old_mtu, new PMTU new_mtu.`

説明 SA の MTU が変更されました。IPSec トンネル用のパケットを受信すると、対応する SA が特定され、ICMP パケットで推奨されている MTU に基づいて MTU がアップデートされます。推奨された MTU が 0 より大きく 256 未満の場合、新規 MTU は 256 に設定されます。推奨された MTU が 0 の場合、前の MTU から 256 を引いた値または 256 のどちらか大きい値に設定されます。推奨された MTU が 256 より大きい場合、新規 MTU は推奨された値に設定されます。

- src_addr：PMTU 送信側の IP アドレス
- rcvd_mtu：PMTU メッセージで受信した推奨 MTU

- peer_addr：IPSec ピアの IP アドレス
- spi：IPSec のセキュリティ パラメータ インデックス
- username：IPSec トンネルに関連付けられているユーザー名
- old_mtu：IPSec トンネルに関連付けられている前の MTU
- new_mtu：IPSec トンネルに関連付けられている新規 MTU

推奨アクション 不要。

602104

エラーメッセージ `%FTD-6-602104: IPSEC: Received an ICMP Destination Unreachable from src_addr , PMTU is unchanged because suggested PMTU of rcvd_mtu is equal to or greater than the current PMTU of curr_mtu , for SA with peer peer_addr , SPI spi , tunnel name username .`

説明 IPSec トンネル経由で送信されたパケットがパス MTU を超えたことを示す ICMP メッセージを受信し、推奨 MTU が現行 MTU 以上でした。MTU 値はすでに訂正されているので、MTU の調整は行われません。これは、さまざまな中間ステーションから複数の PMTU メッセージが受信され、現在の PMTU メッセージが処理される前に MTU が調整された場合に発生します。

- **src_addr**：PMTU 送信側の IP アドレス
- **rcvd_mtu**：PMTU メッセージで受信した推奨 MTU
- **curr_mtu**：IPSec トンネルに関連付けられている現行 MTU
- **peer_addr**：IPSec ピアの IP アドレス
- **spi**：IPSec のセキュリティ パラメータ インデックス
- *username*：IPSec トンネルに関連付けられているユーザー名

推奨アクション 不要。

602303

エラーメッセージ `%FTD-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi ) between local_IP and remote_IP (username ) has been created.`

説明 新しい SA が作成されました。

- direction：SA の方向（インバウンドまたはアウトバウンド）
- tunnel_type：SA のタイプ（リモート アクセスまたは L2L）
- spi：IPSec のセキュリティ パラメータ インデックス
- local_IP：トンネルのローカル エンドポイントの IP アドレス
- remote_IP：トンネルのリモート エンドポイントの IP アドレス
- >*username*：IPSec トンネルに関連付けられているユーザー名

推奨アクション 不要。

602304

エラーメッセージ %Threat Defense-6-602304: IPSEC: An *direction tunnel_type* SA (SPI=*spi*) between *local_IP* and *remote_IP* (*username*) has been deleted.

説明 SA が削除されました。

- direction：SA の方向（インバウンドまたはアウトバウンド）
- tunnel_type：SA のタイプ（リモート アクセスまたは L2L）
- spi：IPSec のセキュリティ パラメータ インデックス
- local_IP：トンネルのローカル エンドポイントの IP アドレス
- remote_IP：トンネルのリモート エンドポイントの IP アドレス
- >*username*：IPSec トンネルに関連付けられているユーザー名

推奨アクション 不要。

602305

エラーメッセージ %Threat Defense-3-602305: IPSEC: SA creation error, source *source address* , destination *destination address* , reason *error string*

説明 IPSec セキュリティ アソシエーションの作成中に、エラーが発生しました。

推奨アクション通常、これは一時的なエラー状態です。このメッセージが連続して発生する場合は、Cisco TAC にお問い合わせください。

602306

エラーメッセージ %Threat Defense-3-602306: IPSEC: SA change peer IP error, SPI: *IPsec SPI*, (src {*original src IP address* | *original src port*}, dest {*original dest IP address*| *original dest port*} => src {*new src IP address* | *new src port*}, dest: {*new dest IP address* | *new dest port*}), reason *failure reason*

説明モバイル IKE の IPsec トンネルのピア アドレスを更新中にエラーが発生し、ピア アドレスを変更できませんでした。

推奨アクション通常、これは一時的なエラー状態です。このメッセージが連続して発生する場合は、Cisco TAC にお問い合わせください。

604101

エラーメッセージ %Threat Defense-6-604101: DHCP client interface *interface_name* : Allocated ip = *IP_address* , mask = *netmask* , gw = *gateway_address*

説明 Secure Firewall Threat Defense DHCP クライアントが DHCP サーバーから IP アドレスを正常に取得しました。dhcpc コマンド文によって、Secure Firewall Threat Defense デバイス は、ネットワーク インターフェイスの IP アドレスおよびネットワーク マスクを DHCP サーバーから取得でき、またデフォルト ルートを取得できます。デフォルト ルート文では、ゲートウェイ アドレスがデフォルト ルータのアドレスとして使用されます。

推奨アクション 不要。

604102

エラーメッセージ `%Threat Defense-6-604102: DHCP client interface interface_name : address released`

説明 Secure Firewall Threat Defense DHCP クライアントが、割り当てられた IP アドレスを解放して DHCP サーバーに戻しました。

