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

Contenu

Introduction

Ce document explique comment visualiser le Cisco Secure ACS pour la version de Windows et comment installer et obtenir l'Authentification, autorisation et comptabilité (AAA) mettez au point les informations.

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.

Composants utilisés

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

Obtenir Cisco Secure pour les informations de version de Windows

Vous pouvez visualiser les informations de version à l'aide de la ligne de commande de DOCUMENTATION ou à l'aide du GUI.

Utilisant la ligne de commande DOS

Pour visualiser le numéro de version de Cisco Secure ACS pour Windows par l'option de la ligne de commande dans le DOS, les **cstacacs d'**utilisation ou le **csradius** ont suivi par **- v** pour le RAYON et **- le x** pour TACACS+. Voyez les 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 de Cisco Secure ACS dans le registre de Windows. Exemple :

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

Utilisant le GUI

Pour visualiser la version avec le GUI de Cisco Secure ACS, allez à la page d'accueil ACS. Vous pouvez faire ceci à tout moment en cliquant sur le logo de Cisco Systems dans le coin supérieur gauche de l'écran. La moitié inférieure de la page d'accueil affichera la version complète.

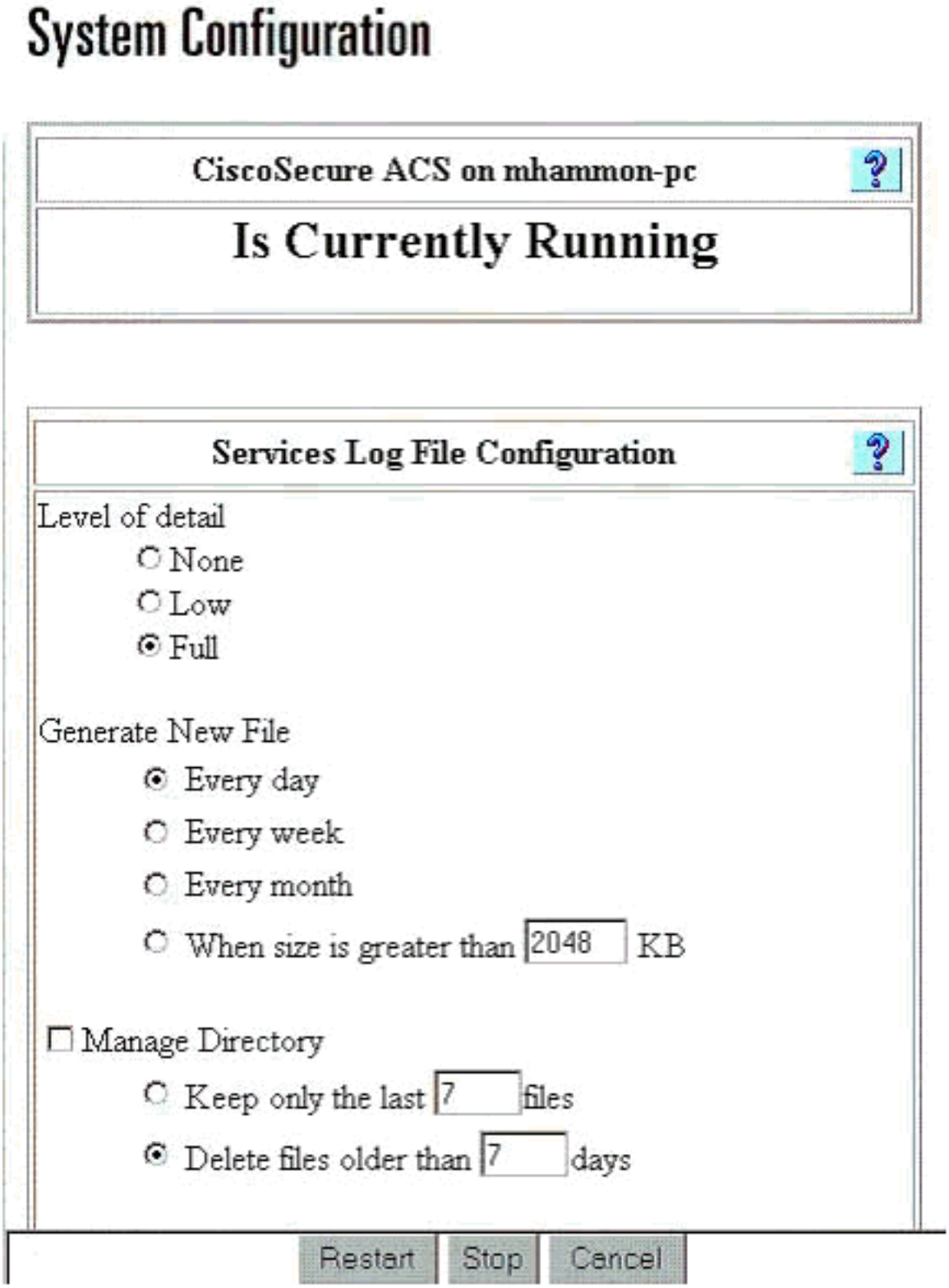
Établissement du Cisco Secure ACS pour Windows mettant au point des niveaux

Ce qui suit est une explication des différentes options d'élimination des imperfections qui sont nécessaires pour obtenir les informations de débogage maximum.

