

# 获取 Cisco Secure ACS for Windows 的版本和 AAA 调试信息

## 目录

[简介](#)

[开始使用前](#)

[规则](#)

[先决条件](#)

[使用的组件](#)

[获取Windows版本信息的Cisco Secure](#)

[使用DOS Line命令](#)

[使用GUI](#)

[设置Cisco Secure ACS for Windows调试级别](#)

[如何设置日志级别到全双工在ACS GUI](#)

[如何设置Dr.Watson记录](#)

[创建package.cab文件](#)

[什么是package.cab ?](#)

[创建一个package.cab文件用CSSupport.exe工具](#)

[手工收集package.cab文件](#)

[获取Cisco Secure对于Windows NT AAA调试信息](#)

[获取Cisco Secure对于Windows NT AAA复制调试信息](#)

[测试脱机的用户认证](#)

[确定Windows 2000/NT数据库故障的原因](#)

[示例](#)

[RADIUS成功验证](#)

[RADIUS未成功认证](#)

[TACACS+成功验证](#)

[TACACS+未成功认证\(汇总\)](#)

[相关信息](#)

## [简介](#)

本文解释如何查看Cisco Secure ACS for Windows版本和如何设置和得到验证、授权和统计(AAA)调试信息。

## [开始使用前](#)

## [规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## [先决条件](#)

本文档没有任何特定的前提条件。

## [使用的组件](#)

本文档中的信息根据Cisco Secure ACS for Windows 2.6。

## [获取Windows版本信息的Cisco Secure](#)

通过使用GUI，您能查看版本信息通过使用DOCS line命令或。

### [使用DOS Line命令](#)

通过在DOS的line命令选项要查看Cisco Secure ACS for Windows版本号，请使用- RADIUS的v和-x或csradius跟随的cstacacs TACACS+。参见下面示例：

```
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
```

您可以也发现Cisco Secure ACS程序的版本号在Windows注册表的。例如：

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

### [使用GUI](#)

要查看与Cisco Secure ACS GUI的版本，请去ACS主页。您能通过单击在屏幕的左上角的Cisco系统徽标在任何时间执行此。主页的一半将显示全双工版本。

## [设置Cisco Secure ACS for Windows调试级别](#)

下列是需要的得到最大调试信息不同的调试选项的说明。

### [如何设置日志级别到全双工在ACS GUI](#)

您将需要设置ACS记录所有消息。要执行此，请遵从如下所示的步骤：

1. 从ACS主页，请去**系统Configuration>服务控制**。
2. 在服务日志文件配置标题下，设置详细程度对**全双工**。若需要您能修改生成新的文件和管理目

