

Cisco Secure ACS for Windows のバージョン情報および AAA デバッグ情報の取得

目次

[概要](#)

[はじめに](#)

[表記法](#)

[前提条件](#)

[使用するコンポーネント](#)

[Cisco Secure for Windows のバージョン情報の取得](#)

[バージョン情報の取得](#)

[GUI の使用](#)

[Cisco Secure ACS for Windows のデバッグ レベルの設定](#)

[ACS GUI でログレベルを Full に設定する方法 Dr. Watson ロギングの設定方法](#)

[Dr. Watson ロギングの設定方法](#)

[package.cab ファイルの作成](#)

[package.cab とは](#)

[CSSupport.exe ユーティリティによる package.cab ファイル の作成](#)

[package.cab ファイルの手動での収集](#)

[Cisco Secure for Windows NT の AAA デバッグ情報の取得](#)

[Cisco Secure for Windows NT の AAA 複製デバッグ情報の取得](#)

[ユーザ認証のオフラインでのテスト](#)

[Windows 2000/NT データベース障害の原因の判別](#)

[例](#)

[RADIUS による正常な認証 RADIUS による認証の失敗 TACACS+ による正常な認証 TACACS+ による認証の失敗](#)

[ツール情報 関連情報](#)

[TACACS+ による正常な認証](#)

[TACACS+ による認証の失敗 \(要約 \)](#)

[関連情報](#)

概要

このドキュメントは、Cisco Secure ACS for Windows のバージョンを調べる方法、および Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウントिंग) に関するデバッグ情報を設定および取得する方法について説明しています。

[はじめに](#)

[表記法](#)

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

[前提条件](#)

このドキュメントに関する固有の要件はありません。

[使用するコンポーネント](#)

このドキュメントの情報は、Cisco Secure ACS for Windows 2.6 に基づいています。

[Cisco Secure for Windows のバージョン情報の取得](#)

バージョン情報を表示するには、DOS コマンドラインまたは GUI を使用します。

[バージョン情報の取得](#)

Cisco Secure ACS for Windows のバージョン番号を DOS のコマンドライン オプションを利用して表示するには、cstacacs または csradius の後に -v (RADIUS の場合)、および -x (TACACS+ の場合) を続けて入力します。次の例を参照してください。

```
C:\Program Files\CiscoSecure ACS v2.6\CS Tacacs>cstacacs -s CSTacacs v2.6.2, Copyright 2001, Cisco Systems Inc
C:\Program Files\CiscoSecure ACS v2.6\CS Radius>csradius -v CSTacacs v2.6.2), Copyright 2001, Cisco Systems Inc
```

Cisco Secure ACS プログラムのバージョン番号は Windows レジストリにも表示されます。次に、例を示します。

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

[GUI の使用](#)

Cisco Secure ACS の GUI を使用してバージョンを調べるには、ACS のホームページにアクセスします。これを行うには、画面左上隅にある Cisco Systems のロゴをクリックします。ホームページの下半分にフルバージョンが表示されます。

[Cisco Secure ACS for Windows のデバッグレベルの設定](#)


次に、最大限のデバッグ情報を得るために必要なさまざまなデバッグ オプションについて説明します。


[ACS GUI でログレベルを Full に設定する方法 Dr. Watson ロギングの設定方法](#)

ACS がすべてのメッセージをロギングするように設定する必要があります。そのためには、次の手順に従います。

1. ACS ホーム ページから Systems Configuration > Service Control の順に移動します。
2. Service Log File Configuration の見出しの下で、Level of Detail を Full に設定します。必要であれば、Generate New File および Manage Directory のセクションも変更します。

