Obtention d'informations de version et de débogage AAA pour Cisco Secure ACS pour Windows

Contenu

Introduction

Ce document explique comment afficher la version de Cisco Secure ACS pour Windows et comment configurer et obtenir des informations de débogage AAA (Authentication, Authorization and Accounting).

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur Cisco Secure ACS pour Windows 2.6.

Obtention d'informations sur la version de Cisco Secure pour Windows

Vous pouvez afficher les informations de version à l'aide de la ligne de commande DOC ou de l'interface utilisateur graphique.

Utilisation de la ligne de commande DOS

Pour afficher le numéro de version de Cisco Secure ACS pour Windows via l'option de ligne de commande dans DOS, utilisez **cstacacs** ou **csradius**, suivi de **-v** pour RADIUS et **-x** pour TACACS+. Reportez-vous aux exemples ci-dessous :

```
C:\Program Files\CiscoSecure ACS v2.6\CSTacacs>cstacacs -s
CSTacacs v2.6.2, Copyright 2001, Cisco Systems Inc

C:\Program Files\CiscoSecure ACS v2.6\CSRadius>csradius -v
CSTacacs v2.6.2), Copyright 2001, Cisco Systems Inc
```

Vous pouvez également voir le numéro de version du programme Cisco Secure ACS dans le Registre Windows. Exemple :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv2.1\CSAuth]
Version=2.6(2)
```

Utilisation de l'interface utilisateur graphique

Pour afficher la version à l'aide de l'interface utilisateur graphique Cisco Secure ACS, accédez à la page d'accueil ACS. Pour ce faire, cliquez à tout moment sur le logo Cisco Systems dans le coin supérieur gauche de l'écran. La moitié inférieure de la page d'accueil affiche la version complète.

