Verfahren zur Aktivierung der TLS 1.2-Unterstützung für CVP Call Studio Web Services

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Problemübersicht](#)
[Mögliche Ursachen](#)
[Empfohlene Maßnahmen](#)

Einführung

In diesem Dokument wird beschrieben, wie die Unterstützung von TLS 1.2 für Cisco Customer Voice Portal (CVP) Call Studio Web Services aktiviert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CVP Call Studio
- Transport Layer Security (TLS)
- Java Runtinme Environment (JRE)

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- CVP-Server 11.5
- CVP Call Studio 11.5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problemübersicht

In Call Studio-Webdienstelement wird TLS 1.0 ausgehandelt, selbst wenn der Webdienstserver TLS1.2 unterstützt.

Mögliche Ursachen

JRE 7 verwendet standardmäßig TLS1.0.

Empfohlene Maßnahmen

Installieren Sie Patch CVP 10.5 - ES24 (veraltet) und ES26, CVP 11.0 - ES23, CVP 11.5 - ES7 für Unified CVP Release 10.5, 11.0 bzw. 11.5.

Dieser Patch zwingt Java, den Kontext für TLS 1.2 festzulegen, sodass alle ausgehenden HTTPS-Anfragen von CVP TLS 1.2 verwenden.

> **Hinweis**: Dieser Fehler CSCvc39129 wurde wegen des Problems geöffnet.