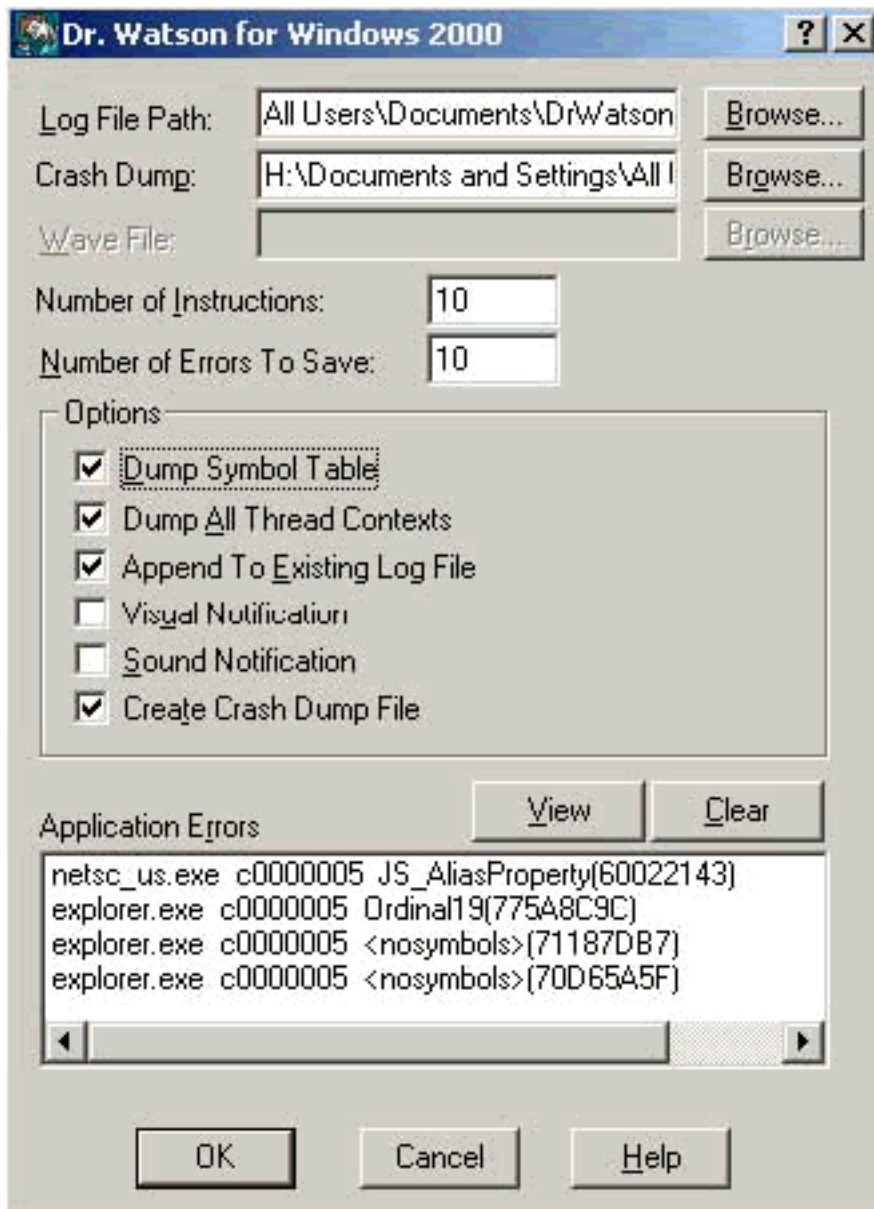
System Configuration

CiscoSecure ACS on mhammon-pc 	
Is Currently Running	

Services Log File Configuration 	
Level of detail	
<input type="radio"/> None	
<input type="radio"/> Low	
<input checked="" type="radio"/> Full	
Generate New File	
<input checked="" type="radio"/> Every day	
<input type="radio"/> Every week	
<input type="radio"/> Every month	
<input type="radio"/> When size is greater than <input type="text" value="2048"/> KB	
<input type="checkbox"/> Manage Directory	
<input type="radio"/> Keep only the last <input type="text" value="7"/> files	
<input checked="" type="radio"/> Delete files older than <input type="text" value="7"/> days	

