Resolver problemas de conectividad del agente de cowork (Frontier) cuando Umbrella está habilitado

Contenido

Problema

El agente Cowork (Frontier) no funcionaba correctamente en los portátiles cuando se habilitó Cisco Umbrella. Cuando Cisco Umbrella estaba inactivo, el agente funcionaba como se esperaba. Los usuarios no pudieron utilizar la funcionalidad de agente de Cowork cuando Umbrella estaba activo y no se veían registros de bloques en Cisco Umbrella cuando los usuarios experimentaron este problema. Se proporcionaron capturas de pantalla de error que mostraban los errores de la aplicación durante el funcionamiento de Umbrella.

Entorno

- Cisco Umbrella implementado en portátiles empresariales
- Aplicación de agente Cowork (Frontier)
- Inspección de tráfico SSL/TLS habilitada en Cisco Umbrella
- Asignación de certificados implementada en la aplicación Cowork

Resolución

El problema se resolvió agregando la aplicación Cowork a la lista No descifrar (NoMIsta) en Cisco Umbrella. Este cambio de configuración permite al agente de Cowork omitir la inspección SSL/TLS y mantener su conexión directa cifrada con los servidores de Cowork.

Pasos para configurar la lista DND

Paso 1: Acceda al panel de Cisco Umbrella y navegue hasta la configuración de la política de descifrado SSL.

Paso 2: Agregue dominios relacionados con la colaboración y URL a la lista No descifrar para omitir la inspección SSL para esta aplicación.

Paso 3: Aplique los cambios de política y deje tiempo para que la configuración se propague a todos los terminales.

Paso 4: Pruebe la funcionalidad del agente Cowork con Cisco Umbrella habilitado para verificar el funcionamiento correcto.

Validación

Después de implementar la configuración de la lista DND, la aplicación Cowork funcionó normalmente con Cisco Umbrella activado. Las pruebas internas confirmaron que el problema no se reprodujo durante varios días de supervisión, y todos los usuarios pudieron acceder a la funcionalidad de Cowork como se esperaba.

Causa

El agente Cowork (Frontier) utiliza la fijación de certificados como mecanismo de seguridad. La fijación de certificados significa que la aplicación está codificada para aceptar y confiar únicamente en su propio certificado de servidor específico. Cuando Cisco Umbrella intercepta el tráfico y presenta el certificado de Cisco en lugar del certificado de servidor original, la aplicación Cowork detecta este cambio, asume que la conexión no es segura y descarta intencionadamente la conexión para proteger los datos. Este es el comportamiento esperado para las aplicaciones que implementan medidas de seguridad de fijación de certificados.

Contenido relacionado

- Crear lista efectiva de no descifrado para aplicaciones de Microsoft
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).