Recupero delle informazioni di debug su versione e AAA per Cisco Secure ACS per Windows

Sommario

Introduzione
Operazioni preliminari
Convenzioni
Prerequisiti
Componenti usati
Informazioni sulla versione di Cisco Secure for Windows
Utilizzo della riga di comando DOS
Uso della GUI
Impostazione di Cisco Secure ACS per i livelli di debug di Windows
Come impostare il livello di registrazione su Full nell'interfaccia grafica di ACS
Come impostare la registrazione di Dr. Watson
Creazione di un file package.cab
Cos'è il file package.cab?
Creazione di un file package.cab con l'utilità CSSupport.exe
Raccolta manuale di un file package.cab
Informazioni sul debug di Cisco Secure for Windows NT AAA
Recupero delle informazioni di debug della replica di Cisco Secure per Windows NT AAA
Test dell'autenticazione utente offline
Determinazione delle cause degli errori del database Windows 2000/NT
Esempi
Autenticazione valida RADIUS
Autenticazione non valida RADIUS
Autenticazione TACACS+ corretta
Autenticazione TACACS+ non valida (riepilogo)
Informazioni correlate

Introduzione

Questo documento spiega come visualizzare la versione di Cisco Secure ACS per Windows e come configurare e ottenere le informazioni di debug per l'autenticazione, l'autorizzazione e l'accounting (AAA).

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni di questo documento si basano su Cisco Secure ACS per Windows 2.6.

Informazioni sulla versione di Cisco Secure for Windows

Èpossibile visualizzare le informazioni sulla versione utilizzando la riga di comando DOC o la GUI.

Utilizzo della riga di comando DOS

Per visualizzare il numero di versione di Cisco Secure ACS per Windows tramite l'opzione della riga di comando in DOS, utilizzare **cstacacs** o **csradius** seguito da **-v** per RADIUS e **-x** per TACACS+. Vedere gli esempi seguenti:

```
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
```

Èinoltre possibile visualizzare il numero di versione del programma Cisco Secure ACS nel Registro di sistema di Windows. Ad esempio:

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

Uso della GUI

Per visualizzare la versione con l'interfaccia utente grafica di Cisco Secure ACS, andare alla home page di ACS. È possibile eseguire questa operazione in qualsiasi momento facendo clic sul logo Cisco Systems nell'angolo in alto a sinistra dello schermo. Nella metà inferiore della home page verrà visualizzata la versione completa.

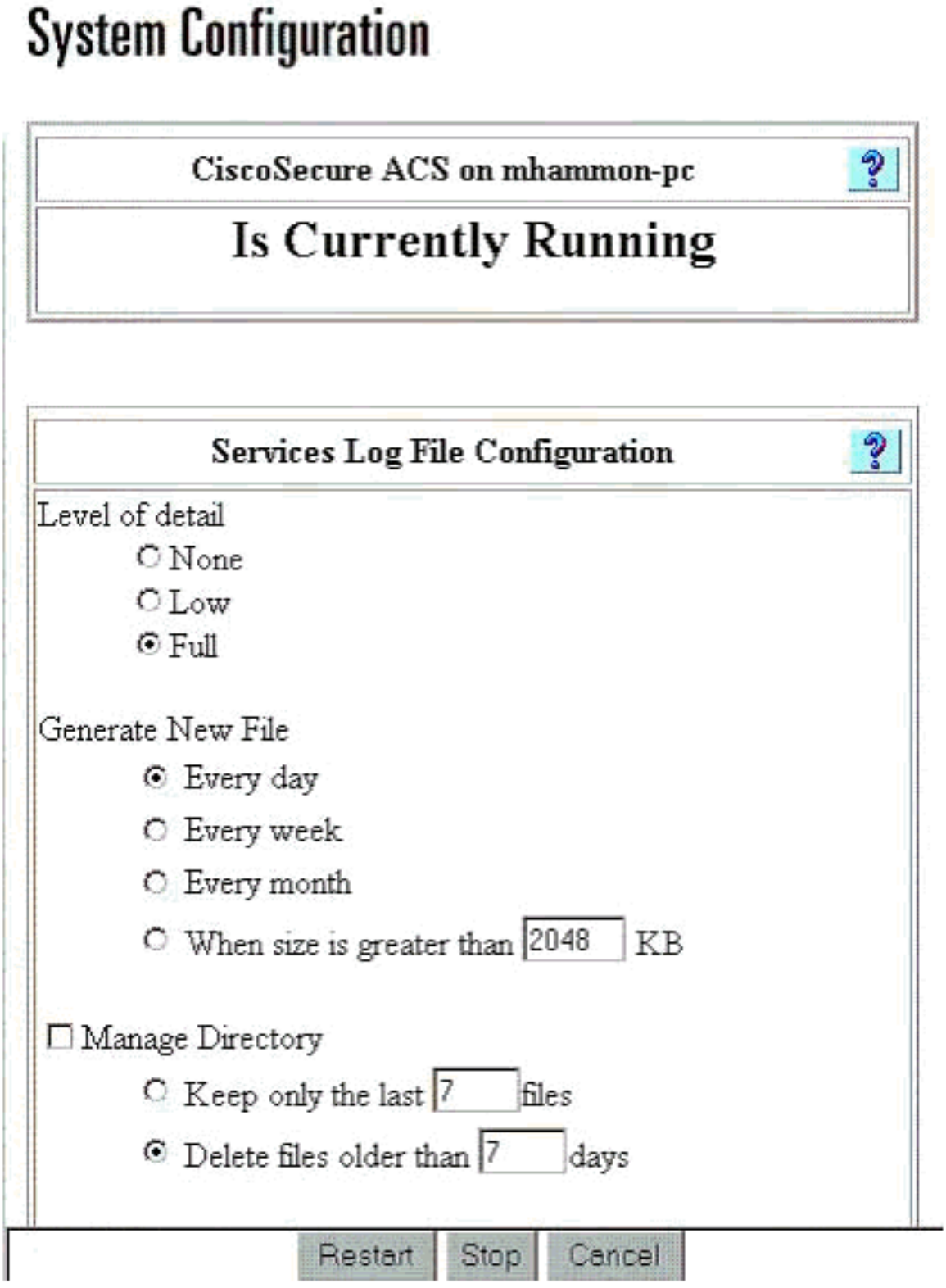
Impostazione di Cisco Secure ACS per i livelli di debug di Windows