推奨アクション 不要。

604103

エラーメッセージ `%Threat Defense-6-604103: DHCP daemon interface interface_name : address granted MAC_address (IP_address )`

説明 Secure Firewall Threat Defense DHCP サーバーによって、IP アドレスが外部クライアントに付与されました。

推奨アクション 不要。

604104

エラーメッセージ `%Threat Defense-6-604104: DHCP daemon interface interface_name : address released build_number (IP_address )`

説明外部クライアントが、IP アドレスを解放して Secure Firewall Threat Defense DHCP サーバーに戻しました。

推奨アクション 不要。

604105

エラーメッセージ `%Threat Defense-4-604105: DHCPD: Unable to send DHCP reply to client hardware_address on interface interface_name . Reply exceeds options field size (options_field_size ) by number_of_octets octets.`

説明管理者は、DHCP クライアントに返す DHCP オプションを設定できます。DHCP クライアントが要求するオプションに応じて、オファーの DHCP オプションはメッセージの長さの制限を超える場合があります。DHCP オファーは、メッセージの制限内に収まらないため、送信できません。

- *hardware_address*：要求元クライアントのハードウェア アドレス
- *interface_name*：サーバー メッセージを送受信するインターフェイス
- *options_field_size*：オプション フィールドの最大長。デフォルトは 312 オクテットであり、終端のための 4 オクテットを含みます。
- *number_of_octets*：超過したオクテット数

推奨アクション 設定されている DHCP オプションのサイズまたは数を減らします。

604201

エラーメッセージ `%Threat Defense-6-604201: DHCPv6 PD client on interface <pd-client-iface> received delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

説明この syslog は、最初の 4 ウェイ交換の一部として、PD サーバーから委任されたプレフィックスを使用して DHCPv6 PD クライアントが受信されると表示されます。複数のプレフィックスの場合は、プレフィックスごとに syslog が表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *server-address*：DHCPv6 PD サーバー アドレス。
- *in-seconds*：委任されたプレフィックスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604202

エラーメッセージ `%Threat Defense-6-604202: DHCPv6 PD client on interface <pd-client-iface> releasing delegated prefix <prefix> received from DHCPv6 PD server <server-address>.`

説明この syslog は、無設定時に DHCPv6 PD クライアントが PD サーバーから受信した委任されたプレフィックスを解放している場合に表示されます。複数のプレフィックスの場合は、プレフィックスごとに syslog が表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *server-address*：DHCPv6 PD サーバー アドレス。

推奨アクション なし。

604203

エラーメッセージ `%Threat Defense-6-604203: DHCPv6 PD client on interface <pd-client-iface> renewed delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

説明この syslog は、DHCPv6 PD クライアントが以前に割り当てられた委任されたプレフィックスの更新を PD サーバーから開始し、成功した場合に表示されます。複数のプレフィックスの場合は、プレフィックスごとに syslog が表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *server-address*：DHCPv6 PD サーバー アドレス。
- *in-seconds*：委任されたプレフィックスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604204

エラーメッセージ `%Threat Defense-6-604204: DHCPv6 delegated prefix <delegated prefix> got expired on interface <pd-client-iface>, received from DHCPv6 PD server <server-address>.`

説明この syslog は、DHCPv6 PD クライアントが受信した委任されたプレフィックスが期限切れになっている場合に表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *delegated prefix*：DHCPv6 PD サーバーから受信した委任プレフィックス。

推奨アクション なし。

604205

エラーメッセージ `%Threat Defense-6-604205: DHCPv6 client on interface <client-iface> allocated address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds`

説明この syslog は、最初の 4 ウェイ交換の一部として DHCPv6 クライアント アドレスが DHCPv6 サーバーから受信され、有効な場合に表示されます。アドレスが複数の場合は、受け取ったアドレスごとに syslog が表示されます。

- *client-iface*：DHCPv6 クライアント アドレスがイネーブルになっているインターフェイス名。
- *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
- *server-address*：DHCPv6 サーバー アドレス。
- *in-seconds*：クライアントアドレスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604207

エラーメッセージ `%Threat Defense-6-604207: DHCPv6 client on interface <client-iface> renewed address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

説明この syslog は、DHCPv6 クライアントが DHCPv6 サーバーから以前に割り当てられたアドレスの更新を開始すると表示されます。アドレスが複数の場合は、更新したアドレスごとに syslog が表示されます。

- *client-iface*：DHCPv6 クライアント アドレスがイネーブルになっているインターフェイス名。
- *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
- *server-address*：DHCPv6 サーバー アドレス。

• *in-seconds*：クライアントアドレスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604206

エラーメッセージ `%Threat Defense-6-604206: DHCPv6 client on interface <client-iface> releasing address <ipv6-address> received from DHCPv6 server <server-address>.`

説明 DHCPv6 クライアントアドレスのコンフィギュレーションが実行されない場合、DHCPv6 クライアントは受信したクライアントアドレスを解放しています。アドレスが複数の場合は、アドレスごとに syslog が表示されます。

• *client-iface*：DHCPv6 クライアント アドレスが有効になっているインターフェイス名。
• *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
• *server-address*：DHCPv6 サーバー アドレス。

推奨アクション なし。

604208

エラーメッセージ `%Threat Defense-6-604208: DHCPv6 client address <ipv6-address> got expired on interface <client-iface>, received from DHCPv6 server <server-address>`