[Dr. Watson ログिंगの設定方法](#)

コマンドプロンプトで `drwtsn32` と入力すると、Dr. Watson ウィンドウが表示されます。Dump All Thread Contexts および Dump Symbol Table のオプションがチェックされていることを確認します。



[package.cab ファイルの作成](#)

[package.cab とは](#)

package.cab は、ACS のトラブルシューティングを効率的に行うために必要なすべてのファイルを含む Zip ファイルです。 [CSSupport.exe ユーティリティを使用して package.cab を作成したり、手動でファイルを収集したりできます。](#)

[CSSupport.exe ユーティリティによる package.cab ファイルの作成](#)

ACS の問題について情報を収集することが必要になった場合は、問題発見後できるだけ早く CSSupport.exe ファイルを実行します。 C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe から CSSupport を実行するのに DOS コマンド・ラインか Windows エクスプローラ GUI を使って下さい。

CSSupport.exe ファイルを実行すると、次のウィンドウが表示されます。



この画面には、次の2つのメイン オプションがあります。

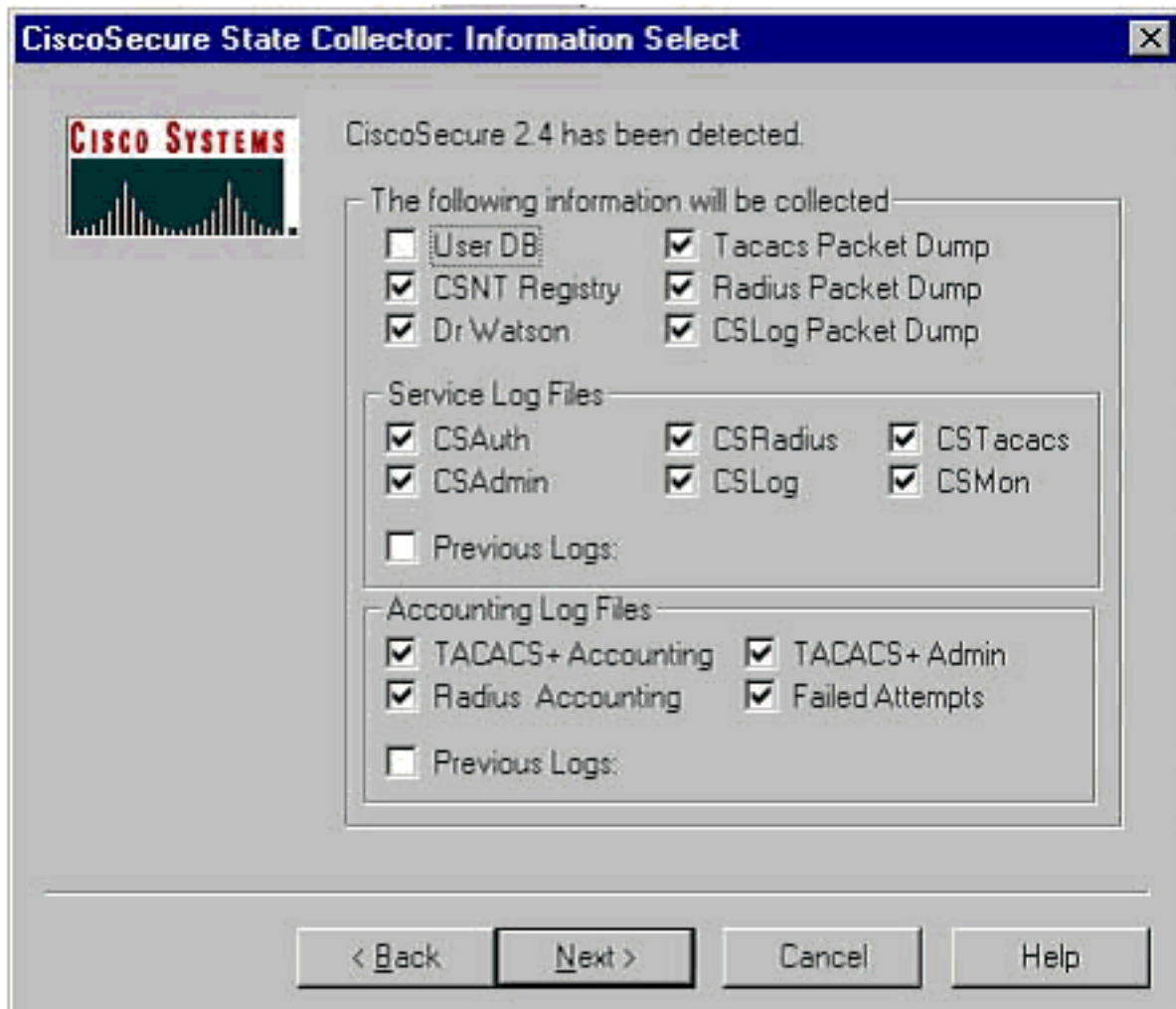
- [Run Wizard - このオプションの後には、次の4つのステップが続きます。](#) Cisco Secure State Collector: Information SelectCisco Secure State Collector: Installation SelectCisco Secure State Collector: Log VerbosityCisco Secure State Collector (実際の収集) または
- [水平な一定ログただ](#)、はじめの幾つかのステップをスキップし、Cisco Secure State Collector に直接行くことを可能にする: ログ 冗長画面