Configuration de Cisco Secure ACS pour les niveaux de débogage Windows

Voici une explication des différentes options de débogage nécessaires pour obtenir les

informations de débogage maximales.

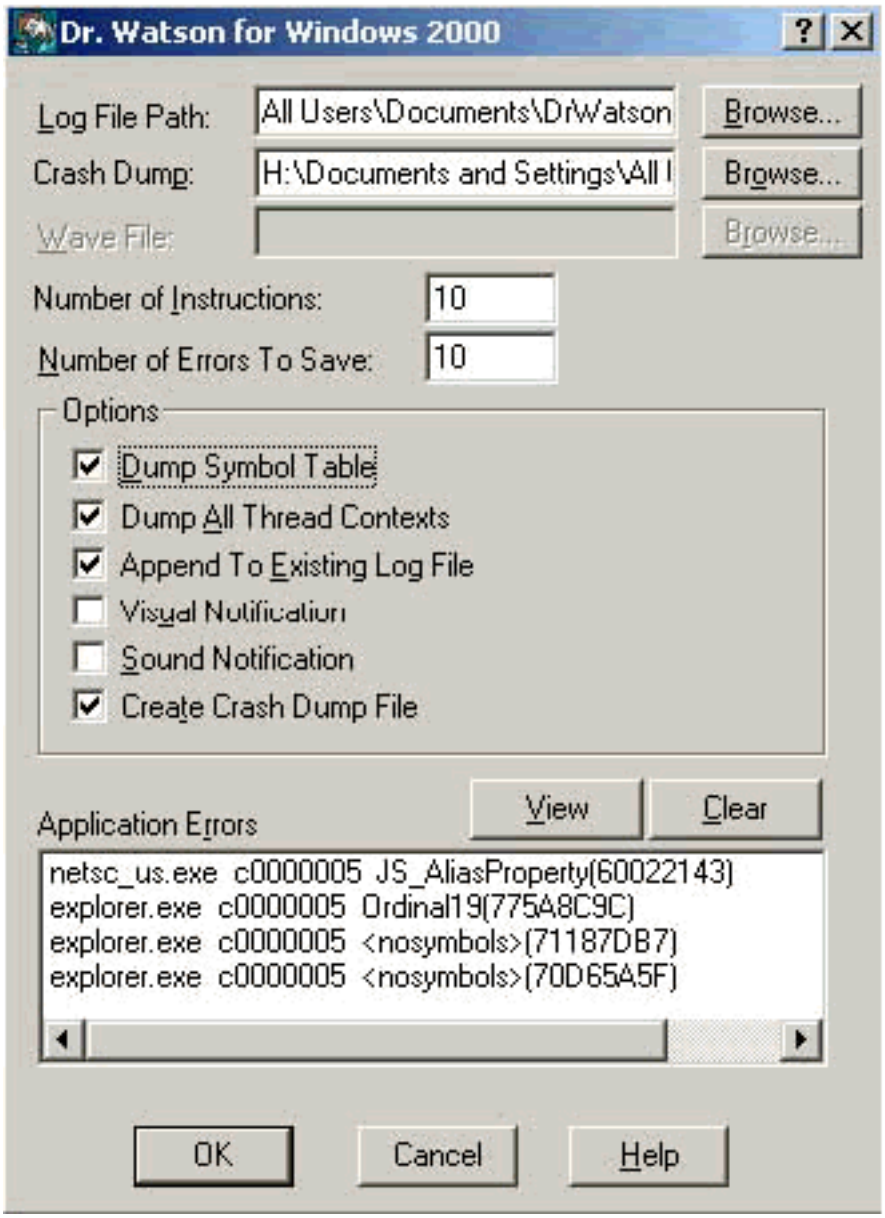
Comment définir le niveau de journalisation sur Complet dans l'interface utilisateur graphique ACS

Vous devez configurer ACS pour enregistrer tous les messages. Pour ce faire, procédez comme suit :

1. Àpartir de la page d'accueil ACS, accédez à **Configuration des systèmes > Contrôle des services**.
2. Sous l'en-tête Configuration du fichier journal de service, définissez le niveau de détail sur **Complet**.Vous pouvez modifier les sections Générer un nouveau fichier et Gérer le répertoire si
nécessaire.

Comment configurer la journalisation Dr Watson

Àl'invite de commande, tapez **drwtsn32** et la fenêtre Dr Watson s'affiche. Assurez-vous que les options de la case **Dépouiller tous les contextes de thread** et de la **table des symboles de vidage** sont cochées.



Création d'un fichier package.cab

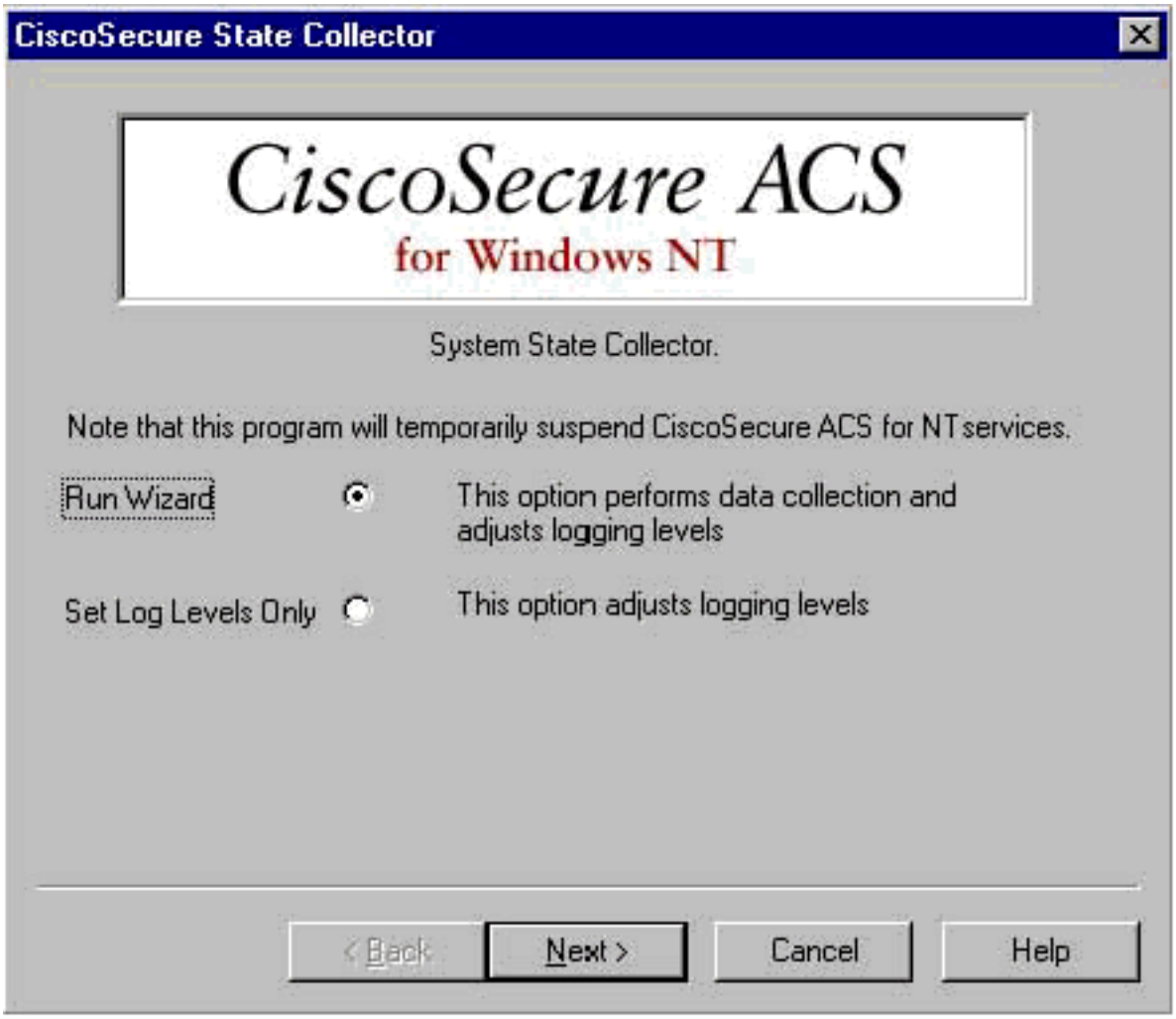
Qu'est-ce que package.cab ?

Le fichier package.cab est un fichier Zip qui contient tous les fichiers nécessaires au dépannage efficace d'ACS. Vous pouvez utiliser l'utilitaire CSSupport.exe pour créer le fichier package.cab ou collecter les fichiers manuellement.

Création d'un fichier package.cab avec l'utilitaire CSSupport.exe