説明 この syslog は、DHCPv6 クライアントが受信したアドレスが期限切れになっている場合に表示されます。

• *client-iface*：DHCPv6 クライアント アドレスがイネーブルになっているインターフェイス名。
• *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
• *server-address*：DHCPv6 サーバー アドレス。

推奨アクション なし。

605004

エラーメッセージ `%Threat Defense-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username "`

説明 ユーザーがコンソールにログインしようとすると、次の形式のメッセージが表示されます。

```
Login denied from serial to console for user "username"
```

Secure Firewall Threat Defense デバイス への誤ったログインの試行、またはログインの失敗が発生しました。すべてのログインに対して、セッションあたり 3 回の試行が許容され、不正な試行が 3 回行われると、そのセッションは終了します。SSH ログインおよび Telnet ログインの場合、このメッセージは、3 回目の試行の失敗後、または 1 回以上の試行の失敗後に TCP セッションが終了したときに、生成されます。他のタイプの管理セッションの場合、このメッセージは試行に失敗するたびに生成されます。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。

- *source-address*：ログイン試行の送信元アドレス
- *source-port*：ログイン試行の送信元ポート
- *interface*：宛先管理インターフェイス
- *destination*：宛先 IP アドレス
- *service*：宛先サービス
- *username*：宛先管理インターフェイス

推奨アクション このメッセージの表示頻度が少ない場合、処置は不要です。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。ユーザーと通信して、ユーザー名とパスワードを確認します。

605005

エラーメッセージ `%Threat Defense-6-605005: Login permitted from source-address /source-port to interface:destination /service for user "username "`

ユーザーがコンソールにログインすると、次の形式のメッセージが表示されます。

```
Login permitted from serial to console for user "username"
```

説明 ユーザーは認証に成功し、管理セッションが開始されました。

- *source-address*：ログイン試行の送信元アドレス
- *source-port*：ログイン試行の送信元ポート
- *interface*：宛先管理インターフェイス
- *destination*：宛先 IP アドレス
- *service*：宛先サービス
- *username*：宛先管理インターフェイス

推奨アクション 不要。

607001

エラーメッセージ `%Threat Defense-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message`

説明 SIP メッセージの検査後、**fixup sip** コマンドによって SIP 接続が割り当て済みでした。**connection_type** は、次の文字列のいずれかです。

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route

- RTP
- RTCP

推奨アクション 不要。

608001

エラーメッセージ `%Threat Defense-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message`

接続 Skinny メッセージの検査後、**inspect skinny** コマンドによって Skinny 接続が割り当て済みでした。**connection_type** は、次の文字列のいずれかです。

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

推奨アクション 不要。

608002

エラーメッセージ `%Threat Defense-4-608002: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too small`

説明設定済みの最小長より短い SCCP プレフィックス長を持つ Skinny（SSCP）メッセージを受信しました。

- *in_ifc*：入力インターフェイス
- *src_ip*：パケットの送信元 IP アドレス
- *src_port*：パケットの送信元ポート
- *out_ifc*：出力インターフェイス
- *dest_ip*：パケットの宛先 IP アドレス
- *dest_port*：パケットの宛先ポート
- *value*：パケットの SCCP プレフィックス長

推奨アクション SCCP メッセージが有効である場合は、Skinny ポリシー マップをカスタマイズして、SSCP プレフィックスの最小長の値を大きくします。

608003

エラーメッセージ `%Threat Defense-4-608003: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too large`

説明設定済みの最大長より長い SCCP プレフィックス長を持つ Skinny（SSCP）メッセージを受信しました。

- *in_ifc*：入力インターフェイス
- *src_ip*：パケットの送信元 IP アドレス
- *src_port*：パケットの送信元ポート
- *out_ifc*：出力インターフェイス
- *dest_ip*：パケットの宛先 IP アドレス
- *dest_port*：パケットの宛先ポート
- *value*：パケットの SCCP プレフィックス長

推奨アクション SCCP メッセージが有効である場合は、Skinny ポリシー マップをカスタマイズして、SCCP プレフィックスの最大長の値を大きくします。

609001

エラーメッセージ `%Threat Defense-7-609001: Built local-host zone-name/* :ip-address`

説明ネットワーク状態コンテナは、ゾーン *zone-name* に接続されたホスト **ip-address** 用に予約済みでした。zone-name/* パラメータは、ホストが作成されているインターフェイスがゾーンの一部である場合に使用されます。ホストはいずれのインターフェイスにも属していないため、アスタリスクはすべてのインターフェイスを表します。

推奨アクション 不要。

609002

エラーメッセージ `%Threat Defense-7-609002: Teardown local-host zone-name/* :ip-address duration time`

説明ゾーン **zone-name** に接続されたホスト **ip-address** 用のネットワーク状態コンテナが削除されました。zone-name/* パラメータは、ホストが作成されているインターフェイスがゾーンの一部である場合に使用されます。ホストはいずれのインターフェイスにも属していないため、アスタリスクはすべてのインターフェイスを表します。

推奨アクション 不要。

メッセージ 610101 ～ 622102

この項では、610101 から 622102 までのメッセージについて説明します。

611101

エラーメッセージ `%Threat Defense-6-611101: User authentication succeeded: IP, IP address : Uname: user`

説明 Secure Firewall Threat Defense デバイス へのアクセス時にユーザー認証が成功しました。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。

- *IP address*：ユーザー認証に成功したクライアントの IP アドレス
- *user*：認証されたユーザー

推奨アクション 不要。

611102

エラーメッセージ `%Threat Defense-6-611102: User authentication failed: IP = IP address, Uname: user`