Comment placer le niveau se connectant à complètement dans le GUI ACS

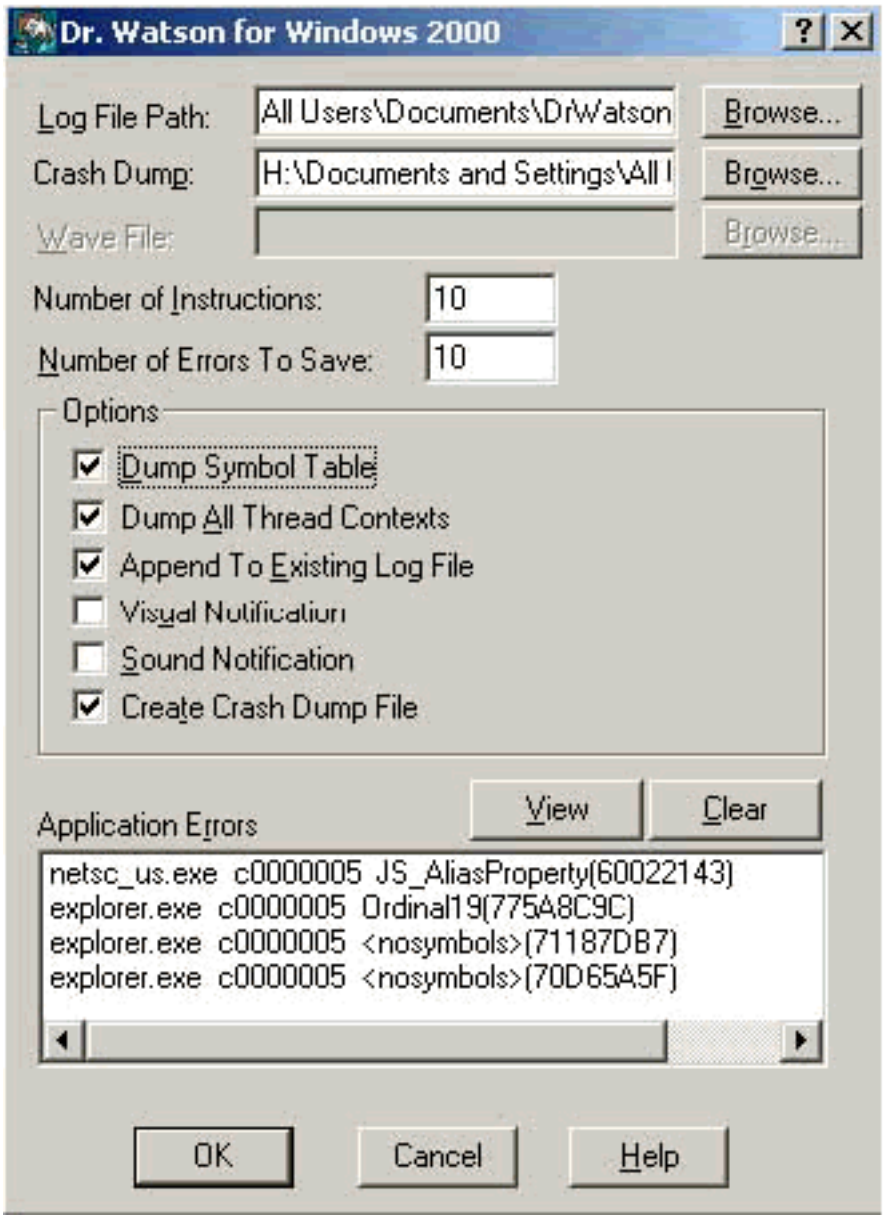
Vous devrez placer ACS pour se connecter tous les messages. Pour faire ceci, suivez les étapes répertoriées ci-dessous :

1. De la page d'accueil ACS, allez à la **configuration > au contrôle des services de systèmes**.
2. Sous le titre de configuration de fichier journal du service, placez le niveau de précision à **complètement**.Vous pouvez modifier le nouveau fichier de générer et gérer des sections de répertoire si
nécessaire.



