

3000エラーによるTETRA定義の更新エラーのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決方法](#)

[関連情報](#)

はじめに

このドキュメントでは、エラー3000エラーでTETRA定義の障害をトラブルシューティングする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Endpoint

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Secure Endpointコネクタ (任意のバージョン)
- Wireshark (任意のバージョン)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

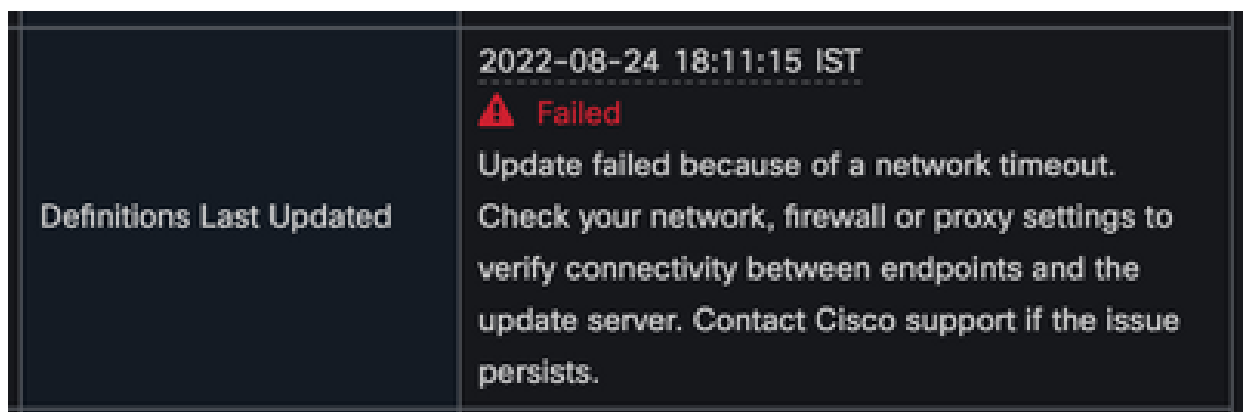
問題

1. エンドポイントで、TETRA定義の更新が「Unable to install updates.Please try again later」というエラーメッセージで失敗します。



2. Cisco Secure Endpoint Consoleで、前述の障害エラーが表示されます。

「ネットワークのタイムアウトのため、更新に失敗しました。ネットワーク、ファイアウォール、またはプロキシの設定を確認して、エンドポイントと更新サーバー間の接続を確認してください。問題が解決しない場合は、Ciscoサポートにお問い合わせください」



3. debug sfc.exe.logで、「definitions updated failed with error 3000」エラーが表示されます。これは、文書化されているUnknown_Errorを意味します。

<#root>

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdateInterface::update updateDir: C:\Progr
(978223515, +0 ms) Aug 04 07:30:23 [11944]: ERROR: TETRAUpdateInterface::update
```

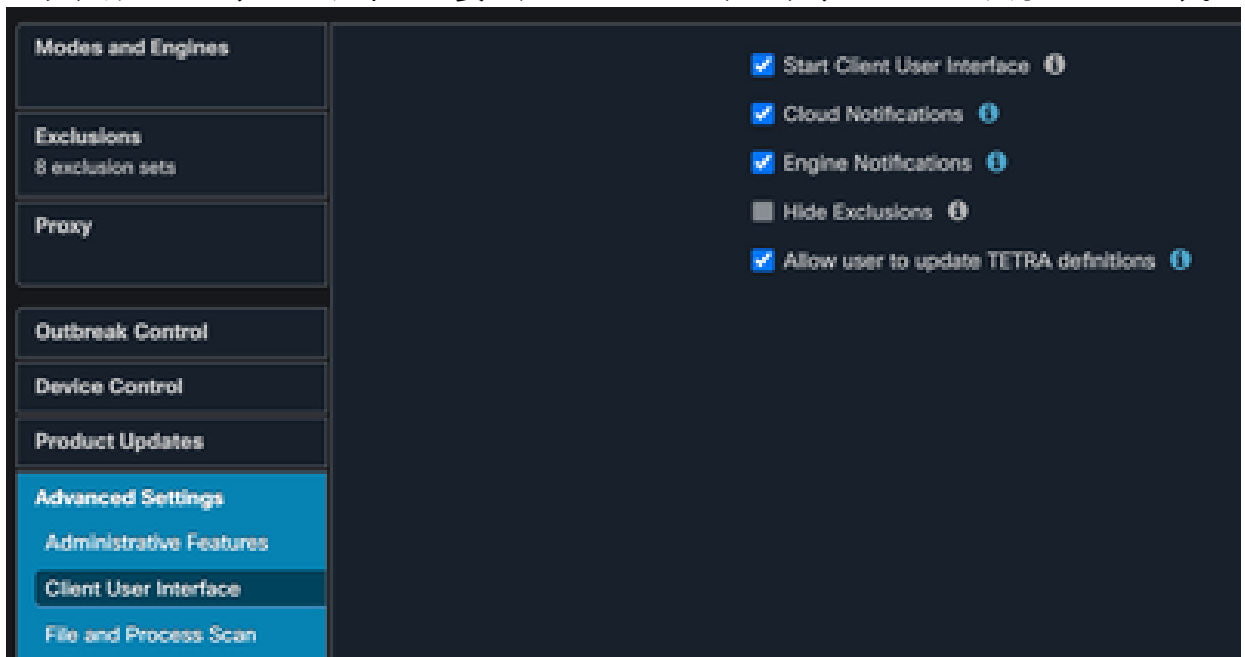
Update failed with error -3000

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PipeSend: sending message to user interface: 26,
(978223515, +0 ms) Aug 04 07:30:23 [860]: PipeWrite: waiting on pipe event handle
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit defInit: 0, bUpdate: 0
```

