Abrufen von Version- und AAA-Debuginformationen für Cisco Secure ACS für Windows

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Sie die Cisco Secure ACS-Version für Windows anzeigen und wie Sie AAA-Debugging-Informationen (Authentication, Authorization, Accounting) einrichten und abrufen.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure ACS für Windows 2.6.

Abrufen von Cisco Secure for Windows-Versionsinformationen

Sie können Versionsinformationen über die DOC-Befehlszeile oder über die GUI anzeigen.

Verwenden der DOS-Befehlszeile

Um die Versionsnummer von Cisco Secure ACS für Windows über die Befehlszeilenoption in DOS anzuzeigen, verwenden Sie **cstacs** oder **csradius** gefolgt von **-v** für RADIUS und **-x** für TACACS+. Beispiele finden Sie unten:

```
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
```

Möglicherweise sehen Sie auch die Versionsnummer des Cisco Secure ACS-Programms in der Windows-Registrierung. Beispiel:

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

Verwenden der Benutzeroberfläche

Um die Version mit der Cisco Secure ACS-GUI anzuzeigen, gehen Sie zur ACS-Startseite. Sie können dies jederzeit tun, indem Sie auf das Cisco Systems-Logo in der oberen linken Ecke des Bildschirms klicken. In der unteren Hälfte der Startseite wird die Vollversion angezeigt.

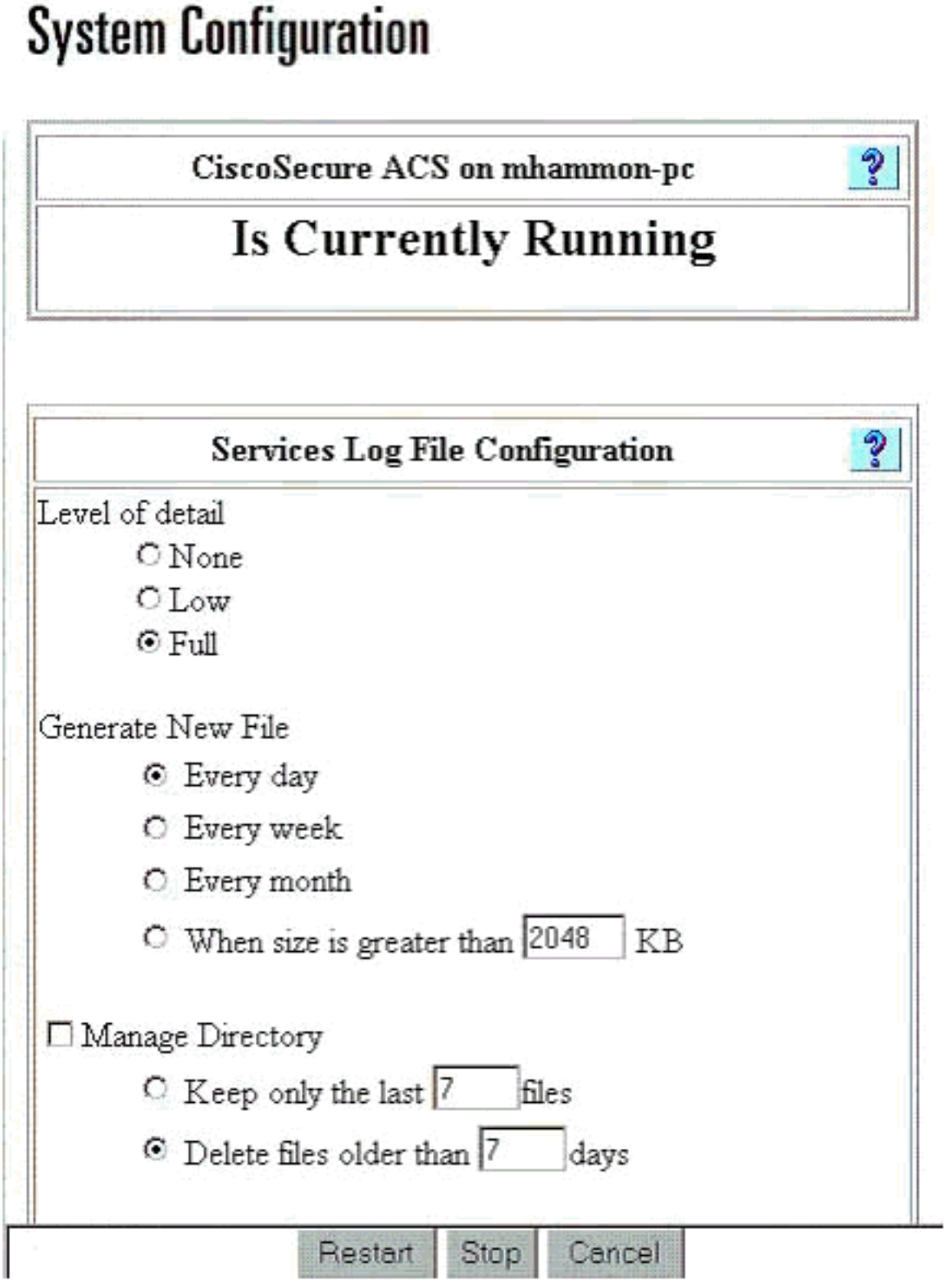
Festlegen von Cisco Secure ACS für Windows Debugging-Ebenen

Im Folgenden werden die verschiedenen Debugoptionen erläutert, die zum Abrufen der maximalen Debuginformationen erforderlich sind.