[Comment placer Dr. Watson Logging]

Au type **drwtsn32 d'**invite de commande et à la fenêtre de Dr. Watson apparaîtra. Assurez-vous que **toutes les** options pour le **vidage mémoire filètent des contextes** et **table des symboles de vidage mémoire** sont vérifiés.



Création d'un fichier package.cab

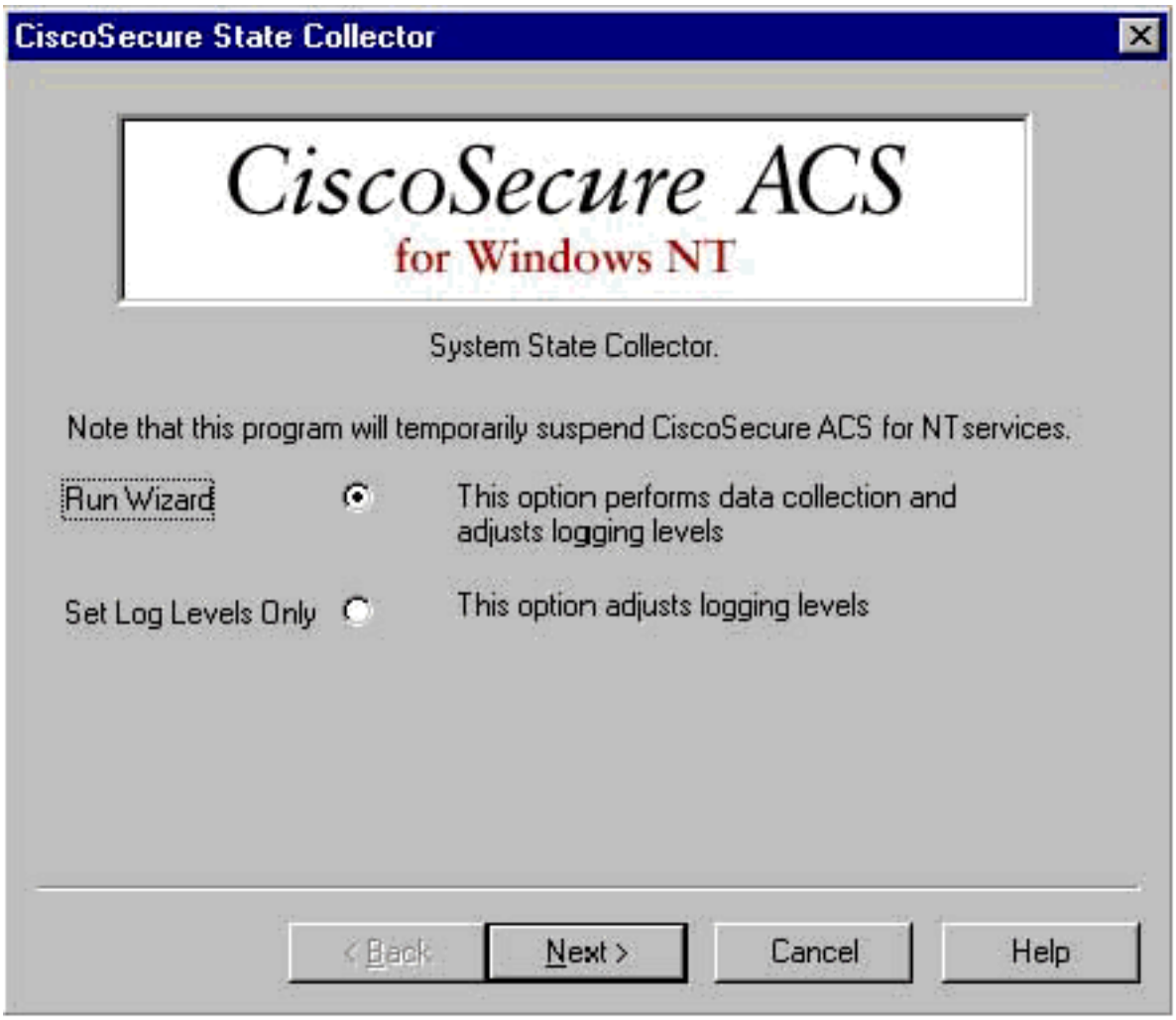
Quel est le package.cab ?

Le package.cab est un fichier zip qui contient tous les fichiers nécessaires requis pour dépanner ACS efficacement. Vous pouvez utiliser l'utilitaire CSSupport.exe pour créer le fichier package.cab ou collecter les fichiers manuellement.