Si vous rencontrez un problème ACS pour lequel vous devez collecter des informations, exécutez le fichier CSSupport.exe dès que possible après avoir détecté le problème. Utilisez la ligne de commande DOS ou l'interface utilisateur graphique de l'Explorateur Windows pour exécuter CSSupport à partir de C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe.

Lorsque vous exécutez le fichier CSSupport.exe, la fenêtre suivante apparaît.



Dans cet écran, vous avez deux options principales :

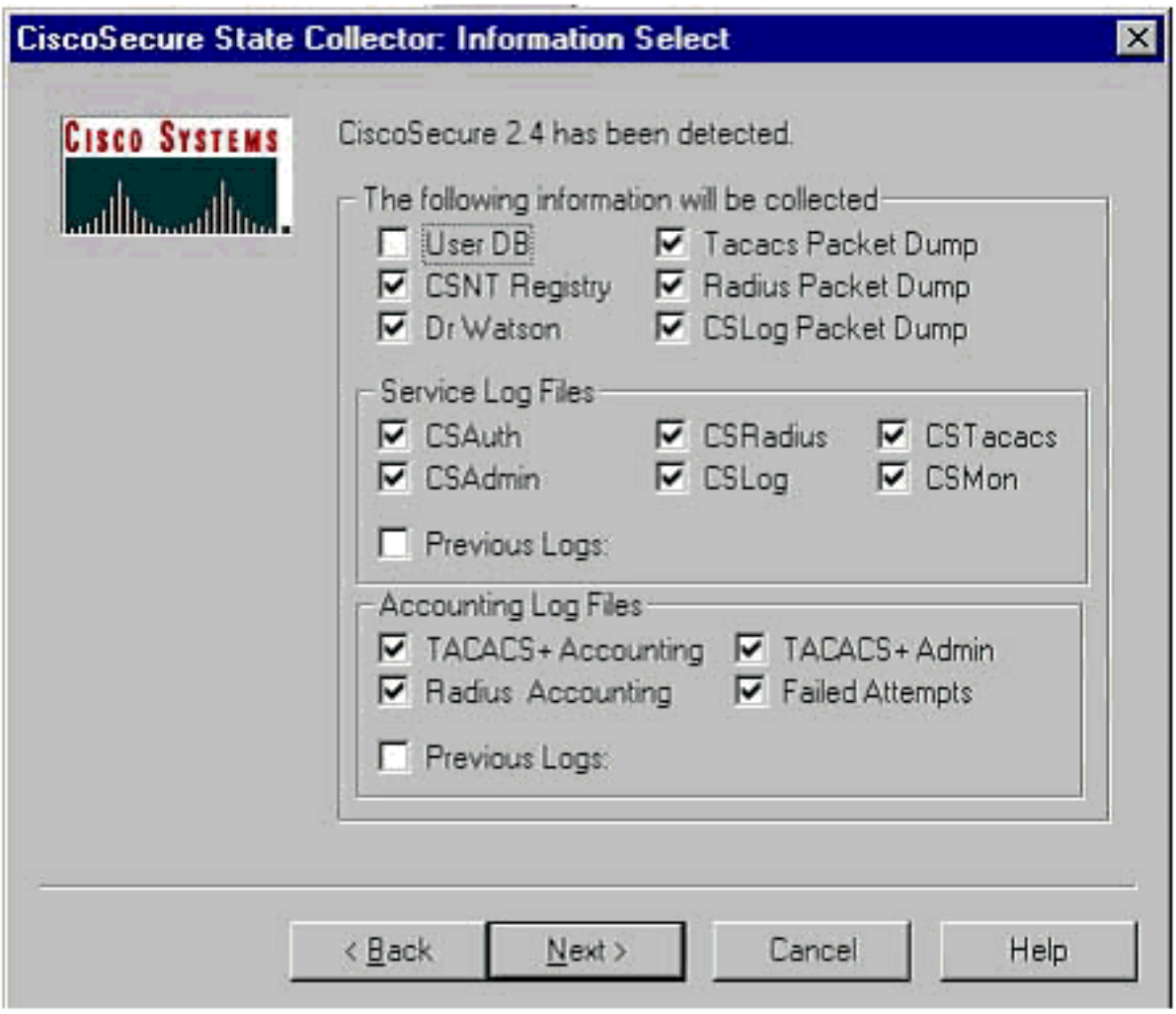
- Exécuter l'Assistant, qui vous guide dans une série de quatre étapes :Cisco Secure State Collector : Sélection des informationsCisco Secure State Collector : Sélection d'installationCisco Secure State Collector : Verbosité du journalCisco Secure State Collector (la collection réelle)ou
- Définissez uniquement le niveau de journal, qui vous permet d'ignorer les premières étapes et d'accéder directement au collecteur d'état sécurisé Cisco : Écran Log Verbosity

Pour une première configuration, sélectionnez **Exécuter l'Assistant** pour passer aux étapes nécessaires à la définition du journal. Après la configuration initiale, vous pouvez utiliser l'option **Définir les niveaux de journal uniquement** pour ajuster les niveaux de journalisation. Faites votre sélection, puis cliquez sur **Suivant**.

Assistant Exécuter

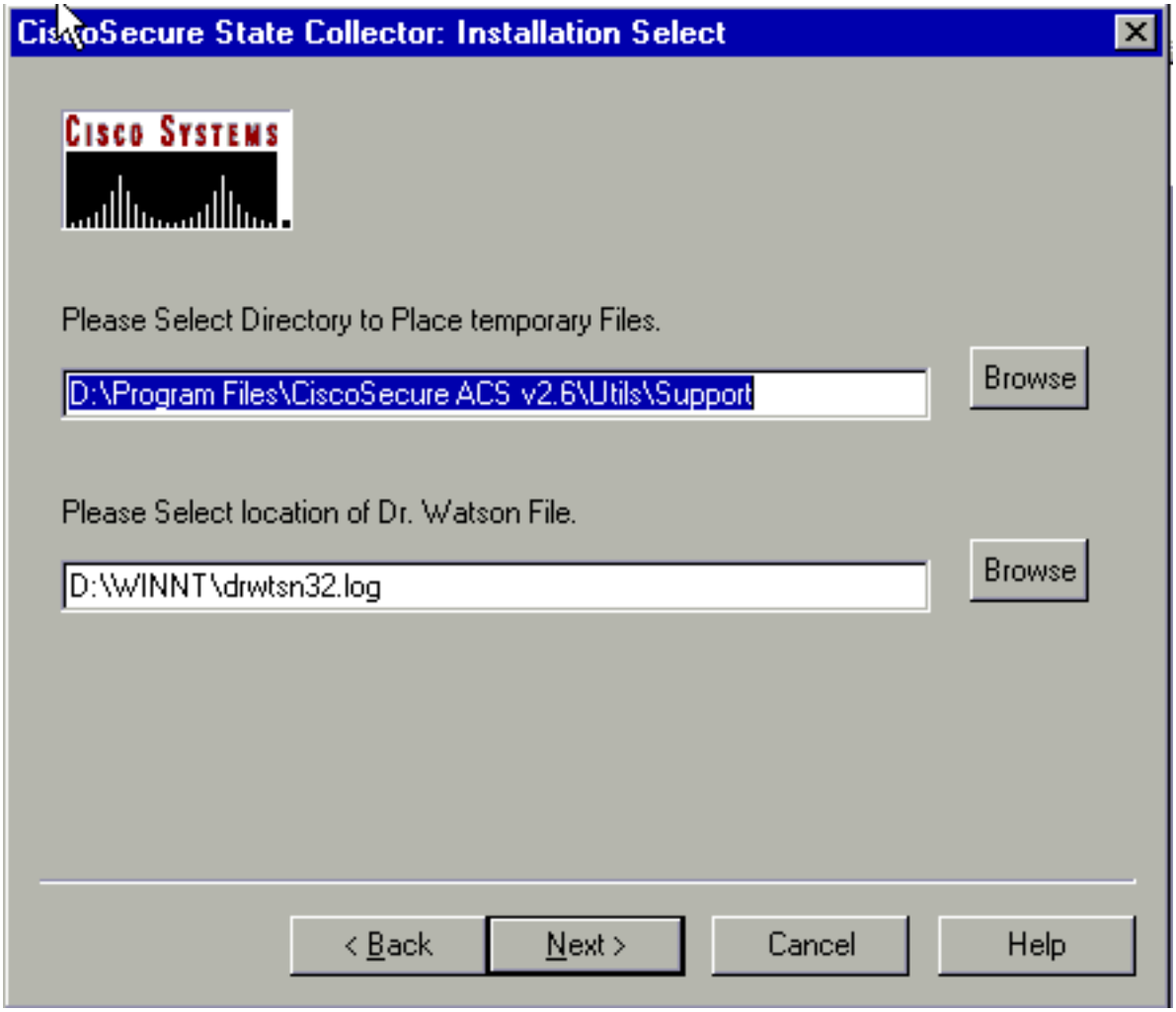
Les informations suivantes expliquent comment sélectionner des informations à l'aide de l'option Exécuter l'Assistant.