# System Configuration

**CiscoSecure ACS on mhammon-pc** ?

**Is Currently Running**

**Services Log File Configuration** ?

Level of detail

None

Low

Full

Generate New File

Every day

Every week

Every month

When size is greater than  KB

Manage Directory

Keep only the last  files

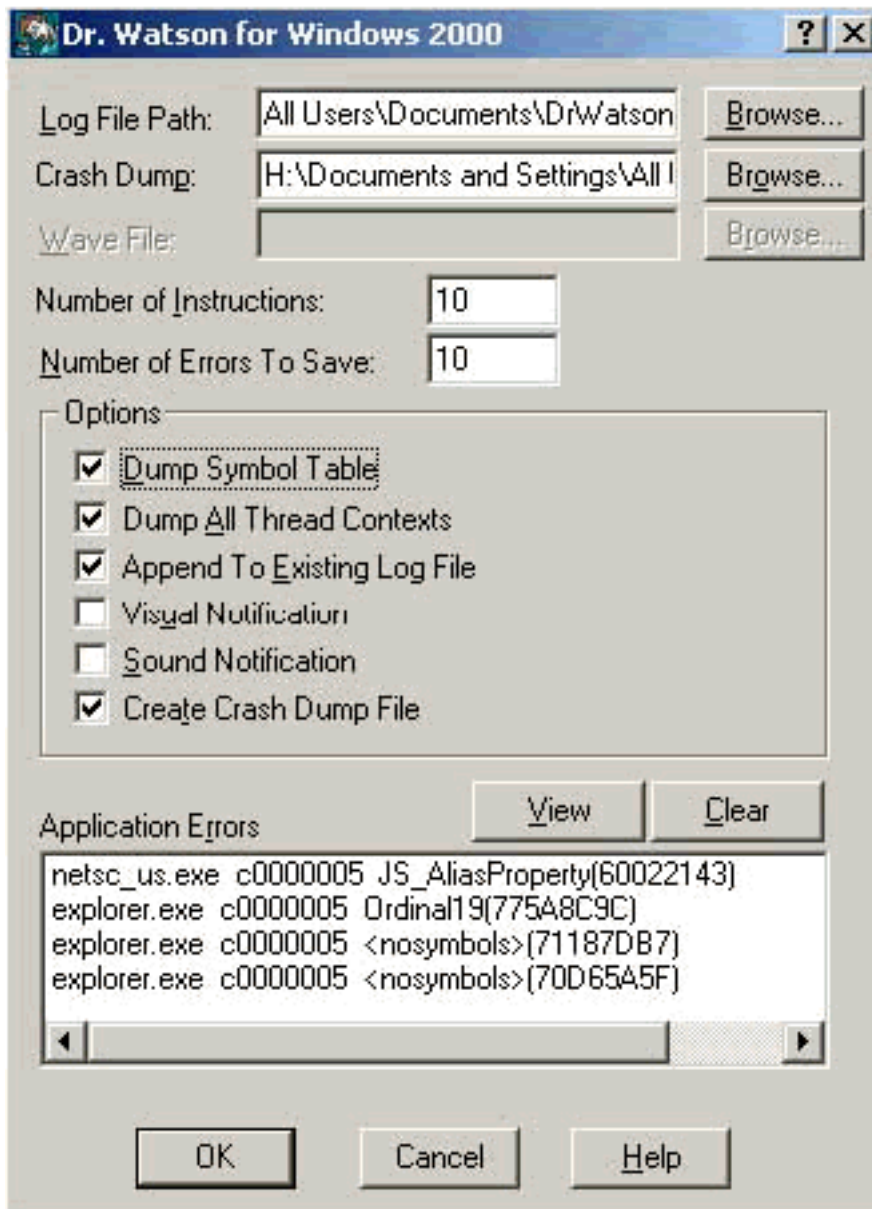
Delete files older than  days

Restart Stop Cancel

录部分。

## [如何设置Dr.Watson记录](#)

在prompt命令类型drwtsn32和Dr.Watson窗口将出现。确保转储的选项所有线索上下文和转储符号表被检查。



## [创建package.cab文件](#)

### [什么是package.cab ?](#)

package.cab是包含必要的所有必要的文件高效地排除故障ACS的压缩文件。[可以使用 CSSupport.exe 实用程序创建 package.cab](#)，也可以手动收集文件。

### [创建package.cab文件用CSSupport.exe工具](#)

如果有您需要收集信息的一ACS问题，请尽快运行CSSupport.exe文件，在您看到问题后。请使用DOS line命令或Windows Explorer GUI从C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe运行CSSupport。