En créant un package.cab classez avec l'utilitaire CSSupport.exe

Si vous avez un problème ACS pour lequel vous devez collecter des informations, exécutez le fichier CSSupport.exe dès que possible après que vous voyiez le problème. Utilisez le GUI de ligne ou d'Explorateur Windows de commande DOS pour exécuter CSSupport du Secure ACS v2.6\Utils>CSSupport.exe de C:\program files\Cisco.

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



De cet écran, vous avez deux principales options :

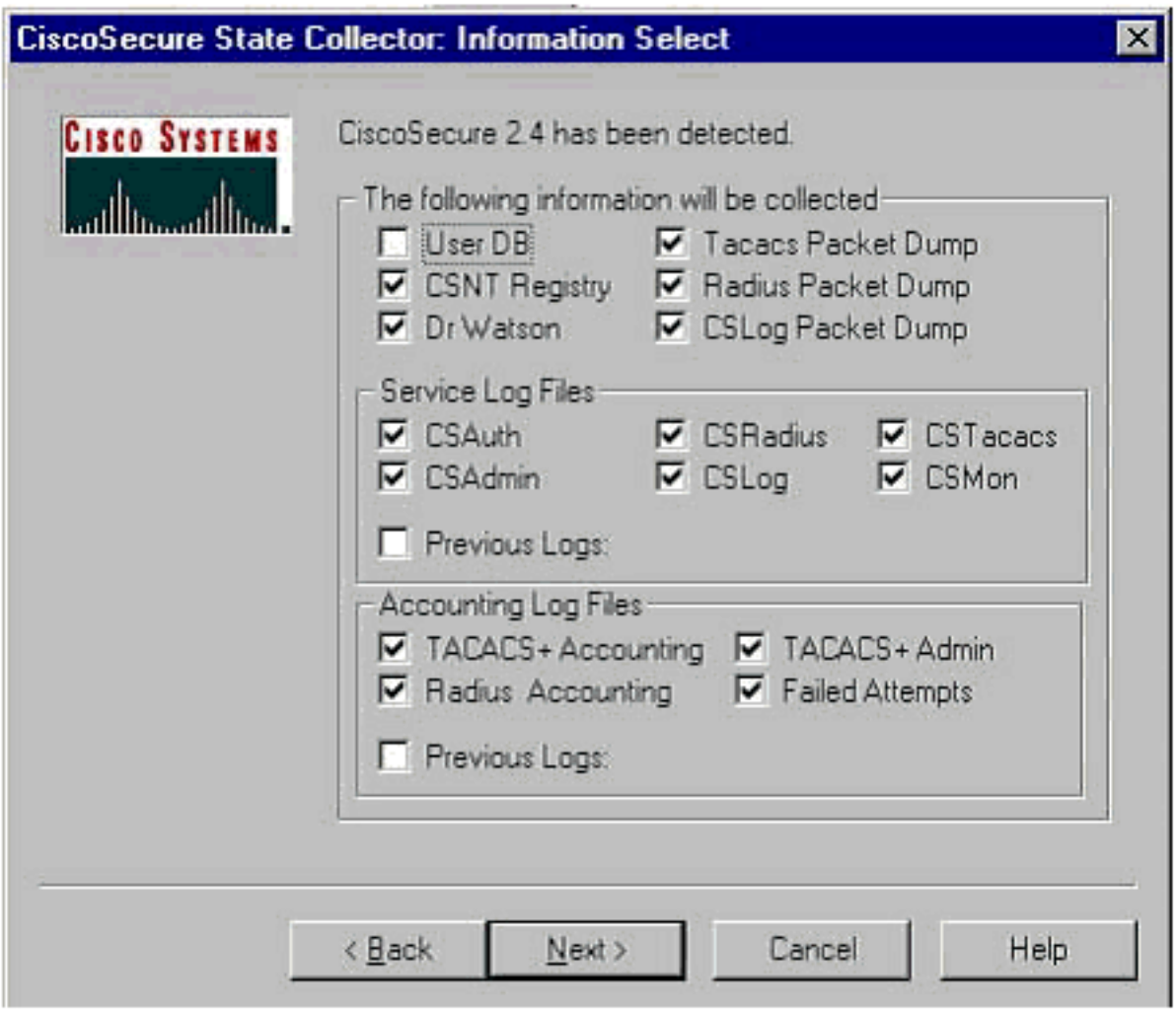
- Exécutez l'assistant, qui vous mène par une gamme de quatre étapes :Collecteur d'état Cisco Secure : Les informations choisiesCollecteur d'état Cisco Secure : Installation choisieCollecteur d'état Cisco Secure : Verbosité de logCollecteur d'état Cisco Secure (la collection réelle)ou
- Placez le log de niveau seulement, qui te permet pour ignorer les étapes premières et pour aller directement au collecteur d'état Cisco Secure : Écran Verbosity de log

Pour une installation pour la première fois, l'**assistant** choisi de **passage** à poursuivre par les étapes a dû placer le log. Après la première installation, vous pouvez employer l'**option Set Log Levels Only** pour ajuster les niveaux se connectants. Faites votre sélection, et cliquez sur Next.