Di seguito viene fornita una spiegazione delle diverse opzioni di debug necessarie per ottenere le informazioni di debug massime.

Come impostare il livello di registrazione su Full nell'interfaccia grafica di ACS

Per registrare tutti i messaggi, è necessario impostare ACS. A tale scopo, eseguire la procedura seguente:

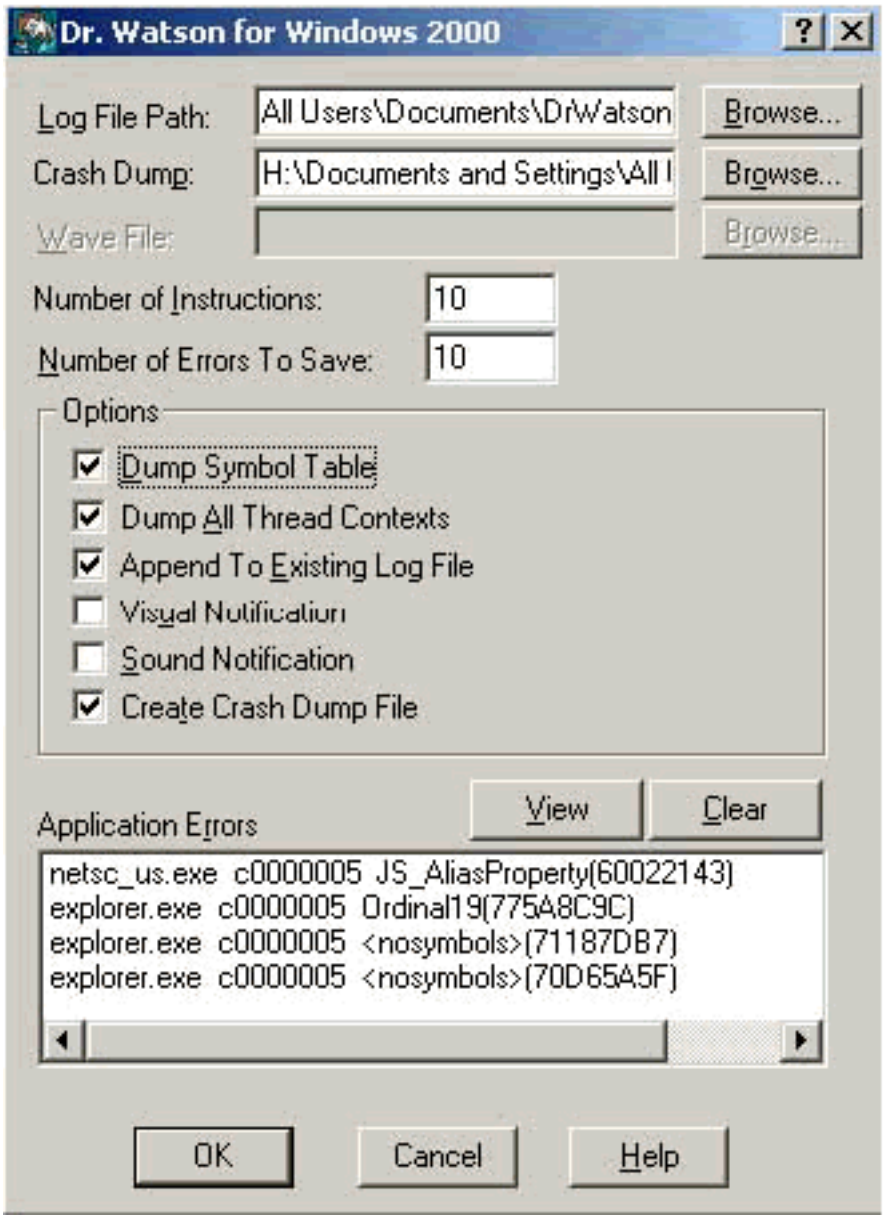
1. Dalla home page di ACS, selezionare **Configurazione sistemi > Controllo servizio**.
2. In Configurazione file di log del servizio impostare il livello di dettaglio su **Completo**.Se necessario, è possibile modificare le sezioni Genera nuovo file e Gestisci