1. **Cisco Secure State Collector :** Sélectionner **les informations**Toutes les options doivent être sélectionnées par défaut, à l'exception de la base de données utilisateur et des journaux précédents. Si vous pensez que votre problème est la base de données utilisateur ou de groupe, sélectionnez **User DB**. Si vous souhaitez inclure les anciens journaux, sélectionnez l'option **Journaux précédents**. Cliquez sur **Suivant** lorsque vous avez

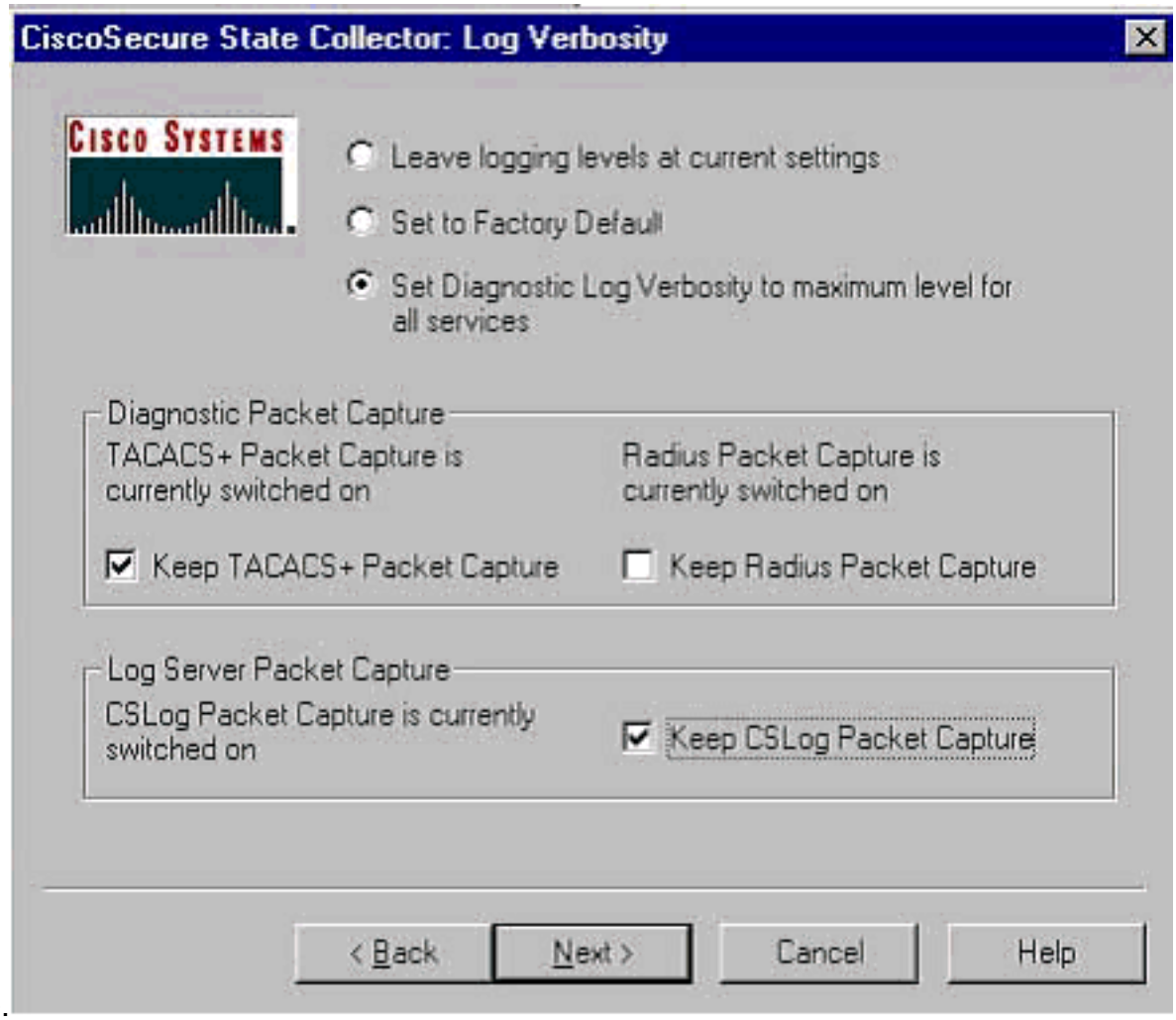


terminé.

2. **Cisco Secure State Collector : Sélection d'installation**Choisissez le répertoire dans lequel vous voulez placer le fichier package.cab. La valeur par défaut est C:\Program Files\Cisco Secure ACS v.26\Utils\Support. Vous pouvez changer cet emplacement si vous le désirez. Assurez-vous que l'emplacement correct de votre Dr Watson est spécifié. L'exécution de CSSupport nécessite que vous démarriez et arrêtiez les services. Si vous êtes sûr de vouloir arrêter et démarrer les services Cisco Secure, cliquez sur **Suivant** pour continuer.

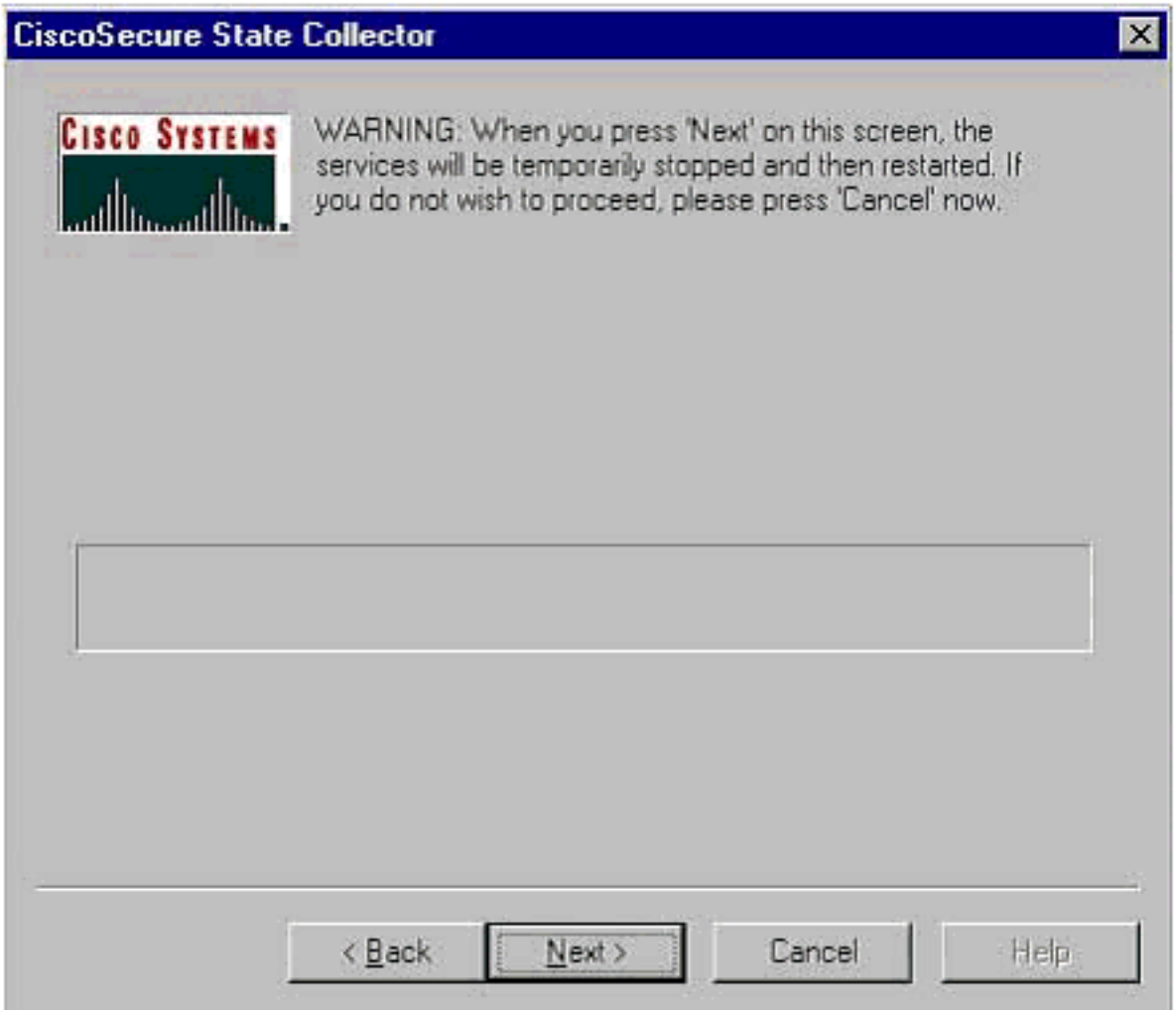


3. **Cisco Secure State Collector : Verbosité du journal**Sélectionnez l'option **Définir la version du journal de diagnostic au niveau maximal pour tous les services**. Sous l'en-tête Capture de paquets de diagnostic, sélectionnez TACACS+ ou RADIUS, selon ce que vous exécutez. Sélectionnez l'option **Keep CSLog Packet Capture**. Lorsque vous avez terminé, cliquez sur **Suivant**.**Remarque :** Si vous souhaitez avoir des journaux des jours précédents, vous devez sélectionner l'option **Journaux précédents** à l'étape 1, puis définir le nombre de jours que vous souhaitez revenir en



arrière.

