

VCS Web インターフェイスでの TLS ハンドシェイクの失敗

目次

[概要](#)

[問題](#)

[解決策](#)

概要

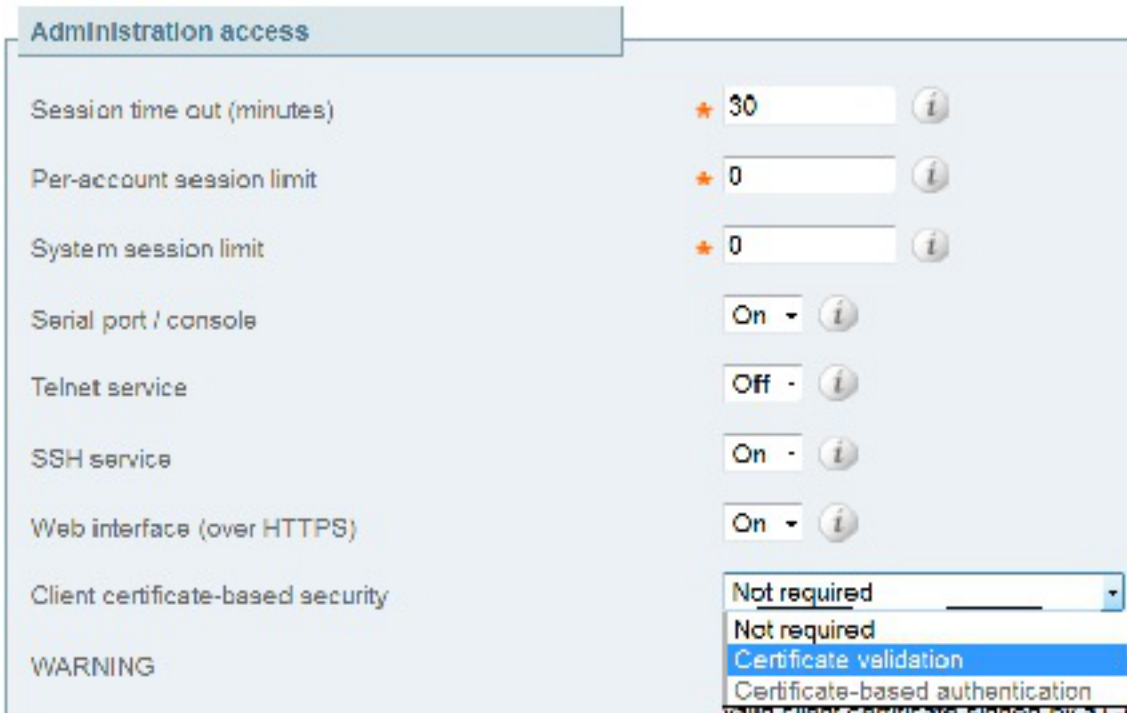
Cisco Video Communication Server (VCS) は、認証プロセスと認可プロセスにクライアント証明書を使用します。この機能はセキュリティを強化し、シングル サインオンの目的で使用できるため、一部の環境では非常に便利です。ただし設定が誤っている場合、管理者が VCS Web インターフェイスからロックアウトされることがあります。

このドキュメントで説明する手順は、Cisco VCS でクライアント証明書ベースのセキュリティを無効にするときに使用します。

問題

クライアント証明書ベースのセキュリティが VCS で有効であるものの、誤って設定されている場合、ユーザが VCS Web インターフェイスにアクセスできない可能性があります。Web インターフェイスにアクセスしようとすると、Transport Layer Security (TLS) ハンドシェイク エラーが発生します。