Festlegen der Protokollierungsebene in der ACS-GUI auf "Voll"

Sie müssen ACS festlegen, um alle Nachrichten zu protokollieren. Führen Sie dazu die unten aufgeführten Schritte aus:

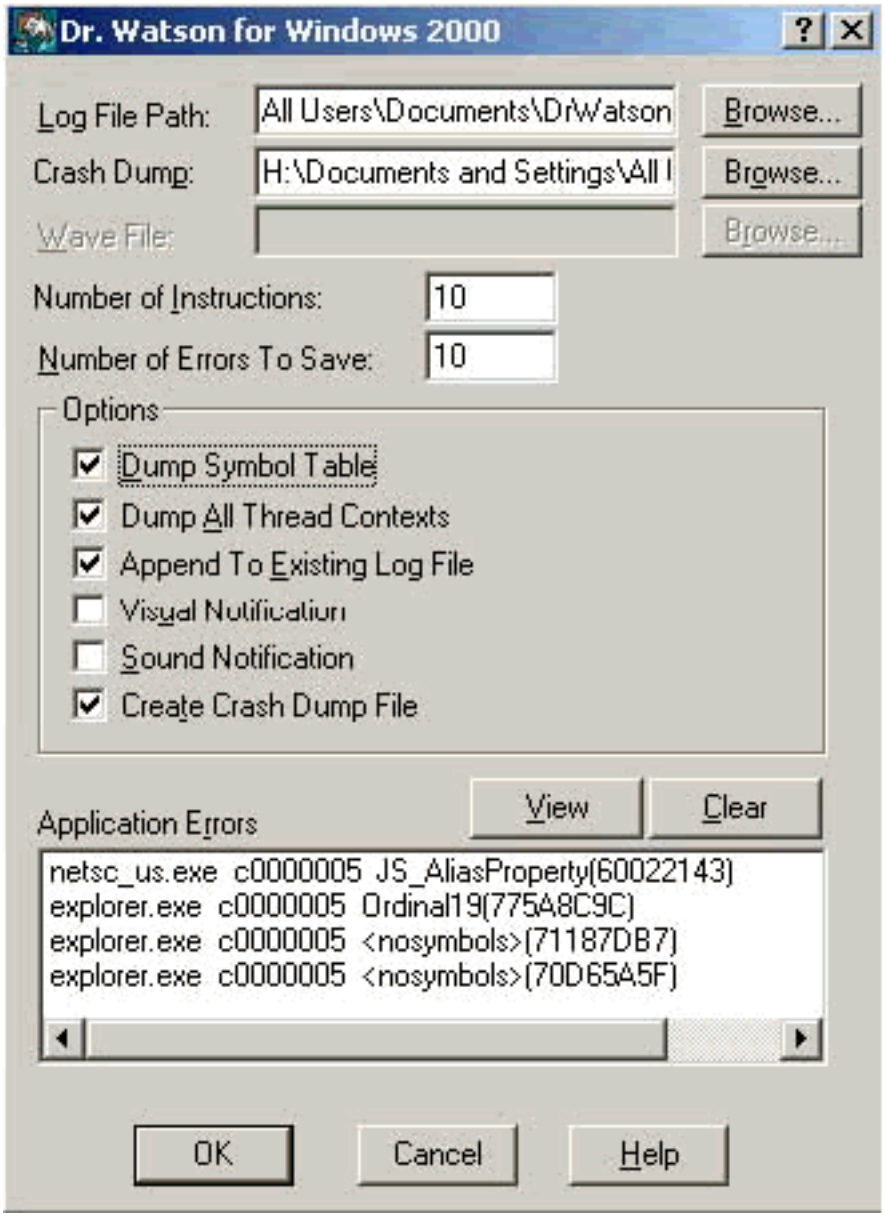
1. Gehen Sie auf der ACS-Startseite zu **Systems Configuration > Service Control**.
2. Legen Sie unter der Überschrift "Konfiguration der Service-Protokolldatei" die Detailstufe auf **Vollständig fest**.Sie können bei Bedarf die Abschnitte Neue Datei generieren und Verzeichnis verwalten



ändern.

Festlegen der Dr. Watson-Protokollierung

Geben Sie an der Eingabeaufforderung **drwtsn32** ein, und das Fenster Dr. Watson wird angezeigt. Stellen Sie sicher, dass die Optionen für **Dump All Thread Contexts** und **Dump Symbol Table** aktiviert sind.