4. **Collecteur Cisco Secure State**Un avertissement s'affiche, indiquant que lorsque vous continuerez, vos services seront arrêtés, puis redémarrés. Cette interruption est nécessaire pour que CSSupport puisse récupérer tous les fichiers nécessaires. Le temps d'arrêt doit être minimal. Vous pourrez voir les services s'arrêter et redémarrer dans cette fenêtre. Cliquez sur **Suivant** pour
continuer.



Lorsque les services redémarrent, package.cab se trouve à l'emplacement spécifié. Cliquez sur **Terminer** et votre fichier package.cab est prêt.Accédez à l'emplacement que vous avez spécifié pour package.cab et délocalisez-le dans un répertoire où il peut être enregistré. Votre ingénieur du support technique peut le demander à tout moment pendant le processus de dépannage.

Définir uniquement les niveaux de journal

Si vous avez déjà exécuté le collecteur d'état et que vous devez uniquement modifier les niveaux de journalisation, vous pouvez utiliser l'option Définir les niveaux de journal uniquement pour passer à Cisco Secure State Collector : Écran Log Verbosity, dans lequel vous définissez la capture de paquets de diagnostic. Lorsque vous cliquez sur **Suivant**, vous accédez directement à la page Avertissement. Cliquez ensuite à nouveau sur **Suivant** pour arrêter le service, rassembler le fichier et redémarrer les services.

Collecte manuelle d'un fichier package.cab

Voici une liste des fichiers compilés dans un package.cab. Si le CSSupport ne fonctionne pas correctement, vous pouvez rassembler ces fichiers à l'aide de l'Explorateur Windows.

