# Obtendo a versão e informações sobre a depuração AAA para o Cisco Secure ACS para Windows

## Índice



## Introdução

Esse documento explica como visualizar a versão do Cisco Secure ACS for Windows e como configurar e obter autenticação, autorização e informações de depuração de contabilidade (AAA).

## Antes de Começar

### Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

### Pré-requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações contidas neste documento são baseadas no Cisco Secure ACS para Windows 2.6.

## Obtendo o Cisco Secure para informações sobre versões do Windows

Você pode ver a informação de versão usando a linha de comando DOC ou usando o GUI.

### Utilizando a linha de comando do DOS

Para exibir o número de versão do Cisco Secure ACS para Windows por meio da opção de linha do comando no DOS, use o comando cstacacs ou csradius seguido por -v para o RADIUS e por -x para oTACACS+. Veja os exemplos abaixo:

```
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
```

Você pode igualmente ver o número de versão do programa do Cisco Secure ACS no registro de Windows. Por exemplo:

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

### Utilizando a GUI

Para ver a versão com a GUI do Cisco Secure ACS, acesse a home page do ACS. Você pode fazer isso a qualquer momento, clicando no logotipo da Cisco Systems no canto superior esquerdo da tela. A metade inferior da página inicial irá exibir a versão completa.

## Configurando os níveis de depuração do Cisco Secure ACS para Windows

Segue-se uma explicação sobre as diferentes opções de depuração necessárias para obter o máximo de informações de depuração.

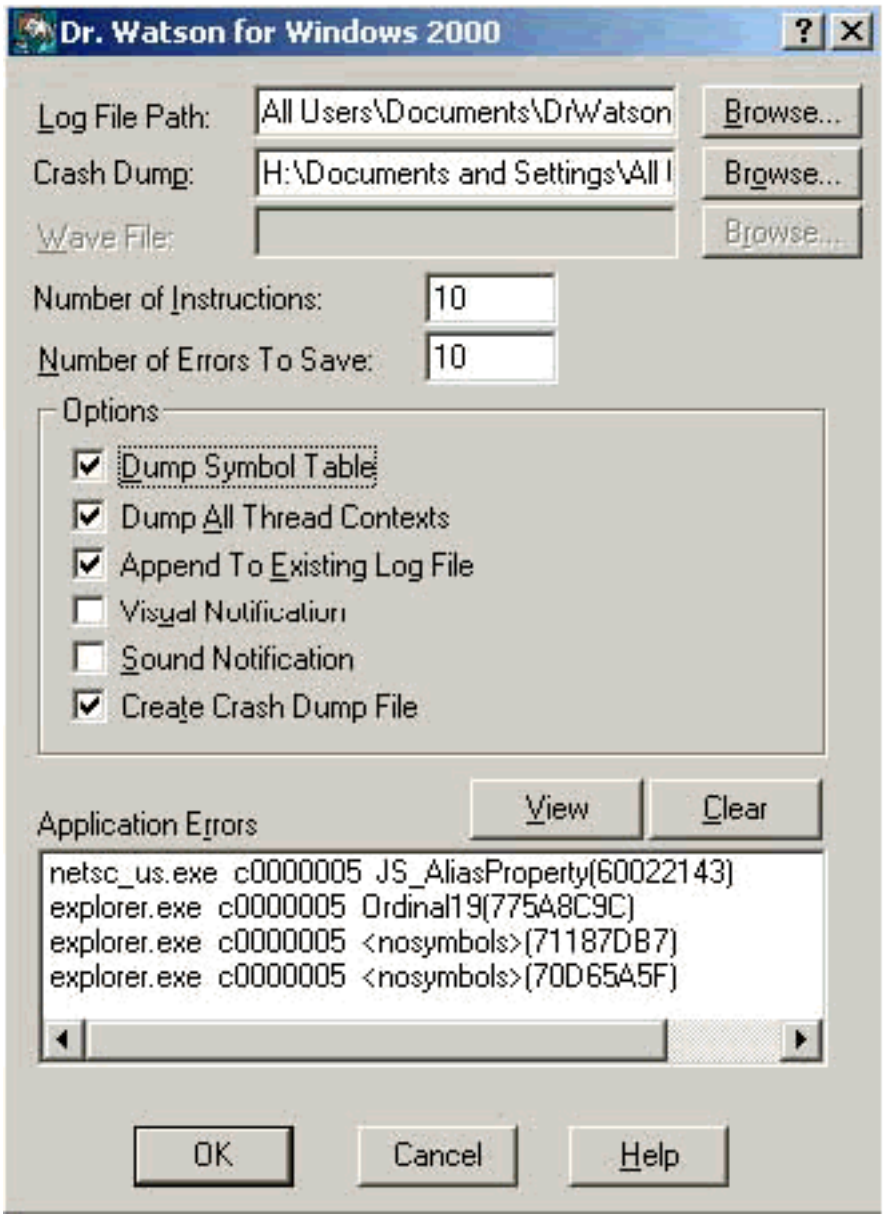
### Como configurar o nível de registro para Full na GUI do ACS