初めて設定するときには、Run Wizard を選択してログの設定に必要なステップをすべて実行します。いったん初期設定した後は、Set Log Levels Only オプションを使用してログレベルを修正できます。どちらかのオプションを選択し、Next をクリックします。

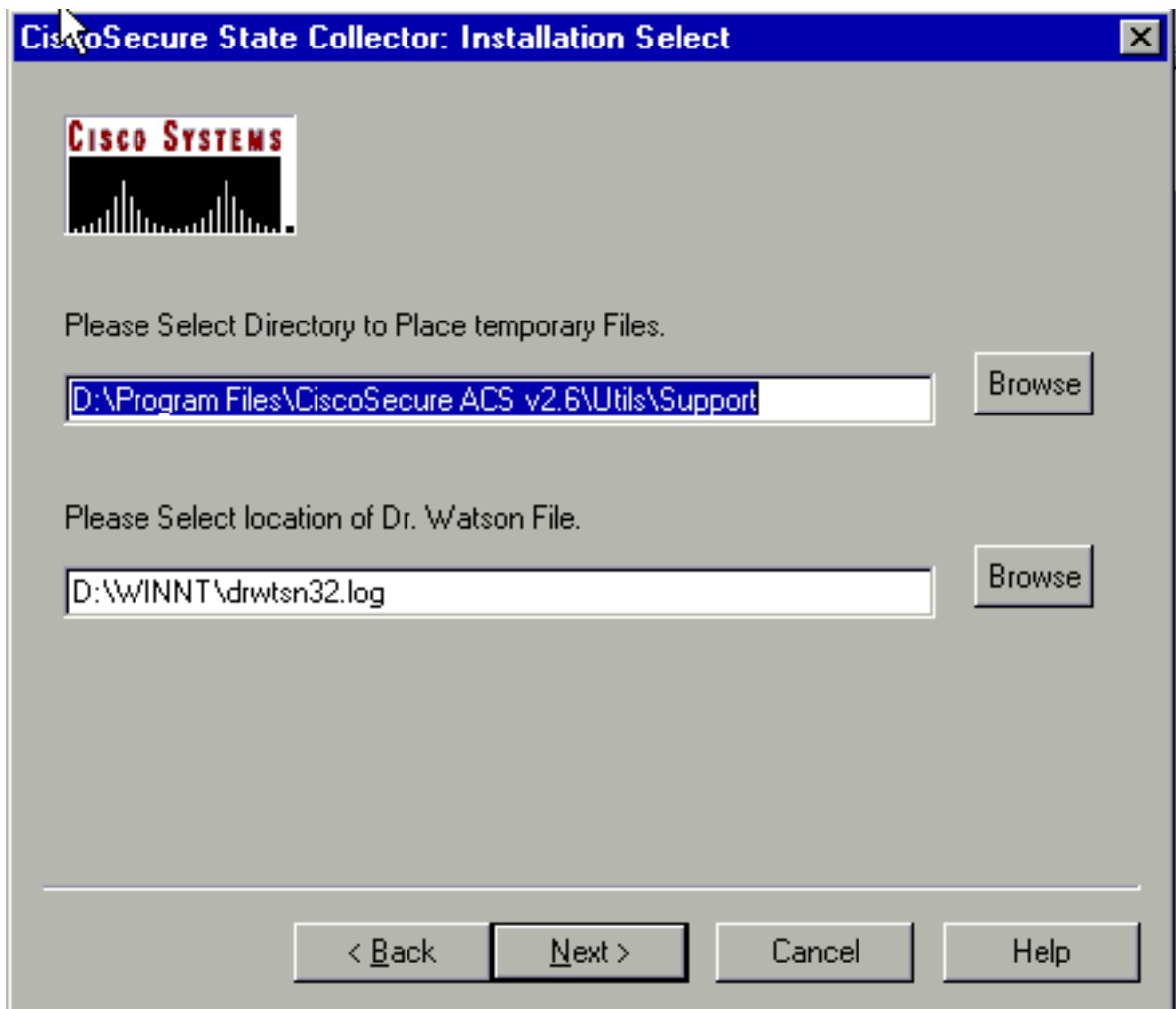
[Run Wizard](#)