当您执行CSSupport.exe文件时，以下窗口出现。



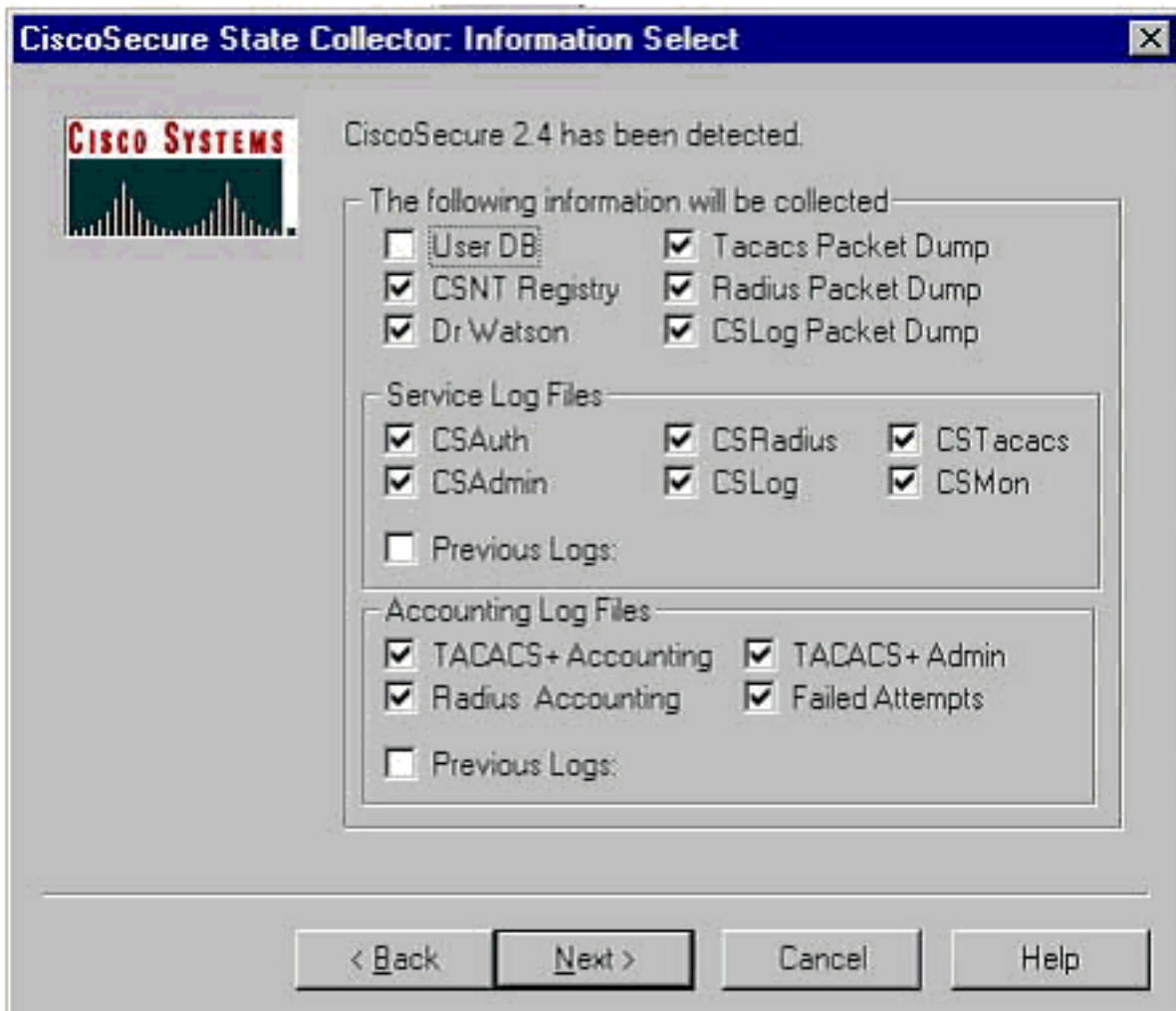
从此屏幕，您有两个主要选项：

- [Run向导](#)，通过一系列的四个步骤导致您：Cisco安全状态收集器：精选的信息Cisco安全状态收集器：精选的安装Cisco安全状态收集器：日志冗余Cisco安全状态收集器(实际收藏)或
  - [仅集合日志级别](#)，允许您跳到最初的少数步骤和去直接地Cisco安全状态收集器：日志冗长画面
- 对于一个首次设置，请选择Run向导通过必要的步骤继续设置日志。在初始设置以后，您能使用集合日志级别唯一选择调整日志级别。做您的选择，并且其次单击。