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit bUpdate: 0, bReload: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: FASharedPtr<class TETRAUpdateInterface>::Release
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: bUpdated = FALSE, state: 20,
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: sig count: 0, version: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: Config::IsUploadEventEnabled: returns 1, 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
```

解決方法

1. コンソールでAMP Policy > Client User Interfaceの順に選択し、Allow user to update TETRA definitionsオプションを有効にしてください。このパラメータを使用すると、トラブルシューティング中に必要に応じてTETRAアップデートをトリガーできます。



2. また、エンドポイントで、またはAMPポリシーを介して、コネクタとトレイレベルのデバッグログを有効にします。
3. エンドポイントでUpdate TETRAをクリックしながら、TETRA DefinitionsのTETRA更新の成功と失敗したエンドポイントの両方でパケットキャプチャを取得してください。
4. TETRAアップデートが成功したエンドポイントでは、パケットキャプチャでhttp.host == "tetra-defs.amp.cisco.com:443"を含むパケットをフィルタリングし、次に各パケットの"tcp.stream"を追跡して、関連するトラフィックを分析します。
5. Server Helloパケットで、Server accepts "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"という暗号がServer Helloパケットで確認できます。

No.	Time	Source	Destination	Protocol	Length	Info
169	17:54:13.501878			TCP	68	60649 -> 6050 [SYN, ECN, CWR] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
170	17:54:13.501885			TCP	68	6050 -> 60649 [SYN, ACK, ECN] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
171	17:54:13.501321			TCP	62	60649 -> 6050 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
172	17:54:13.501438			HTTP	141	CONNECT tetra-defs.amp.cisco.com:443 HTTP/1.1
173	17:54:13.501449			TCP	56	6050 -> 60649 [ACK] Seq=1 Ack=86 Win=29312 Len=0
174	17:54:13.519661			HTTP	155	HTTP/1.1 200 Connection established
175	17:54:13.528100			TLSv1..	255	Client Hello
176	17:54:13.559031			TCP	56	6050 -> 60649 [ACK] Seq=100 Ack=285 Win=30336 Len=0
181	17:54:17.326736			TLSv1..	7356	Server Hello
182	17:54:17.326748			TLSv1..	1343	Certificate, Server Key Exchange, Server Hello Done
183	17:54:17.327138			TCP	62	60649 -> 6050 [ACK] Seq=285 Ack=8687 Win=2102272 Len=0
184	17:54:17.329911			TLSv1..	182	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
185	17:54:17.329925			TCP	56	6050 -> 60649 [ACK] Seq=8687 Ack=411 Win=30336 Len=0
186	17:54:17.784930			TLSv1..	346	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
187	17:54:17.785908			TLSv1..	355	Application Data
188	17:54:17.785921			TCP	56	6050 -> 60649 [ACK] Seq=8977 Ack=710 Win=31360 Len=0
189	17:54:18.134677			TLSv1..	7356	Application Data
190	17:54:18.134689			TCP	6924	6050 -> 60649 [PSH, ACK] Seq=16277 Ack=710 Win=31360 Len=6868 [TCP segment of a reassembled PDU]
191	17:54:18.135276			TCP	62	60649 -> 6050 [ACK] Seq=710 Ack=23145 Win=2102272 Len=0
192	17:54:18.370029			TLSv1..	9600	Application Data [TCP segment of a reassembled PDU]
193	17:54:18.370461			TCP	62	60649 -> 6050 [ACK] Seq=710 Ack=32769 Win=2102272 Len=0
194	17:54:18.370471			TCP	4600	6050 -> 60649 [PSH, ACK] Seq=32769 Ack=710 Win=31360 Len=4544 [TCP segment of a reassembled PDU]
195	17:54:18.370703			TCP	62	60649 -> 6050 [ACK] Seq=710 Ack=35689 Win=2102272 Len=0
196	17:54:18.370839			TCP	62	60649 -> 6050 [ACK] Seq=710 Ack=37313 Win=2102272 Len=0
197	17:54:18.640107			TLSv1..	2799	Application Data, Encrypted Alert
198	17:54:18.640464			TCP	62	60649 -> 6050 [ACK] Seq=710 Ack=40056 Win=2102272 Len=0