Erstellen einer Package.cab-Datei

Was ist die Datei package.cab?

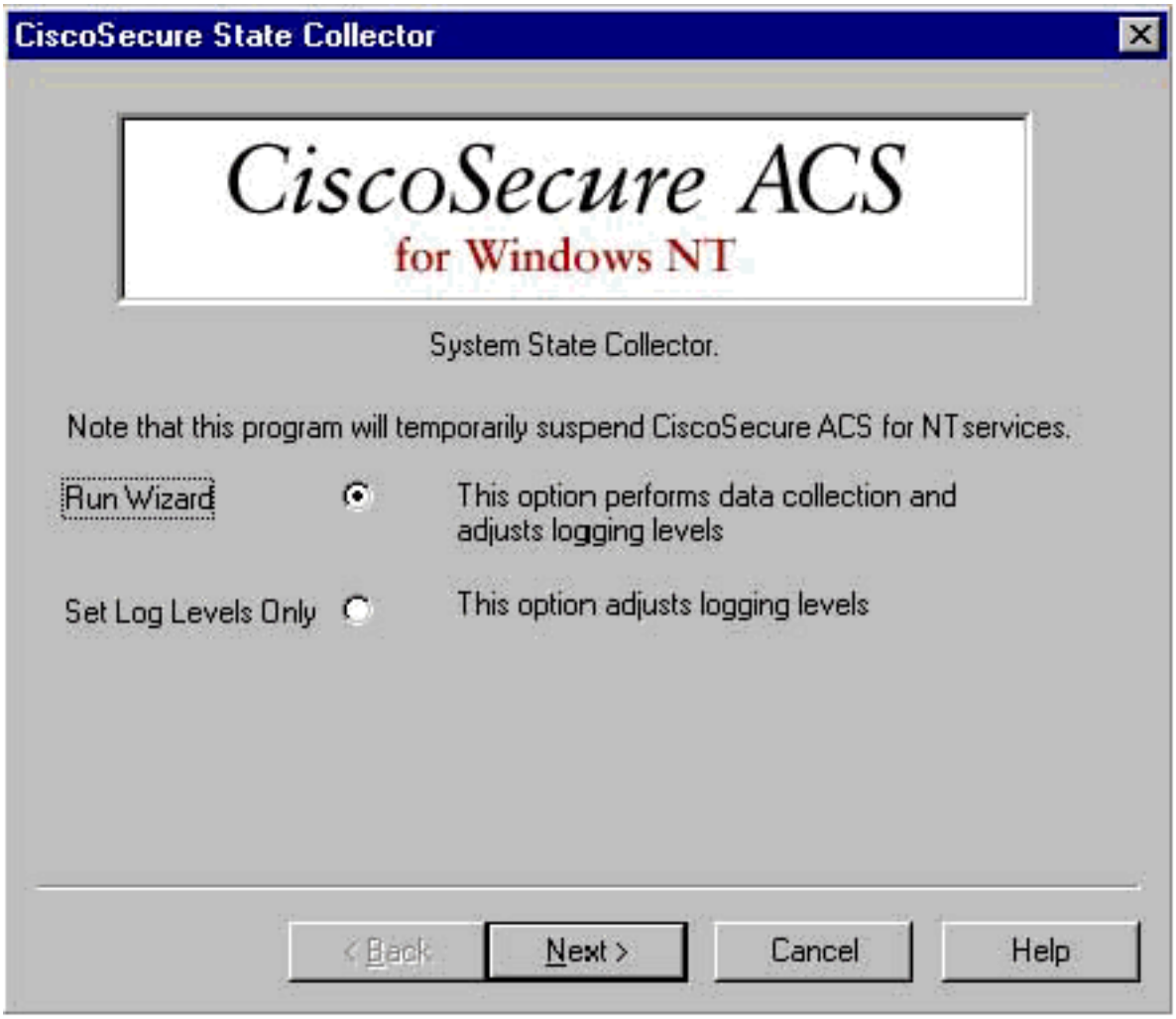
Die Datei package.cab ist eine Zip-Datei, die alle Dateien enthält, die für eine effiziente Fehlerbehebung im ACS erforderlich sind. Sie können das Dienstprogramm CSSupport.exe verwenden, um die Datei package.cab zu erstellen, oder Sie können die Dateien manuell erfassen.

Erstellen einer Datei "package.cab" mit dem Dienstprogramm "CSSupport.exe"

Wenn Sie ein ACS-Problem haben, für das Sie Informationen sammeln müssen, führen Sie die

Datei CSSupport.exe so schnell wie möglich aus, nachdem Sie das Problem festgestellt haben. Verwenden Sie die DOS-Befehlszeile oder die Windows Explorer-GUI, um CSSupport von C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe auszuführen.

