TMS に追加された TelePresence エンドポイントが自動的にステータスを「Behind the Firewall」に変更する問題のトラブルシューティング

目次

概要

この資料に問題を引き起こす IP アドレスを TelePresence 管理 サーバ (TMS) にエンドポイントに代わってパケットを送信する隔離する方法を記述されています。 どの管理対象装置でも TMS に追加されるとき、ステータスはしかしデフォルトでしばらくの間ファイアウォールの後ろでに変更するかもしれませんことをいつかステータスの後で LAN で到達可能ことを示します。 これは一般に TMS によってデバイスの xstatus から届くデバイスから受信されるパケットにシステムIP アドレスと別のソース IP アドレスがあると起こります。

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。

- TC （ TelePresence コーデック) ソフトウェアか MXP を実行する Cisco TelePresence エンドポイント
- TMS

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

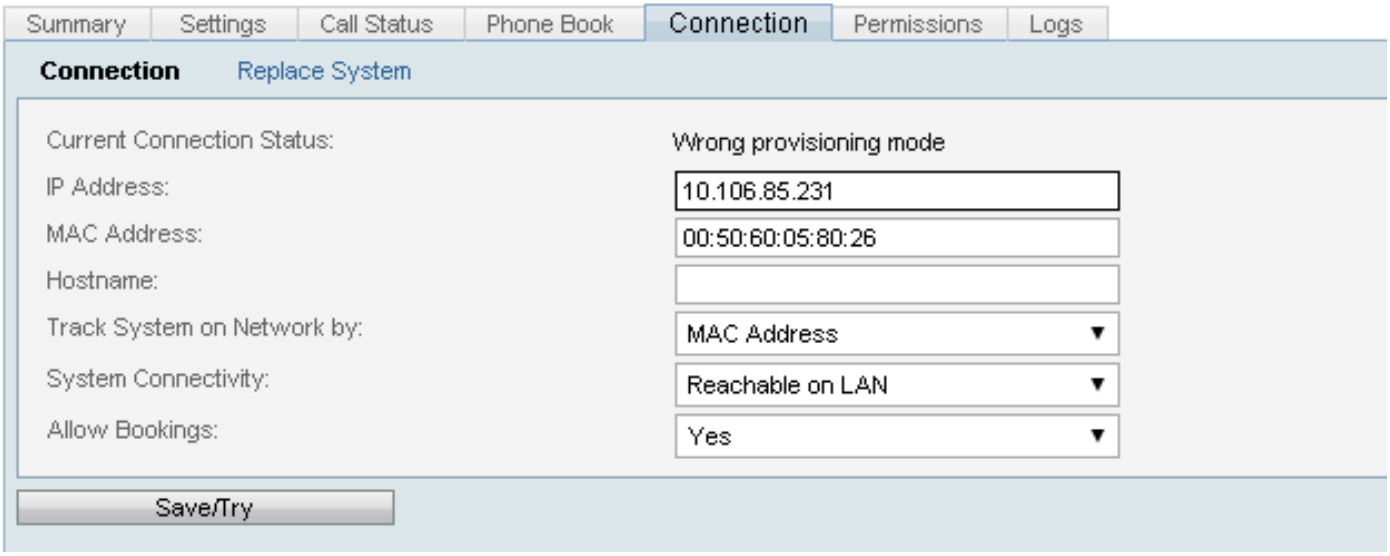
問題

TMS によって管理されるエンドポイントはファイアウォール ステータスの後ろのに LAN ステータスの到達可能から自動的に変更しま、デバイスの管理を停止するために TMS を引き起こします。 解決するために、管理対象装置と TMS 間のネットワークで許可される HTTP 通信を持たなければならないことが考慮されます。

トラブルシューティング

TMS からのパケットキャプチャを確認することが必要となります:

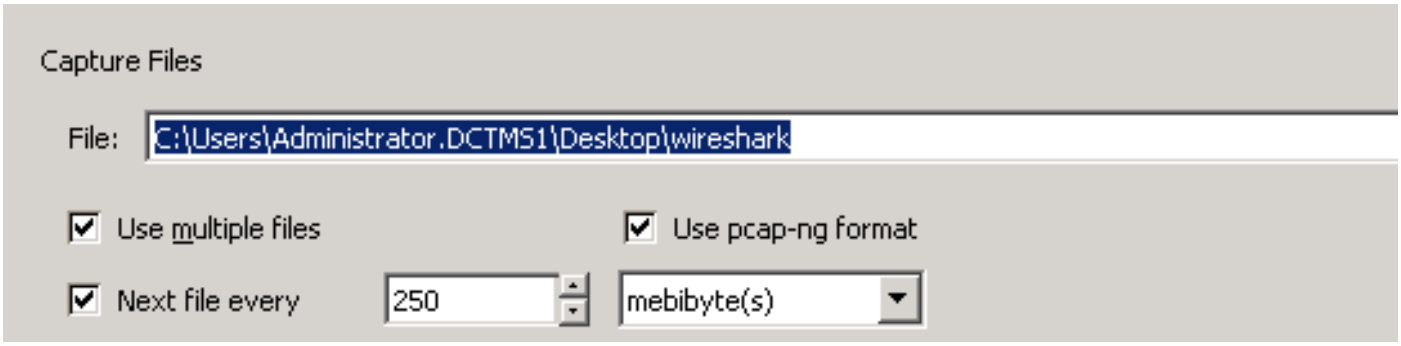
1. リモート デスクトッププロトコル（RDP）によって TMS サーバに接続して下さい。
2. TMS におよびエンドポイントに有効に なる HTTP 通信があること、そして HTTPS が無効であることを確認して下さい。
3. /Wireshark インストールして下さいおよび Select default 実行されたネットワーク インターフェイス。
4. フィルタを適用しないし、キャプチャを開始して下さい。
5. 、このイメージに示すように『SAVE』 をクリック しましたり/**試み**ボタンは問題に直面しているエンドポイントの Connection タブにナビゲート します。



6. エンドポイントが後ろファイアウォールに戻って下るとき、wireshark キャプチャを停止して下さい。

> **注:** 時々問題は期待されるより時間がかかるかもしれません。 複数のファイルで保存するために Wireshark キャプチャを開始している間それ故に作り直すために確認して下さい。

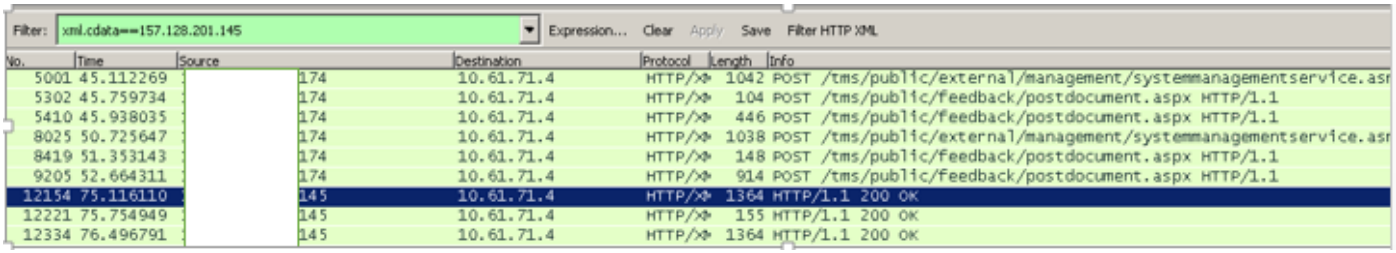
7.**キャプチャ ファイル** オプションに行き、**使用 複数のファイル** チェックボックスを選択して下さい。



Wireshark を開いて下さい

- xml.cdata ==IP_ADDRESS_OF_DEVICE のようなフィルタを適用して下さい
- このフィルタを適用した後応答が実機器 IP アドレスから別の IP アドレスに変更することがわかるかもしれません。

このイメージに示すように、デバイスの実際の IP アドレスは x.x.x.174 です; ただしこの IP が x.x.x.145 に変更する以降



この IP アドレスの変更すること当然 TMS は xstatus で送信 される デバイス IP アドレスが IP ヘッダーの IP アドレスがそれ故にそれファイアウォール ステータスの後ろのにデバイスを変更する同じではないことを確認し。

解決策

IP ヘッダーのソース IP アドレスを変更しているエンドポイントの実際の IP と異ならせますそれ故に IP ヘッダーで出典 IP を、エンドポイントと TMS 間のネットワークにデバイスがないことを確認する必要があるこの問題を解決するため。