```

[Proxy-Connect-Port: 443]
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 65
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 61
      Version: TLS 1.2 (0x0303)
      Random: d19d47a9913f35df7270c3acee595422552881e62044737e9ee4e5fe776255
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Compression Method: null (0)
      Extension Length: 33
  
```

6. Cisco Secure Endpoint TETRAサーバは、言及された暗号のみを受け入れます。

```

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_128_GCM_SHA256
  
```

7. TETRAアップデートが失敗したエンドポイントでは、パケットキャプチャで、Client

Helloパケットの後にSSLハンドシェイクの致命的なエラーが表示されます。



8. Client Helloパケットでは、エンドポイントから提供される暗号を確認できます。



9. また、エンドポイントで有効になっている暗号をGet-TlsCipherSuiteで相互検証できます | ft name PowerShellコマンドを使用します。

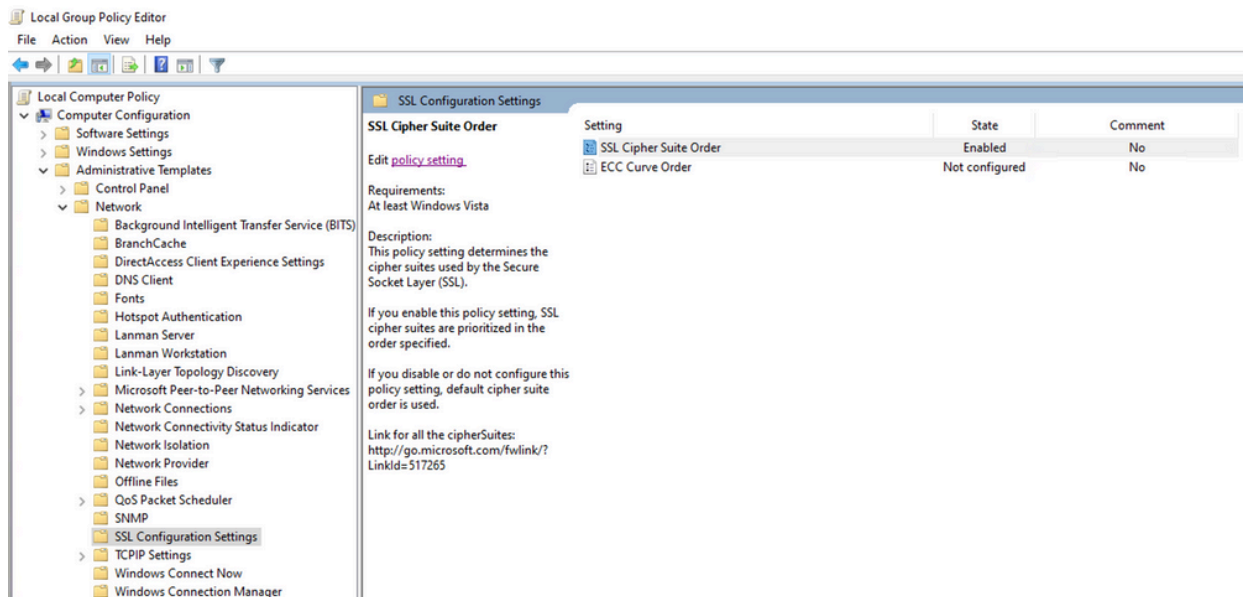