次に、Run Wizard オプションを使用して情報を選択する方法を説明します。

1. **Cisco Secure State Collector: Information Select**デフォルトでは、User DB と Previous Logs 以外のすべてのオプションが選択されています。問題がユーザまたはグループ データベースと考えられる場合は、User DB を選択します。古いログを含めたい場合は、Previous Logs のオプションを選択します。完了したら、[Next] をクリックします。

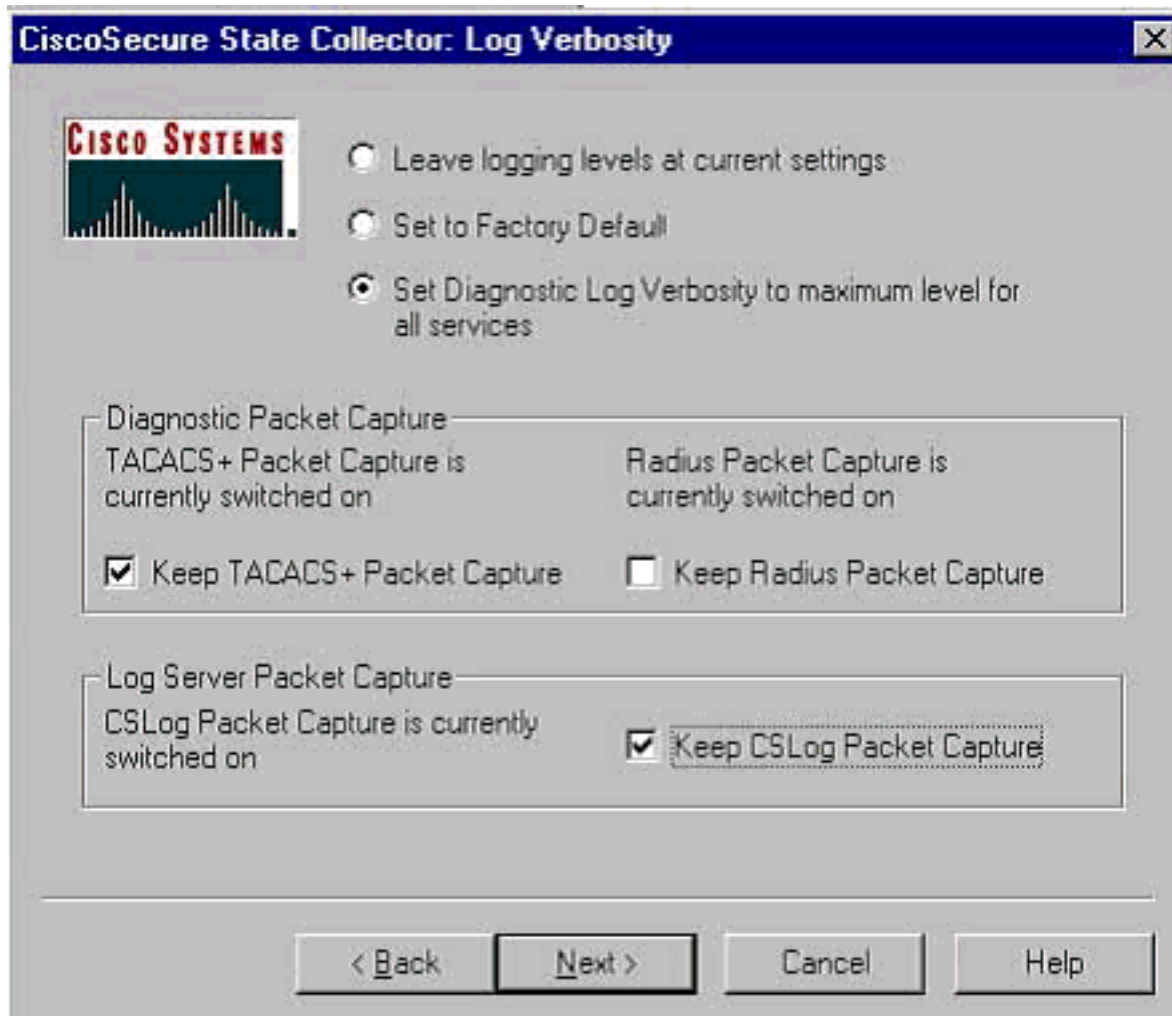


2. Cisco Secure State Collector: Installation Selectpackage.cab を置きたいと思うディレクトリを選択して下さい。デフォルトは C:\Program Files\Cisco Secure ACS v.26\Utils\Support です。必要であれば、この位置を変更できます。Dr. Watson の場所が正しく指定されていることを確認します。CSSupport を続行すると、いったんサービスが停止してから再開されます。Cisco Secure のサービスを停止および再開してよければ、Next をクリックして続け