Será necessário definir o ACS de forma a registrar todas as mensagens. Para fazer isso, siga as etapas listadas abaixo:

1. Na home page de ACS, vá para Systems Configuration > Service Control.
2. No cabeçalho Service Log File (Arquivo de Registro de Serviço), configure o nível de detalhes para Full (Total).Você pode modificar as seções Generate New File (Gerar novo arquivo) e Manage Directory (Gerenciar diretório), se necessário.


## Como definir os registros do Dr. Watson

No prompt de comandos, digite drwtsn32 e a janela Dr. Watson será exibida. Certifique-se de que as opções Descartar todos os contextos de segmentos e Descartar tabela de símbolos estejam selecionadas.




# Criando um arquivo package.cab

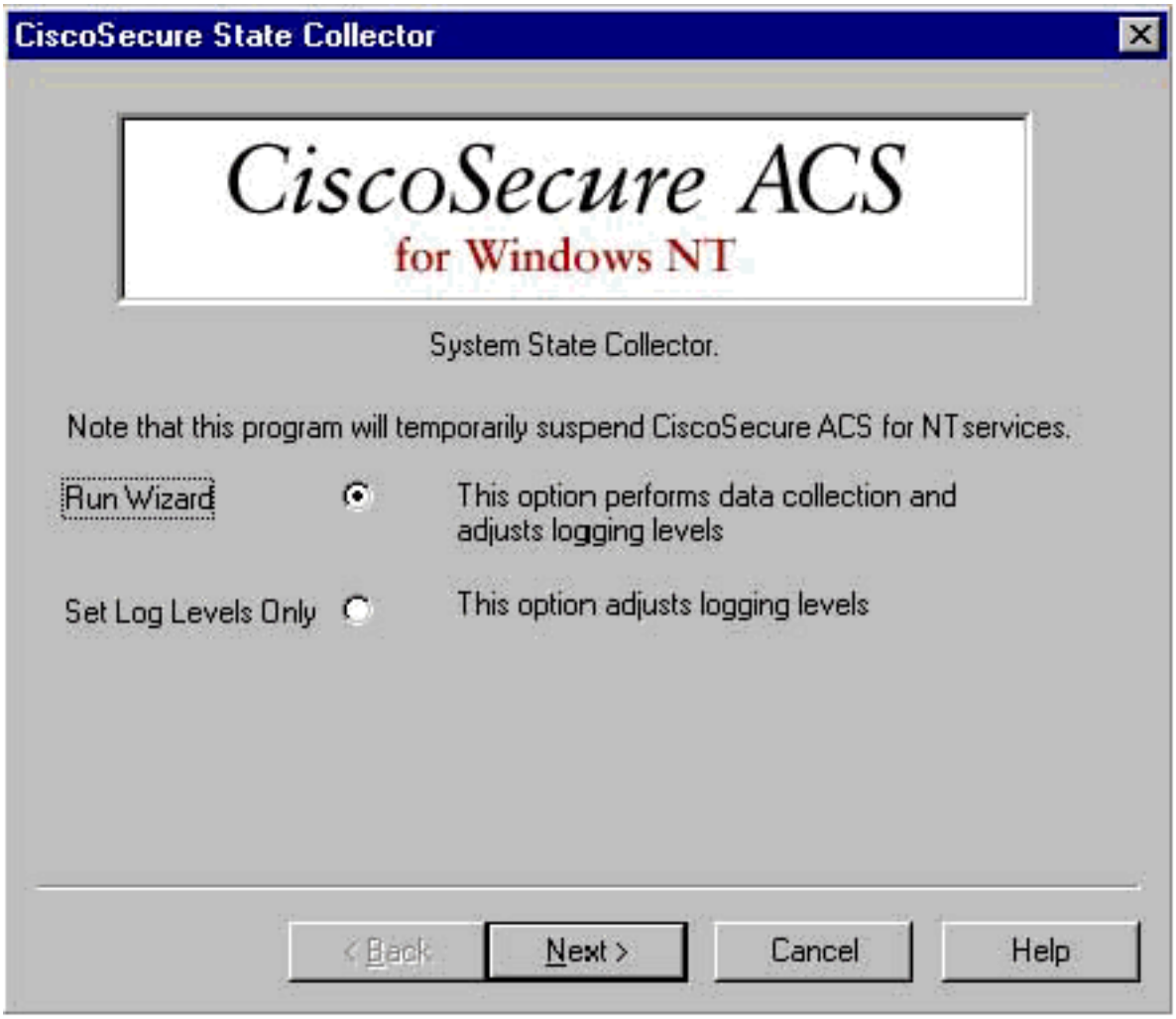
## O que é o package.cab?