Exécutez l'assistant

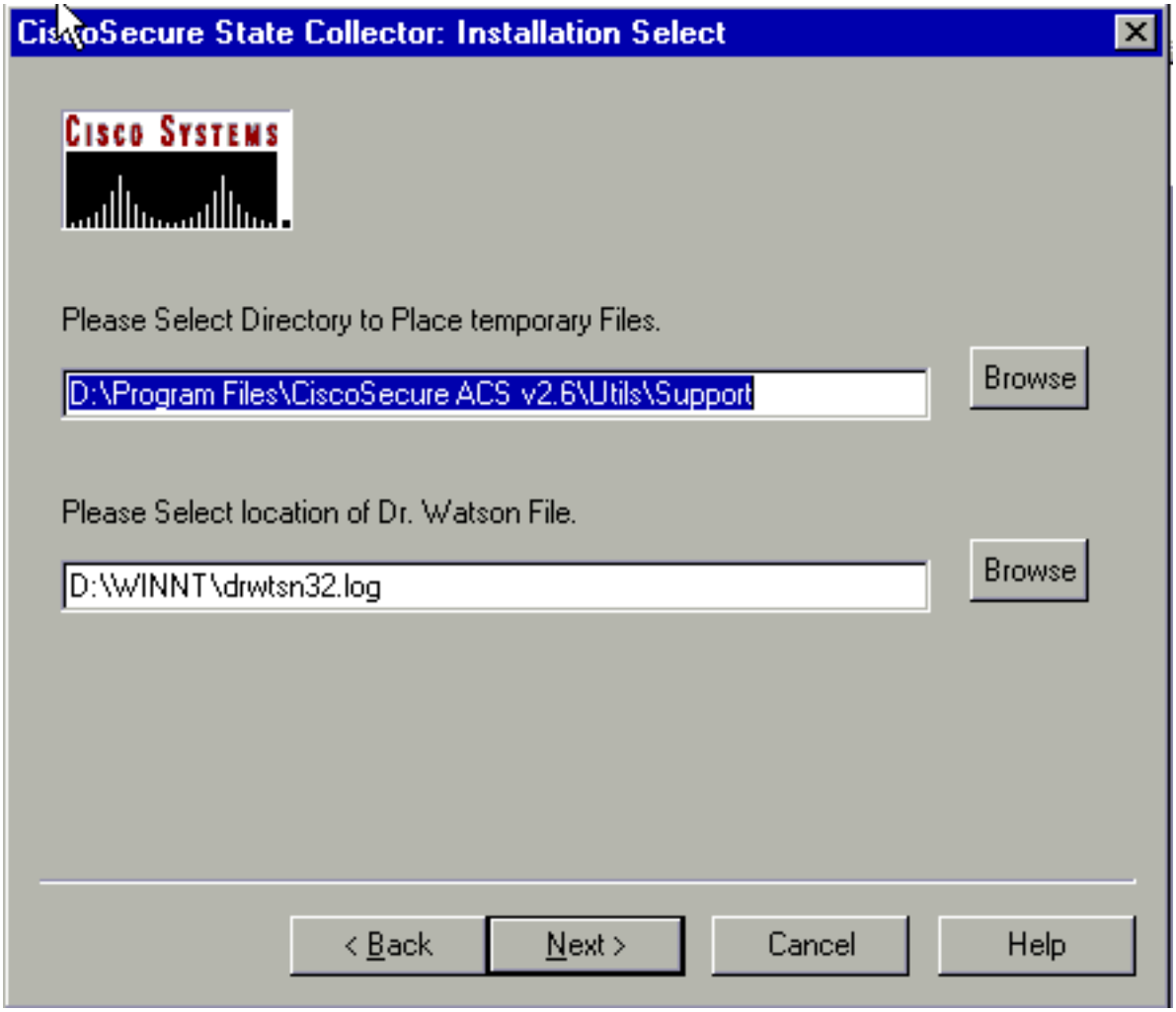
Ce qui suit explique comment sélectionner les informations utilisant l'option d'assistant de passage.