```
Registry (ACS.reg)

Failed Attempts File
(C:\program files\Cisco Secure acs v2.6\Logs\Failed Attempts active.csv)
```

```
TACACS+ Accounting
(C:\program files\Cisco Secure acs v2.6\Logs\TACACS+ Accounting\
TACACS+ Accounting active.csv)

RADIUS Accounting
(C:\program files\Cisco Secure acs v2.6\Logs\RADIUS Accounting\
RADIUS Accounting active.csv)

TACACS+ Administration
(C:\program files\Cisco Secure acs v2.6\Logs\TACACS+ Administration\
TACACS+ Administration active.csv)

Auth log
(C:\program files\Cisco Secure acs v2.6\CSAuth\Logs\auth.log)

RDS log
(C:\program files\Cisco Secure acs v2.6\CSRadius\Logs\RDS.log)

TCS log
(C:\program files\Cisco Secure acs v2.6\CSTacacs\Logs\TCS.log)

ADMN log
(C:\program files\Cisco Secure acs v2.6\CSAdmin\Logs\ADMIN.log)

Cslog log
(C:\program files\Cisco Secure acs v2.6\CSLog\Logs\cslog.log)

Csmon log
(C:\program files\Cisco Secure acs v2.6\CSMon\Logs\csmon.log)

DrWatson
(drwtsn32.log)  See section 3 for further details
```

Obtention des informations de débogage AAA de Cisco Secure pour Windows NT

Les services CSRadius, CSTacacs et CSAuth de Windows NT peuvent être exécutés en mode ligne de commande lorsque vous dépannez un problème.

Remarque : l'accès à l'interface utilisateur graphique est limité si des services Cisco Secure pour Windows NT sont exécutés en mode ligne de commande.

Pour obtenir les informations de débogage CSRadius, CSTacacs ou CSAuth, ouvrez une fenêtre DOS et réglez la hauteur de tampon d'écran de la propriété Windows sur 300.

Utilisez les commandes suivantes pour CSRadius :

```
c:\program files\ciscosecure acs v2.1\csradius>net stop csradius

c:\program files\ciscosecure acs v2.1\csradius>csradius -d -p -z
```

Utilisez les commandes suivantes pour CSTacacs :

```
c:\program files\ciscosecure acs v2.1\cstacacs>net stop cstacacs
```

```
c:\program files\ciscosecure acs v2.1\cstacacs>cstacacs -e -z
```

Obtention des informations de débogage de la réplication AAA Cisco Secure pour Windows NT

Les services CSAuth de Windows NT peuvent être exécutés en mode ligne de commande lorsque vous dépannez un problème de réplication.

Remarque : l'accès à l'interface utilisateur graphique est limité si des services Cisco Secure pour Windows NT sont exécutés en mode ligne de commande.

Pour obtenir les informations de débogage de réplication CSAuth, ouvrez une fenêtre DOS et réglez la hauteur de tampon d'écran de la propriété Windows sur 300.

Utilisez les commandes suivantes pour CSAuth sur les serveurs source et cible :

```
c:\program files\ciscosecure acs v2.6\csauth>net stop csauth

c:\program files\ciscosecure acs v2.1\csauth>csauth -p -z
```

Le débogage est écrit dans la fenêtre d'invite de commandes, et il se trouve également dans le fichier $BASE\csauth\logs\auth.log.

Test de l'authentification utilisateur hors connexion

L'authentification des utilisateurs peut être testée via l'interface de ligne de commande (CLI). RADIUS peut être testé avec « radtest », et TACACS+ peut être testé avec « tactest ». Ces tests peuvent être utiles si le périphérique de communication ne génère pas d'informations de débogage utiles et s'il y a une question sur un problème de système Cisco Secure ACS Windows ou un problème de périphérique. Le plus rapide et le plus rapide se trouvent dans le répertoire $BASE\utils. Voici des exemples de chaque test.

Test de l'authentification utilisateur RADIUS hors connexion avec Radtest

```
SERVER TEST PROGRAM

1...Set Radius IP, secret & timeout
2...Authenticate user
3...Authenticate from file
4...Authenticate with CHAP
5...Authenticate with MSCHAP
6...Replay log files
7...Drive authentication and accounting from file
8...Accounting start for user
9...Accounting stop for user
A...Extended Setup
B...Customer Packet Builder
0...Exit

Defaults server:172.18.124.99 secret:secret_value timeout:2000mSec
        auth:1645 acct:1646 port:999 cli:999
```

```
Choice>2

User name><>abcde
User pasword><>abcde
Cli><999>
NAS port id><999>
State><>
User abcde authenticated
Request from host 172.18.124.99:1645 code=2, id=0, length=44 on port 1645
        [080] Signature         value: A6 10 00 96 6F C2 AB 78 B6 9F CA D9 01 E3 D7 C6
        [008] Framed-IP-Address value: 10.1.1.5

Hit Return to continue.
```

Test de l'authentification utilisateur TACACS+ hors connexion avec Tactest

```
tactest -H 127.0.0.1 -k secret
TACACS>
Commands available:
        authen action type service port remote [user]
                action <login,sendpass,sendauth>
                type <ascii,pap,chap,mschap,arap>
                service <login,enable,ppp,arap,pt,rcmd,x25>
        author arg1=value1 arg2=value2 ...
        acct arg1=value1 arg2=value2 ...
TACACS> authen login ascii login tty0 abcde
Username: abcde
Password: abcde
Authentication succeeded :
TACACS>
```

Détermination des raisons des pannes de base de données Windows 2000/NT

Si l'authentification est passée à Windows 2000/NT mais échoue, vous pouvez activer la fonction d'audit Windows en accédant à **Programmes > Outils d'administration > Gestionnaire d'utilisateurs pour les domaines, les stratégies > Audit**. Accéder à **Programmes > Outils d'administration > Observateur d'événements** affiche les échecs d'authentification. Les échecs détectés dans le journal des échecs de tentatives sont affichés dans un format comme indiqué dans l'exemple ci-dessous.

```
NT/2000 authentication FAILED (error 1300L)
```

Ces messages peuvent être recherchés sur le site Web de Microsoft à l'adresse Windows 2000 Event & Error Messages and Error Codes in Windows NT .

Le message d'erreur 1300L est décrit ci-dessous.