O package.cab é um arquivo Zip que contém todos os arquivos necessários para solucionar com eficiência os problemas de ACS. Você pode usar o utilitário CSSupport.exe para criar o package.cab ou pode obter os arquivos manualmente.

## Criando um arquivo package.cab com o utilitário CSSupport.exe

Se você está tendo um problema no ACS para que você precisa de recolher a informação, execute o arquivo CSSupport.exe o mais cedo possível depois que você vê o problema. Use a linha de comando dos ou o Windows Explorer GUI para executar o CSSupport do Secure ACS v2.6\Utils>CSSupport.exe de C:\program files\Cisco.

Quando você executa o arquivo CSSupport.exe, é exibida a janela a seguir.




Nesta tela, há duas opções principais:

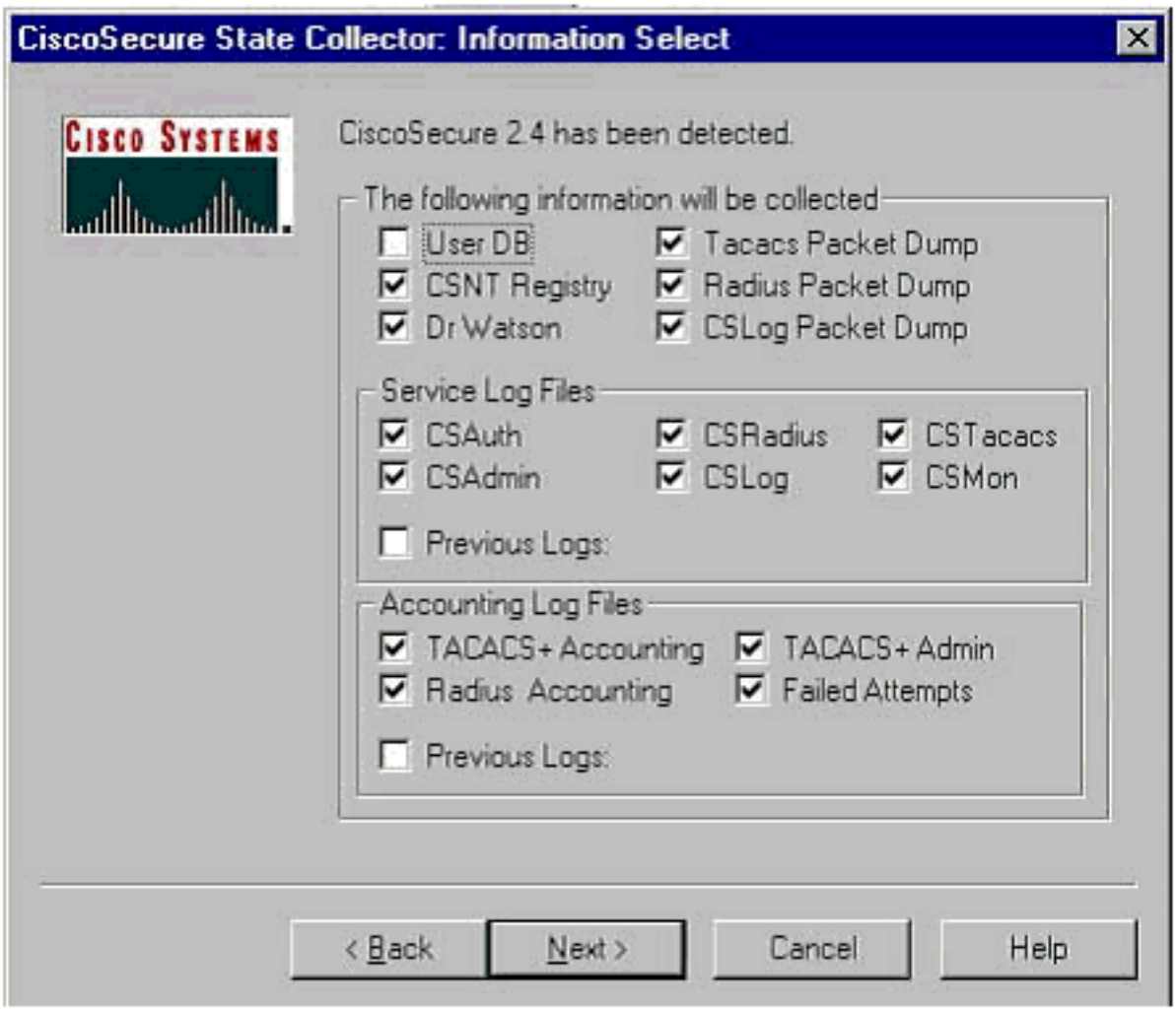
- Execute o assistente, que o conduz com uma série de quatro etapas:Coletor de estado seguro Cisco: Seleção de informaçõesColetor de estado seguro Cisco: Seleção de instalaçãoColetor de estado seguro Cisco: Eloqüência dos registrosColetor de estado de segurança Cisco (coleção verdadeira)ou
- Ajuste o log em nível somente, que permite que você salte as etapas primeiras e vá diretamente ao coletor de estado seguro Cisco: Tela Log Verbosity

Para uma instalação principiante, o **assistente** seleto da **corrida** a continuar com as etapas precisou de ajustar o log. Após a configuração inicial, a opção Set Log Levels Only para ajustar os níveis de registro. Faça sua seleção, e clique-a **em seguida**.