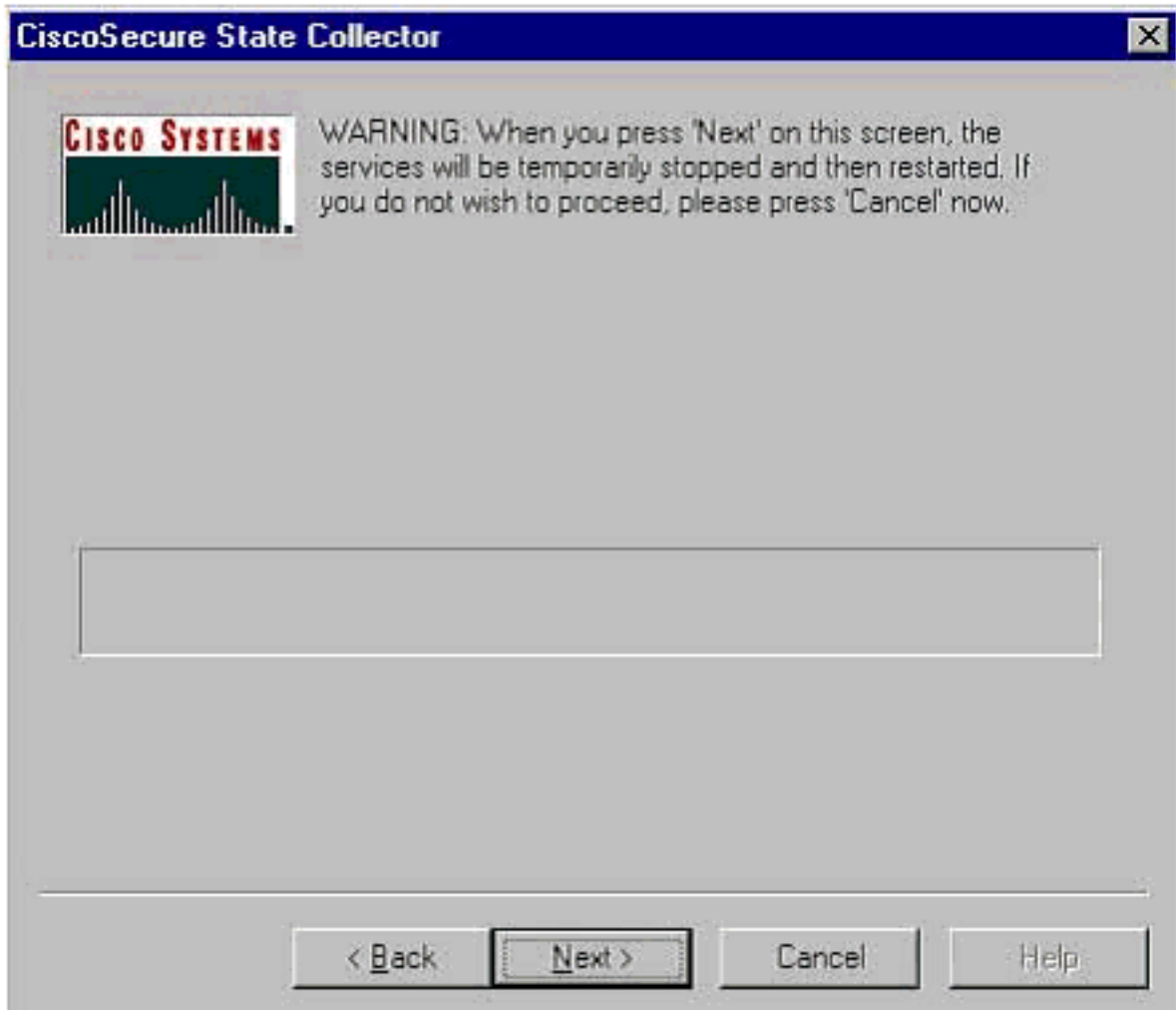


ます。

3. **Cisco Secure State Collector: Log Verbosity** Set Diagnostic Log Verbosity to maximum level for all services のオプションを選択します。 Diagnostic Packet Capture の見出しの下で、実行されているプロトコルに応じて TACACS+ または RADIUS を選択します。 Keep CSLog Packet Capture オプションを選択します。 終了したら、[Next] をクリックします。注: 前日からのログがありたいと思う場合ステップ 1 の前のログ オプションにオプションを選択し、次に戻りたいと思う日数を設定して下さい。



4. Cisco Secure State Collectorこのまま続けるとサービスがいったん停止した後、再開されることを示す警告が表示されます。この中断は、CSSupportが必要なファイルをすべて取り込むために必要なものです。ダウンタイムは必要最小限に限られます。このウィンドウで、サービスの停止と再開を確認できます。Next をクリックして続けます。



サービスが再開したときには、指定された場所に package.cab が存在します。Finish をクリックします。これで package.cab ファイルの準備は完了です。package.cab 用に指定した場所にブラウザし、このファイルを保存できるディレクトリに移します。トラブルシューティングプロセスの過程で、テクニカル サポート エンジニアからこのファイルを要求されることがあります。