説明 Secure Firewall Threat Defense デバイス にアクセスしようとしたときに、ユーザー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。

- *IP address*：ユーザー認証に失敗したクライアントの IP アドレス
- *user*：認証されたユーザー

推奨アクション 不要。

611103

エラーメッセージ `%Threat Defense-5-611103: User logged out: Uname: user`

説明指定されたユーザーがログアウトしました。

推奨アクション 不要。

611104

エラーメッセージ `%Threat Defense-5-611104: Serial console idle timeout exceeded`

説明ユーザー アクティビティがなかったために、Secure Firewall Threat Defense のシリアル コンソールに設定されたアイドル タイムアウトを超えました。

推奨アクション 不要。

611301

エラーメッセージ `%Threat Defense-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address`

説明スプリット トンネリングなしでクライアント モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611302

エラーメッセージ `%Threat Defense-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling`

説明スプリット トンネリングなしでネットワーク拡張モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611303

エラーメッセージ `%Threat Defense-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask`

説明スプリット トンネリング付きでクライアント モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611304

エラーメッセージ `%Threat Defense-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask`

説明スプリット トンネリング付きでネットワーク拡張モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611305

エラーメッセージ `%Threat Defense-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address`

説明 DHCP 用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611306

エラーメッセージ `%Threat Defense-6-611306: VPNClient: Perfect Forward Secrecy Policy installed`

説明 VPN クライアント ダウンロード ポリシーの一部として、完全転送秘密が設定されました。

推奨アクション 不要。

611307

エラーメッセージ `%Threat Defense-6-611307: VPNClient: Head end: IP_address`

説明 VPN クライアントが、指摘されたヘッドエンドに接続されています。

推奨アクション 不要。

611308

エラーメッセージ `%Threat Defense-6-611308: VPNClient: Split DNS Policy installed: List of domains: string string`

説明 VPN クライアント ダウンロード ポリシーの一部として、スプリット DNS ポリシーがインストールされました。

推奨アクション 不要。

611309

エラーメッセージ `%Threat Defense-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address`

説明 VPN クライアントが、前にインストールされたポリシーを切断しアンインストールしています。

推奨アクション 不要。

611310

エラーメッセージ `%Threat Defense-6-611310: VNPClient: XAUTH Succeeded: Peer: IP_address`

説明 VPN クライアント Xauth が、指摘されたヘッドエンドで成功しました。

推奨アクション 不要。

611311

エラーメッセージ `%Threat Defense-6-611311: VNPClient: XAUTH Failed: Peer: IP_address`

説明 VPN クライアント Xauth が、指摘されたヘッドエンドで失敗しました。

推奨アクション 不要。

611312

エラーメッセージ `%Threat Defense-6-611312: VPNClient: Backup Server List: reason`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、Easy VPN サーバーがバックアップ サーバーのリストを Secure Firewall Threat Defense デバイス にダウンロードしました。このリストによって、ローカルで設定済みのバックアップ サーバーはすべて

上書きされます。ダウンロードされたリストが空の場合、Secure Firewall Threat Defense デバイスはバックアップ サーバーを使用しません。**reason** は、次のメッセージのどちらかです。

- A list of backup server IP addresses
- Received NULL list. Deleting current backup servers

推奨アクション 不要。

611313

エラーメッセージ `%Threat Defense-3-611313: VPNClient: Backup Server List Error: reason`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスであり、Easy VPN サーバーがバックアップ サーバーのリストを Secure Firewall Threat Defense デバイス にダウンロードする場合、リストに無効な IP アドレスまたはホスト名が含まれています。Secure Firewall Threat Defense デバイスは、DNS はサポートしません。したがって、**name** コマンドを使用して名前を IP アドレスに手動でマッピングしない限り、サーバーのホスト名はサポートされません。

推奨アクション Easy VPN サーバー上で、サーバーの IP アドレスが正しいことを確認して、ホスト名ではなく IP アドレスでサーバーを設定します。サーバーでホスト名を使用する必要がある場合は、Easy VPN リモート デバイスで **name** コマンドを使用して IP アドレスを名前にマッピングします。

611314

エラーメッセージ `%Threat Defense-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモートデバイスの場合、ロードバランシンググループのディレクタサーバーによって、Secure Firewall Threat Defense デバイス が特定のサーバーに接続するようにリダイレクトされました。

推奨アクション 不要。

611315

エラーメッセージ `%Threat Defense-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP_address`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、ロード バランシング クラスタ サーバーから切断しました。

推奨アクション 不要。

611316

エラーメッセージ `%Threat Defense-6-611316: VPNClient: Secure Unit Authentication Enabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって SUA がイネーブルにされました。

推奨アクション 不要。

611317

エラーメッセージ `%Threat Defense-6-611317: VPNClient: Secure Unit Authentication Disabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって SUA がディセーブルにされました。

推奨アクション 不要。

611318

エラーメッセージ `%Threat Defense-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって、ネットワーク内側の Secure Firewall Threat Defense デバイス上のユーザーに対して IUA がイネーブルにされました。

- **IP_address**：Secure Firewall Threat Defense デバイスから認証要求が送信されるサーバーの IP アドレス
- **port**：Secure Firewall Threat Defense デバイスから認証要求が送信されるサーバーのポート
- **time**：認証クレデンシャルのアイドル タイムアウト値

