Erstellen eines benutzerdefinierten Umbrella-Stammzertifikats mit AD-Zertifikatdiensten

Inhalt

Einleitung

In diesem Dokument werden Anweisungen zum Erstellen eines benutzerdefinierten Stammzertifikats mithilfe der Microsoft Windows Active Directory (AD)-Zertifikatdienste beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Eine derzeit von Microsoft unterstützte Version von Microsoft Windows Server.
- Auf dem Windows-Server installierte Active Directory-Zertifikatdienste
- Ein Konto mit den Active Directory-Zertifikatdiensten und den Webdienst-/Webregistrierungsdienstrollen
- Zertifikatdienste, die für die Ausgabe von Zertifikaten mit UTF-8-Codierung ("UTF8STRING") konfiguriert sind

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Dieser Artikel enthält Anweisungen zum Erstellen eines benutzerdefinierten Stammzertifikats (das anstelle des standardmäßigen Cisco Umbrella Root CA-Zertifikats verwendet wird) mithilfe der Microsoft Windows Active Directory-Zertifikatdienste und zum anschließenden Verwenden dieses Stammzertifikats zum Signieren einer Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) aus der Funktion Customer CA-signierter Zertifizierungsstellen von Umbrella.

Verschlüsselung der Zertifikatszeichenfolge

Wenn Ihre Zertifikatdienste so konfiguriert sind, dass sie die Standardcodierung ("PRINTABLESTRING") verwenden, kann die erzeugte Zertifikatskette von bestimmten Web-Clients, insbesondere Firefox, nicht als vertrauenswürdig angesehen werden.

Der Cisco Umbrella Secure Web Gateway-Proxy verwendet eine Zertifikatskette, die Zeichenfolgen mit UTF8STRING-Codierung codiert. Wenn Ihr ausstellendes Zertifikat (z. B. Ihr Stammzertifikat), das den CSR signiert, um das Zwischenzertifikat der Cisco Umbrella Customers CA zu erstellen, mit PRINTABLESTRING codiert ist, dann ist die Codierung des Betrefffelds des Zertifikats Cisco Umbrella Customers CA PRINTABLESTRING. Diese Codierung kann nicht mit der UTF8STRING-Codierung des Felds Issuer im Zwischenzertifikat der Cisco Umbrella R1 CA übereinstimmen, das sich in der Zertifikatskette als Nächstes befindet.

Gemäß RFC 5280 Abschnitt 4.1.2.6 muss eine Zertifikatskette die gleiche Zeichenfolgencodierung zwischen dem Ausstellerfeld eines ausgestellten Zertifikats und dem Betreff-Feld im ausstellenden Zertifikat beibehalten:

"Handelt es sich bei dem Antragsteller des Zertifikats um eine Zertifizierungsstelle, MUSS das Antragstellerfeld in allen von der Antragstellerin ausgestellten Zertifikaten genauso codiert sein wie im Feld des Ausstellers (Abschnitt 4.1.2.4)."

Viele Browser erzwingen diese Anforderung nicht, aber einige (insbesondere Firefox) tun es. Daher können Web-Clients wie Firefox einen nicht vertrauenswürdigen Standortfehler generieren und Websites nicht laden, wenn Secure Web Gateway (SWG) mit der vom Kunden CA signierten Zertifizierungsstellenzertifikatfunktion verwendet wird.

Um dieses Problem zu umgehen, verwenden Sie einen Browser wie Chrome, der die Anforderungen von RFC 5280 nicht erzwingt.

Schritt 1: Vorlage für AD-Zertifikatdienste wird vorbereitet

1. Öffnen Sie die MMC der Active Directory-Zertifizierungsstelle, indem Sie zu Start > Ausführen > MMC navigieren.

2. Wählen Sie Datei > Snap-In hinzufügen/entfernen, und fügen Sie die Zertifikatvorlagen und Zertifizierungsstellen-Snap-Ins hinzu. Wählen Sie OK aus.

3. Erweitern Sie Zertifikatvorlagen, und klicken Sie mit der rechten Maustaste auf Untergeordnete Zertifizierungsstelle. Klicken Sie auf Vorlage duplizieren.

Sie können jetzt eine benutzerdefinierte Zertifikatvorlage erstellen, um die in der Umbrella-Dokumentation aufgeführten Anforderungen zu erfüllen.