Wenn Sie die Datei CSSupport.exe ausführen, wird das folgende Fenster angezeigt.



In diesem Bildschirm stehen zwei Hauptoptionen zur Verfügung:

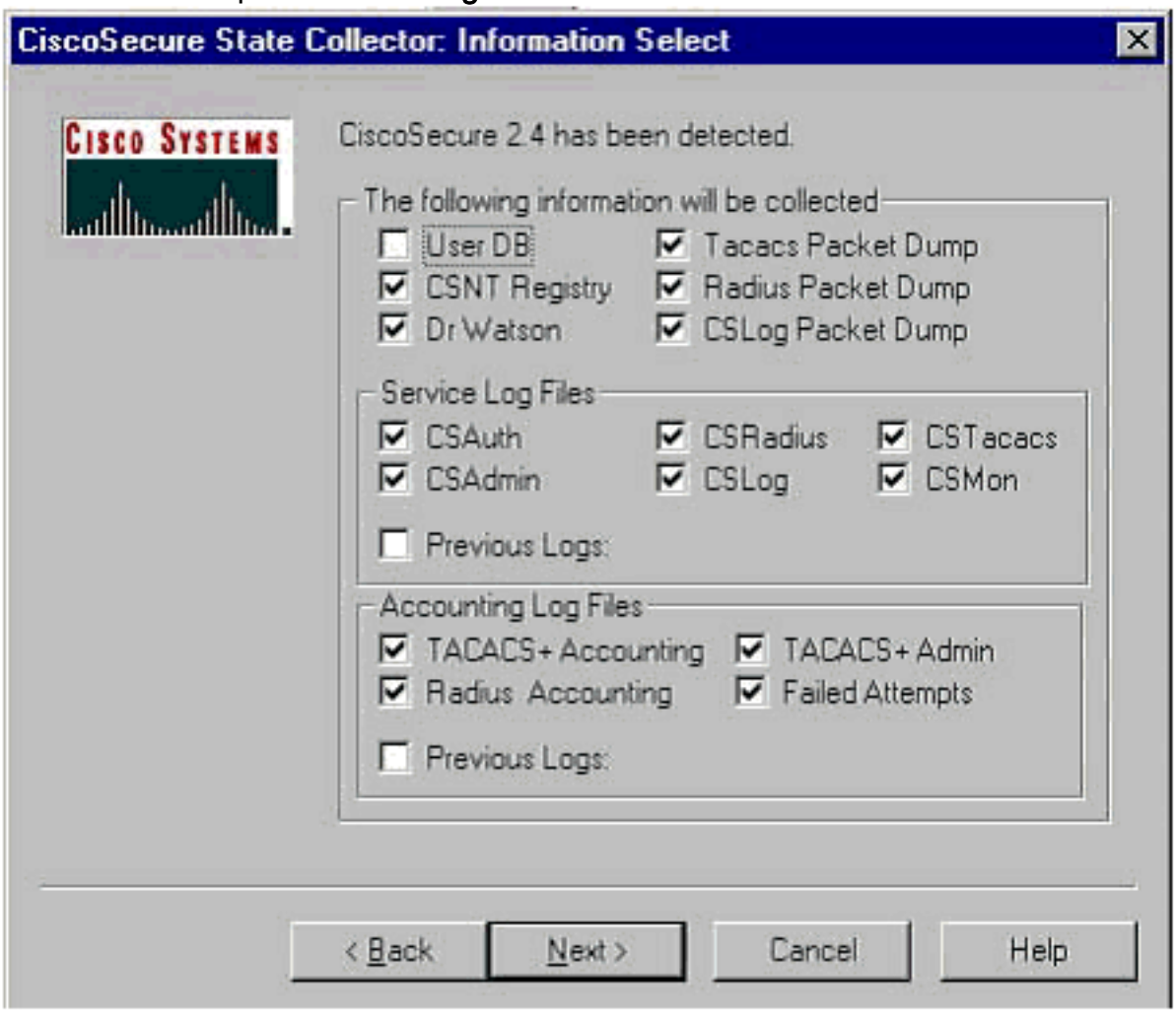
- Führen Sie einen Assistenten aus, der Sie in vier Schritten führt:Cisco Secure State Collector: InformationsauswahlCisco Secure State Collector: InstallationsauswahlCisco Secure State Collector: ProtokollausführlichkeitCisco Secure State Collector (die eigentliche Sammlung)oder
- Legen Sie nur Protokollstufe fest, sodass Sie die ersten Schritte überspringen und direkt zum Cisco Secure State Collector wechseln können: ProtokollVerbotsbildschirm

Wählen Sie für eine Ersteinrichtung die Option **Assistent ausführen** aus, um die zum Einrichten des Protokolls erforderlichen Schritte durchzuführen. Nach der Ersteinrichtung können Sie die Protokollierungsebenen mit der Option **Nur Protokollstufen festlegen** anpassen. Wählen Sie eine Option aus, und klicken Sie auf **Weiter**.