推奨アクション 不要。

611319

エラーメッセージ `%Threat Defense-6-611319: VPNClient: User Authentication Disabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって、ネットワーク内側の Secure Firewall Threat Defense 上のユーザーに対して IUA がディセーブルにされました。

推奨アクション 不要。

611320

エラーメッセージ `%Threat Defense-6-611320: VPNClient: Device Pass Thru Enabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによってデバイス パススルーがイネーブルにされました。デバイス パススルー機能によって、認証を実行できないデバイス（IP 電話など）は、IUA がイネーブルの場合、認証が免除されます。Easy VPN サーバーによってこの機能がイネーブルにされている

場合、Secure Firewall Threat Defense デバイス で **vpnclient mac-exempt** コマンドを使用して、認証（IUA）を免除するデバイスを指定できます。

推奨アクション 不要。

611321

エラーメッセージ `%Threat Defense-6-611321: VPNClient: Device Pass Thru Disabled`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによってデバイス パススルーがディセーブルにされました。

推奨アクション 不要。

611322

エラーメッセージ `%Threat Defense-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスであり、ダウンロードされた VPN ポリシーによって SUA がディセーブルにされている場合、Easy VPN サーバーは 2 要素/SecurID/cryptocard ベースの認証メカニズムで、XAUTH を使用している Secure Firewall Threat Defense デバイス を認証します。

推奨アクション 2 要素/SecurID/cryptocard ベースの認証メカニズムを使用して Easy VPN リモート デバイスを認証する場合は、サーバー上の SUA をイネーブルにします。

611323

エラーメッセージ `%Threat Defense-6-611323: VPNClient: Duplicate split nw entry`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーに重複したスプリット ネットワーク エントリが含まれていました。エントリは、ネットワーク アドレスとネットワーク マスクの両方に一致する場合、重複と見なされます。

推奨アクション Easy VPN サーバー上の VPN ポリシーから重複したスプリット ネットワーク エントリを削除します。

612001

エラーメッセージ `%Threat Defense-5-612001: Auto Update succeeded:`*`filename`*` , version:`*`number`*

説明 Auto Update Server からのアップデートが成功しました。**filename** 変数は、image、ASDM file、または configuration です。**version number** 変数は、アップデートのバージョン番号です。

推奨アクション 不要。

612002

エラーメッセージ `%Threat Defense-4-612002: Auto Update failed:filename , version:number , reason:reason`

説明 Auto Update Server からのアップデートが失敗しました。

- **filename**：イメージ ファイル、ASDM ファイル、またはコンフィギュレーション ファイル。
- **number**：アップデートのバージョン番号。
- **reason**：失敗の原因。次のいずれかの可能性があります。

- フェールオーバー モジュールがストリーム バッファを開くことができなかった。

- フェールオーバー モジュールがストリーム バッファにデータを書き込むことができなかった。

- フェールオーバー モジュールがストリーム バッファに対して制御動作を行うことができなかった。

- フェールオーバー モジュールがフラッシュ ファイルを開くことができなかった。

- フェールオーバー モジュールがフラッシュにデータを書き込むことができなかった。

- フェールオーバー モジュールの動作のタイムアウト。

- フェールオーバー コマンド リンクがダウンしている。

- フェールオーバー リソースを使用できない。

- 相手装置の無効なフェールオーバー状態。

- フェールオーバー モジュールがファイル転送データの破損を検出した。

- フェールオーバー アクティブ状態の変更。

- フェールオーバー コマンドの EXEC に失敗した。

- イメージは、現在のシステムで動作できない。

- サポートされていないファイル タイプ。

推奨アクション Auto Update Server の設定を確認します。スタンバイ装置が障害状態であるかどうかを確認します。Auto Update Server が正しく設定されており、スタンバイ装置が障害状態でない場合は、Cisco TAC にお問い合わせください。

612003

エラーメッセージ `%Threat Defense-4-612003:Auto Update failed to contact:url , reason:reason`

説明 Auto Update デーモンが指摘された URL **url** にアクセスできませんでした。これは、Auto Update Server の URL、または Auto Update Server から返されたファイル サーバー URL の 1 つである場合があります。**reason** フィールドには、接続が失敗した原因が記述されています。考

えられる失敗の原因としては、サーバーからの応答がない、認証の失敗、またはファイルが見つからないことが挙げられます。

推奨アクション Auto Update Server の設定を確認します。

613001

エラーメッセージ `%Threat Defense-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number`

説明メモリ破損のために、OSPF がデータベースでチェックサム エラーを検出しました。

推奨アクション OSPF プロセスを再起動します。

613002

エラーメッセージ `%Threat Defense-6-613002: interface interface_name has zero bandwidth`

説明このインターフェイスの帯域幅がゼロと報告されました。

推奨アクション 表示されているとおりにメッセージをコピーして、Cisco TAC に報告してください。

613003

エラーメッセージ `%Threat Defense-6-613003: IP_address netmask changed from area string to area string`

説明 OSPF コンフィギュレーションの変更によって、ネットワーク範囲のエリアが変更されました。

推奨アクション 正しいネットワーク範囲で OSPF を再設定します。

613004

エラーメッセージ `%Threat Defense-3-613004: Internal error: memory allocation failure`

説明内部ソフトウェア エラーが発生しました。

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

613005

エラーメッセージ `%Threat Defense-3-613005: Flagged as being an ABR without a backbone area`