1. **Collecteur d'état Cisco Secure : Les informations** choisiesToutes les options devraient être sélectionnées par défaut excepté le DB d'utilisateur et les logs précédents. Si vous pensez que votre problème est la base de données d'utilisateur ou de groupe, alors sélectionnez le **DB d'utilisateur**. Si vous voudriez faire inclure de vieux logs, sélectionnez l'option pour les **logs précédents**. Cliquez sur Next quand vous êtes de

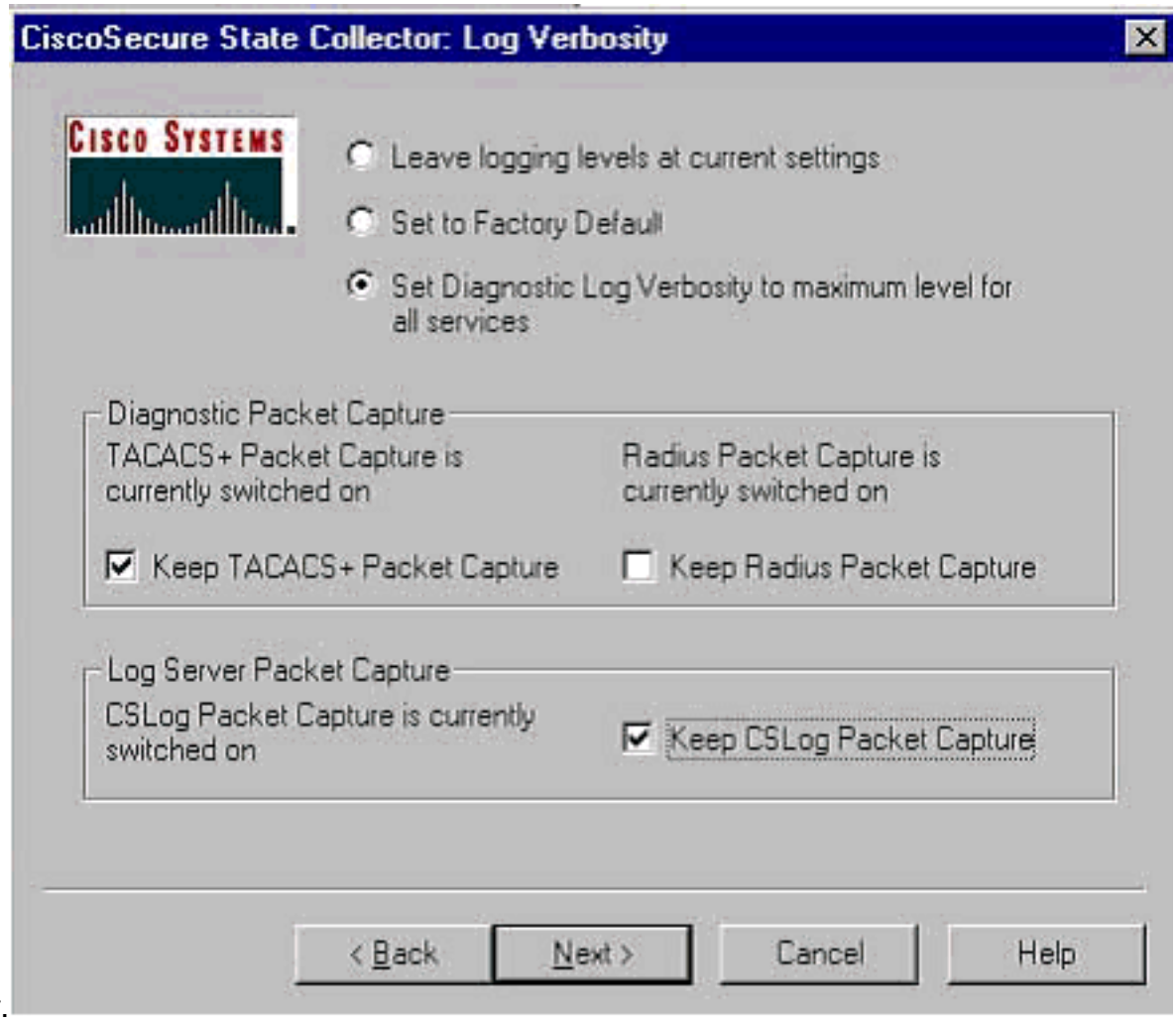


finition.

2. **Collecteur d'état Cisco Secure : Installation choisie**Choisissez le répertoire dans lequel vous voulez placer le package.cab. Le par défaut est le Secure ACS v.26\Utils\Support de C:\Program Files\Cisco. Vous pouvez changer cet emplacement si vous désirez. Assurez-vous que l'emplacement approprié de votre Dr. Watson est spécifié. Exécuter CSSupport exige que vous commencez et arrêtez les services. Si vous êtes sûr que vous voulez arrêter et commencer les services Cisco Secures, le clic à côté de continuent.

