Dépannage et collecte des informations de base pour l'équipe d'assistance Secure Access

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Localisez L'ID De L'Organisation Secure Access
- Outil Cisco Secure Client Diagnostic and Reporting Tool (DART)
- Activer les journaux de débogage pour les modules ZTNA et SWG
  - Activer les journaux de débogage pour ZTNA
  - Activer les journaux de débogage pour SWG
  - Activer les journaux de débogage pour DUO
- Collecter les journaux KDF pour les modules ZTNA et SWG, DNS (Windows)
  - Conditions préalables
- Captures d'archives HTTP (HAR)
- Captures de paquets
- Sortie du débogage de stratégie
- Commandes courantes Dépannage d'un tunnel de site à site
- Commandes courantes Dépannage du connecteur de ressources
- Télécharger les résultats dans la demande de service d'assistance Cisco
- Informations connexes

Introduction

Ce document décrit les informations de base à collecter lors de l'utilisation de l'équipe d'assistance Cisco Secure Access

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé Cisco
- Client sécurisé Cisco
- Captures de paquets via Wireshark et tcpdump

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lorsque vous travaillez sur Cisco Secure Access, vous pouvez rencontrer des problèmes pour lesquels vous devez contacter l'équipe d'assistance Cisco, ou vous souhaitez effectuer une enquête de base sur le problème et essayer de parcourir les journaux et de localiser le problème. Cet article explique comment collecter les journaux de dépannage de base relatifs à l'accès sécurisé. notez que toutes les étapes ne s'appliquent pas à chaque scénario.

Localisez L'ID De L'Organisation Secure Access

Afin que l'Ingénieur Cisco puisse localiser votre compte, fournissez l'ID de votre organisation qui se trouve dans l'URL une fois que vous êtes connecté au Tableau de bord d'accès sécurisé.

Étapes de recherche de l'ID d'organisation :

1. Connectez-vous à sse.cisco.com
2. Si vous avez plusieurs organisations, passez à la bonne.
3. L'ID de l'organisation se trouve dans l'URL de ce modèle :
https://dashboard.sse.cisco.com/org/{7_digit_org_id}/présentation

Outil Cisco Secure Client Diagnostic and Reporting Tool (DART)

Cisco Secure Client Diagnostic and Reporting Tool (DART) est un outil installé avec le package Secure Client, qui permet de collecter des informations importantes sur le terminal utilisateur.

Exemple d'informations collectées par le bundle DART :

- Journaux ZTNA
- Journaux clients sécurisés et informations de profil
- Informations système
- Autres journaux des modules complémentaires ou des modules d'extension du client sécurisé installés sur

Instructions pour la collecte de DART :