directory.

Come impostare la registrazione di Dr. Watson

Al prompt dei comandi digitare **drwtsn32** per visualizzare la finestra Dr. Watson. Accertatevi che le opzioni **Dump tutti i contesti di filetto** e **Dump tabella simboli (Dump Symbol Table)** siano selezionate.



Creazione di un file package.cab

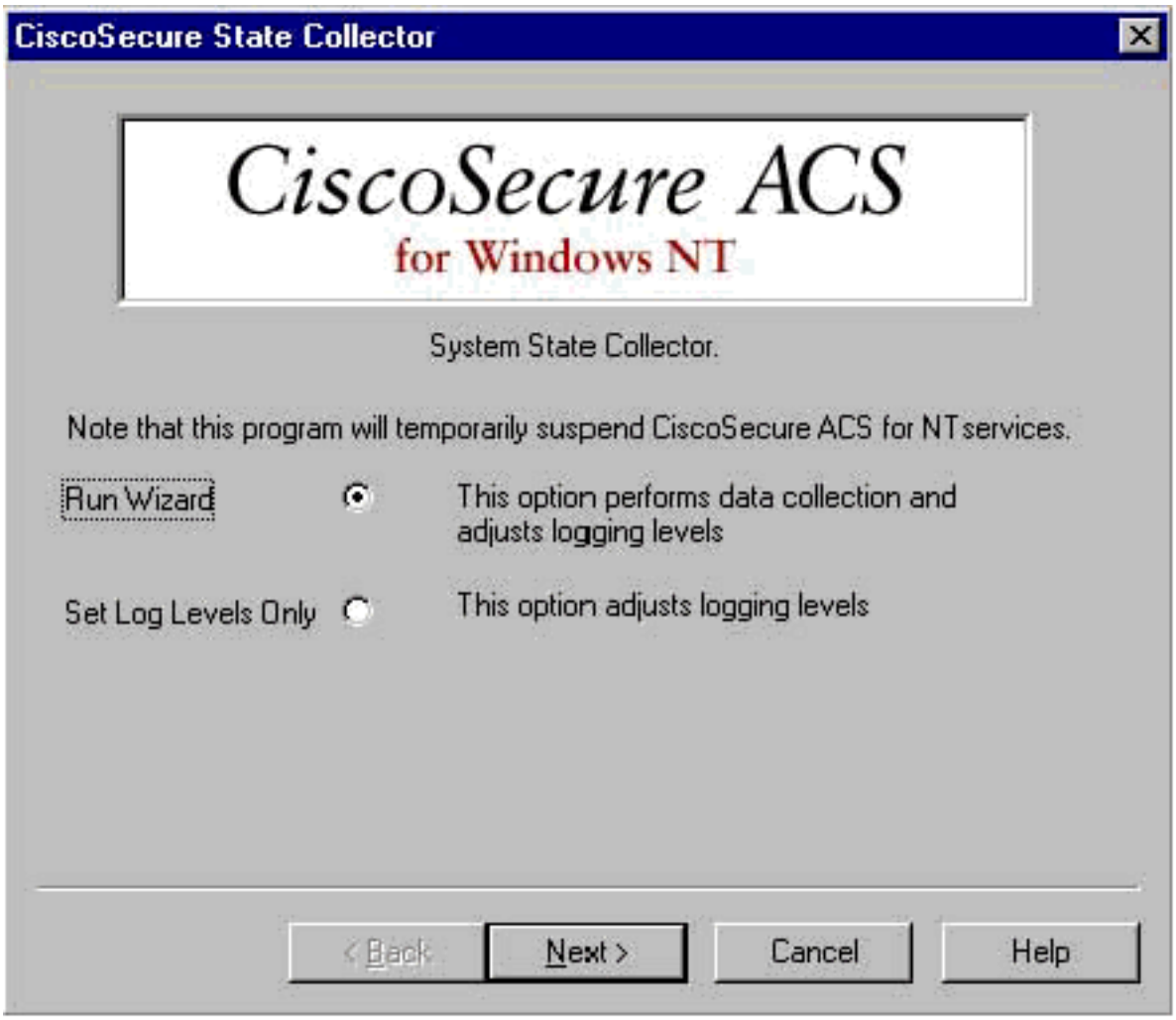
Cos'è il file package.cab?