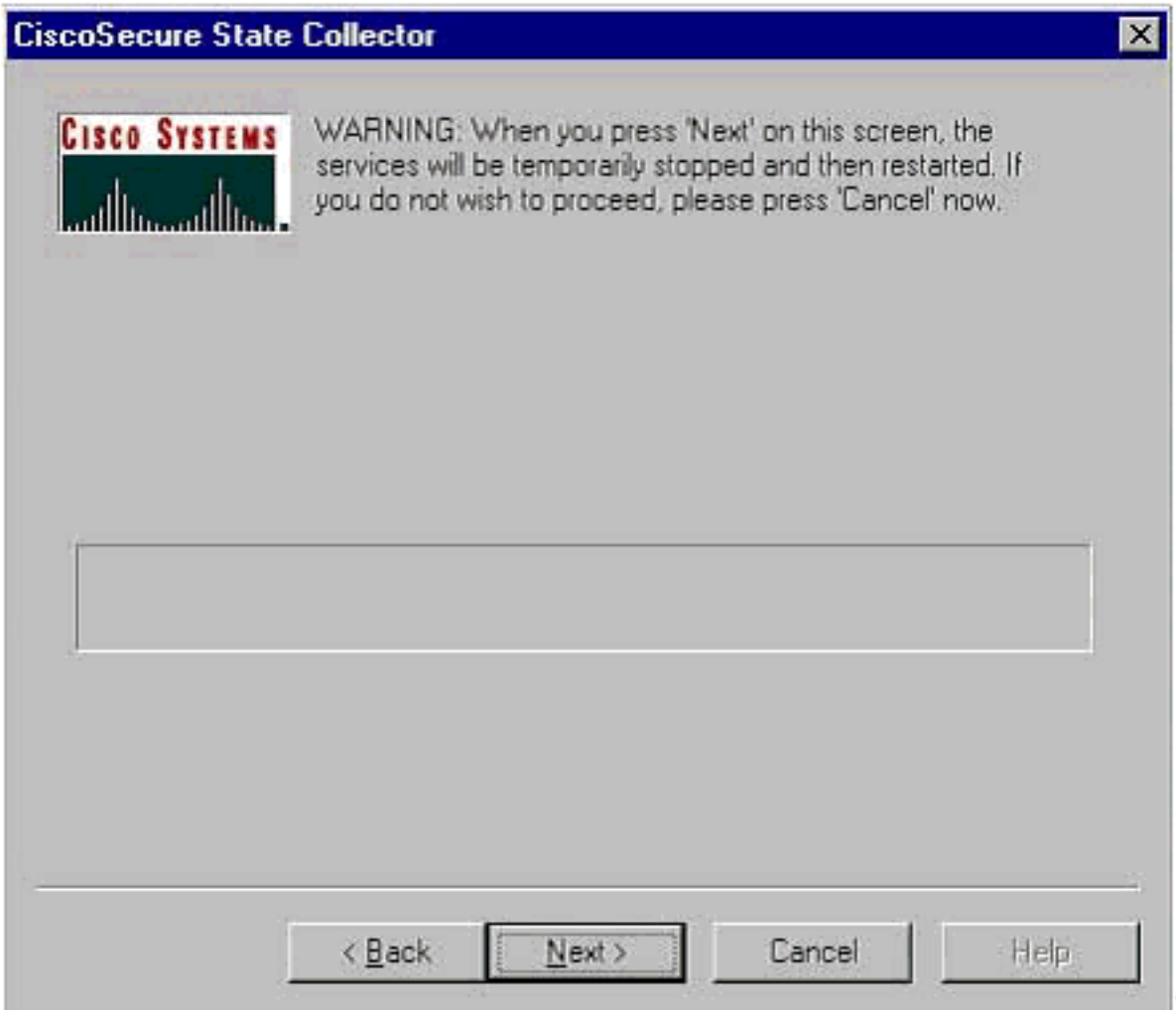


3. **Collecteur d'état Cisco Secure : Verbosité de log**Sélectionnez l'option pour la **verbosité de log diagnostique de positionnement au taux maximum pour tous les services**. Sous le titre de capture de paquet de diagnostic, sélectionnez TACACS+ ou RAYON, selon ce que vous exécutez. Sélectionnez l'option de **capture de paquet de CSLog de conservation**. Quand vous êtes de finition, cliquez sur Next.**Remarque:** Si vous voulez avoir des logs des veilles, vous devez sélectionner l'option pour l'option **précédente de logs** dans l'étape 1 et puis placer le nombre de jours où vous voulez



retourner.