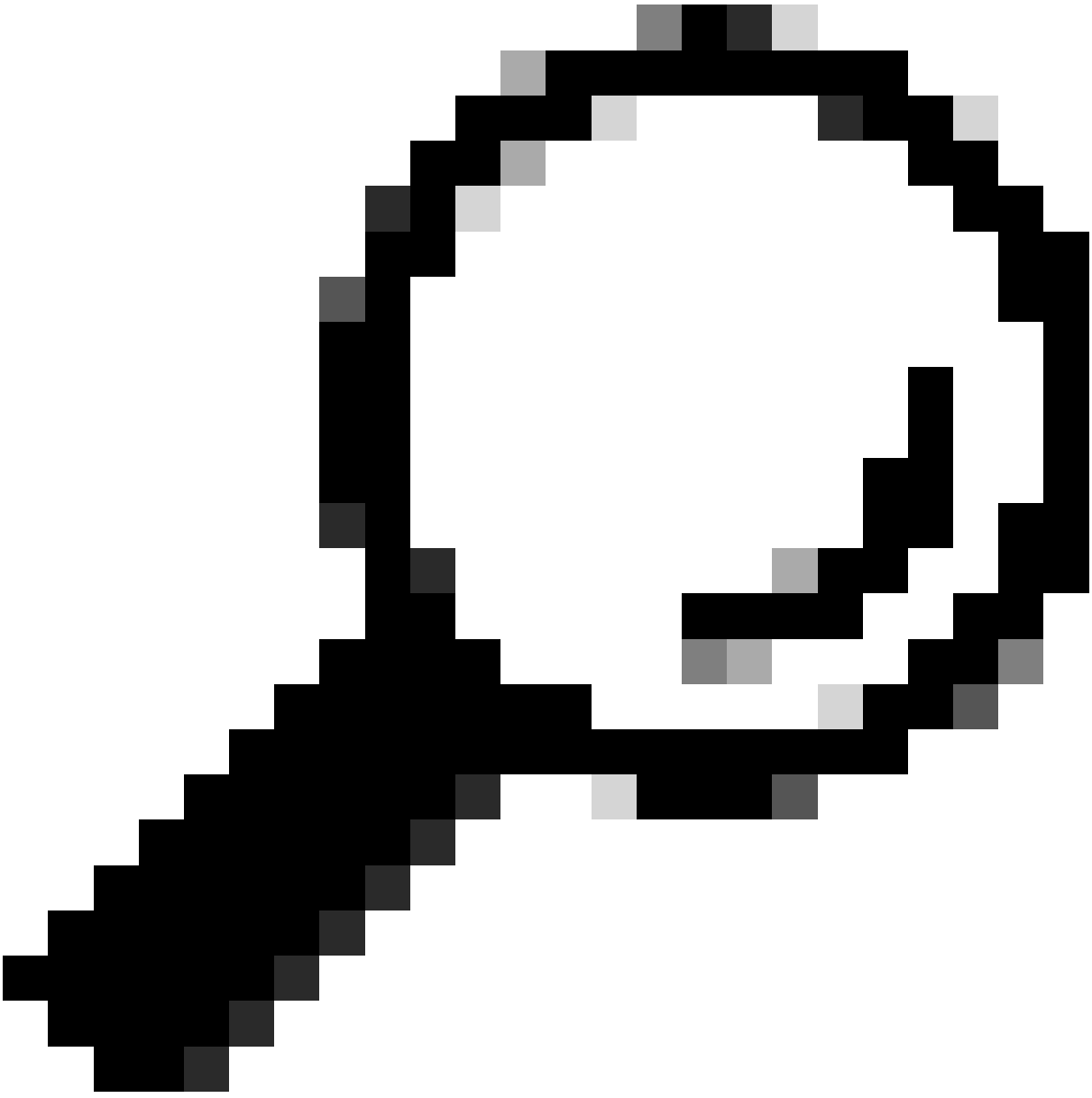
Étape 1 : lancement de DART

1. Pour un ordinateur Windows, lancez le client sécurisé Cisco.
2. Pour un ordinateur Linux, choisissez **Applications** > **Internet** > **Cisco DART**ou /opt/cisco/anyconnect/dart/dartui.