## Executar Assistente.

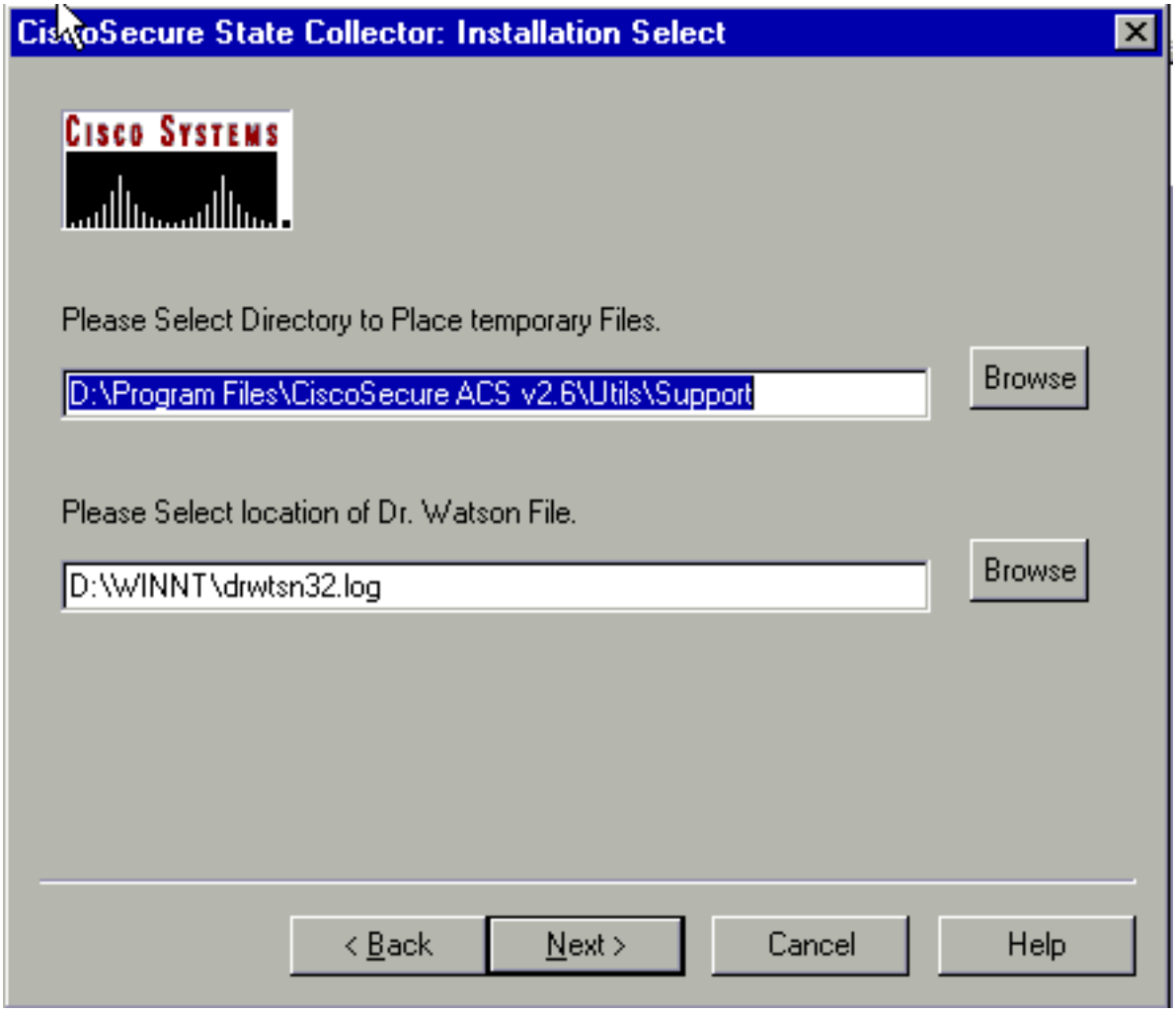
As informações a seguir explicam como selecionar informações sobre como usar a opção Run Wizard (Executar Assistente).

1. **Coletor de estado seguro Cisco:** Seleção de informaçõesTodas as opções devem ser selecionadas como padrão, exceto User DB e Previous Logs. Caso ache que o problema é o banco de dados de usuários ou grupos, selecione User DB. Para ter registros antigos incluídos, selecione a opção Previous Logs (Registros Anteriores). Clique em Avançar quando