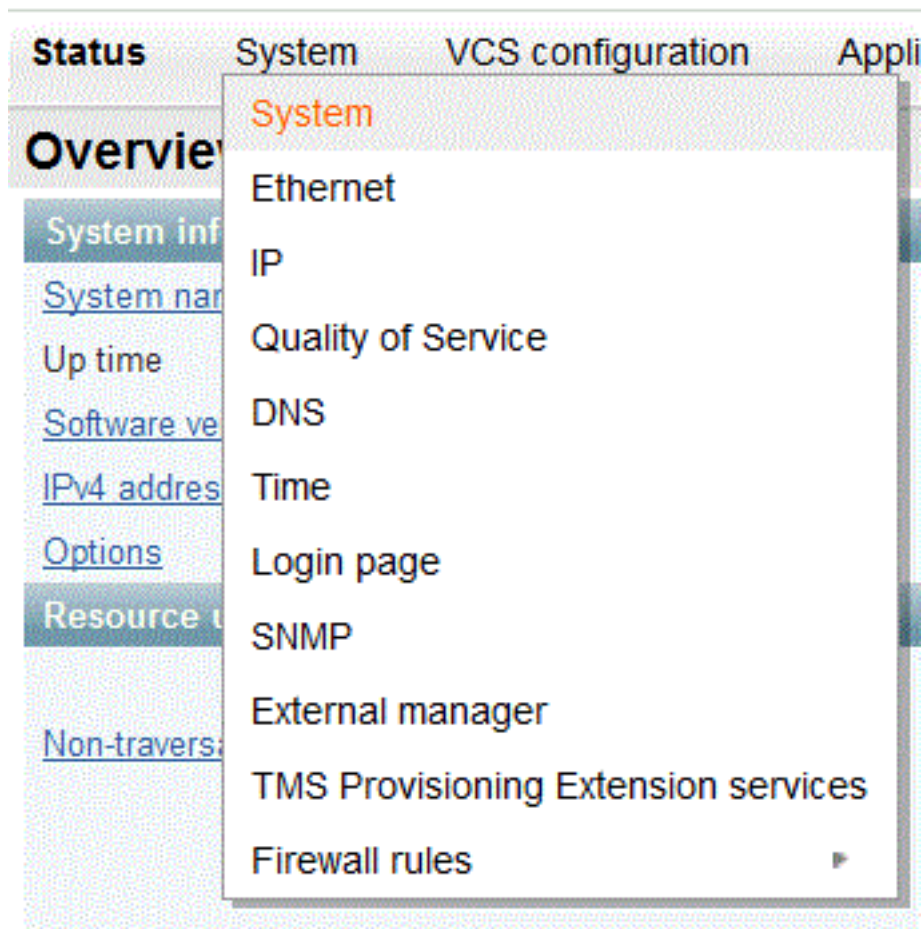
この問題は、次に示す設定変更が原因で発生します。



解決策

クライアント証明書ベースのセキュリティを無効にし、管理者が VCS の Web インターフェイスにアクセスできる状態にシステムを戻すには、次の手順を実行します。

1. root としてセキュア シェル (SSH) を介して VCS に接続します。
2. クライアント証明書ベースのセキュリティを使用することがないように Apache をハードコーディングするため、root として次のコマンドを入力します。echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf 注: このコマンドの入力後は、**removecba.conf** ファイルを削除し、VCS を再起動するまでは、VCS でクライアント証明書ベースのセキュリティを再度設定することはできません。
3. この設定変更を有効にするために VCS を再起動する必要があります。VCS を再起動する準備ができたなら、次のコマンドを入力します。tshell
xcommand restart 注: これにより VCS が再起動し、すべてのコール/登録が削除されます。
4. VCS がリロードすると、クライアント証明書ベースのセキュリティが無効になります。ただし、これは適切な方法で無効にされたわけではありません。VCS に読み取り/書き込み可能な管理者アカウントでログインします。VCS で [System] > [System] ページに移動します。



VCS のシステム管理ページで、クライアント証明書ベースのセキュリティが [Not required] に設定されていることを確認します。

Administration access	
Session time out (minutes)	★ 30 ⓘ
Per-account session limit	★ 0 ⓘ
System session limit	★ 0 ⓘ
Serial port / console	On ⓘ
Telnet service	Off ⓘ
SSH service	On ⓘ
Web interface (over HTTPS)	On ⓘ
Client certificate-based security	Certificate validation ⓘ
Certificate revocation list (CRL) checking	Not required ⓘ

この変更を行ったら、変更内容を保存します。

- 完了したら、Apache を通常の状態にリセットするため、SSH で root として次のコマンドを入力します。`rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf` **警告**： このステップを省略する場合、クライアント証明書ベースのセキュリティを再び有効にすることはできません。
- この手順が適切に機能することを確認するため、VCS をもう一度再起動します。これで Web にアクセスできるようになりました。Web インターフェイスの [Maintenance] > [Restart] で VCS を再起動します。

これですべての作業は完了しました。クライアント証明書ベースのセキュリティが無効な状態で VCS が動作します。