```
Code  Name                                  Description
-------------------------------------------------------------------------
1300L ERROR_NOT_ALL_ASSIGNED                Indicates not all privileges
                                            referenced are assigned to the
```

```
                                        caller. This allows, for
                                        example, all privileges to be
                                        disabled without having to
                                        know exactly which privileges
                                        are assigned.
```

Exemples

Authentification RADIUS correcte

```
F:\Program Files\Cisco Secure ACS v2.6\CSRadius>csradius -p -z
CSRadius v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
Debug logging on
Command line mode
============================== SERVICE STARTED ==============================
Version is 2.6(2.4)
Server variant is Default
10 auth threads, 20 acct threads
NTlib The local computer name is YOUR-PC
NTlib We are NOT a domain controller
NTlib We are a member of the RTP-APPS domain
NTlib An additional domain list is defined: \LOCAL,RTP-APPS,somedomain
Winsock initialsed ok
Created shared memory
ExtensionPoint: Base key is [SOFTWARE\Cisco\CiscoAAAv2.6\CSRadius\ExtensionPoint
s]
ExtensionPoint: Entry [001] for supplier [Cisco Aironet] via dll [AironetEAP.dll
]
ExtensionPoint: Looking for vendor associations for supplier [Cisco Aironet]
ExtensionPoint: Found vendor association [RADIUS (Cisco Aironet)] for supplier [
Cisco Aironet]
ExtensionPoint: Supplier [Cisco Aironet] is disabled, ignoring...
CSAuth interface initialised
About to retreive user profiles from CSAuth
Profile 0, Subset for vendor 1 - RADIUS (Cisco IOS/PIX)
    [026] Vendor-Specific                   vsa id: 9
          [103] cisco-h323-return-code      value:  01
Profile 0, Subset for vendor 8 - RADIUS (Cisco Aironet)
    [026] Vendor-Specific                   vsa id: 9
          [103] cisco-h323-return-code      value:  01
Starting auth/acct worker threads
RADIUS Proxy: Proxy Cache successfully initialized.
Hit any key to stop

Dispatch thread ready on Radius Auth Port [1645]
Dispatch thread ready on Radius Auth Port [1812]
Dispatch thread ready on Radius Acct Port [1646]
Dispatch thread ready on Radius Acct Port [1813]
Request from host 172.18.124.154:1645 code=1, id=6, length=55 on port 1645
    [001] User-Name                         value:  roy
    [004] NAS-IP-Address                    value:  172.18.124.154
    [002] User-Password                     value:  BF 37 6D 76 76 22 55 88 83
 AD 6F 03 2D FA 92 D0
    [005] NAS-Port                          value:  5
Sending response code 2, id 6 to 172.18.124.154 on port 1645
    [008] Framed-IP-Address                 value:  255.255.255.255

RADIUS Proxy: Proxy Cache successfully closed.
Calling CMFini()
```

```
CMFini() Complete
============================== SERVICE STOPPED==============================
Server stats:
Authentication packets : 1
  Accepted             : 1
  Rejected             : 0
  Still in service     : 0
Accounting packets     : 0
Bytes sent             : 26
Bytes received         : 55
UDP send/recv errors   : 0

F:\Program Files\Cisco Secure ACS v2.6\CSRadius>
```

Authentification RADIUS incorrecte

```
F:\Program Files\Cisco Secure ACS v2.6\CSRadius>
F:\Program Files\Cisco Secure ACS v2.6\CSRadius>csradius -p -z
CSRadius v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
Debug logging on
Command line mode
============================== SERVICE STARTED ==============================
Version is 2.6(2.4)
Server variant is Default
10 auth threads, 20 acct threads
NTlib The local computer name is YOUR-PC
NTlib We are NOT a domain controller
NTlib We are a member of the RTP-APPS domain
NTlib An additional domain list is defined: \LOCAL,RTP-APPS,somedomain
Winsock initialsed ok
Created shared memory
ExtensionPoint: Base key is [SOFTWARE\Cisco\CiscoAAAv2.6\CSRadius\ExtensionPoint
s]
ExtensionPoint: Entry [001] for supplier [Cisco Aironet] via dll [AironetEAP.dll
]
ExtensionPoint: Looking for vendor associations for supplier [Cisco Aironet]
ExtensionPoint: Found vendor association [RADIUS (Cisco Aironet)] for supplier [
Cisco Aironet]
ExtensionPoint: Supplier [Cisco Aironet] is disabled, ignoring...
CSAuth interface initialised
About to retreive user profiles from CSAuth
Profile 0, Subset for vendor 1 - RADIUS (Cisco IOS/PIX)
    [026] Vendor-Specific                   vsa id: 9
          [103] cisco-h323-return-code      value:  01
Profile 0, Subset for vendor 8 - RADIUS (Cisco Aironet)
    [026] Vendor-Specific                   vsa id: 9
          [103] cisco-h323-return-code      value:  01
Starting auth/acct worker threads
RADIUS Proxy: Proxy Cache successfully initialized.
Hit any key to stop

Dispatch thread ready on Radius Auth Port [1645]
Dispatch thread ready on Radius Auth Port [1812]
Dispatch thread ready on Radius Acct Port [1646]
Dispatch thread ready on Radius Acct Port [1813]
Request from host 172.18.124.154:1645 code=1, id=7, length=55 on port 1645
    [001] User-Name                         value:  roy
    [004] NAS-IP-Address                    value:  172.18.124.154
    [002] User-Password                     value:  47 A3 BE 59 E3 46 72 40 B3
 AC 40 75 B3 3A B0 AB
    [005] NAS-Port                          value:  5
```