Dies sind die Anforderungen, die zum Zeitpunkt der Erstellung dieses Artikels detailliert sind:

- Allgemein, Registerkarte
  - Geben Sie der Vorlage einen Namen, der für Sie von Bedeutung ist.
  - Legen Sie den Gültigkeitszeitraum auf 35 Monate (3 Jahre weniger pro Monat) fest.
  - Legen Sie den Verlängerungszeitraum auf 20 Tage fest.
- Registerkarte "Erweiterungen"
  - Doppelklicken Sie auf Basic Constraints (Grundlegende Einschränkungen).
    - Stellen Sie sicher, dass diese Erweiterung als kritisch markiert ist.
  - Unter Schlüsselverwendung:
    - Stellen Sie sicher, dass Zertifikatssignatur & Zertifikatsperrlisten-Signatur ausgewählt sind.
    - Deaktivieren Sie die digitale Signatur.
    - Stellen Sie sicher, dass diese Erweiterung "Kritisch" (Make this extension critical) auch hier aktiviert ist.
- Wählen Sie Übernehmen und OK.

Phase 2: Vorlage erstellen

1. Erweitern Sie in der MMC, die Sie in Schritt 2 des vorherigen Prozesses eingerichtet haben, den Abschnitt Zertifizierungsstelle.

2. Klicken Sie im neuen erweiterten Abschnitt mit der rechten Maustaste auf den Ordner Zertifikatvorlagen, und wählen Sie Neu > Zertifikatvorlage zur Ausgabe aus.

3. Wählen Sie im neuen Fenster den Namen der Zertifikatvorlage aus, die Sie im letzten Abschnitt erstellt haben, und wählen Sie OK.

Die Zertifizierungsstelle ist jetzt bereit, die Anforderung zu vereinfachen.

Schritt 3: Herunterladen und Signieren des CSR

1. Melden Sie sich bei Ihrem Umbrella Dashboard an (https://dashboard.umbrella.com).

2. Navigieren Sie zu Deployments > Configuration > Root Certificate.

3. Wählen Sie in der Ecke das Symbol Hinzufügen (+) aus, und benennen Sie Ihre Zertifizierungsstelle im neuen Fenster.

4. Laden Sie die Zertifikatsanforderung (Certificate Signing Request, CSR) herunter.

5. Navigieren Sie in einer neuen Browserregisterkarte zu Webdiensten für Active Directory-

Zertifikatdienste. (Wenn Sie den lokalen Computer verwenden, lautet die Adresse 127.0.0.1/certsrv/ oder ähnlich.)

6. Wählen Sie auf der neuen Seite Zertifikat anfordern.

7. Wählen Sie Erweiterte Zertifikatanforderung.

8. Kopieren und fügen Sie unter Gespeicherte Anforderung den Inhalt der CSR-Datei ein, die Sie in Schritt 4 heruntergeladen haben (Sie müssen sie mit einem Texteditor öffnen).

9. Wählen Sie unter Zertifikatvorlage den Namen der Zertifikatvorlage aus, die Sie im Abschnitt "Vorbereiten der AD-Zertifikatdienstvorlage" erstellt haben, und wählen Sie Senden aus.

10. Wählen Sie Base64 Encoded aus, wählen Sie Download Certificate aus, und notieren Sie sich den Speicherort der CER-Datei.

Schritt 4: Signierten CSR hochladen (und öffentliches Root-Zertifikat)

1. Navigieren Sie auf Ihrem Umbrella Dashboard zu Bereitstellung > Konfiguration > Root-Zertifikat.

2. Wählen Sie das Stammzertifikat aus, das Sie in Schritt 3 des vorherigen Abschnitts erstellt haben.

3. Wählen Sie CA hochladen unten rechts in der Zeile*.

4. Wählen Sie die obere Schaltfläche Durchsuchen (Zertifizierungsstelle (Signierter CSR)).

5. Navigieren Sie zum Speicherort der CER-Datei, die Sie im vorherigen Abschnitt erstellt haben, und wählen Sie Speichern aus.

6. Wählen Sie Weiter und dann die Gruppen von Computern/Benutzern aus, mit denen das Zertifikat verwendet werden soll (anstelle des Cisco Root-Zertifikats), und wählen Sie Speichern.

* Sie können das CA-Zertifikat auch optional hochladen. Sie können dies über die Webschnittstelle Ihres Zertifizierungsstellen-Servers (http://127.0.0.1/certsrv/) abrufen und dann CA-Zertifikat, Zertifikatskette oder Zertifikatsperrliste herunterladen.Füllen Sie die Eingabeaufforderungen auf dem Bildschirm aus, um das CA-Zertifikat in Base 64 herunterzuladen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.