

# Résolution des ID de périphériques ZTNA dupliqués dans les déploiements d'accès sécurisé à l'aide des images SysPrep Golden

## Table des matières

---

---

## Problème

Plusieurs machines physiques Windows déployées à partir d'une image SysPrep Gold génèrent des ID de périphérique ZTNA identiques, en particulier le même `ztnaDeviceId` sur plusieurs points d'extrémité. Cette duplication pose plusieurs problèmes critiques :

- Réinscription répétée de périphériques avec le même ID de périphérique ZTNA
- Remplacement de la clé publique lors de chaque processus de réinscription
- Échecs de contrôle de position sur toutes les machines, à l'exception du dernier périphérique inscrit
- Échecs d'accès via Secure Access pour les terminaux affectés

Le comportement observé se produit lorsque plusieurs machines de la flotte partagent le même ID de périphérique ZTNA, ce qui entraîne l'écrasement de la clé publique de la machine précédente par chaque inscription. Toutes les machines, à l'exception de la dernière à inscrire, ne parviennent pas à envoyer des contrôles de position, ce qui entraîne un refus d'accès via l'infrastructure d'accès sécurisé.

Plusieurs paires de noms d'hôte et d'ID utilisateur ont été identifiées comme étant liées au même ID de périphérique ZTNA, ce qui démontre l'étendue du problème de duplication à travers le déploiement.

## Environnement

- Cisco Secure Access (implémentation ZTNA)

- Machines physiques Windows (pas les machines virtuelles)
- Méthodologie de déploiement d'images SysPrep
- Outils Windows ADK (Assessment and Deployment Kit) pour le déploiement d'images
- Format de fichier ESD (Electronic Software Delivery) pour la capture d'images
- Processus de renforcement du système d'exploitation normalisé avec installation logicielle obligatoire
- Configuration standard des comptes administrateur local et invité

## Résolution

Le processus de résolution comprenait une analyse exhaustive des journaux et l'identification de la cause première par une enquête détaillée.

### Identification et résolution de la cause première

L'enquête a révélé que le processus SysPrep ne générait pas correctement des identifiants de périphérique uniques pendant le déploiement de l'image en or.

L'analyse a comporté :

Examen des clés de registre Windows, en particulier :

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion`

Collecte des informations d'identificateur de sécurité utilisateur à l'aide :

`whoami /user`

La résolution nécessitait de modifier le processus SysPrep pour garantir que les identifiants spécifiques aux périphériques soient correctement régénérés pendant le déploiement, empêchant

la duplication des ID de périphériques ZTNA sur plusieurs machines physiques.

- Le renouvellement d'UDID en exécutant la commande `dartcli.exe -nu` modifie la valeur de Nounce sous le chemin d'accès du Registre « `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails` ».
- La suppression du fichier JSON de `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments` et le redémarrage du service ZTA désinscrit l'utilisateur. Vous devez inscrire manuellement l'utilisateur. Ceci génère un nouveau fichier JSON sans aucun autre impact.
- Le renouvellement d'UDID sur tous les terminaux ne doit avoir aucun impact tant que la valeur n'est pas vérifiée/évaluée sur aucun serveur.

1. Lancez l'invite de commandes en tant qu'administrateur et accédez au répertoire « `%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART` ».

2. Exécutez `dartcli.exe -u` pour vérifier la valeur de l'UDID actuel.

3. Exécutez la commande `dartcli.exe -nu`. Cette commande renouvelle l'UDID.

4. Vérifiez la nouvelle valeur en répétant la commande à l'étape 2.

5. Supprimer le fichier JSON du répertoire `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments`

6. Redémarrez les services VPN et ZTA. À ce stade, ZTA doit être à l'état non inscrit.

7. Permettre à l'utilisateur d'inscrire manuellement le ZTA

9. Vérifiez la valeur de `new ztnaDeviceId` dans le fichier JSON.

## Surveillance et validation

Après la mise en oeuvre des mesures correctives pour garantir la génération unique d'ID de périphérique ZTNA :

- Surveillance du processus d'inscription sur plusieurs machines
- Vérifiez que chaque ordinateur a généré des ID de périphérique ZTNA uniques - effectué
- Confirmation de la fonctionnalité de contrôle de position sur tous les périphériques inscrits
- Validation de la suppression des remplacements de clés publiques lors de l'inscription

## Motif

La cause principale a été identifiée comme étant le processus de déploiement de l'image d'or SysPrep ne générant pas correctement des identifiants de périphérique uniques pour l'inscription ZTNA. Lorsque plusieurs machines physiques Windows sont déployées à partir de la même image SysPrep, certains identificateurs spécifiques au périphérique utilisés pour générer l'ID de périphérique ZTNA restent identiques sur toutes les machines déployées.

Le processus SysPrep, bien qu'il soit efficace pour standardiser la configuration du système d'exploitation et le déploiement de logiciels, n'a pas été configuré pour régénérer les identifiants spécifiques que le client sécurisé Cisco utilise pour créer des ID de périphérique ZTNA uniques. Toutes les machines déployées à partir de la même image en or héritent de paramètres d'identification de périphérique ZTNA identiques, ce qui entraîne des conflits d'inscription et des échecs d'authentification dans l'infrastructure d'accès sécurisé.

## Autres informations utiles

- [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.