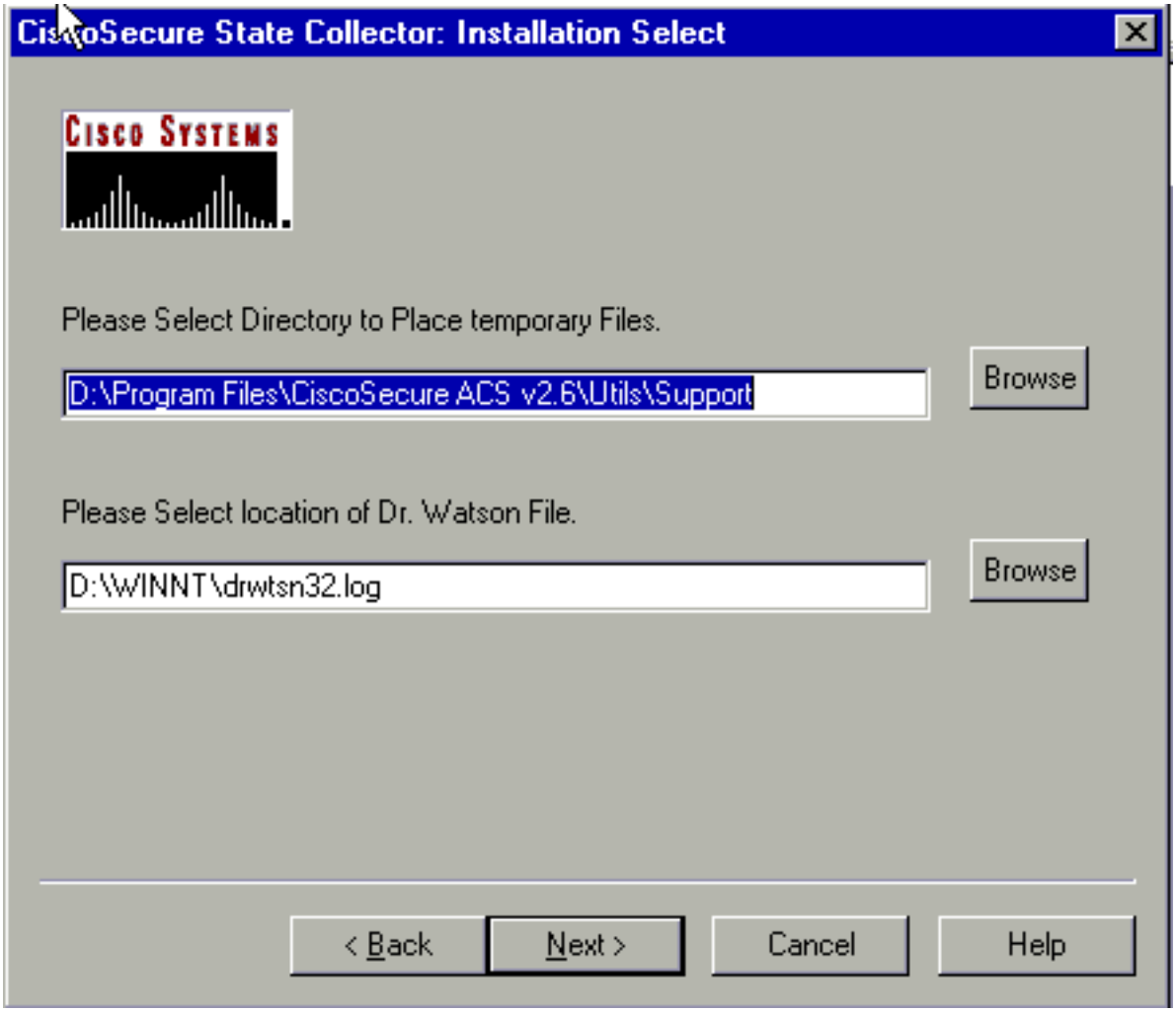
Assistent ausführen

Im Folgenden wird erläutert, wie Sie mithilfe der Option Assistent ausführen Informationen auswählen.