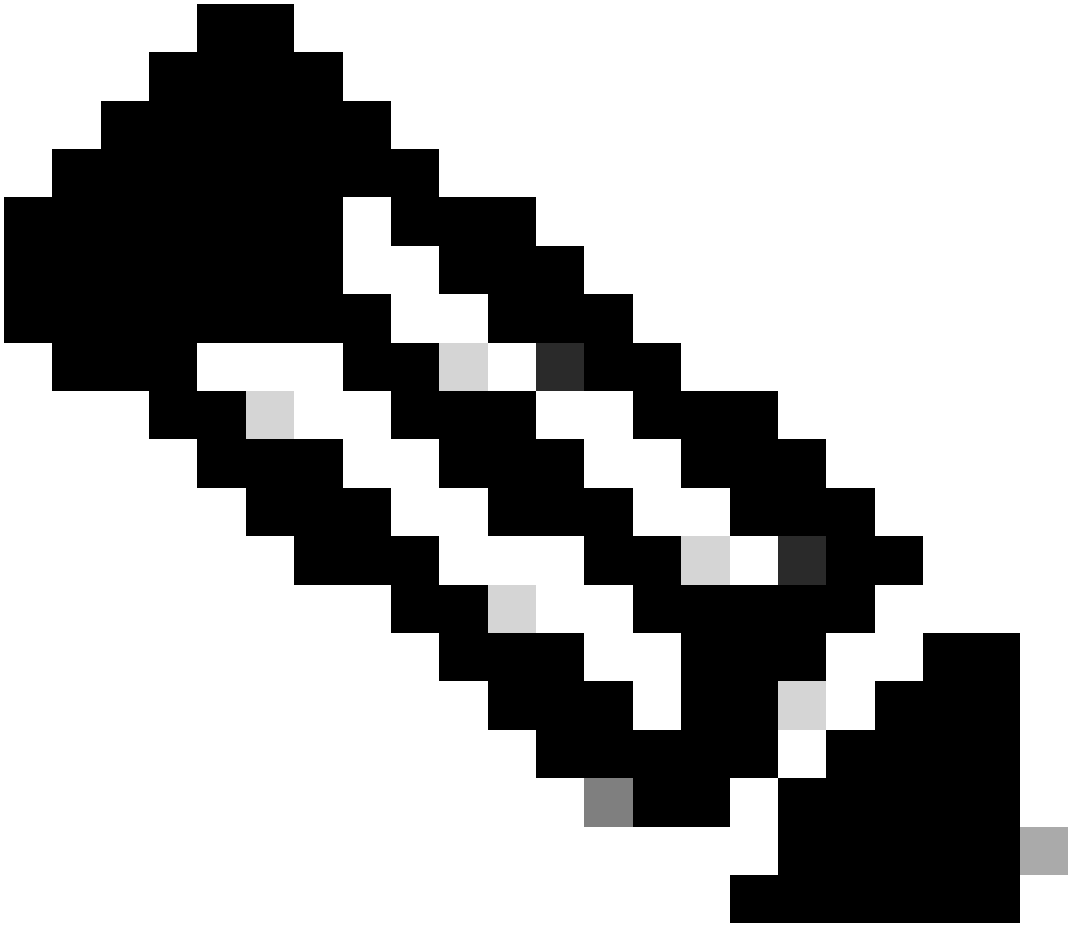
3. Pour un ordinateur Mac, sélectionnezApplications > Cisco > Cisco DART.

Étape 2. Cliquez sur l'onglet Statistiques, puis sur Détails.

Étape 3. Choisissez Création d'une offre groupée par défaut ou personnalisée.



Conseil : Le nom par défaut de l'offre groupée est DARTBundle.zip et elle est enregistrée sur le bureau local.



Remarque : Si vous avez sélectionné Par défaut, DART commence à créer le bundle. Si vous avez choisi Personnalisé, continuez l'exécution des invites de l'Assistant pour spécifier les journaux, les fichiers de préférences, les informations de diagnostic et toute autre personnalisation

Activer les journaux de débogage pour les modules ZTNA et SWG

Dans certains scénarios, l'équipe d'assistance doit activer les journaux de niveau de suivi ou de débogage afin d'identifier des problèmes plus complexes.

suivez les étapes fournies dans cette section pour activer les débogages pour chacun des modules.

Activer les journaux de débogage pour ZTNA

Étape 1. Créez un fichier json nommé logconfig.json

Étape 2. Entrez ce texte dans le fichier

```
{ "global": "DBG_TRACE" }
```

Étape 3. Placez le fichier dans le répertoire approprié en fonction du système d'exploitation

- Fenêtres: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- MacOS : /opt/cisco/secureclient/zta

Étape 4. Redémarrez le module ZTNA ou le client sécurisé Cisco pour que les journaux prennent effet.

Activer les journaux de débogage pour SWG

Étape 1 : créez un fichier json nommé SWGConfigOverride.json

Étape 2. Entrez ce texte dans le fichier

```
{"logLevel": "1"}□
```

Étape 3. Placez le fichier dans le répertoire approprié en fonction du système d'exploitation

- Windows : C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
- MacOS : /opt/cisco/secureclient/umbrella/swg

Étape 4. Redémarrez le module SWG ou le client sécurisé Cisco pour que les journaux prennent effet.