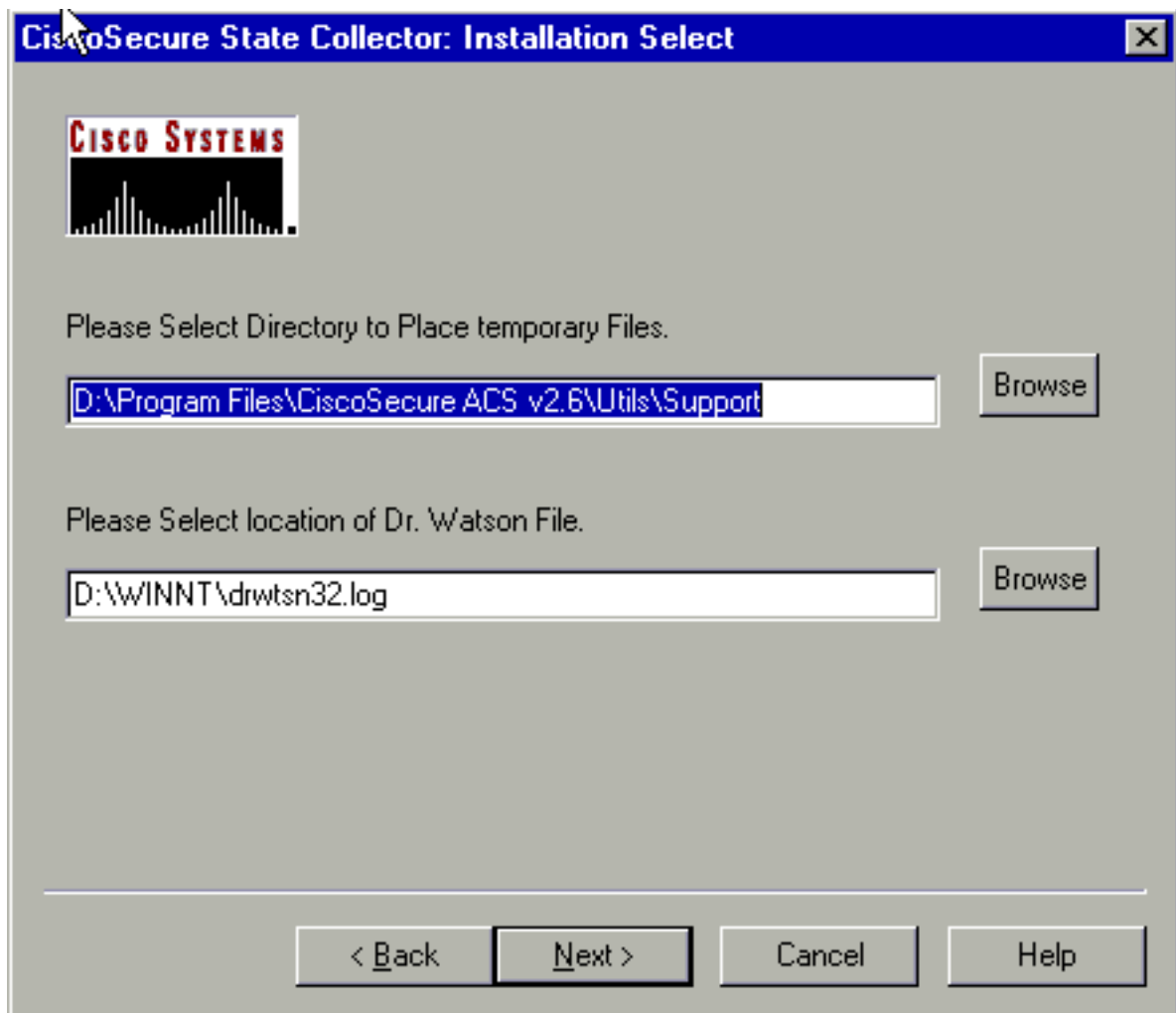
## [Run向导](#)