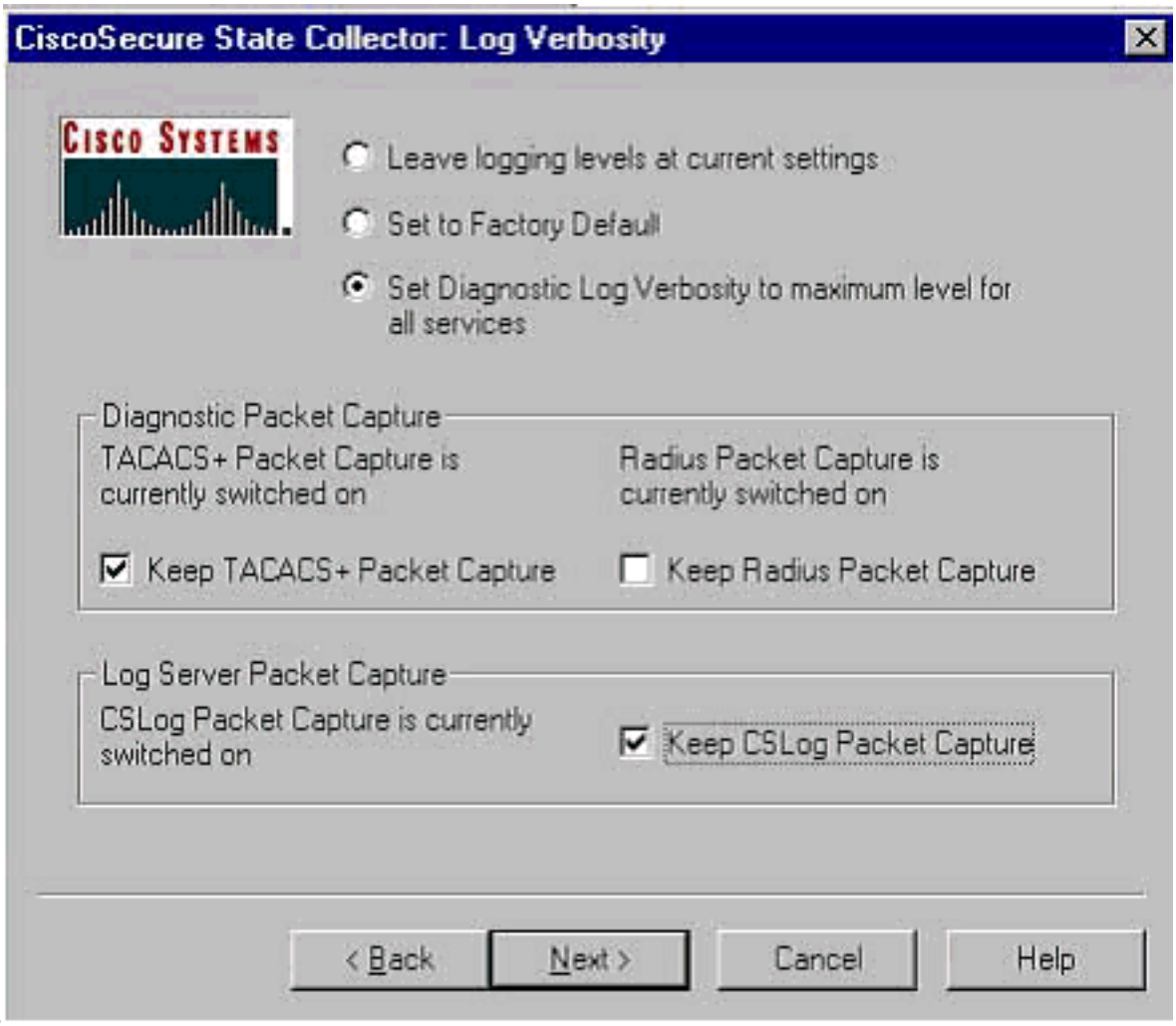
1. **Cisco Secure State Collector:** Auswahl **von Informationen**Alle Optionen sollten standardmäßig ausgewählt werden, mit Ausnahme der Benutzer-DB und der vorherigen Protokolle. Wenn Sie der Meinung sind, dass Ihr Problem die Benutzer- oder Gruppendatenbank ist, wählen Sie **Benutzerdatenbank**. Wenn alte Protokolle enthalten sein sollen, wählen Sie die Option für **Vorherige Protokolle**. Klicken Sie abschließend auf **Weiter**.



2. **Cisco Secure State Collector: Installationsauswahl**Wählen Sie das Verzeichnis aus, in das Sie die Datei package.cab platzieren möchten. Der Standardwert ist "C:\Program Files\Cisco Secure ACS v.26\Utils\Support". Sie können diesen Standort bei Bedarf ändern. Stellen Sie sicher, dass der richtige Standort Ihres Dr. Watson angegeben ist. Wenn Sie CSSupport ausführen, müssen Sie die Dienste starten und beenden. Wenn Sie sicher sind, dass Sie die Cisco Secure Services beenden und starten möchten, klicken Sie auf **Weiter**, um fortzufahren.

