目次

概要

この資料にネットワークか Webサーバによってブロックされる Cisco TelePresence Management Suite（TMS）にフィードバックの問題を解決する方法を記述されています。

前提条件

要件

Cisco は Cisco TMS のナレッジがあることを推奨します。

使用するコンポーネント

この文書に記載されている情報は Cisco TMS に基づいています。

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。

ネットワークか Webサーバによってブロックされる Cisco TMS へのシステム フィードバック

Cisco TMS はシステムから送信 される フィードバックに頼り、シリアル番号、MAC アドレスおよび IP アドレスに基づいていたそれに接続するエンドポイントことを確認します。 ほとんどの Cisco TelePresence およびサード パーティ システムは認証を必要とするネットワークに Web プロキシがある場合ブロックすることができる匿名 HTTP または HTTPS 接続とのこのフィードバックを送信 します。 この場合、プロキシの管理者に Cisco TMS に向かうトラフィックのための

例外を追加するために話す必要があります。

ファイアウォールはまた Cisco TMS にシステムから Cisco TMS に新しい接続をブロックする場合フィードバックをブロックできます。

> **ヒント**： ポート および プロトコルが各システム型のために利用可能である必要がある Cisco TMS サポート ドキュメント輪郭。

最後のよくある接続障害は Cisco TMS がインストールされていた修正し、Web ディレクトリに匿名アクセスをディセーブルにする後管理者が手動で Internet Information Services （ IIS ）設定をと発生します。

> **注** 匿名アクセスはフィードバックを送信 するときシステムがユーザ名 および パスワードを使用しないので Cisco TMS の一部分にだけ開いて、無効でなければなりません。

IIS ミスコンフィギュレーションを訂正するために、Cisco TMS をアンインストールし、それを再インストールして下さい。 データはデータベースがそのまま残って、インストーラが Webサイト プロパティを正しく再製する限り、失われません。