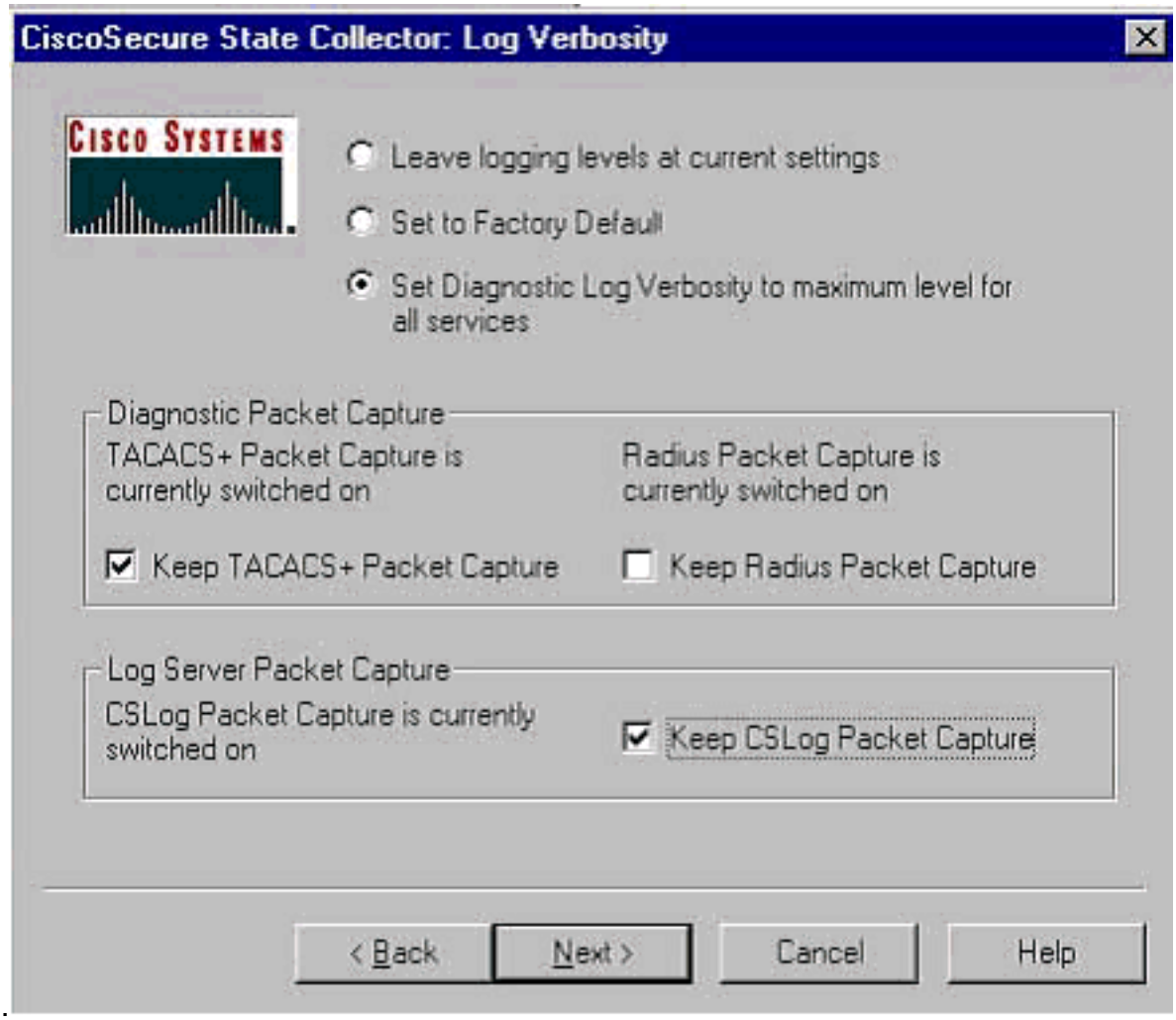



terminar.

2. **Coletor de estado seguro Cisco: Seleção de instalação**Escolha o diretório em que você quer colocar o package.cab. O padrão é o Secure ACS v.26\Utils\Support de C:\Program Files\Cisco. Este local pode ser alterado, se desejado. Verifique se o local correto do Dr. Watson foi especificado. O CSSupport running exige que você enfia e para os serviços. Se você tiver certeza de que deseja interromper e iniciar os serviços do Cisco Secure, clique em Avançar para
continuar.