Activer les journaux de débogage pour DUO

Activer les journaux DUO KDF (Dépannage de la position, Problèmes d'inscription)

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 1 /f
```

Désactiver les journaux DUO KDF

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 0 /f
```

Collecter les journaux KDF pour les modules ZTNA et SWG, DNS (Windows)

Dans certains scénarios, l'équipe de support doit collecter des journaux kdf afin d'identifier des problèmes plus complexes.

suivez les étapes fournies dans cette section pour configurer et collecter les journaux kdf.

Conditions préalables

L'installation de DebugView est nécessaire pour collecter correctement les journaux. qui peut être installé à l'aide de cette source : https://learn.microsoft.com/en-us/sysinternals/downloads/debugview

Activer la clé de registre DNS

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x20801FF /t reg
```

Activer la clé de registre SWG

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x70C01FF /t reg
```

Activer la clé de registre ZTNA

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x40018EF52
```

Désactiver tous les indicateurs

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

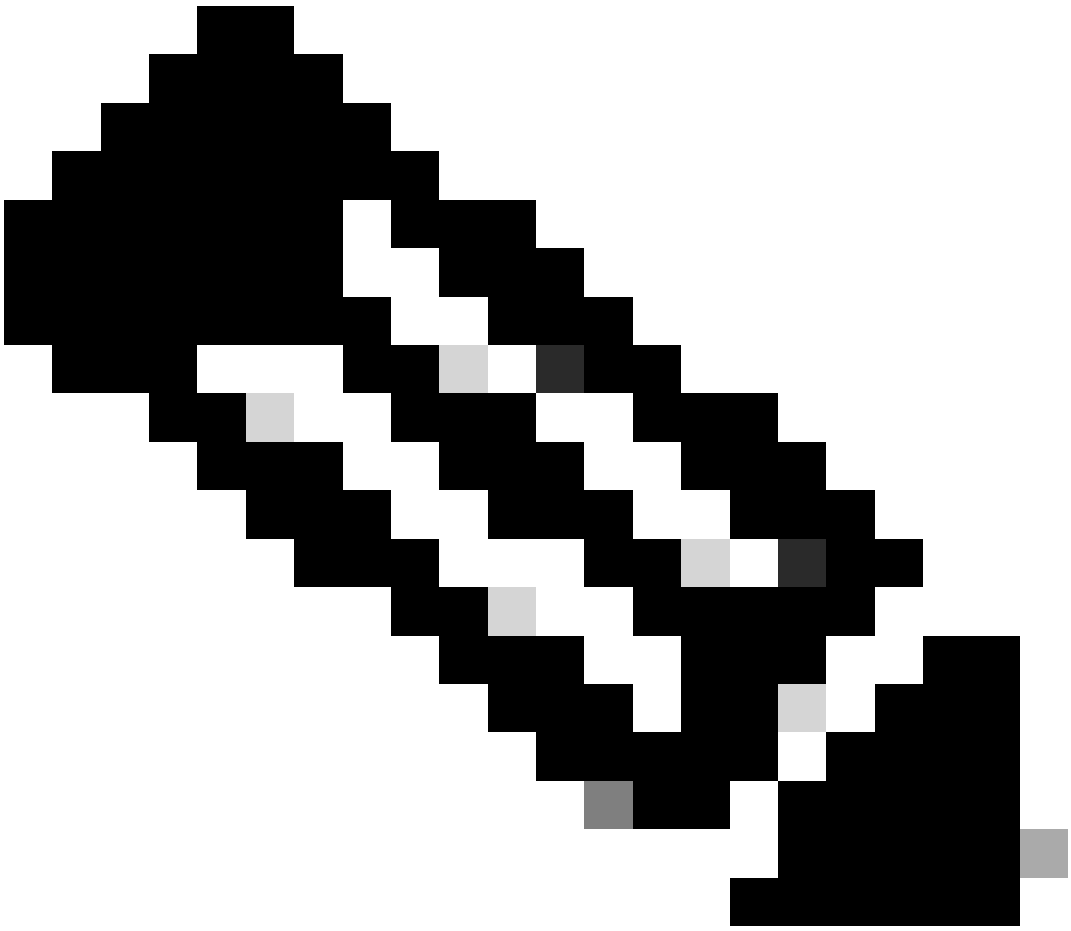
Captures d'archives HTTP (HAR)

HAR peut être collecté depuis différents navigateurs. il fournit plusieurs informations, notamment :

1. Version déchiffrée des requêtes HTTPS.
2. Informations internes sur les messages d'erreur, les détails des demandes et les en-têtes.

3. Informations sur le calendrier et les retards
4. Autres informations diverses sur les requêtes basées sur le navigateur.

Pour collecter des captures HAR, suivez les étapes décrites dans cette source : https://toolbox.googleapps.com/apps/har_analyzer/



Remarque : Vous devez actualiser votre session de navigateur afin de collecter les bonnes données

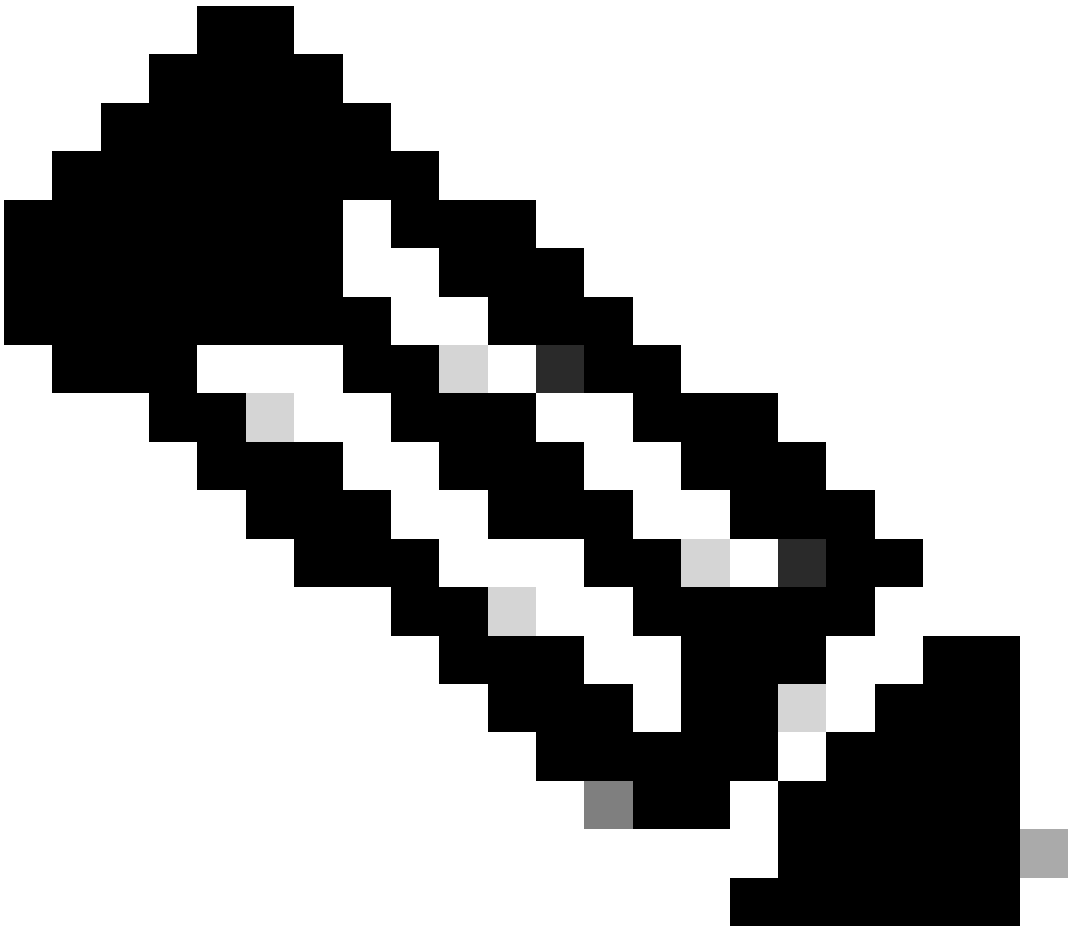
---

Captures de paquets