Il file package.cab è un file Zip che contiene tutti i file necessari per risolvere in modo efficiente i problemi relativi ad ACS. È possibile utilizzare l'utilità CSSupport.exe per creare package.cab oppure raccogliere i file manualmente.

Creazione di un file package.cab con l'utilità CSSupport.exe

Se si verifica un problema ACS per il quale è necessario raccogliere informazioni, eseguire il file CSSupport.exe il più presto possibile dopo aver rilevato il problema. Utilizzare la riga di comando DOS o l'interfaccia utente di Esplora risorse per eseguire CSSupport da C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe.

Quando si esegue il file CSSupport.exe, viene visualizzata la seguente finestra.



In questa schermata sono disponibili due opzioni principali:

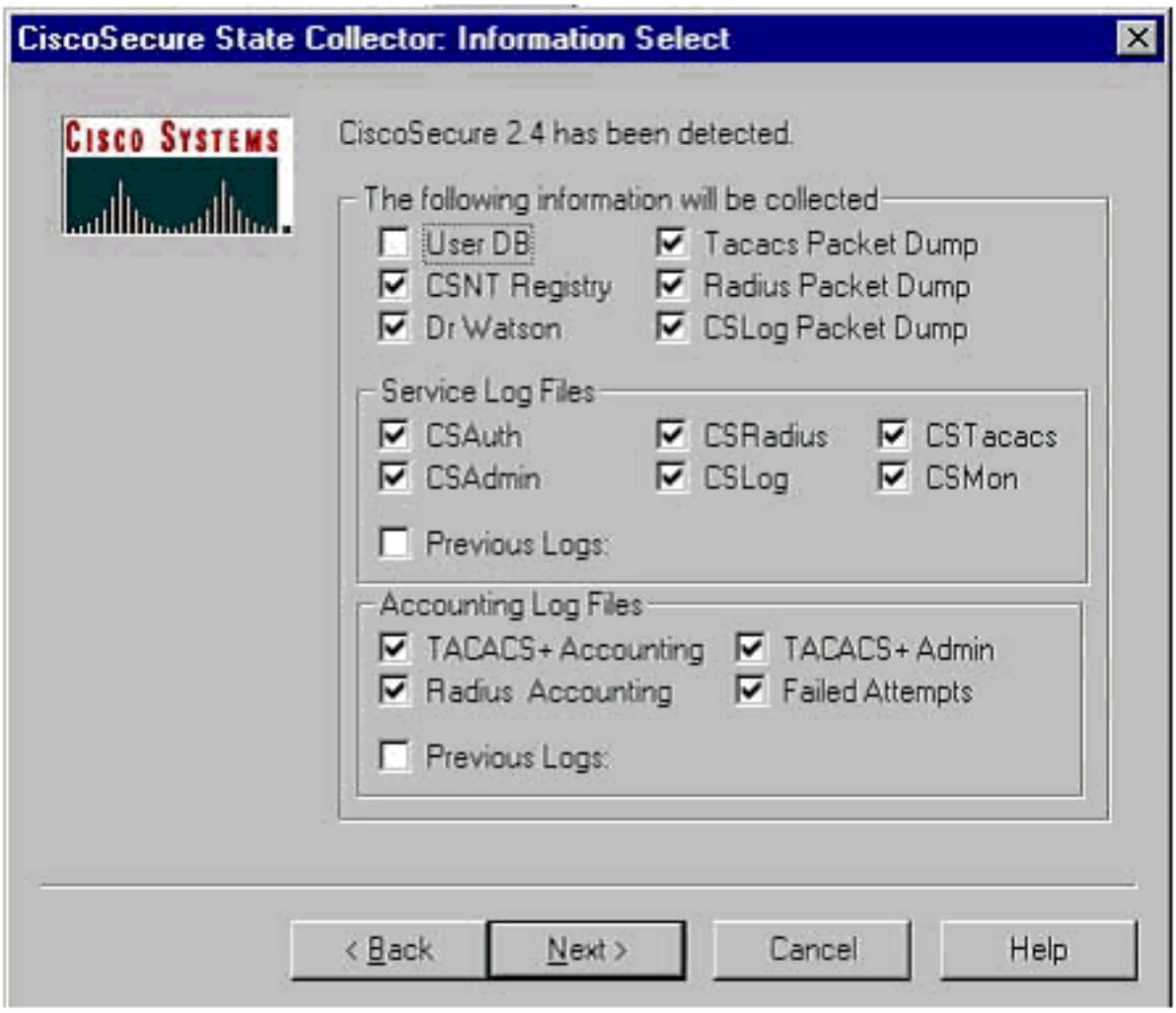
- Eseguire la procedura guidata, che consente di eseguire una serie di quattro passaggi:Cisco Secure State Collector: Selezione informazioniCisco Secure State Collector: Selezione installazioneCisco Secure State Collector: Livello di dettaglio logCisco Secure State Collector (raccolta effettiva)o
- Set Log Level Only, per ignorare i primi passaggi e accedere direttamente a Cisco Secure State Collector: schermata Log Verbosity