```
User:roy - Password supplied for user was not valid
Sending response code 3, id 7 to 172.18.124.154 on port 1645
Request from host 172.18.124.154:1645 code=1, id=8, length=55 on port 1645
    [001] User-Name                         value:  roy
    [004] NAS-IP-Address                    value:  172.18.124.154
    [002] User-Password                     value:  FE AF C0 D1 4D FD 3F 89 BA
 0A C7 75 66 DC 48 27
    [005] NAS-Port                          value:  5
User:roy - Password supplied for user was not valid
Sending response code 3, id 8 to 172.18.124.154 on port 1645
Request from host 172.18.124.154:1645 code=1, id=9, length=55 on port 1645
    [001] User-Name                         value:  roy
    [004] NAS-IP-Address                    value:  172.18.124.154
    [002] User-Password                     value:  79 1A 92 14 D6 5D A5 3E D6
 7D 09 D2 A5 8E 65 A5
    [005] NAS-Port                          value:  5
User:roy - Password supplied for user was not valid
Sending response code 3, id 9 to 172.18.124.154 on port 1645
Request from host 172.18.124.154:1645 code=1, id=10, length=55 on port 1645
    [001] User-Name                         value:  roy
    [004] NAS-IP-Address                    value:  172.18.124.154
    [002] User-Password                     value:  90 4C 6D 39 66 D1 1C B4 F7
 87 8B 7F 8A 29 60 9E
    [005] NAS-Port                          value:  5
User:roy - Password supplied for user was not valid
Sending response code 3, id 10 to 172.18.124.154 on port 1645

RADIUS Proxy: Proxy Cache successfully closed.
Calling CMFini()
CMFini() Complete
============================== SERVICE STOPPED ==============================
Server stats:
Authentication packets : 4
  Accepted             : 0
  Rejected             : 4
  Still in service     : 0
Accounting packets     : 0
Bytes sent             : 128
Bytes received         : 220
UDP send/recv errors   : 0

F:\Program Files\Cisco Secure ACS v2.6\CSRadius>
```

Authentification TACACS+ correcte

```
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>cstacacs -e -z
CSTacacs v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
CSTacacs server starting ============================
Base directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs
Log  directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs\Logs
CSTacacs version is 2.6(2.4)
Running as console application.
Doing Stats


**** Registry Setup ****
Single TCP connection operation enabled
Base Proxy enabled.
**********************

TACACS+ server started
```

```
Hit any key to stop

Created new session f3f130 (count 1)
All sessions busy, waiting
Thread 0 waiting for work
Thread 0 allocated work
Waiting for packetRead AUTHEN/START size=38

Packet from NAS***********
CONNECTION: NAS 520b Socket 2d4
PACKET: version 192 (0xc0), type 1, seq no 1, flags 1
session_id 1381473548 (0x52579d0c), Data length 26 (0x1a)
End header
Packet body hex dump:
01 01 01 01 03 01 0e 00 72 6f 79 30 31 37 32 2e 31 38 2e 31 32 34 2e 31 35 34
type=AUTHEN/START, priv_lvl = 1
action = login
authen_type=ascii
service=login
user_len=3 port_len=1 (0x1), rem_addr_len=14 (0xe)
data_len=0
User: roy
port: 0
rem_addr: 172.18.124.154End packet***********
Created new Single Connection session num 0 (count 1/1)
All sessions busy, waiting
All sessions busy, waiting
Listening for packet.Single Connect thread 0 waiting for work
Single Connect thread 0 allocated work
thread 0 sock: 2d4 session_id 0x52579d0c seq no 1 AUTHEN:START login ascii login
 roy 0 172.18.124.154
Authen Start request
Authen Start request
Calling authentication function
Writing AUTHEN/GETPASS size=28

Packet from CST+***********
CONNECTION: NAS 520b Socket 2d4
PACKET: version 192 (0xc0), type 1, seq no 2, flags 1
session_id 1381473548 (0x52579d0c), Data length 16 (0x10)
End header
Packet body hex dump:
05 01 00 0a 00 00 50 61 73 73 77 6f 72 64 3a 20
type=AUTHEN status=5 (AUTHEN/GETPASS) flags=0x1
msg_len=10, data_len=0
msg: Password:
data:
End packet***********
Read AUTHEN/CONT size=22

Packet from NAS***********
CONNECTION: NAS 520b Socket 2d4
PACKET: version 192 (0xc0), type 1, seq no 3, flags 1
session_id 1381473548 (0x52579d0c), Data length 10 (0xa)
End header
Packet body hex dump:
00 05 00 00 00 63 69 73 63 6f
type=AUTHEN/CONT
user_msg_len 5 (0x5), user_data_len 0 (0x0) flags=0x0
User msg: cisco
User data: End packet***********
Listening for packet.login query for 'roy' 0 from 520b accepted
Writing AUTHEN/SUCCEED size=18
```

```
Packet from CST+***********
CONNECTION: NAS 520b Socket 2d4
PACKET: version 192 (0xc0), type 1, seq no 4, flags 1
session_id 1381473548 (0x52579d0c), Data length 6 (0x6)
End header
Packet body hex dump:
01 00 00 00 00 00
type=AUTHEN status=1 (AUTHEN/SUCCEED) flags=0x0
msg_len=0, data_len=0
msg:
data:
End packet***********
Single Connect thread 0 waiting for work
520b: fd 724 eof (connection closed)
Thread 0 waiting for work
Release Host Cache
Close Proxy Cache
Calling CMFini()
CMFini() Complete
Closing Password Aging
Closing Finished

F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>
```

Authentification TACACS+ incorrecte (résumée)

```
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>cstacacs -e -z
CSTacacs v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
CSTacacs server starting ==============================
Base directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs
Log  directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs\Logs
CSTacacs version is 2.6(2.4)
Running as console application.
Doing Stats


**** Registry Setup ****
Single TCP connection operation enabled
Base Proxy enabled.
***********************

TACACS+ server started
Hit any key to stop

Created new session f3f130 (count 1)
All sessions busy, waiting
Thread 0 waiting for work
Thread 0 allocated work
Waiting for packetRead AUTHEN/START size=38



Packet from NAS***********
CONNECTION: NAS 520b Socket 2d4
PACKET: version 192 (0xc0), type 1, seq no 3, flags 1
session_id 714756899 (0x2a9a5323), Data length 11 (0xb)
End header
Packet body hex dump:
00 06 00 00 00 63 69 73 63 6f 31
type=AUTHEN/CONT
```

```
user_msg_len 6 (0x6), user_data_len 0 (0x0) flags=0x0
User msg: cisco1
User data: End packet***********
Listening for packet.login query for 'roy' 0 from 520b rejected
Writing AUTHEN/FAIL size=18

Release Host Cache
Close Proxy Cache
Calling CMFini()
CMFini() Complete
Closing Password Aging
Closing Finished

F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>
```

Informations connexes

- Support technique - Cisco Systems