Procedure om ondersteuning van TLS 1.2 voor CVP Call Studio-webservices mogelijk te maken

Inhoud

Inleiding

Dit document beschrijft hoe u TLS 1.2-ondersteuning voor Cisco Customer Voice Portal (CVP) Call Studio Services kunt inschakelen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CVP Call Studio
- Transport Layer Security (TLS)
- JavaRuntinme (JRE)

De informatie in dit document is gebaseerd op deze softwareversies:

- CVP-server 11.5
- CVP Call Studio 11.5

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleemsamenvatting

In Call Studio Web Service Element wordt TLS 1.0 onderhandeld zelfs als de Web Service Server TLS1.2 ondersteunt.

Mogelijke oorzaken

JRE 7 gebruikt standaard TLS1.0.

Aanbevolen actie

Installeer de pleister CVP 10.5 - ES24 (afgekeurd) en ES26, CVP 11.0 - ES23, CVP 11.5 - ES7 voor Unified CVP release 10.5, 11.0 respectievelijk 11.5.

Deze patch dwingt Java om de context voor TLS 1.2 in te stellen, zodat alle uitgaande https-verzoeken van CVP TLS 1.2 zullen gebruiken.

> Opmerking: Dit defect CSCvc39129 werd voor de uitgifte geopend.