ASA による Cisco Unified Mobility Advantage サーバ証明書の問題

目次

概要

この資料に適応型セキュリティ アプライアンス（ASA）ソフトウェア交換する方法を（ASA）と Cisco Unified Mobility Advantage （CUMA）サーバ間の自己署名証明書をまたその逆にも記述されています。 発生する認証をインポートする間、それはまたよくある 問題を解決する方法を説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA 5500 シリーズ
- Cisco Unified Mobility Advantage サーバ 7

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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

導入シナリオ

Cisco モビリティ長所ソリューションによって使用される **TLS プロキシ**のための 2 つのデプロイメントシナリオがあります。

注: 両方のシナリオで、クライアントはインターネットから接続します。

1. 適応性があるセキュリティ アプライアンス モデルはファイアウォールおよび TLS プロキシ両方として機能します。
2. 適応性があるセキュリティ アプライアンス モデルは TLS プロキシだけとして機能します。

両方のシナリオで、**PKCS-12** 形式の **Cisco UMA サーバ証明**および**キー ペアを**エクスポートし、適応性があるセキュリティ アプライアンス モデルにインポートする必要があります。 認証は Cisco UMA クライアントとハンドシェイクの間に使用されます。

適応性があるセキュリティ アプライアンス モデル truststore の Cisco UMA サーバ 自己署名証明書のインストールは適応性があるセキュリティ アプライアンス モデルが適応性があるセキュリティ アプライアンス モデル プロキシと Cisco UMA サーバ間のハンドシェイクの間に Cisco UMA サーバを認証することができるように必要です。

Cisco UMA サーバ 自己署名証明書をインストールして下さい

CUMA サーバでされるタスク

これらのステップは CUMA サーバで実行される必要があります。 これらのステップによって、CN=portal.aipc.com で ASA を使うと交換するために CUMA の自己署名証明書を作成します。 これは ASA 信頼ストアでインストールされる必要があります。 次の手順を実行します。

1. CUMA サーバの自己署名証明書を作成して下さい。Cisco Unified Mobility Advantage Admin ポータルに署名して下さい。セキュリティ コンテキスト管理の側の**[+]**選択して下さい。**コンテキストを**『Security』 を選択 して下さい。**コンテキストを**『Add』 を選択 して下さい。次の情報を入力します。`Do you want to create/upload a new certificate? create`
   ```
   Context Name "cuma"
   Description "cuma"
   Trust Policy "Trusted Certificates"
   Client Authentication Policy "none"
   Client Password "changeme"
   Server Name cuma.ciscodom.com
   Department Name "vsec"
   Company Name "cisco"
   City "san jose"
   State "ca"
   Country "US"
   ```
2. Cisco Unified Mobility Advantage から自己署名証明書をダウンロードして下さい。 この作業

を行うには、次の手順を実行します。セキュリティ コンテキスト管理の側の**[+]**選択して下さい。**コンテキストを**『Security』 を選択 して下さい。ダウンロードするために認証を保持するセキュリティ コンテキストの側の**コンテキストを**『Manage』 を選択 して下さい。**認証を**『Download』 を選択 して下さい。**注:** 認証がチェーンで、ルートまたは中間物認証を関連付けたら、チェーンの最初の認証だけがダウンロードされます。 これは自己署名証明書のために十分です。ファイルを保存します。