Per eseguire la prima installazione, selezionare **Esegui procedura guidata** per eseguire i passaggi necessari per impostare il registro. Dopo la configurazione iniziale, è possibile utilizzare l'opzione **Imposta solo livelli di log** per regolare i livelli di log. Effettuare la selezione e fare clic su **Avanti**.

Esegui procedura guidata

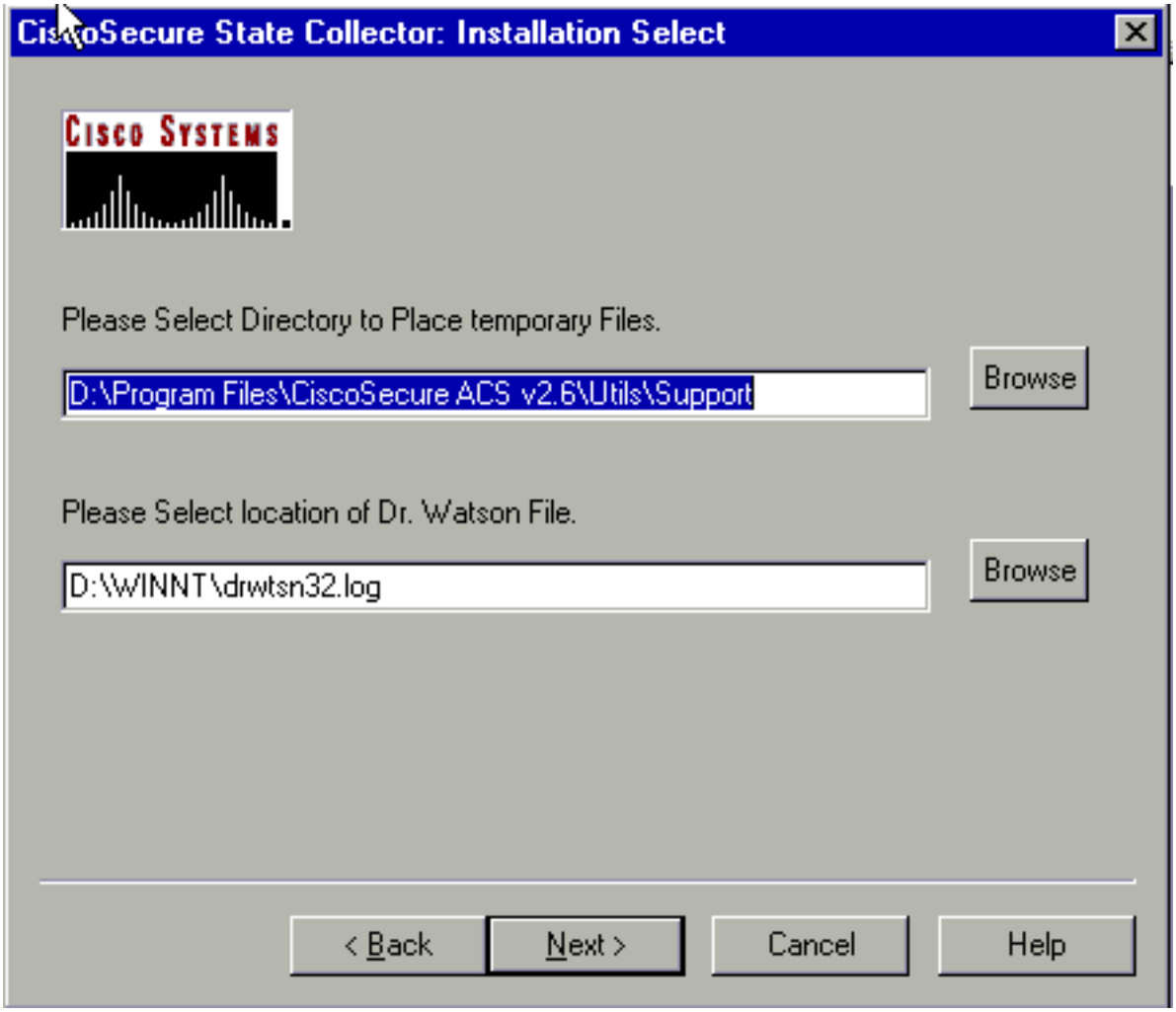
Di seguito viene illustrato come selezionare le informazioni utilizzando l'opzione Esegui procedura guidata.