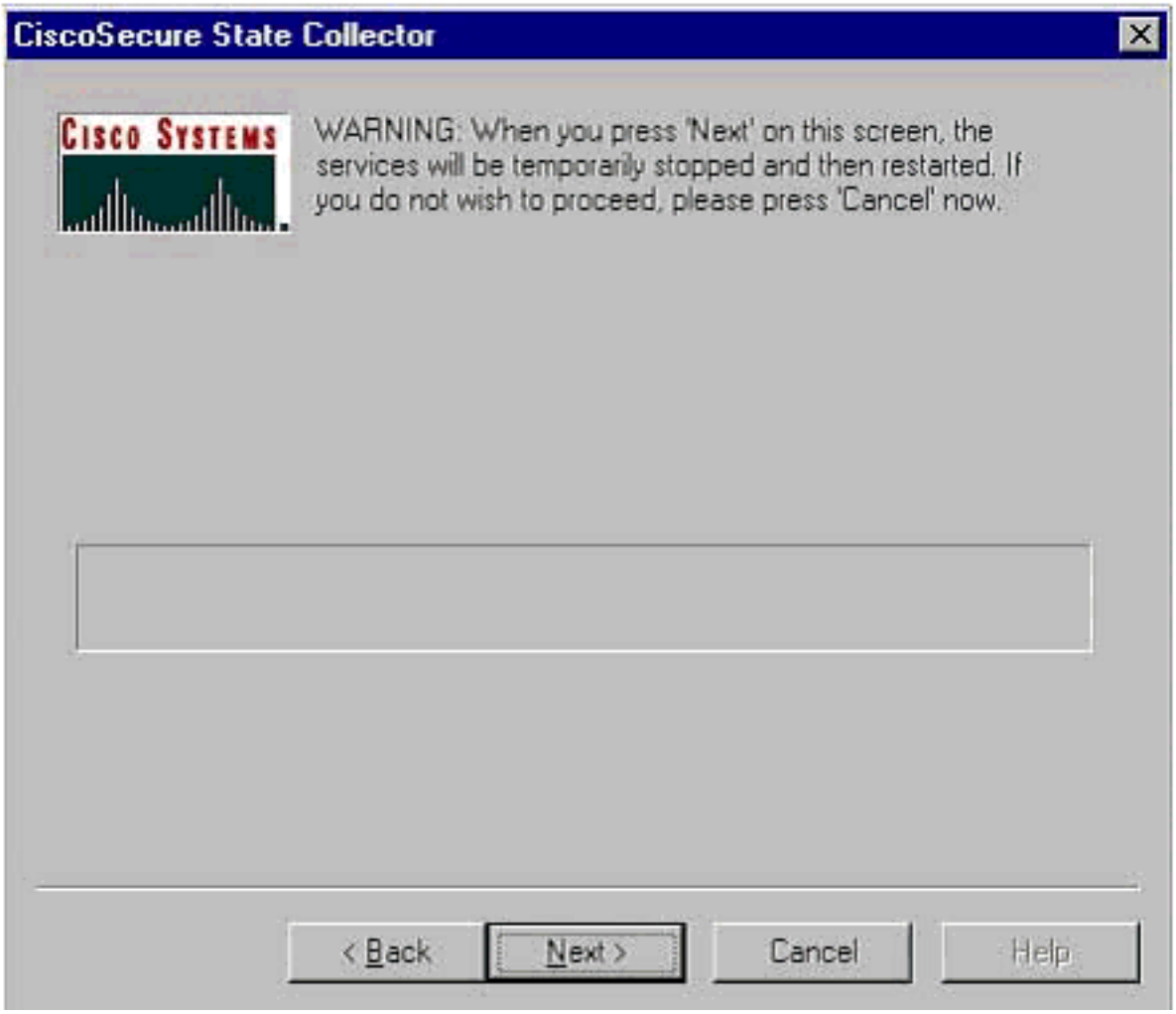


3. **Cisco Secure State Collector: Protokollausführlichkeit**Wählen Sie die Option **Diagnoseprotokoll-Verbosity für alle Dienste auf Höchststufe festlegen aus**. Wählen Sie unter der Überschrift Diagnostic Packet Capture (Paketerfassung für Diagnosepakete) je nach ausgeführter Aktion entweder TACACS+ oder RADIUS aus. Wählen Sie die Option **CSLog-Paketerfassung beibehalten aus**. Wenn Sie fertig sind, klicken Sie auf **Weiter**.**Hinweis:** Wenn Sie Protokolle von früheren Tagen haben möchten, müssen Sie in Schritt 1 die Option **Previous Logs (Vorherige Protokolle)** auswählen und dann die Anzahl der Tage festlegen, die zurückgehen



sollen.

4. **Cisco Secure State Collector**Sie sehen eine Warnung, dass Ihre Dienste beim Fortfahren beendet und dann neu gestartet werden. Diese Unterbrechung ist erforderlich, damit CSSupport alle erforderlichen Dateien abrufen kann. Die Ausfallzeit sollte minimal sein. In diesem Fenster können Sie beobachten, wie der Dienst beendet und neu gestartet wird. Klicken Sie auf **Weiter**, um
fortzufahren.