3. 次 の ステップは ASA に Cisco Unified Mobility Advantage から自己署名証明書を追加することです。 ASA のこれらのステップを完了して下さい:テキストエディタの Cisco Unified Mobility Advantage からの自己署名証明書を開いて下さい。信頼ストアに認証を Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア インポートして下さい:`cuma-asa(config)# **crypto ca trustpoint cuma-server-id-cert** cuma-asa(config-ca-trustpoint)# **enrollment terminal** cuma-asa(config-ca-trustpoint)# **crypto ca authenticate** cuma-server-id-cert Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself ----BEGIN CERTIFICATE---- ** paste the contents from wordpad ** ----END CERTIFICATE----`
4. CUMA サーバの ASA 自己署名証明書をエクスポートして下さい。 からの認証を Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア必要とするために Cisco Unified Mobility Advantage を設定する必要があります。 必須自己署名証明書を提供するためにこれらのステップを完了して下さい。 これらのステップは ASA で実行される必要があります。New 鍵ペアを作成して下さい:`cuma-asa(config)# **crypto key generate rsa label asa-id-key mod 1024** INFO: The name for the keys will be: asa-id-key Keypair generation process begin. Please wait...`新しいトラストポイントを追加して下さい:`cuma-asa(config)# **crypto ca trustpoint asa-self-signed-id-cert** cuma-asa(config-ca-trustpoint)# **keypair asa-id-key** cuma-asa(config-ca-trustpoint)# **enrollment self**` トラストポイントを登録して下さい:`cuma-asa(config-ca-trustpoint)# **crypto ca enroll asa-self-signed-id-cert** % The fully-qualified domain name in the certificate will be: cuma-asa.cisco.com % Include the device serial number in the subject name? [yes/no]: n Generate Self-Signed Certificate? [yes/no]: y`テキストファイルに認証をエクスポートして下さい。`cuma-asa(config)# **crypto ca export asa-self-signed-id-cert** identity-certificate The PEM encoded identity certificate follows: -----BEGIN CERTIFICATE----- Certificate data omitted -----END CERTIFICATE-----`
5. 前の出力をテキストファイルにコピーし、CUMA サーバ信頼ストアに追加し、このプロシージャを使用して下さい:セキュリティ コンテキスト管理の側の**[+]**選択して下さい。**コンテキストを**『Security』 を選択 して下さい。署名入り認証をインポートするセキュリティ コンテキストの側の**コンテキストを**『Manage』 を選択 して下さい。信頼できる証明書バーで『Import』 を選択 して下さい。認証テキストを貼り付けて下さい。認証を挙げて下さい。『Import』 を選択 して下さい。**注:** リモート宛先 設定に関しては、卓上電話機へのコール 携帯 電話が同時に鳴るかどうか判別するため。 これはモービルが作業を接続すること、そしてリモート宛先 設定においての問題がないことを確認します。

他の認証権限への CUMA 証明書要求の追加を悩まして下さい

問題 1

多くの CUMC/CUMA ソリューションが信頼できる証明書を使用する場合それが助けるデモ/プロトタイプ インストールは*他の認証機関*から自己署名または得られて。 Verisign 認証は高く、これらの認証を得る長い 時間かかります。 それはよいです他の CA からのソリューションサポート自己署名証明書および認証。

サポートされる現在の認証は GeoTrust および Verisign です。 これは Cisco バグ ID CSCta62971 (登録ユーザのみ) で文書化されています

エラー： 不可能接続することが

`https://<host>:8443` ユーザ門脈ページに、たとえばアクセスすることを、試みるとき、`Connect` 現われます。

解決策

この問題は Cisco バグ ID CSCsm26730 （登録ユーザのみ）で文書化されています。 ユーザ門脈ページにアクセスするために、この回避策を完了して下さい:

この問題の原因はドル文字です、従って管理されたサーバの **server.xml ファイル**の別のドル文字が付いているドル文字をエスケープして下さい。 **たとえば**、/opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml を編集して下さい。

行: **keystorePass= " pa$word」**maxSpareThreads="15"

`$$` と `$` 文字を取り替えて下さい。 それは **keystorePass= " pa$$word」**maxSpareThreads="15" のように見えます。

CUMA Admin ポータルのいくつかのページはアクセスが不可能です

これらのページは **CUMA Admin ポータル**で表示することができません:

- アクティブ化/無効にする ユーザ
- 検索/メンテナンス

ユーザが左にメニューの上記の 2 つのページの 1 つをクリックする場合、ブラウザは示すようですページをロードしているが、何も起こらないことを（ブラウザにあった前 ページだけ目に見えます）。

解決策

この問題を解決することはユーザページに関連し、**3268** にアクティブ ディレクトリのために使用されたポートを変更し、CUMA を再起動します。

関連情報

- ASA-CUMA プロキシ ステップバイステップ設定
- Introduccion Al ASR5000 v1
- Cisco Unified Mobility Advantage のアップグレード手順
- **音声に関する技術サポート**
- **音声とユニファイド コミュニケーションに関する製品サポート**
- テクニカルサポートとドキュメント - Cisco Systems