Genera certificati autofirmati SHA-256 per i servizi Web Cisco UCCE

Sommario

[Introduzione](#)
[Problema](#)
[Soluzione](#)
[Soluzione per l'amministrazione di WebSetup e CCE](#)
[Soluzione per Diagnostic Framework Portico](#)
[Verifica](#)
[Articoli correlati](#)

Introduzione

In questo documento viene descritto un processo di generazione di certificati autofirmati utilizzando l'algoritmo di firma del certificato SHA-256 per i servizi Web Cisco Unified Contact Center Enterprise (UCCE), ad esempio Installazione Web o Amministrazione CCE.

Problema

Cisco UCCE dispone di diversi servizi Web ospitati dal server Microsoft Internet Information Services (IIS). Per impostazione predefinita, Microsoft IIS nella distribuzione UCCE utilizza certificati autofirmati con algoritmo di firma del certificato SHA-1.

L'algoritmo SHA-1 è considerato non sicuro dalla maggior parte dei browser, pertanto a un certo punto strumenti critici come l'amministrazione CCE utilizzati dai supervisori per la riqualificazione degli agenti potrebbero non essere disponibili.

Soluzione

Per risolvere il problema, generare certificati SHA-256 per l'utilizzo da parte del server IIS.

> **Avviso:** È consigliabile utilizzare certificati firmati da Autorità di certificazione. Pertanto, la generazione dei certificati autofirmati descritti in questo documento deve essere considerata una soluzione temporanea per ripristinare rapidamente il servizio.

> **Nota:** Se per la gestione remota degli script viene utilizzata l'applicazione ICM Internet Script Editor, è necessario utilizzare l'utilità di crittografia SSL per generare il relativo certificato.

Soluzione per l'amministrazione di WebSetup e CCE

1. Avviare lo strumento Windows PowerShell nel server UCCE.

2. In PowerShell digitare il comando

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

Dove il parametro dopo **DnsName** specificherà il nome comune del certificato (CN). Sostituire il parametro dopo DnsName con quello corretto per il server. Il certificato verrà generato con una validità di un anno.

> **Nota:** Il nome comune nel certificato deve corrispondere al nome di dominio completo (FQDN) del server.

3. Aprire lo strumento Microsoft Management Console (MMC). Selezionare File -> **Aggiungi/Rimuovi snap-in...** -> selezionare **Certificati**, scegliere **Account computer** e **aggiungerlo** agli snap-in selezionati. Fare clic su OK, quindi selezionare **Console Root** -> **Certificates (Local Computer)** -> **Personal** -> **Certificates**.

Verificare che il certificato appena creato sia presente in questo punto. Per il certificato non verrà configurato un nome descrittivo, pertanto sarà possibile riconoscerlo in base al CN e alla data di scadenza.

Èpossibile assegnare un nome descrittivo al certificato selezionando le **proprietà** del certificato e immettendo il nome appropriato nella casella di testo **Nome descrittivo**.

4. Avviare Gestione Internet Information Services (IIS). Selezionare Sito Web predefinito IIS e nel riquadro di destra scegliere **Associazioni**. Selezionare **HTTPS** -> **Edit** (Modifica) e dall'elenco dei certificati SSL selezionare il certificato generato autofirmato SHA-256.

5. Riavviare il servizio "Pubblicazione sul Web".

Soluzione per Diagnostic Framework Portico

1. Ripetere i punti 1-3.

Verrà generato un nuovo certificato autofirmato. Per lo strumento Portico è disponibile un altro modo per associare il certificato.

2. Rimuovere il binding del certificato corrente per lo strumento Portico.

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

DiagFwCertMgr /task:UnbindCert
```

3. Associare il certificato autofirmato generato per Portico.

Aprire il certificato autofirmato generato per lo strumento Portico e selezionare la scheda **Dettagli**. Copiare il valore dell'identificazione personale nell'editor di testo.

> **Nota:** In alcuni editor di testo l'identificazione digitale viene anteposta automaticamente a un punto interrogativo. Rimuovilo.

Rimuovere tutti i caratteri di spazio dall'identificazione personale e utilizzarli nel comando seguente.

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

4. Verificare che il binding dei certificati sia riuscito utilizzando questo comando.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Nell'output dovrebbe essere visualizzato un messaggio simile.
"Il binding del certificato è VALIDO"

5. Riavviare il servizio Framework di diagnostica.

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

Verifica

Cancella la cache e la cronologia del browser. Accedere alla pagina Web del servizio di amministrazione CCE e visualizzare un avviso di certificato autofirmato.

Visualizzare i dettagli del certificato e verificare che il certificato disponga dell'algoritmo di firma del certificato SHA-256.

Articoli correlati

Genera certificato firmato CA per lo strumento di diagnostica Portico UCCE

Genera certificato firmato CA per installazione Web UCCE

Genera certificato firmato CA per server basato su VOS tramite CLI

Genera certificato CA firmato per il server CVP OAMP