Aangepast basiscertificaat met AD-certificaatservices maken

Inhoud

Inleiding

In dit document worden instructies beschreven voor het maken van een aangepast hoofdcertificaat met Microsoft Windows Active Directory (AD) Certificate Services.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een versie van Microsoft Windows Server die momenteel wordt ondersteund door Microsoft
- Active Directory Certificate Services geïnstalleerd op de Windows Server
- Een account met de Active Directory Certificate Services en Web Service/Web Enrollment Service-rollen
- Certificaatservices geconfigureerd voor het uitgeven van certificaten met UTF-8-codering ("UTF8STRING")

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Dit artikel bevat instructies voor het maken van een aangepast root-certificaat (dat wordt gebruikt in plaats van het standaard Cisco Umbrella Root CA-certificaat) met behulp van Microsoft Windows Active Directory Certificate Services en vervolgens dat root-certificaat gebruiken om een Certificate Signing Request (CSR) te ondertekenen van de CA-functie voor CA-certificaten van de klant die door de overkoepelende CA is ondertekend.

codering van tekenreeksen voor certificaten

Als uw Certificate Services is geconfigureerd om de standaardcodering ("PRINTABLESTRING") te gebruiken, kan de geproduceerde certificaatketen niet worden vertrouwd door bepaalde webclients, met name Firefox.

De Cisco Umbrella Secure Web Gateway-proxy maakt gebruik van een certificaatketen die tekenreeksen codeert met UTF8STRING-codering. Als het certificaat van afgifte (bijvoorbeeld uw basiscertificaat) dat de CSR ondertekent om het Cisco Umbrella Customers CA intermediate-certificaat te maken, is gecodeerd met PRINTABLESTRING, dan is de codering van het veld Onderwerp van het Cisco Umbrella Customers CA-certificaat PRINTABLESTRING. Deze codering kan niet overeenkomen met de UTF8STRING-codering van het veld Uitgever in het tussenliggende Cisco Umbrella R1 CA-certificaat, dat de volgende is in de certificaatketen.

RFC 5280, punt 4.1.2.6, vereist dat een certificaatketen dezelfde tekenreeks behoudt tussen het veld Uitgever van een afgegeven certificaat en het veld Onderwerp in het certificaat van afgifte:

"Wanneer het onderwerp van het certificaat een CA is, MOET het onderwerpveld op dezelfde manier worden gecodeerd als in het veld van de uitgevende instelling (paragraaf 4.1.2.4) in alle certificaten die door de betreffende CA zijn uitgegeven."

Veel browsers handhaven deze vereiste niet, maar sommige (met name Firefox) doen dat wel. Als gevolg hiervan kunnen webclients zoals Firefox een niet-vertrouwde sitefout genereren en websites niet laden wanneer ze Secure Web Gateway (SWG) gebruiken met de CA-certificeringsfunctie van de klant.

Om dit probleem te omzeilen, gebruikt u een browser zoals Chrome die de eis van RFC 5280 niet afdwingt.

Stap 1: sjabloon voor AD-certificaatservices voorbereiden

1. Open de Active Directory Certification Authority MMC door naar Start > Uitvoeren > MMC te navigeren.

2. Selecteer Bestand > Module toevoegen/verwijderen en voeg de module Certificaatsjablonen en Certificeringsinstantie toe. Selecteer OK.

3. Vouw certificaatsjablonen uit en klik met de rechtermuisknop op Ondergeschikte certificeringsinstantie. Klik op Template dupliceren.

U kunt nu een aangepaste certificaatsjabloon maken om te voldoen aan de vereisten die worden vermeld in de overkoepelende documentatie.

Dit zijn de vereisten die worden beschreven op het moment van de creatie van dit artikel:

- Tabblad Algemeen
  - Geef de template een naam die voor jou betekenis heeft.
  - Stel de geldigheidsperiode in op 35 maanden (3 jaar minder per maand).
  - Stel de verlengingstermijn in op 20 dagen.
- Tabblad Extensies
  - Dubbelklik op Basisbeperkingen.
    - Zorg ervoor dat Deze extensie kritisch maken is geselecteerd.
  - Onder Sleutelgebruik:
    - Zorg ervoor dat Certificaatondertekening & CRL-ondertekening zijn geselecteerd.
    - Schakel Digitale handtekening uit.
    - Zorg ervoor dat Make this extension critical ook hier wordt aangevinkt.
- Selecteer Toepassen en OK

Stap 2: geef de template uit

1. Vouw het gedeelte Certificaatautoriteit uit in de MMC die u in stap 2 van het vorige proces hebt ingesteld.

2. Klik in het onlangs uitgevouwen gedeelte met de rechtermuisknop op de map Certificaatsjablonen en selecteer Nieuw > Te verstrekken certificaatsjabloon.

3. Selecteer in het nieuwe venster de naam van de certificaatsjabloon die u in de laatste sectie hebt gemaakt en selecteer OK.

De CA is nu klaar om het verzoek te vergemakkelijken.

Stap 3: Het downloaden en ondertekenen van de CSR

1. Log in op uw Paraplu Dashboard (https://dashboard.umbrella.com).

2. Ga naar Implementaties > Configuratie > Hoofdcertificaat.

3. Selecteer het pictogram Toevoegen (+) in de hoek en geef uw CA een naam in het nieuwe venster.

4. Download het Certificate Signing Request (CSR).

5. Navigeer in een nieuw browsertabblad naar webservices voor Active Directory Certificate Services. (Als u een lokale machine gebruikt, is dit 127.0.0.1/certsrv/ of vergelijkbaar.)

6. Selecteer op de nieuwe pagina Certificaat aanvragen.

7. Selecteer Geavanceerd certificaatverzoek.

8. Onder Opgeslagen verzoek kopieer en plak de inhoud van de CSR die u in stap 4 hebt gedownload (u moet deze openen met een teksteditor).

9. Selecteer onder Certificaatsjabloon de naam van de certificaatsjabloon die u hebt gemaakt in het gedeelte "Sjabloon voor AD-certificaatservices voorbereiden" en selecteer Indienen.

10. Selecteer Base64 Encoded en selecteer Download Certificate en noteer de locatie van het .cer-bestand.

Stap 4: Upload de ondertekende CSR (en Public Root Cert)

1. Navigeer op uw overkoepelende dashboard naar Implementatie > Configuratie > Hoofdcertificaat.

2. Selecteer het basiscertificaat dat u in stap 3 van de vorige sectie hebt gemaakt.

3. Selecteer CA uploaden rechtsonder in de regel*.

4. Selecteer bovenaan de knop Bladeren (Certificate Authority (Signed CSR)).

5. Blader naar de locatie van het .cer-bestand dat u in de vorige sectie hebt gemaakt en selecteer Opslaan.

6. Selecteer Volgende en selecteer de groepen computers/gebruikers waarmee u het certificaat wilt gebruiken (in plaats van het Cisco-basiscertificaat) en selecteer Opslaan.

*U kunt het CA-certificaat ook optioneel uploaden. Dit kan worden opgehaald via de webinterface van de server van uw certificeringsinstantie (http://127.0.0.1/certsrv/) en vervolgens een CA-certificaat, certificaatketen of CRL downloaden selecteren. Voltooi de aanwijzingen op het scherm om het CA-certificaat te downloaden in Base 64.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.