Generate SHA-256 zelfgetekende certificaten voor Cisco UCCE Web Services

Inhoud

Inleiding

Dit document beschrijft een proces voor het genereren van zelf-ondertekende certificaten met behulp van SHA-256 algoritme voor de ondertekening van certificaten voor Cisco Unified Contact Center Enterprise (UCCE) web services zoals Web Setup of CCE Administration.

Probleem

Cisco UCCE heeft verschillende webservices die worden gehost door Microsoft Internet Information Services (IS) server. Microsoft IS in UCCE-implementatie door standaard gebruik te maken van zelfondertekende certificaten met SHA-1 algoritme voor de handtekening van het certificaat.

Het SHA-1-algoritme wordt door de meeste browsers als onveilig beschouwd en daarom kunnen de kritische tools zoals CCE Administration die door supervisors wordt gebruikt voor het opnieuw scannen van agents niet beschikbaar worden.

Oplossing

De oplossing voor dat probleem is om SHA-256 certificaten voor te gebruiken server te genereren.

> **Waarschuwing**: Aanbevolen wordt om certificaten te gebruiken die door de certificaatinstantie zijn ondertekend. Het genereren van zelfgetekende certificaten, zoals hier beschreven, moet dus worden beschouwd als een tijdelijke tijdelijke tijdelijke oplossing om de service snel te herstellen.

> Opmerking: Indien de ICM-toepassing van de Lijst van de Lijst van de Lijst van Internet wordt gebruikt voor het beheer van het ver script is er een behoefte om SSL Encryption Utility te gebruiken om certificaat voor het te genereren.

Oplossing voor WebexSetup en CCE-beheer

1. Start Windows PowerShell-gereedschap op UCCE server.

2. Type de opdracht in PowerShell

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation
"cert:\LocalMachine\My"
```

Wanneer de parameter na **DnsName** de gemeenschappelijke naam van het certificaat (CN) zal vermelden. Vervang de parameter na DNSName in de juiste voor de server. Het certificaat wordt opgesteld met een geldigheidsduur van één jaar.

> Opmerking: De gemeenschappelijke naam in het certificaat moet Fully Qualified Domain Name (FQDN) van de server overeenkomen.

3. Open Microsoft Management Console (MMC)-gereedschap. Selecteer **Bestand** -> **Magnetisch toevoegen/verwijderen...** -> **Certificaten selecteren**, **Computer-account** kiezen en **toevoegen aan de geselecteerde invoegtoepassingen.** Druk op OK, en navigeer vervolgens naar **console Root** -> **Certificaten (lokale computer)** -> **Persoonlijk** -> **Certificaten**.

Zorg ervoor dat het nieuwe certificaat hier aanwezig is. Het certificaat wordt niet voorzien van een gebruiksvriendelijke naam, zodat het kan worden herkend op basis van de GN-code en de vervaldatum.

De naam van een vriend kan aan het certificaat worden toegewezen door de **eigenschappen van** het certificaat te selecteren en het tekstvak **van** de **vriendschappelijke naam** met de juiste naam te vullen.

4. Start Internet Information Services (IS) Manager. Selecteer IS Standaard Website en kies in het rechtervenster **Bindingen**. Selecteer **HTTPS** -> **Bewerken** en selecteer vanuit de SSL-certificaatlijst de optie Automatisch getekend SHA-256 gegenereerd certificaat.

5. Start de wereldwijd gepubliceerde dienst voor het Web opnieuw.

Oplossing voor diagnostisch framework Portico

1. Herhaal de stappen 1-3.

Er wordt een nieuw zichzelf ondertekend certificaat gegenereerd. Voor het gereedschap Portico is er een andere manier om het certificaat te binden.

2. Verwijder de huidige certificaatbinding voor Portico.

```
cd c:\icm\serviceability\diagnostics\bin

DiagFwCertMgr /task:UnbindCert
```

3. Bind het voor Portico gegenereerde zelfgetekende certificaat.

Open het zelf-ondertekende certificaat dat voor het gereedschap Portico is gegenereerd en selecteer het tabblad **Details**. Kopieert de Thumbprint waarde naar de teksteditor.

Opmerking: In sommige tekstredacteuren wordt de thumbnail automatisch met een vraagteken voorgezet. Verwijder het.

Verwijder alle ruimtetekens uit de thumbnail en gebruik deze in de volgende opdracht.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:
```

4. Zorg ervoor dat de certificatenbinding met deze opdracht succesvol was.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Een soortgelijk bericht moet in de output worden weergegeven.
"De certificatenbinding is GELDIG"

5. Start de diagnostische kaderdienst opnieuw.

```
sc stop "diagfwsvc"
sc start "diagfwsvc"
```

Verificatie

Schakel de browser cache en geschiedenis uit. Toegang tot de website van de Dienst van het CCE van het Beheer en u zou een zelfgetekende certificaatwaarschuwing moeten krijgen.

Bekijk de certificeringsgegevens en zorg ervoor dat het certificaat een SHA-256-algoritme voor de handtekening van het certificaat heeft.

Verwante artikelen

CA-ondertekend certificaat voor UCCE diagnostisch portoprogramma genereren

CA-ondertekend certificaat voor UCCE Web Setup genereren

CA-ondertekend certificaat voor VOS-gebaseerde server genereren met CLI

CA-ondertekend certificaat voor CVP OAMP-server genereren