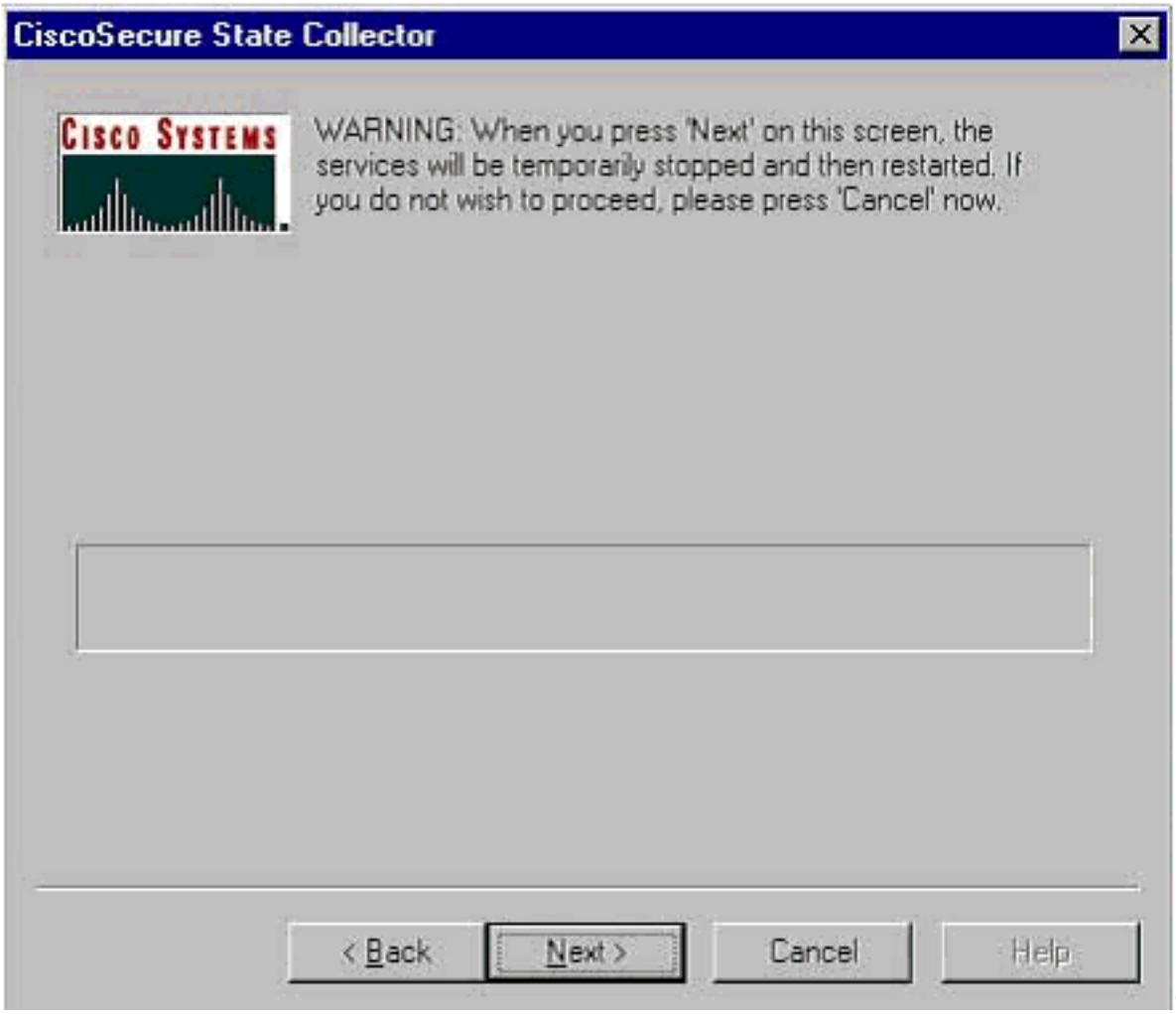



3. **Coletor de estado seguro Cisco: Eloqüência dos registros**Selecione a opção para a **verbosidade do log de diagnóstico do grupo ao nível máximo para todos os serviços**. No título Captura do Pacote de Diagnóstico, selecione TACACS+ ou RADIUS, dependendo daquilo que estiver executando. Selecione a opção Manter captura do pacote CSLog. Quando você finalizar, clique em Next.**Nota:** Se você quer ter logs dos dias anteriores, você deve selecionar a opção de opção de Registros Anterior em etapa 1 e então ajustar o número de dias onde você quer ir para




trás.

4. **Coletor de estado seguro Cisco**Você verá um aviso que indica quando continuar, os serviços que serão parados e em seguida reiniciados. Esta interrupção é necessária para que o CSSupport agarre todos os arquivos necessários. O tempo de interrupção deve ser mínimo. Será possível observar a parada e reinício dos serviços nessa janela. Clique em Avançar para
continuar.