Beim Neustart der Dienste befindet sich die Datei package.cab im angegebenen Speicherort. Klicken Sie auf **Fertig stellen**, und Ihre Datei "package.cab" ist fertig.Navigieren Sie zu dem Speicherort, den Sie für die Datei package.cab angegeben haben, und verschieben Sie ihn in ein Verzeichnis, in dem die Datei gespeichert werden kann. Ihr Techniker der technischen Unterstützung kann diese während der Fehlerbehebung jederzeit anfordern.

Nur Protokollstufen festlegen

Wenn Sie den State Collector bereits ausgeführt haben und nur die Protokollierungsebenen ändern müssen, können Sie die Option Nur Protokollstufen festlegen verwenden, um zum Cisco Secure State Collector zu springen: Bildschirm "Verbosity" protokollieren, auf dem Sie die Diagnosepaketerfassung festlegen. Wenn Sie auf **Weiter** klicken, gelangen Sie direkt zur Seite Warnung. Klicken Sie anschließend erneut auf **Weiter**, um den Dienst zu beenden, die Datei zu sammeln und die Dienste neu zu starten.

Manuelles Erfassen einer Package.cab-Datei

Im Folgenden finden Sie eine Liste der Dateien, die in package.cab kompiliert werden. Wenn die CSSupport nicht ordnungsgemäß funktioniert, können Sie diese Dateien mit Windows Explorer sammeln.

```
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
```

Abrufen von Cisco Secure for Windows NT AAA-Debuginformationen

Die Dienste Windows NT CSRadius, CSTacacs und CSAuth können im Befehlszeilenmodus ausgeführt werden, wenn Sie ein Problem beheben.

Hinweis: Der Zugriff auf die Benutzeroberfläche ist beschränkt, wenn Cisco Secure for Windows NT-Dienste im Befehlszeilenmodus ausgeführt werden.

Um Informationen zum CSRadius-, CSTacacs- oder CSAuth-Debuggen abzurufen, öffnen Sie ein DOS-Fenster, und passen Sie die Puffer-Höhe der Windows-Eigenschaft auf 300 an.

Verwenden Sie die folgenden Befehle für CSRadius:

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

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

Verwenden Sie die folgenden Befehle für CSTacs:

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

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

Abrufen von Cisco Secure für Windows NT AAA-Replikationsdebuginformationen

Die CSAuth-Dienste von Windows NT können im Befehlszeilenmodus ausgeführt werden, wenn Sie ein Replikationsproblem beheben.

Hinweis: Der Zugriff auf die Benutzeroberfläche ist beschränkt, wenn Cisco Secure for Windows NT-Dienste im Befehlszeilenmodus ausgeführt werden.

Um Informationen zum CSAuth-Replikations-Debuggen zu erhalten, öffnen Sie ein DOS-Fenster, und passen Sie die Puffer-Höhe der Windows-Eigenschaft auf 300 an.

Verwenden Sie die folgenden Befehle für CSAuth sowohl auf dem Quell- als auch auf dem Zielserver:

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

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

Das Debuggen wird in das Eingabeaufforderungsfenster geschrieben und in die Datei $BASE\csauth\logs\auth.log.

Offline testen der Benutzerauthentifizierung

Die Benutzerauthentifizierung kann über die Kommandozeile (CLI) getestet werden. RADIUS kann mit "radtest" getestet werden, TACACS+ mit "tactest". Diese Tests können nützlich sein, wenn das kommunizierende Gerät keine hilfreichen Debuginformationen liefert und wenn es Fragen gibt, ob ein Problem mit Cisco Secure ACS Windows oder ein Geräteproblem vorliegt. Radtest und Taktest befinden sich im Verzeichnis $BASE\utils. Im Folgenden sind Beispiele für jeden Test aufgeführt.

Testen der RADIUS-Benutzerauthentifizierung offline mit 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.
```

Testen der TACACS+-Benutzerauthentifizierung offline mit 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>
```

Ermitteln von Gründen für Windows 2000/NT-Datenbankfehler

Wenn die Authentifizierung an Windows 2000/NT übergeben wird, aber fehlschlägt, können Sie die Windows-Überwachungsfunktion einschalten, indem Sie **Programme > Verwaltung > Benutzer-Manager für Domänen, Richtlinien > Audit** wählen. Wechseln Sie zu **Programme > Verwaltung > Ereignisanzeige** zeigt Authentifizierungsfehler an. Fehler im Protokoll fehlgeschlagener Versuche werden in einem Format angezeigt, wie im Beispiel unten gezeigt.

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

Diese Meldungen können auf der Microsoft-Website unter Windows 200 unter Event & Error Messages and Error Codes in Windows NT recherchiert werden.

Die 1300L-Fehlermeldung wird wie unten dargestellt beschrieben.

```
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.

Beispiele

RADIUS Good Authentication

```
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>
```

Ungültige RADIUS-Authentifizierung

```
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>
```

Gute TACACS+-Authentifizierung

```
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>
```

TACACS+ Bad Authentication (Zusammenfassung)

```
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>
```

Zugehörige Informationen

- Technischer Support - Cisco Systems