

Résolution DNS ZTNA du client sécurisé et perte de connectivité après la mise en veille prolongée macOS

Table des matières

Problème

Cisco SecureClient ZTNA sur les terminaux macOS connaît une défaillance de résolution DNS et une perte de connectivité ZTA après la reprise du système en mode veille ou hibernation. Ce problème concerne les fonctionnalités ZTNA IA (Identity Access) et ZTNA PA (Private Access). Bien que la connectivité IP de base reste fonctionnelle (la requête ping ICMP vers les adresses IP externes telles que 8.8.8.8 et 208.67.222.222 fonctionne correctement), la résolution de noms DNS échoue complètement, empêchant l'accès aux ressources Internet et aux ressources privées configurées via ZTNA.

Les symptômes spécifiques observés sont les suivants :

- Les recherches DNS échouent en utilisant les commandes nslookup (comme nslookup de www.cisco.com via 8.8.8.8 et 208.67.222.222 ne fonctionne pas).
- Les connexions ZTNA IA et ZTNA PA deviennent indisponibles.
- Le problème se produit régulièrement après les cycles de veille et de veille prolongée des terminaux.
- Le problème peut également se produire de manière aléatoire lorsque le périphérique est en cours d'utilisation.
- La suppression du processus ZTNA entraîne un redémarrage immédiat, mais le problème de connectivité persiste généralement.
- Seul un redémarrage complet du système restaure la résolution DNS complète et la connectivité ZTNA.

Environnement

- Système d'exploitation : macOS (version 26.3 documentée dans le cas)
- Cisco SecureClient : Version 5.1.14.x (versions affectées antérieures à 5.1.16)
- Module ZTNA : Actif avec les configurations d'accès aux identités (IA) et d'accès privé (PA)
- Surveillance du réseau : Peut inclure des solutions de sécurité tierces telles que Sentinel One
- Logiciels de sécurité supplémentaires : Peut inclure Cisco Secure Endpoint
- Serveurs DNS : Serveurs DNS externes (8.8.8.8, 208.67.222.222) accessibles via ICMP, mais la résolution DNS échoue
- Module UMB : Non utilisé

Résolution

Le problème a été résolu par le biais d'un correctif logiciel fourni par Cisco Engineering. Le processus de résolution comprenait les étapes décrites dans les sections suivantes.

Étape 1: Identification des problèmes et suivi des bogues

Cisco Engineering l'a identifié comme un défaut connu et l'a consigné sous l'ID de bogue Cisco CSCwt24392 avec la description « macOS: DNS cesse de fonctionner avec ZTA SIA-all et NVM active.

Étape 2: Collecte des données de diagnostic

Ces informations de diagnostic ont été collectées pour soutenir l'analyse technique :

- Ensembles DART (Diagnostic and Reporting Tool) à partir des terminaux affectés.
- Fichiers de capture de paquets (ZTNA Issue1.pcapng).
- Captures d'écran illustrant l'échec de connectivité.
- Enregistrements d'écran montrant la reproduction du problème.

- Journaux d'interaction du processus montrant le comportement du processus d'extension du système et `com.cisco.secureclient.zta.app.service`.

Étape 3: Développement de solutions techniques

Cisco Engineering a développé un correctif ciblé pour CSCwt24392 et l'a inclus dans la version 5.1.16 de SecureClient. Le correctif concerne spécifiquement l'échec de résolution DNS qui se produit lorsque ZTA SIA-all et NVM sont actifs sur les systèmes macOS après les cycles de veille/hibernation.

Étape 4: Installation des mises à jour logicielles

Installez Cisco SecureClient version 5.1.16 ou ultérieure sur les terminaux macOS concernés. Cette version contient le correctif pour les problèmes de résolution DNS et de connectivité ZTA.

Étape 5: Test de validation

Après avoir installé SecureClient 5.1.16, effectuez les étapes de validation suivantes :

- 1.- Autorisez le terminal macOS à passer en mode veille ou hibernation.
- 2.- Mettre le système en veille ou en veille prolongée.
- 3.- Testez la résolution DNS à l'aide des commandes `nslookup`.
- 4.- Vérifiez la connectivité des ZTNA IA et ZTNA PA aux ressources configurées.
- 5.- Vérifiez que l'accès à Internet et l'accès aux ressources privées fonctionnent correctement sans nécessiter de redémarrage du système.

Solution pour les versions antérieures

Pour les environnements où une mise à niveau immédiate vers SecureClient 5.1.16 n'est pas possible, cette solution de contournement temporaire peut être utilisée :

- Effectuez un redémarrage complet du système après chaque cycle de veille/hibernation pour restaurer la résolution DNS et la connectivité ZTNA.
- Envisagez de vous désinscrire temporairement de ZTNA si le problème de veille/hibernation affecte considérablement la productivité (notez que cela supprime la protection ZTNA).

Motif

La cause principale de ce problème est un défaut logiciel dans les versions de Cisco SecureClient antérieures à la version 5.1.16, spécifiquement suivi sous l'ID de bogue Cisco CSCwt24392. Le défaut se produit lorsque les composants ZTA (Zero Trust Access) SIA-all (Secure Internet Access) et NVM (Network Visibility Module) sont actifs sur les systèmes macOS. Pendant le cycle de veille ou de veille prolongée et de réveil, ces composants ne parviennent pas à restaurer correctement la fonctionnalité de résolution DNS, tout en conservant la connectivité IP de base. Cela crée un état dans lequel le trafic ICMP (ping) fonctionne normalement, mais les requêtes DNS échouent, bloquant ainsi l'accès aux ressources Internet et aux ressources privées protégées par ZTNA. Le problème implique une interaction incorrecte entre le processus `com.cisco.secureclient.zta.app.service` et le processus d'extension du système lors des transitions d'état du système.

Autres informations utiles

- ID de bogue Cisco CSCwt24392 - macOS : DNS cesse de fonctionner avec ZTA SIA-all et NVM actifs
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.