使用Run向导选项，下列解释如何选择信息。

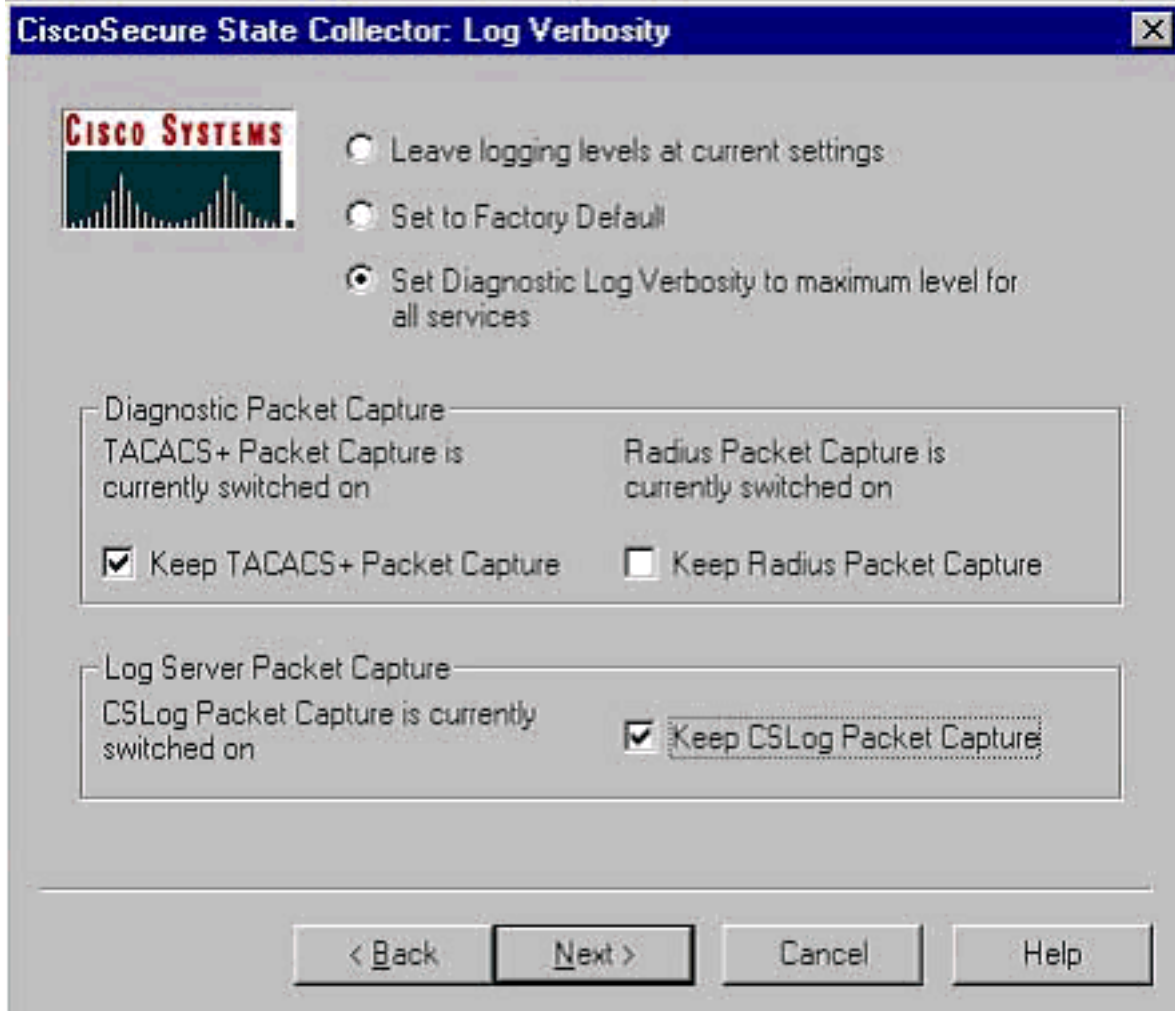
1. **Cisco安全状态收集器：精选的信息**应该选择默认情况下所有选项除了用户DB和上一个日志。如果认为您的问题是用户或组数据库，则请选择**用户DB**。如果希望安排旧有日志包括，请选择**上一个日志**的选项。当你完成的时候，其次请单击。



2. Cisco安全状态收集器：精选的安装选择您要放置package.cab的目录。默认是C:\Program Files\Cisco Secure ACS v.26\Utils\Support。如果希望，您可以更改此位置。确保您的Dr.Watson的正确位置指定。运行CSSupport要求您开始并且终止服务。如果肯定您要终止和开始Cisco Secure服务，请单击在旁边继续。