4. **Collecteur d'état Cisco Secure**Vous verrez un avertissement que les déclarer qui quand vous continuez, vos services seront arrêtés et puis redémarrés. Cette interruption est nécessaire pour que CSSupport saisisse tous les fichiers nécessaires. Le temps d'arrêt devrait être minimal. Vous pourrez observer l'arrêt et la reprise de services sur cette fenêtre. Le clic **à côté de**
poursuivent.



Quand la reprise de services, le package.cab peut être trouvée dans l'emplacement spécifié. Cliquez sur Finish**, et** votre fichier package.cab est prêt.Parcourez à l'emplacement que vous avez spécifié pour le package.cab et replacez l'à un répertoire où il peut être enregistré. Votre ingénieur de Soutien technique peut le demander à tout moment pendant le processus de dépannage.

Placez les niveaux de log seulement

Si vous avez précédemment exécuté le collecteur d'état et devez seulement changer les niveaux se connectants, vous pouvez employer l'option Set Log Levels Only pour ignorer au collecteur d'état Cisco Secure : Connectez-vous l'écran Verbosity, où vous placez la capture de paquet de diagnostic. Quand vous cliquez sur Next, vous irez directement à la page d'avertissement. Cliquez sur Next alors de nouveau pour arrêter le service, recueillez le fichier, et redémarrez les services.

Collectant un fichier package.cab manuellement

Ce qui suit est une liste des fichiers qui sont compilés dans un package.cab. Si le CSSupport ne fonctionne pas correctement, vous pouvez recueillir ces fichiers utilisant 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
```

Obtenir Cisco Secure pour les informations de debug d'AAA de Windows NT

Des services de Windows NT CSRadius, de CSTacacs, et de CSAuth peuvent être dirigés dans le mode ligne de commande quand vous dépannez un problème.

Remarque: L'accès GUI est limité si Cisco Secures pour des services de Windows NT s'en exécutent dans le mode ligne de commande.

Pour obtenir CSRadius, CSTacacs, ou CSAuth mettent au point les informations, ouvrent une fenêtre DOS et s'ajustent la taille du tampon d'écran des propriétés de Windows à 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
```

Obtenir Cisco Secure pour les informations de debug de réplication d'AAA de Windows NT

Les services de Windows NT CSAuth peuvent être dirigés dans le mode ligne de commande

quand vous dépannez un problème de réplication.

Remarque: L'accès GUI est limité si Cisco Secures pour des services de Windows NT s'en exécutent dans le mode ligne de commande.

Pour obtenir la réplication de CSAuth mettez au point les informations, ouvrez une fenêtre DOS et ajustez la taille du tampon d'écran des propriétés de Windows à 300.

Utilisez les commandes suivantes pour CSAuth sur la source et les serveurs de 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 commande, et il entre également dans le fichier $BASE \ csauth \ logs \ auth.log.

Authentification de l'utilisateur de test hors ligne

L'authentification de l'utilisateur peut être testée par l'interface de ligne de commande (CLI). Le RAYON peut être testé avec « radtest, » et TACACS+ peut être testé avec « tactest. » Ceci teste peut être utile si le périphérique de communication n'est pas production utile mettent au point les informations, et s'il y a une certaine question de savoir si il y a un problème de Windows de Cisco Secure ACS ou un problème de périphérique. Radtest et tactest trouvez-vous dans le répertoire $BASE \ utils. Ce qui suit sont des exemples de chaque test.

Authentification d'utilisateur RADIUS de test off-line 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.
```

Authentification de l'utilisateur de test TACACS+ off-line 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 pour des pannes de base de données de Windows 2000/NT

Si l'authentification est passée à Windows 2000/NT mais manque, vous pouvez activer l'installation d'audit de Windows en allant **programme > les outils d'administration > l'User Manager pour des domaines, des stratégies > audit**. Aller **programme > des** échecs d'authentification d'expositions d'**Administrative Tools > Event Viewer**. Des pannes trouvées dans le log des essais ratés sont affichées dans un format suivant les indications de l'exemple ci-dessous.

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

Ces messages peuvent être recherchés sur le site Web de Microsoft au Windows 2000 événement et messages d'erreur et codes d'erreur dans Windows NT .

Le message d'erreur 1300L est décrit comme affiché 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

Bonne authentification de RAYON

```
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 erronée de RAYON

```
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>

Bonne authentification TACACS+

```
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 erronée TACACS+ (récapitulée)

```
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