

Procedimiento para habilitar el soporte de TLS 1.2 para los servicios web del estudio de la llamada del CVP

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Resumen de problemas](#)

[Posibles Causas](#)

[Acción Recomendada](#)

Introducción

Este documento describe cómo habilitar el soporte de TLS 1.2 para los servicios web porta del estudio de la llamada de la Voz de cliente de Cisco (CVP).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Estudio de la llamada del CVP
- Transport Layer Security (TLS)
- Entorno de Runtinme de las Javas (JRE)

La información que contiene este documento se basa en estas versiones de software:

- Servidor 11.5 del CVP
- Estudio 11.5 de la llamada del CVP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Resumen de problemas

En el elemento de servicio web del estudio de la llamada, se negocia el TLS1.0 incluso si los soportes de servidor TLS1.2 del servicio web.

Posibles Causas

Aplicaciones TLS1.0 JRE 7 por abandono.

Acción Recomendada

Instale el CVP 10.5 de la corrección – ES24 (desaprobado) y ES26, CVP 11.0 – ES23, CVP 11.5 – ES7 para la versión unificada 10.5, 11.0 y 11.5 del CVP respectivamente.

Esta corrección fuerza las Javas para fijar el contexto para TLS 1.2, así que todas las peticiones salientes del https del CVP utilizarán TLS 1.2.

Note: Este defecto [CSCvc39129was](#) abierto para el problema.