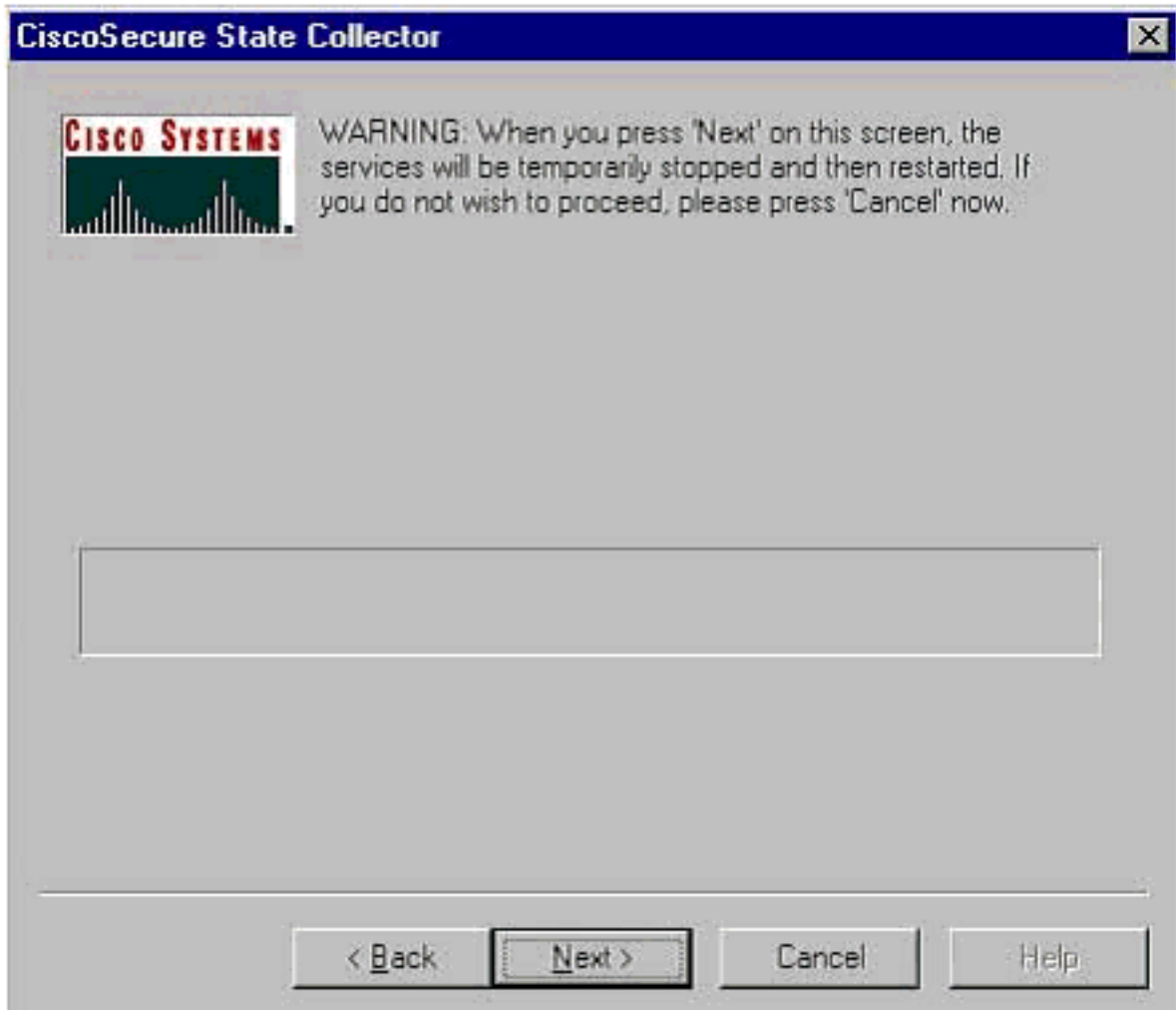


3. Cisco安全状态收集器：日志冗余选择集合诊断记录冗余的选项对所有服务的最高标准。在诊断信息包捕捉标题下，请根据什么选择TACACS+或RADIUS，您运行。选择保持CSLog数据包捕获选项。当你完成的时候，其次请单击。注意：如果要有从前一天的日志，您必须选择上一个日志选项的选项在step1然后设置您要返回几天的数量。