ログレベルのみの設定

State Collector をすでに実行したことがあり、ログレベルのみを変更すればよい場合は、Set Log Levels Only オプションを使用して直接 Cisco Secure State Collector: Log Verbosity の画面に進むことができます。この画面で、診断パケットの取り込みに関する設定を行います。Next をクリックすると、そのまま警告ページに進みます。もう一度 Next をクリックすると、サービスが停止し、ファイルが収集されてから、再びサービスが開始されます。

package.cab ファイルの手動での収集

以下は package.cab にコンパイルされるファイルのリストです。CSSupport が適切に機能しない場合、Windowsエクスプローラを使用してこれらのファイルを収集できます。

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

Cisco Secure for Windows NT の AAA デバッグ情報の取得

トラブルシューティングを行う際に、コマンドライン モードで Windows NT CSRADIUS、CSTacacs、および CSAAuth サービスを実行できます。

注: GUIアクセスは Windows NT サービスのためのどの Cisco Secure でもコマンド・ライン モードで動作する場合限られています。

CSRADIUS、CSTacacs、または CSAAuth のデバッグ情報を取得するには、DOS ウィンドウを開き、Windows プロパティの Screen Buffer を高さ 300 に変更します。

CSRADIUS の場合は、次のコマンドを使用します。

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

CSTacacs の場合は、次のコマンドを使用します。

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

Cisco Secure for Windows NT の AAA 複製デバッグ情報の取得

複製の問題に関するトラブルシューティングを行う際は、コマンドライン モードで Windows NT CSAAuth サービスを実行できます。

注: GUIアクセスは Windows NT サービスのためのどの Cisco Secure でもコマンド・ライン モー

ドで動作する場合限られています。

CSAuth の複製デバッグ情報を取得するには、DOS ウィンドウを開き、Windows プロパティの Screen Buffer を高さ 300 に変更します。

CSAuth の場合は、ソース サーバとターゲット サーバの両方で次のコマンドを使用します。

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

デバッグはコマンドプロンプトウィンドウに書かれ、また \$BASE \ csauth \ ログ \ auth.log ファイルで入ります。

ユーザ認証のオフラインでのテスト

ユーザ認証は Command Line Interface (CLI; コマンド行インターフェイス) を使用してテストできます。RADIUS のテストには「radtest」、TACACS+ のテストには「tactest」を使用します。このテストは、通信デバイスから有益なデバッグ情報が得られない場合、および問題が Cisco Secure ACS Windows にあるのかデバイスにあるのかわからない場合に役立ちます。radtest および tactest \$BASE \ utils ディレクトリにあります。次に各テストの例を示します。

radtest による RADIUS ユーザ認証のオフライン テスト

```
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
      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.
```

tactest による TACACS+ ユーザ認証のオフライン テスト

```
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>
```

Windows 2000/NT データベース障害の原因の判別

認証が Windows 2000/NT に渡されているにもかかわらず失敗する場合は、プログラム> 管理ツール> ドメインのユーザ管理、ポリシー> 監査 の順に選択して Windows の監査機能をオンにします。プログラム> 管理ツール> イベント ビューア の順に選択すると、認証障害が表示されます。認証が失敗したときのログは、次の例のような形式で表示されます。

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

これらのメッセージは [Windows NT の Windows 2000 イベント](#) の Microsoft の Webサイトで[及びエラーメッセージ](#) および[エラーコード](#) 研究することができます。

1300L のエラー メッセージについては、次のように説明されています。

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.

例

RADIUS による正常な認証 RADIUS による認証の失敗 TACACS+ による正常な認証 TACACS+ による認証の失敗

```
F:\Program Files\Cisco Secure ACS v2.6\CSRradius>csradius -p -z
CSRradius 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>
```

[ツール情報 関連情報](#)

```
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\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=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+ による正常な認証

```
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+ による認証の失敗 (要約)

```
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>

[関連情報](#)

- [テクニカルサポート - Cisco Systems](#)