説明ルータ内のバックボーン領域なしに、ルータが Area Border Router（ABR）としてフラグが設定されました。

推奨アクション OSPF プロセスを再起動します。

613006

エラーメッセージ %Threat Defense-3-613006: Reached unknown state in neighbor state machine

説明このルータ内の内部ソフトウェアエラーにより、データベース交換中に無効なネイバー状態が発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613007

エラーメッセージ %Threat Defense-3-613007: area string lsid IP_address mask netmask type number

説明 OSPF がデータベースに既存の LSA を追加しようとしています。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613008

エラーメッセージ %Threat Defense-3-613008: if inside if_state number

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613011

エラーメッセージ %Threat Defense-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id

説明 OSPF プロセスがリセット中で、新しいルータ ID を選択しようとしています。このアクションによってすべての仮想リンクが停止します。再び動作させるには、すべての仮想リンクネイバー上の仮想リンク設定を変更する必要があります。

推奨アクションすべての仮想リンク ネイバーの仮想リンク コンフィギュレーションを変更し、新しいルータ ID を反映させます。

613013

エラーメッセージ %Threat Defense-3-613013: OSPF LSID IP_address adv IP_address type number gateway IP_address metric number forwarding addr route IP_address/mask type number has no corresponding LSA

説明 OSPF で、そのデータベースと IP ルーティング テーブル間に不整合が検出されました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613014

エラーメッセージ `%Threat Defense-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string`

説明 MTR に互換性がある OSPF エリアに接続された OSPF インターフェイスでは、基本トポロジを有効にする必要があります。

推奨アクション なし。

613015

エラーメッセージ `%Threat Defense-4-613015: Process 1 flushes LSA ID IP_address type-number adv-rtr IP_address in area mask`

説明ルータは、このエラーメッセージによって報告されたLSAを広範囲に再発信またはフラッシュしています。

推奨アクション このルータがネットワーク LSA をフラッシュしている場合は、ルータのいずれかのインターフェイスの IP アドレスと LSA ID が衝突しているネットワーク LSA をルータが受信し、ネットワークの外部にLSAをフラッシュしたことを意味します。OSPF が正しく機能するためには、中継ネットワークの IP アドレスが一意であることが必要です。衝突しているルータは、このエラー メッセージを報告しているルータとこのメッセージで adv-rtr として報告された OSPF ルータ ID を持つルータです。このルータが LSA を再発信している場合は、他のルータがネットワークの外部にこの LSA をフラッシュしている可能性が高くなります。そのルータを見つけて衝突を解消してください。タイプ 2 LSA での衝突は、LSA ID の重複が原因の可能性があります。タイプ 5 LSA の場合、このエラー メッセージを報告しているルータと異なる領域に接続されているルータでルータ ID が重複している可能性があります。不安定なネットワークでは、このメッセージはその他の何らかの理由で LSA が広く再発信されていることを警告している場合もあります。このタイプのケースを調査するには、Cisco TAC にお問い合わせください。

613016

エラーメッセージ `%Threat Defense-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.`

説明ルータは、特大システム バッファ サイズまたはOSPF プロトコルに課された最大サイズより大きいルータ LSA を構築しようとしました。

推奨アクション 報告されたトータル長（LSAサイズ+オーバーヘッド）がHugeシステム バッファ サイズを超えていても、65535 バイト未満の場合は（OSPF プロトコルが指定する最大長）、Hugeシステム バッファ サイズを増やすことができます。報告されたトータル長が65535より大きい場合は、報告された領域の OSPF インターフェイスの数を削減する必要があります。

613017

エラーメッセージ `%Threat Defense-4-613017: Bad LSA mask: Type number, LSID IP_address Mask mask from IP_address`

説明 LSA 発信元の設定が不正であるため、ルータが無効な LSA マスクを持つ LSA を受信しました。結果として、このルートはルーティング テーブルにインストールされていません。

推奨アクション 不正なマスクとともに LSA 発信元ルータを探し、その LSA のネットワークの不良構成を修正します。詳しいデバッグについては、Cisco TAC に問い合わせてください。

613018

エラーメッセージ `%Threat Defense-4-613018: Maximum number of non self-generated LSA has been exceeded “OSPF number” - number LSAs`

説明非自己生成 LSA の最大数を超えました。

推奨アクション ネットワーク内のルータが誤設定の結果として大量の LSA を生成しているかどうかを確認します。

613019

エラーメッセージ `%Threat Defense-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs`

説明非自己生成 LSA の最大数のしきい値に達しました。

推奨アクション ネットワーク内のルータが誤設定の結果として大量の LSA を生成しているかどうかを確認します。

613021

エラーメッセージ `%Threat Defense-4-613021: Packet not written to the output queue`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613022

エラーメッセージ `%Threat Defense-4-613022: Doubly linked list linkage is NULL`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613023

エラーメッセージ `%Threat Defense-4-613023: Doubly linked list prev linkage is NULL number`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、コンフィギュレーション、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 に提出してください。

613024

エラーメッセージ `%Threat Defense-4-613024: Unrecognized timer number in OSPF string`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、コンフィギュレーション、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 に提出してください。

613025

エラーメッセージ `%Threat Defense-4-613025: Invalid build flag number for LSA IP_address, type number`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613026

エラーメッセージ `%Threat Defense-4-613026: Can not allocate memory for area structure`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、コンフィギュレーション、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 に提出してください。

613027

エラーメッセージ `%Threat Defense-6-613027: OSPF process number removed from interface interface_name`