Quando os serviços reiniciam, o package.cab pode ser encontrado no lugar especificado. Clique em Finish e o arquivo package.cab está pronto.Consulte ao lugar que você especificou para o package.cab e relocate o a um diretório onde pudesse ser salvar. O engenheiro do suporte técnico pode solicitá-lo a qualquer momento durante o processo de Troubleshooting.

## Ajuste níveis do log somente

Se você tiver executado o Coletor de Estado anteriormente e precisar apenas mudar os níveis de registros, use a opção Definir Somente Níveis de Registro para saltar para o Cisco Secure State Collector. A tela de registros detalhados na qual você define a captura do pacote de diagnóstico. Ao clicar em Avançar, você vai diretamente para a página de Aviso. Em seguida, clique em Next novamente para parar o serviço, coletar o arquivo e reiniciar os serviços.

## Coletando um arquivo package.cab manualmente

O seguinte é uma lista dos arquivos que são compilados em um package.cab. Se o CSSupport não está funcionando corretamente, você pode recolher estes arquivos usando o Windows Explorer.

```
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
```

## Obtendo informações de depuração de AAA do Cisco Secure para Windows NT

Os serviços Windows NT CSRadius, CSTacacs e CSAuth poderão ser executados no modo de linha de comando quando você Troubleshoot problemas.

**Nota:** O acesso de GUI é limitado se qualquer Cisco seguro para serviços do Windows NT está sendo executado no modo da linha de comando.

Para obter CSRadius, CSTacacs, ou o csauth debuga a informação, abre uma janela do dos e ajusta-à altura de buffer de tela de propriedade de Windows a 300.

Use os comandos seguintes para CSRadius:

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

Use os comandos a seguir para CSTacacs:

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

## Obtendo informações de depuração de réplica de AAA do Cisco Secure para Windows NT

Os serviços de Windows NT CSAuth podem ser executados no modo de linha de comando

quando você estiver Troubleshooting um problema de replicação.

**Nota:** O acesso de GUI é limitado se qualquer Cisco seguro para serviços do Windows NT está sendo executado no modo da linha de comando.

Para obter informações de depuração de replicação CSAuth, abra uma janela do DOS e ajuste a altura de Buffer de Tela de propriedade do Windows para 300.

Use os comandos seguintes para o csauth na fonte e nos servidores de destino:

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

Debugar é escrito à janela de prompt de comando, e igualmente vai no $BASE \ csauth \ logs \ arquivo do auth.log.

## Testando a autenticação de usuário offline

A autenticação de usuários pode ser testada por meio da interface de linha de comando (CLI). O RADIUS pode ser testado com "radtest", e o TACACS+, com "tactest". Isto testa pode ser útil se o dispositivo de comunicação não é produzir útil debuga a informação, e se há alguma pergunta se há um problema com O Windows do Cisco Secure ACS ou um problema do dispositivo. Mais radtest e mais tactest são ficados situado no diretório $BASE \ utils. A seguir são apresentados exemplos de cada teste.

### Autenticação de usuário RADIUS de teste off line com 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.
```

### Testando a autenticação de usuário TACACS+ off-line com 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>
```

## Determinando as causas das falhas com os bancos de dados do Windows 2000/NT

Se a autenticação está sendo passada a Windows 2000/NT mas está falhando, você pode girar sobre a facilidade de exame de Windows indo **programa > ferramentas administrativas > gerenciador de usuário para domínio, políticas > auditoria**. Ir às falhas de autenticação das mostras do **Programas > Ferramentas Administrativas > Visualizador de Evento**. As falhas encontradas no registro de falha de tentativa são exibidas em um formato mostrado no exemplo a seguir.

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

Estas mensagens podem ser pesquisadas no Web site de Microsoft no evento do Windows 2000 & os Mensagens de Erro e os códigos de erro no Windows NT .

O Mensagem de Erro 1300L é descrito como mostrado abaixo.

```
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.
```

## Exemplos

### Boa autenticação 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>
```

## Autenticação RADIUS inválida

```
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>

## Boa autenticação de 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>

## Autenticação incorreta de TACACS+ (resumida)

```
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>
```

# Informações Relacionadas

- Suporte Técnico - Cisco Systems