1. **Cisco Secure State Collector:** Selezione **informazioni**Tutte le opzioni devono essere selezionate per impostazione predefinita, ad eccezione di User DB e Previous Logs. Se si ritiene che il problema riguardi il database utenti o gruppi, selezionare **Database utenti**. Se si desidera includere i log precedenti, selezionare l'opzione **Log precedenti**. Al termine, fare clic su

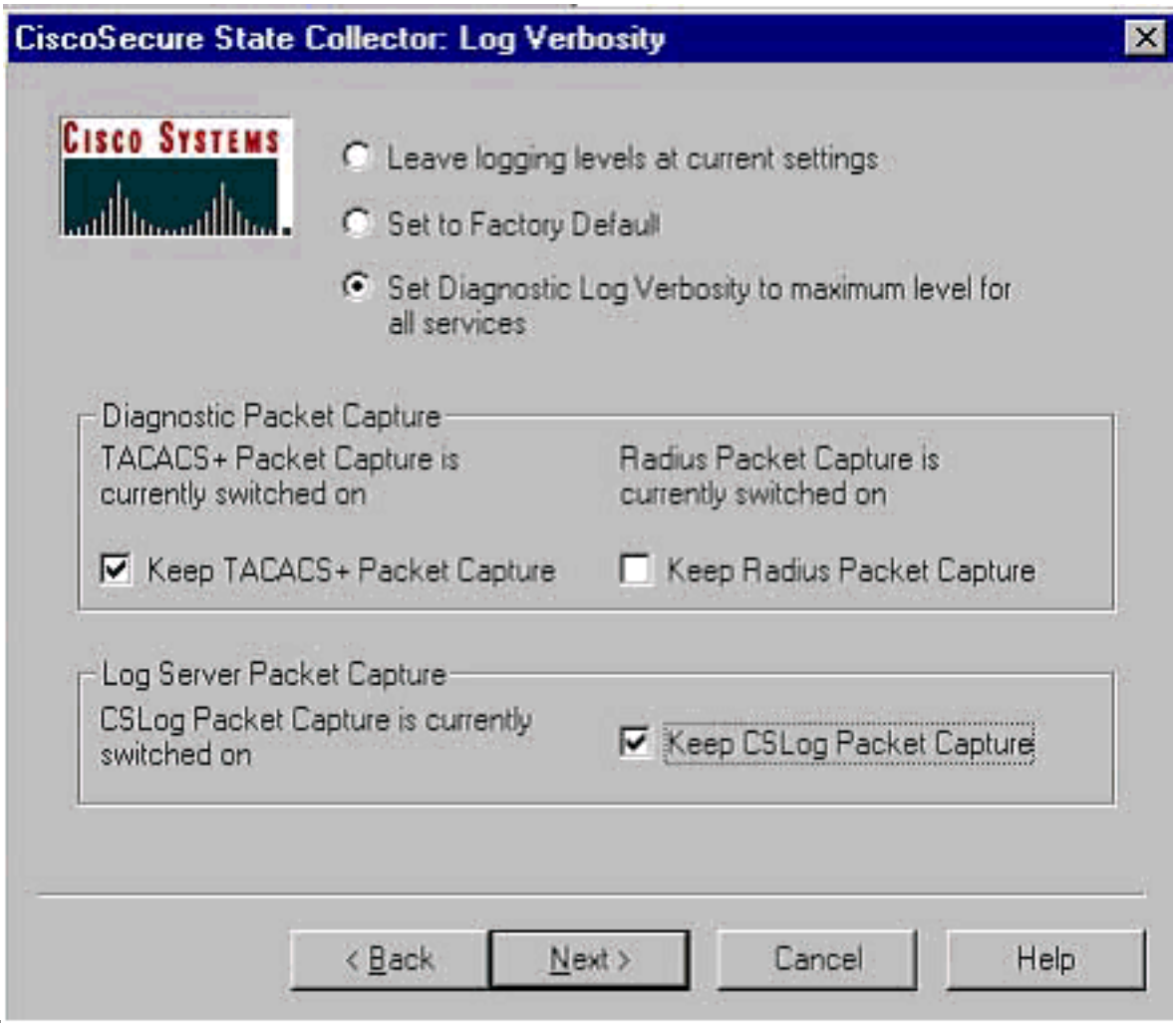


Avanti.