説明 IP VRF が理由で、OSPF プロセスがインターフェイスから削除されました。

推奨アクション なし。

613028

エラーメッセージ `%Threat Defense-6-613028: Unrecognized virtual interface intetface_name. Treat it as loopback stub route`

説明 仮想インターフェイス タイプが OSPF によって認識されなかったため、ループバック インターフェイスのスタブ ルートとして扱われます。

推奨アクション なし。

613029

エラーメッセージ `%Threat Defense-3-613029: Router-ID IP_address is in use by ospf process number`

説明 Secure Firewall Threat Defense デバイス が別のプロセスで使用中のルータ ID を割り当てようとしました。

推奨アクション プロセスの 1 つに別のルータ ID を設定します。

613030

エラーメッセージ `%Threat Defense-4-613030: Router is currently an ASBR while having only one area which is a stub area`

説明 ASBR は AS External または NSSA LSA を伝送できる領域に接続する必要があります。

推奨アクション ルータの接続先となる領域を NSSA または通常の領域にします。

613031

エラーメッセージ `%Threat Defense-4-613031: No IP address for interface inside`

説明インターフェイスはポイントツーポイントではなく、番号が付けられていません。

推奨アクション インターフェイス タイプを変更するか、またはインターフェイスに IP アドレスを指定します。

613032

エラーメッセージ `%Threat Defense-3-613032: Init failed for interface inside, area is being deleted. Try again.`

説明 インターフェイスの初期化に失敗しました。考えられる原因は次のとおりです。

- インターフェイスの接続先となる領域が削除されています。
- ローカル ルータのネイバー データブロックを作成できませんでした。

推奨アクション インターフェイスに関係するコンフィギュレーション コマンドを削除して、再試行します。

613033

エラーメッセージ `%Threat Defense-3-613033: Interface inside is attached to more than one area`

説明インターフェイスが、インターフェイスのリンク先以外の領域のインターフェイス リストに含まれています。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613034

エラーメッセージ `%Threat Defense-3-613034: Neighbor IP_address not configured`

説明設定されたネイバー オプションが有効ではありません。

推奨アクション neighbor コマンドの設定オプションを確認し、そのオプションか、またはネイバー インターフェイスのネットワーク タイプを修正します。

613035

エラーメッセージ `%Threat Defense-3-613035: Could not allocate or find neighbor IP_address`

説明内部エラーが発生しました。

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

613036

エラーメッセージ `%Threat Defense-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network`

説明設定されたネイバーが NBMA ネットワーク上で検出され、cost または database-filter オプションが設定されました。これらのオプションは、ポイントツーマルチポイント タイプのネットワークにのみ使用できます。

推奨アクション neighbor コマンドの設定オプションを確認し、そのオプションか、またはネイバー インターフェイスのネットワーク タイプを修正します。

613037

エラーメッセージ `%Threat Defense-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network`

説明設定されたネイバーは、ポイントツーマルチポイント ネットワークで検出され、pollオプションまたは priority オプションが設定されました。これらのオプションは、NBMA タイプのネットワークにのみ使用できます。

推奨アクション neighbor コマンドの設定オプションを確認し、そのオプションか、またはネイバー インターフェイスのネットワーク タイプを修正します。

613038

エラーメッセージ `%Threat Defense-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network`

説明設定されたネイバーが、ポイントツーマルチポイント ブロードキャスト ネットワーク上で検出されました。**cost** または **database-filter** オプションのいずれかを設定する必要があります。

推奨アクション neighbor コマンドの設定オプションを確認し、そのオプションか、またはネイバー インターフェイスのネットワーク タイプを修正します。

613039

エラーメッセージ `%Threat Defense-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks`

説明ネットワーク タイプが NBMA でもポイントツーマルチポイントでもないネットワーク上で、設定されたネイバーが検出されました。

推奨アクション なし。

613040

エラーメッセージ `%Threat Defense-4-613040: OSPF-1 Area string: Router IP_address originating invalid type number LSA, ID IP_address, Metric number on Link ID IP_address Link Type number`

説明このメッセージに示されたルータから無効なメトリックの LSA が送信されています。これがルータ LSA であり、リンク メトリックがゼロの場合、ネットワーク上にルーティング ループとトラフィック損失が存在する危険性があります。

推奨アクション 報告された LSA を送信したルータに、当該 LSA タイプおよびリンク タイプに有効なメトリックを設定します。

613041

エラーメッセージ `%Threat Defense-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge`

説明内部エラーが修正されました。このエラーメッセージに関連する動作への影響はありません。

推奨アクション システム メモリを確認します。メモリが不足している場合は、そのためにタイマー ホイール機能が初期化されませんでした。メモリが利用可能になったときに、コマンドを再入力してみます。メモリが十分ある場合は、Cisco TAC に連絡し、**show memory** コマンド、**show processes** コマンド、および **show tech-support ospf** コマンドの出力を提供してください。

613042

エラーメッセージ `%Threat Defense-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared`

説明 NSSA エリアに実行可能な転送先アドレスがありません。結果として、P ビットをクリアする必要があります。NSSA トランスレータはタイプ 7 LSA をタイプ 5 LSA に変換しません。RFC 3101 を参照してください。

推奨アクション アドバタイズされた IP アドレスで、少なくとも 1 つのインターフェイスを NSSA に設定します。アドバタイズメントは下位レイヤ 2 の状態に依存しないため、ループバックを選ぶようにしてください。