Les captures de paquets sont utiles dans un scénario où un problème de performances ou une perte de paquets est détecté, ou une panne totale du réseau. Les outils les plus courants pour collecter les captures sontwiresharket **tcpdump**. Ou une fonctionnalité intégrée pour collecter des fichiers au format pcap au sein du périphérique lui-même, comme un pare-feu Cisco ou un routeur.

Pour collecter des captures de paquets utiles sur un terminal, veillez à inclure les éléments suivants :

1. Interface de bouclage pour capturer le trafic envoyé via les modules complémentaires Secure Client.
2. Toutes les autres interfaces impliquées dans le chemin des paquets.
3. Appliquez des filtres minimaux ou aucun filtre pour vous assurer que toutes les données sont collectées.



> Remarque : Lorsque des captures sont collectées sur un périphérique réseau, veillez à filtrer la source et la destination du trafic, et limitez les captures aux ports et services associés uniquement, afin d'éviter toute performance causée par cet exercice.

Sortie du débogage de stratégie

La sortie de débogage de stratégie est une sortie de diagnostic envoyée via le navigateur de

l'utilisateur lorsqu'il est protégé par Secure Access. qui inclut des informations critiques sur le déploiement.

1. ID de l'organisation
2. Type de déploiement
3. Proxy connecté
4. Adresses IP publiques et privées
5. Autres informations relatives à la source du trafic.

Pour exécuter les résultats du test de stratégie, connectez-vous à ce lien à partir d'un point d'extrémité protégé : https://policy.test.sse.cisco.com/

Assurez-vous que vous approuvez le certificat racine d'accès sécurisé si un message d'erreur de certificat s'affiche dans votre navigateur.

Pour télécharger le certificat racine d'accès sécurisé :

Accédez à Secure Access Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

Commandes courantes Dépannage d'un tunnel de site à site

<#root>

