AD証明書サービスを使用したUmbrellaカスタムルート証明書の作成

内容

はじめに

このドキュメントでは、Microsoft Windows Active Directory(AD)証明書サービスを使用してカスタムルート証明書を作成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。

- 現在Microsoftがサポートしている Microsoft Windows Serverのバージョン
- Windows ServerにインストールされたActive Directory証明書サービス
- Active Directory証明書サービスおよびWebサービス/Web登録サービスの役割を持つアカウント
- UTF-8エンコード(「UTF8STRING」)で証明書を発行するように構成された証明書サービス

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

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。

概要

この記事では、Microsoft Windows Active Directory(AD)証明書サービスを使用して、(標準のCisco UmbrellaルートCA証明書の代わりに使用される)カスタムルート証明書を作成し、そのルート証明書を使用してUmbrellaのカスタマーCA署名付きCA証明書機能から証明書署名要求(CSR)に署名する手順について説明します。

証明書文字列のエンコーディング

証明書サービスがデフォルトのエンコーディング(「PRINTABLESTRING」)を使用するように設定されている場合、生成される証明書チェーンは特定のWebクライアント（特にFirefox）によって信頼されません。

Cisco Umbrella Secure Web Gatewayプロキシは、文字列をUTF8STRINGエンコーディングでエンコードする証明書チェーンを使用します。Cisco Umbrella Customers CA中間証明書を作成するためにCSRに署名する発行証明書（ルート証明書など）がPRINTABLESTRINGでエンコードされている場合、Cisco Umbrella Customers CA証明書のSubjectフィールドのエンコードはPRINTABLESTRINGになります。このエンコーディングは、証明書チェーンの次にあるCisco Umbrella R1 CA中間証明書のIssuerフィールドのUTF8STRINGエンコーディングと一致しません。

RFC 5280セクション4.1.2.6では、証明書チェーンで、発行済み証明書のIssuerフィールドと発行済み証明書のSubjectフィールドの間で、同じ文字列エンコーディングを維持することが要求されています。

「証明書のサブジェクトがCAである場合、サブジェクトCAによって発行されるすべての証明書の発行者フィールド（セクション4.1.2.4）でエンコードされるのと同じように、サブジェクトのフィールドをエンコードする必要があります。」

多くのブラウザはこの要件を強制しませんが、一部のブラウザ（特にFirefox）は強制します。その結果、FirefoxなどのWebクライアントは、顧客のCA署名付きCA証明書機能でSecure Web Gateway(SWG)を使用すると、信頼できないサイトのエラーを生成し、Webサイトをロードしない可能性があります。

この問題を回避するには、RFC 5280の要件を適用しないChromeなどのブラウザを使用します。

ステップ1:AD証明書サービステンプレートの準備

1. [スタート] > [ファイル名を指定して実行] > [MMC]の順に移動して、Active Directory証明機関MMCを開きます。

2. File > Add/Remove Snap-inの順に選択し、Certificate TemplatesスナップインとCertification Authorityスナップインを追加します。OKを選択します。

3. Certificate Templatesを展開し、Subordinate Certification Authorityを右クリックします。Duplicate Templateをクリックします。

Umbrellaのドキュメントに記載されている要件に準拠するために、カスタム証明書テンプレート

を作成できるようになりました。

この記事の作成時点で詳細に説明されている要件は次のとおりです。

- [General] タブ
  - テンプレートに、自分にとって意味のある名前を付けます。
  - 有効期間を35か月（3年から1か月）に設定します。
  - 更新期間を20日に設定します。
- [拡張子]タブ
  - Basic Constraintsをダブルクリックします。
    - Make this extension criticalが選択されていることを確認します。
  - Key Usageで次を実行します。
    - Certificate Signing & CRL Signingが選択されていることを確認します。
    - Digital Signatureの選択を解除します。
    - Make this extension criticalも、ここでもチェックが入っていることを確認します。
- Applyを選択して、OKをクリックします。

ステップ2：テンプレートの発行

1. 前のプロセスのステップ2で設定したMMCに戻り、Certificate Authorityセクションを展開します。

2. 新しく展開されたセクションで、Certificate Templatesフォルダを右クリックし、New > Certificate Template to Issueの順に選択します。

3. 新しいウィンドウで、前のセクションで作成した証明書テンプレートの名前を選択し、OKを選択します。

これで、CAは要求を処理する準備ができました。

ステップ3:CSRのダウンロードと署名

1. Umbrellaダッシュボード(https://dashboard.umbrella.com)にログインします。

2. Deployments > Configuration > Root Certificateの順に移動します。

3. 角にある追加(+)アイコンを選択し、新しいウィンドウでCAの名前を指定します。

4. 証明書署名要求(CSR)をダウンロードします。

5. 新しいブラウザタブで、Active Directory証明書サービスのWebサービスに移動します。(ローカルマシンを使用している場合は、127.0.0.1/certsrv/または同様のアドレスになります)。

6. 新しいページでRequest a Certificateを選択します。

7. Advanced Certificate Requestを選択します。

8. 「Saved Request」の下で、手順4でダウンロードしたCSRの内容をコピーして貼り付けます（CSRの内容はテキストエディタで開く必要があります）。

9. 「Certificate Template」で、「Preparing AD Certificate Services Template」セクションで作成した証明書テンプレートの名前を選択し、「Submit」を選択します。

10. Base64 Encodedを選択し、Download Certificateを選択して、.cerファイルの場所をメモします。

ステップ4：署名付きCSR（およびパブリックルート証明書）をアップロードします。

1. Umbrellaダッシュボードで、Deployment > Configuration > Root Certificateの順に移動します。

2. 前のセクションのステップ3で作成したルート証明書を選択します。

3. 行の右下隅で、Upload CAを選択します*。

4. 一番上のBrowseボタン(Certificate Authority (Signed CSR))を選択します。

5. 前のセクションで作成した.cerファイルの場所を参照し、Saveを選択します。

6. Nextを選択し、（シスコルート証明書の代わりに）証明書を使用するコンピュータ/ユーザグループを選択して、Saveを選択します。

* オプションでCA証明書をアップロードすることもできます。この情報は、認証局(CA)サーバのWebインターフェイス(http://127.0.0.1/certsrv/)から取得でき、次にDownload a CA Certificate, Certificate Chain, or CRLを選択します。 画面のプロンプトに従って、Base 64の「Download the CA certificate（CA証明書のダウンロード）」を実行します。

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。