613043

エラーメッセージ `%Threat Defense-6-613043:`

説明負のデータベース リファレンス カウントが発生しました。

推奨アクション システム メモリを確認します。メモリが不足している場合は、そのためにタイマーホイール機能が初期化されませんでした。メモリが利用可能になったときに、コマンドを再入力してみます。メモリが十分ある場合は、Cisco TAC に連絡し、**show memory** コマンド、**show processes** コマンド、および **show tech-support ospf** コマンドの出力を提供してください。

613101

エラーメッセージ `%Threat Defense-6-613101: Checksum Failure in database in area s Link State Id i Old Checksum #x New Checksum #x`

説明メモリ破損のために、OSPF がデータベースでチェックサム エラーを検出しました。

推奨アクション OSPF プロセスを再起動します。

613102

エラーメッセージ `%Threat Defense-6-613102: interface s has zero bandwidth`

説明このインターフェイスの帯域幅がゼロと報告されています。

推奨アクション 不要。

613103

エラーメッセージ `%Threat Defense-6-613103: i m changed from area AREA_ID_STR to area AREA_ID_STR`

説明 OSPF コンフィギュレーションの変更によって、ネットワーク範囲のエリアが変更されました。

推奨アクション 不要。

613104

エラーメッセージ `%Threat Defense-6-613104: Unrecognized virtual interface IF_NAME .`

説明仮想インターフェイス タイプが OSPFv3 によって認識されなかったため、ループバック インターフェイスのスタブ ルートとして扱われます。

推奨アクション 不要。

614001

エラーメッセージ `%Threat Defense-6-614001: Split DNS: request patched from server: IP_address to server: IP_address`

説明スプリット DNS によって、DNS クエリーが元の宛先サーバーから企業のプライマリ DNS サーバーにリダイレクトされています。

推奨アクション 不要。

614002

エラーメッセージ `%Threat Defense-6-614002: Split DNS: reply from server:IP_address reverse patched back to original server:IP_address`

説明スプリット DNS によって、DNS クエリーが企業の DNS サーバーから元の宛先サーバーにリダイレクトされています。

推奨アクション 不要。

615001

エラーメッセージ `%Threat Defense-6-615001: vlan number not available for firewall interface`

説明スイッチによって、VLAN が Secure Firewall Threat Defense デバイス から削除されました。

推奨アクション 不要。

615002

エラーメッセージ `%Threat Defense-6-615002: vlan number available for firewall interface`

説明スイッチによって、VLAN が Secure Firewall Threat Defense デバイス に追加されました。

推奨アクション 不要。

621001

エラーメッセージ `%Threat Defense-6-621001: Interface` *interface_name* does not support multicast, not enabled

説明マルチキャストをサポートしていないインターフェイス上の PIM をイネーブルにしようとしました。

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。

621002

エラーメッセージ `%Threat Defense-6-621002: Interface` *interface_name* does not support multicast, not enabled

説明マルチキャストをサポートしていないインターフェイス上の IGMP をイネーブルにしようとしました。

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。

621003

エラーメッセージ `%Threat Defense-6-621003: The event queue size has exceeded` *number*

説明作成されたイベント マネージャ数が想定された数を超えました。

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。

621006

エラーメッセージ `%Threat Defense-6-621006: Mrib disconnected`, (*IP_address* ,*IP_address*) event cancelled

説明データ駆動イベントを起動するパケットを受信したが、MRIB への接続がダウンしました。通知はキャンセルされました。

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。

621007

エラーメッセージ `%Threat Defense-6-621007: Bad register from` *interface_name* :*IP_address* to *IP_address* for (*IP_address* , *IP_address*)

説明 PIM ルータが、ランデブー ポイントとして設定されている場合、または NAT で別の PIM ルータから PIM レジスタ パケットを受信した場合に表示されます。このパケット内のカプセル化されたデータは無効です。

推奨アクション 送信ルータが誤って RFC 以外のレジスタを送信しています。送信側のルータをアップグレードします。

622001

エラーメッセージ `%Threat Defense-6-622001`: *string* tracked route *network mask address* , distance *number* , table *string* , on interface *interface-name*

説明追跡対象ルートがルーティングテーブルに対して追加または削除されました。これは、追跡対象オブジェクトの状態がアップまたはダウンから変わったことを意味します。

- *string*：Adding または Removing
- *network*：ネットワーク アドレス
- *mask*：ネットワーク マスク
- *address*：ゲートウェイ アドレス
- *number*：ルート アドミニストレーティブ ディスタンス
- *string*：ルーティング テーブル名
- *interface-name*：**nameif** コマンドで指定されたインターフェイス名

推奨アクション 不要。

622101

エラーメッセージ `%Threat Defense-6-622101`: Starting regex table compilation for *match_command* ; table entries = *regex_num* entries

説明正規表現コンパイルのバックグラウンド アクティビティに関する情報が表示されます。

- *match_command*：正規表現テーブルが関連付けられている match コマンド
- *regex_num*：コンパイルされる正規表現エントリの数

推奨アクション 不要。

622102

エラーメッセージ `%Threat Defense-6-622102`: Completed regex table compilation for *match_command* ; table size = *num* bytes

説明正規表現コンパイルのバックグラウンド アクティビティに関する情報が表示されます。

- *match_command*：正規表現テーブルが関連付けられている match コマンド
- *num*：コンパイルされたテーブルのサイズ（バイト単位）

推奨アクション 不要。

622102

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。