4. **Cisco安全状态收集器**您将看到警告的状态，当您继续，您的服务将被终止然后重新启动。此中断是必要为了CSSupport能获取所有需要的文件。停工期应该最小。您能观看服务必须先停止和重新启动在此窗口。单击 Next ( 下一步 ) 继续。





当服务重

新启动， package.cab可以在位置找到指定。点击芬通社，并且您的package.cab文件准备好。浏览到您为package.cab指定并且重新定位它对目录它可以保存的位置。您的技术支持工程师可能在故障排除流程中在任何时间请求它。

### [集合日志只成水平](#)

如果以前运行了状态收集器和只需要改变日志级别，您能使用集合日志级别唯一选择跳过去到[Cisco安全状态收集器：记录冗长画面](#)，您设置诊断信息包捕捉。当您其次单击，您将去直接地警告页。然后其次再请单击终止服务，搜集文件，并且重新启动服务。

### [手工收集package.cab文件](#)

下列是被编译到package.cab文件的列表。如果CSSupport不正常运行，使用Windows Explorer，您能搜集这些文件。

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\CSAcacs\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

## 获取Cisco Secure对于Windows NT AAA调试信息

当您排除故障问题时，Windows NT CSRADIUS、CSAcacs和CSAuth服务在line命令模式可能管理。

**注意：** 如果Windows NT服务的任何Cisco Secure在line命令模式，运行GUI访问被限制。

要获取CSRADIUS，CSAcacs或者Csauth调试信息，打开DOS窗口并且调节Windows属性屏幕缓冲高度到300。

请使用以下命令CSRADIUS：

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

请使用以下命令CSAcacs：

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

## 获取Cisco Secure对于Windows NT AAA复制调试信息

当您排除故障复制问题时，Windows NT CSAuth服务在line命令模式可能管理。

**注意：** 如果Windows NT服务的任何Cisco Secure在line命令模式，运行GUI访问被限制。

要得到Csauth复制调试信息，请打开DOS窗口并且调节Windows属性屏幕缓冲高度到300。

请使用以下命令在来源和目标服务器的Csauth：

```
c:\program files\ciscosecure acs v2.6\csauth>net stop csauth c:\program files\ciscosecure acs  
v2.1\csauth>csauth -p -z
```

调试写入到命令提示符窗口，并且在\$BASE\csauth\日志\auth.log文件也进来。

## 测试脱机的用户认证

用户认证可能通过命令行界面(CLI)测试。RADIUS可以用“radtest测试”，并且TACACS+可以用“tactest测试”。这测试可以是有用的，如果通信设备不导致有用的调试信息，并且，如果有某个问题至于是否有Cisco Secure ACS Windows问题或设备问题。radtest和tactest在\$BASE\使用情况目录查找。下列是每测验示例。

### 测试RADIUS用户验证脱机与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 password><>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.
```

### 测试TACACS+用户认证脱机与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 :
```

## 确定Windows 2000/NT数据库故障的原因

如果验证通过对Windows 2000/NT，但是失败，您能通过去启动Windows审计工具对**Programs > Administrative Tools>域用户管理器，策略>审计**。去**Programs > Administrative Tools > Event Viewer**显示认证失败。在失败的尝试日志找到的失败在格式显示如下面示例所显示。

NT/2000 authentication FAILED (error 1300L)

这些消息在[Windows 2000事件的Microsoft的网站](#)可以被研究[错误消息](#) 和[错误代码在Windows NT](#)

o

1300L 错误消息描述如下所示。

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.

## 示例

### RADIUS成功验证

```
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 initialised 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 retrieve 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>
```

## RADIUS未成功认证

```
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 initialised ok
Created shared memory
ExtensionPoint: Base key is [SOFTWARE\Cisco\CiscoAAAv2.6\CSRadius\ExtensionPoints]
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 retrieve 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/rcv errors : 0 F:\Program

Files\Cisco Secure ACS v2.6\CSRADIUS>

## TACACS+成功验证

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/SUCCESS 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/SUCCESS) 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+未成功认证\(汇总\)](#)

```
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: cisc0l
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>
```

## [相关信息](#)

- [技术支持 - Cisco Systems](#)