# Resolución de DNS de ZTNA de cliente seguro y pérdida de conectividad después de la hibernación de macOS

## Contenido

## Problema

Cisco SecureClient ZTNA en los terminales macOS experimenta una falla de resolución DNS y una pérdida de conectividad ZTA después de que el sistema se reanude del modo de suspensión o hibernación. Este problema afecta a las funciones ZTNA IA (Acceso de identidad) y ZTNA PA (Acceso privado). Mientras la conectividad IP básica sigue funcionando (el ping ICMP a direcciones IP externas como 8.8.8.8 y 208.67.222.222 funciona correctamente), la resolución de nombres DNS falla completamente, lo que impide el acceso a los recursos de Internet y a los recursos privados configurados a través de ZTNA.

Los síntomas específicos observados incluyen:

- Las búsquedas de DNS fallan con los comandos nslookup (como nslookup de www.cisco.com vía 8.8.8.8 y 208.67.222.222 no funciona).
- Las conexiones ZTNA IA y ZTNA PA dejan de estar disponibles.
- Este problema se produce de forma coherente tras los ciclos de hibernación y activación del terminal.
- El problema también puede ocurrir aleatoriamente mientras el dispositivo está en uso activo.
- Si se elimina el proceso ZTNA, se produce un reinicio inmediato, pero el problema de conectividad suele persistir.
- Sólo un reinicio completo del sistema restaura la resolución DNS completa y la conectividad ZTNA.

## Entorno

- Sistema operativo: macOS (versión 26.3 documentada en este caso)
- Cisco SecureClient: Versión 5.1.14.x (versiones afectadas anteriores a 5.1.16)
- Módulo ZTNA: Activo con configuraciones de acceso de identidad (IA) y acceso privado (PA)
- Supervisión de redes: Puede incluir soluciones de seguridad de terceros como Sentinel One
- Software de seguridad adicional: Puede incluir Cisco Secure Endpoint
- Servidores DNS: Servidores DNS externos (8.8.8.8, 208.67.222.222) accesibles a través de ICMP pero la resolución DNS falla
- Módulo UMB: No está en uso

# Resolución

El problema se resolvió mediante una solución de software proporcionada por el departamento de ingeniería de Cisco. El proceso de resolución implicó los pasos descritos en las siguientes secciones.

## Paso 1: Identificación de problemas y seguimiento de errores

El Departamento de Ingeniería de Cisco identificó este defecto como un defecto conocido y lo registró con la ID de error de funcionamiento CSCwt24392 de Cisco con la descripción "macOS: DNS deja de funcionar con ZTA SIA-all y NVM activo".

## Paso 2: Recopilación de datos de diagnóstico

Esta información de diagnóstico fue recolectada para apoyar el análisis de ingeniería:

- Paquetes DART (herramienta de diagnóstico e informes) de los terminales afectados.
- Archivos de captura de paquetes (ZTNA Issue1.pcapng).
- Capturas de pantalla que demuestran el fallo de conectividad.

- Grabaciones de pantalla que muestran la reproducción del problema.
- Registros de interacción del proceso que muestran el comportamiento del proceso com.cisco.secureclient.zta.app.service y extensión del sistema.

## Paso 3: Desarrollo de corrección de ingeniería

Cisco Engineering desarrolló una corrección específica para CSCwt24392 y la incluyó en SecureClient versión 5.1.16. La corrección aborda específicamente la falla de resolución de DNS que ocurre cuando ZTA SIA-all y NVM están activos en los sistemas macOS después de los ciclos de suspensión/hibernación.

## Paso 4: Instalación de actualización de software

Instale Cisco SecureClient versión 5.1.16 o posterior en los terminales macOS afectados. Esta versión contiene la corrección para la resolución de DNS y los problemas de conectividad ZTA.

## Paso 5: Pruebas de validación

Después de instalar SecureClient 5.1.16, realice estos pasos de validación:

1.- Permitir que el terminal macOS entre en modo de hibernación o suspensión.

2.- Reactivar el sistema de la suspensión o hibernación.

3.- Probar la resolución de DNS usando los comandos nslookup.

4.- Verificar la conectividad ZTNA IA y ZTNA PA con los recursos configurados.

5.- Confirmar que tanto el acceso a internet como el acceso a recursos privados funcionan correctamente sin que sea necesario reiniciar el sistema.

### Solución alternativa para versiones anteriores

Para entornos en los que no es posible la actualización inmediata a SecureClient 5.1.16, se puede utilizar esta solución temporal:

- Realice un reinicio completo del sistema después de cada ciclo de suspensión/hibernación para restaurar la resolución DNS y la conectividad ZTNA.
- Considere la posibilidad de anular la inscripción en ZTNA temporalmente si el problema de suspensión/hibernación afecta significativamente a la productividad (tenga en cuenta que esto elimina la protección ZTNA).

## Causa

La causa raíz de este problema es un defecto de software en las versiones de Cisco SecureClient anteriores a la 5.1.16, rastreado específicamente como ID de bug de Cisco CSCwt24392. El defecto ocurre cuando los componentes ZTA (acceso de confianza cero) SIA-all (acceso seguro a Internet) y NVM (módulo de visibilidad de red) están activos en los sistemas macOS. Durante el ciclo de hibernación y reactivación, estos componentes no pueden restaurar correctamente la funcionalidad de resolución DNS, al tiempo que mantienen la conectividad IP básica. Esto crea un estado donde el tráfico ICMP (ping) funciona normalmente, pero las consultas DNS fallan, bloqueando de manera efectiva el acceso a los recursos de Internet y a los recursos privados protegidos por ZTNA. El problema implica una interacción incorrecta entre el proceso com.cisco.secureclient.zta.app.service y el proceso de extensión del sistema durante las transiciones de estado del sistema.

## Contenido relacionado

- ID de bug de Cisco CSCwt24392 - macOS: DNS deja de funcionar con ZTA SIA-all y NVM activos
- 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).