2. **Cisco Secure State Collector: Selezione installazione**Scegliere la directory in cui inserire il file package.cab. Il valore predefinito è C:\Program Files\Cisco Secure ACS v.26\Utils\Support. Se lo desideri, puoi cambiare questa posizione. Verificare che sia specificata la posizione corretta di Dr. Watson. L'esecuzione di CSSsupport richiede l'avvio e l'arresto dei servizi. Se si è certi di voler arrestare e avviare i servizi Cisco Secure, fare clic su **Avanti** per
continuare.

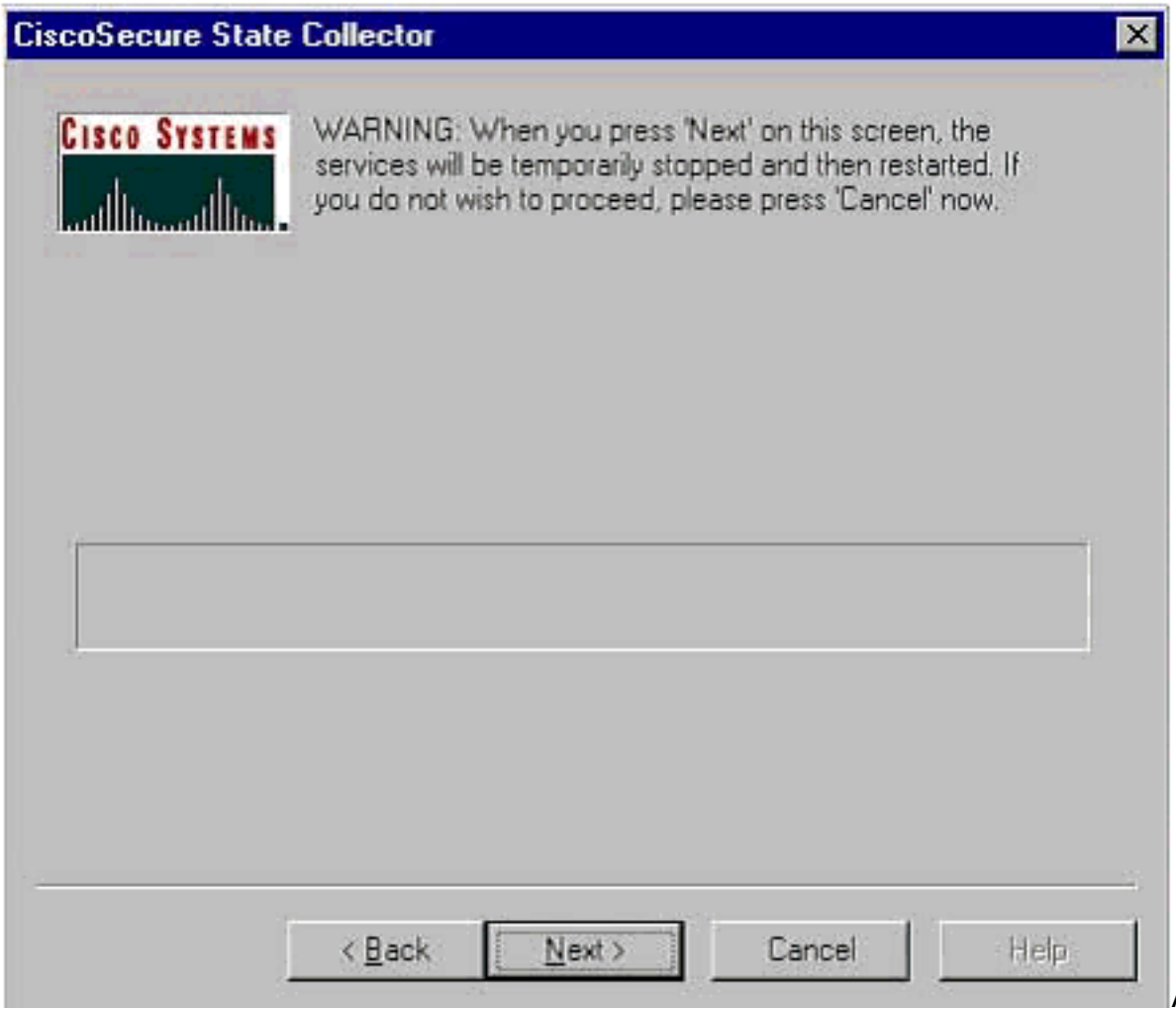


3. **Cisco Secure State Collector: Livello di dettaglio log**Selezionare l'opzione per **Impostare il livello di dettaglio del registro diagnostico sul livello massimo per tutti i servizi**. Sotto l'intestazione Acquisizione pacchetti diagnostici, selezionare TACACS+ o RADIUS, a seconda di cosa si sta eseguendo. Selezionare l'opzione **Keep CSLog Packet Capture**. Al termine, fare clic su **Avanti**.**Nota:** se si desidera disporre di log dei giorni precedenti, è necessario selezionare l'opzione per l'opzione **Log precedenti** nel passo 1 e quindi impostare il numero di giorni che si desidera tornare



indietro.