```
# Tunnel Establishment


asa>show crypto ikev1 sa
asa>show crypto ikev2 sa
asa>show crypto ipsec sa
asa>show crypto session


#BGP Troubleshooting


asa>show running-config router bgp
asa>show bgp summary
asa>show ip bgp neighbors


#Routes Advertisements


asa>show bgp ipv4 unicast neighbors <sse-dc-ip> advertised-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> received-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> routes


#Debug BGP events


asa>debug ip bgp
asa>debug ip bgp events
asa>debug ip bgp updates
asa>debug ip routing
```

```
#Disable Debugs

asa>undebug all
```

Commandes courantes Dépannage du connecteur de ressources

La liste fournie fournit une vue complète du connecteur de ressources et des détails importants de dépannage pour l'équipe d'assistance d'accès sécurisé

<#root>

```
#DNS and connectivity tests on the local IP address, gateway, Secure Access APIs

rc-cli> diagnostic

#Software version, VPN tunnel state, system health, sysctl settings, routes and iptables

rc-cli> techsupport

#Packet captures

rc-cli> tcpdump <host>
```

Télécharger les résultats dans la demande de service d'assistance Cisco

Vous pouvez télécharger des fichiers vers le dossier d'assistance en procédant comme suit :

Étape 1 : connexion à SCM

Étape 2. Pour afficher et modifier le dossier, cliquez sur son numéro ou sur son titre dans la liste. La page Récapitulatif du dossier s'ouvre.

Étape 3. Cliquez sur Add Files afin de choisir un fichier et le télécharger en tant que pièce jointe au dossier. Le système affiche l'outil SCM File Uploader.

Étape 4. Dans la boîte de dialogue Choisir les fichiers à télécharger, faites glisser les fichiers que vous souhaitez télécharger ou cliquez à l'intérieur pour parcourir votre ordinateur local à la

recherche des fichiers à télécharger.

Étape 5. Ajoutez une description et spécifiez une catégorie pour tous les fichiers, ou individuellement.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Documentation et guide de l'utilisateur Secure Access
- Téléchargement du logiciel Cisco Secure Client

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.