 Select Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> Get-TlsCipherSuite | ft name

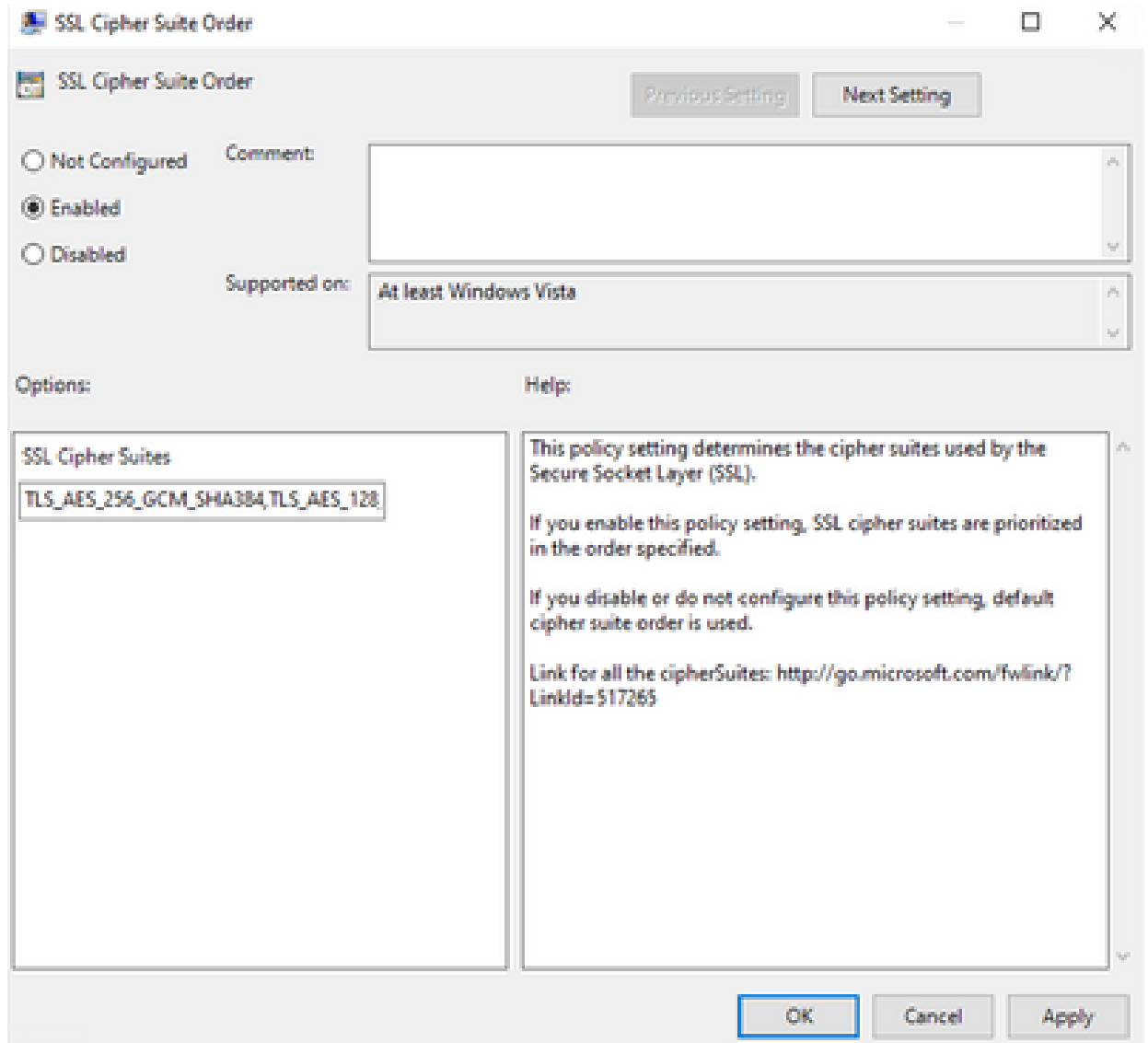
Name
----
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
TLS_PSK_WITH_AES_256_GCM_SHA384
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_PSK_WITH_NULL_SHA384
TLS_PSK_WITH_NULL_SHA256
```

10. ステップ6で説明した暗号がここにリストされていない場合は、SSLハンドシェイクが失敗する理由です。
11. これを修正するには、グループポリシーでSSL暗号スイートの順序を確認してください。

Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Temp1



12. 暗号スイートの順序はNot ConfiguredまたはDisabledである必要があります。
Enabledに設定されている場合は、ステップ6で説明した暗号をリストに追加します。



13. これらの変更を適用し、エンドポイントを再起動して、アプリケーションで使用できるようにします。

14. 再起動が完了したら、Update TETRAを再試行してください。
15. TETRA定義の問題が解決しない場合は、ログを分析して再度キャプチャしてください。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。