4. **Cisco Secure State Collector**Verrà visualizzato un avviso che indica che quando si continua, i servizi verranno arrestati e quindi riavviati. Questa interruzione è necessaria affinché CSSupport possa recuperare tutti i file necessari. Il tempo di inattività deve essere minimo. In questa finestra è possibile visualizzare l'arresto e il riavvio dei servizi. Fare clic su **Avanti** per continuare.



Al riavvio dei servizi, package.cab è disponibile nel percorso specificato. Fare clic su **Finish** e il file package.cab è pronto.Individuare il percorso specificato per il file package.cab e riposizionarlo in una directory in cui è possibile salvarlo. Il tecnico dell'assistenza può richiederlo in qualsiasi momento durante il processo di risoluzione dei problemi.

Imposta solo livelli di log

Se l'agente di raccolta dello stato è già stato eseguito e occorre modificare solo i livelli di registrazione, è possibile utilizzare l'opzione Imposta solo livelli di registrazione per passare a Cisco Secure State Collector: Log Verbosity, schermata in cui è possibile impostare l'acquisizione dei pacchetti diagnostici. Quando si fa clic su **Avanti**, viene visualizzata direttamente la pagina Avviso. Quindi fare di nuovo clic su **Avanti** per arrestare il servizio, raccogliere il file e riavviare i servizi.

Raccolta manuale di un file package.cab

Di seguito è riportato un elenco dei file compilati in package.cab. Se CSSupport non funziona correttamente, è possibile raccogliere questi file utilizzando Esplora risorse.

```
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
```

Informazioni sul debug di Cisco Secure for Windows NT AAA

I servizi CSRadius, CSTacacs e CSAuth di Windows NT possono essere eseguiti in modalità riga di comando quando si sta risolvendo un problema.

Nota: l'accesso alla GUI è limitato se i servizi Cisco Secure for Windows NT sono in esecuzione in modalità riga di comando.

Per ottenere informazioni sul debug di CSRadius, CSTacacs o CSAuth, aprire una finestra DOS e impostare l'altezza del buffer dello schermo della proprietà Windows su 300.

Utilizzare i seguenti comandi per CSRadius:

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

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

Utilizzare i seguenti comandi per CSTacacs:

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

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

Recupero delle informazioni di debug della replica di Cisco Secure per Windows NT AAA

I servizi CSAuth di Windows NT possono essere eseguiti nella modalità riga di comando quando si risolve un problema di replica.

Nota: l'accesso alla GUI è limitato se i servizi Cisco Secure for Windows NT sono in esecuzione in modalità riga di comando.

Per ottenere informazioni sul debug della replica CSAuth, aprire una finestra DOS e impostare la proprietà Windows Screen Buffer height su 300.

Utilizzare i seguenti comandi per CSAuth sia sul server di origine che su quello di destinazione:

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

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

Il comando debug viene scritto nella finestra del prompt dei comandi e nel file $BASE\csauth\logs\auth.log.

Test dell'autenticazione utente offline

L'autenticazione utente può essere verificata tramite l'interfaccia della riga di comando (CLI). RADIUS può essere testato con "radtest" e TACACS+ con "tactest". Questi test possono essere utili se il dispositivo in comunicazione non produce informazioni di debug utili e se ci si chiede se si sia verificato un problema con Cisco Secure ACS in Windows o un problema con il dispositivo. Sia radtest che tactest si trovano nella directory $BASE\utils. Di seguito sono riportati alcuni esempi di ciascun test.

Test dell'autenticazione utente RADIUS offline con 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 dell'autenticazione utente TACACS+ offline con 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>
```

Determinazione delle cause degli errori del database Windows 2000/NT

Se l'autenticazione viene passata a Windows 2000/NT ma non riesce, è possibile attivare la funzione di controllo di Windows selezionando **Programmi > Strumenti di amministrazione > User Manager for Domains, Policy > Controllo**. Passando a **Programmi > Strumenti di amministrazione > Visualizzatore eventi** vengono visualizzati gli errori di autenticazione. Gli errori rilevati nel registro dei tentativi non riusciti vengono visualizzati nel formato indicato nell'esempio seguente.

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

Per ulteriori informazioni su questi messaggi, visitare il sito Web Microsoft all'indirizzo Windows 2000 Event & Error Messages and Error Codes in Windows NT .

Il messaggio di errore 1300L è descritto come mostrato di seguito.

```
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.

Esempi

Autenticazione valida RADIUS

```
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>
```

Autenticazione non valida RADIUS

```
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>
```

Autenticazione TACACS+ corretta

```
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>
```

Autenticazione TACACS+ non valida (riepilogo)

```
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>
```

Informazioni correlate

- Supporto tecnico – Cisco Systems