Cisco Secure UNIX および Secure ID（SDI クライアント）設定

目次

概要

このドキュメントの設定を実装するには、Security Dynamics Incorporated（SDI）の SecureID をサポートする CiscoSecure のバージョンが必要です。

前提条件

要件

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

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

Cisco Secure UNIX マシンへの SDI クライアント (Secure ID) のインストール

注: Secure ID は、通常、Cisco Secure UNIX (CSUnix) をインストールする前にインストールされます。 次の手順は、CSUnix をインストールした後に SDI クライアントをインストールする方法について説明します。

1. SDI サーバで **sdadmin** を実行します。 CSUnix マシンがクライアントであることを SDI サーバに知らせ、問題の SDI ユーザが CSUnix クライアントでアクティブであることを指定します。
2. **nslookup** #.#.#.# または **nslookup** <hostname> コマンドを使用して、CSUnix クライアントおよび SDI サーバが相互に、前方参照と逆引き参照を実行できることを確認します。
3. SDI サーバの /etc/sdace.txt ファイルを、CSUnix クライアントの /etc/sdace.txt ファイルにコピーします。
4. SDI サーバの sdconf.rec ファイルを CSUnix クライアントにコピーします。 このファイルは、CSUnix クライアントのどこにでも配置できます。 ただし、CSUnix クライアントでの配置場所が SDI サーバと同じディレクトリ構造である場合は、sdace.txt を修正する必要はありません。
5. /etc/sdace.txt または VAR_ACE は、sdconf.rec ファイルが置かれているパスをポイントする必要があります。 これを確認するには、cat /etc/sdace.txt を実行するか、env の出力を確認して、ルートの開始時に VAR_ACE がルートのプロファイルで定義されていることを確認します。
6. CSUnix クライアントの CSU.cfg をバックアップし、AUTHEN config_external_authen_symbols セクションを次の各行で変更します。
7. **K80CiscoSecure** と **S80CiscoSecure** を実行して CSUnix を再起動します。
8. CSU.cfg ファイルの変更前には Cisco Secure AAA サーバ プロセスがアクティブであったが、変更後はアクティブでないことが $BASE/utils/psg に表示されている場合は、CSU.cfg ファイルの変更でエラーが発生しています。 元の CSU.cfg ファイルを復元し、ステップ 6 の説明に従って再度変更します。

Secure ID および CSUNIX の初期テスト

Secure ID および CSUNIX をテストするには、次の手順を実行します。

1. 非 SDI ユーザは Telnet でルータに接続し、CSUnix で認証できることを確認します。 このように認証できない場合、SDI は機能しません。
2. ルータで基本的な SDI 認証をテストし、次のコマンドを実行します。
   aaa new-model aaa authentication login default tacacs+ none **注:** ここでは、**tacacs-server commands** コマンドがルータ上ですでにアクティブであると想定しています。
3. CSUnix コマンドラインから SDI ユーザを追加し、次のコマンドを入力します。
   $BASE/CLI/AddProfile -p 9900 -u *sdi_user* **-pw sdi**
4. ユーザとして認証を試みます。 そのユーザが機能する場合は、SDI が機能しており、ユーザプロファイルにさらに情報を追加できます。

5. SDI ユーザは、CSUnix の unknown_user プロファイルでテストできます。（ユーザがすべて SDI に渡されており、そのプロファイルが同じである場合は、CSUnix に明示的にリストされている必要はありません。）すでに未知のユーザ プロファイルがある場合は、次のコマンドを使用して削除します。
   $BASE/CLI/DeleteProfile -p 9900 -u unknown_user
6. 次のコマンドを使用して、別の未知のユーザ プロファイルを追加します。
   $BASE/CLI/AddProfile -p 9900 -u unknown_user -pw sdi このコマンドで、すべての未知ユーザが SDI に渡されます。

Secure ID および CSUNIX： TACACS+ プロファイル

1. SDI を使用せずに初期テストを実行します。 このユーザ プロファイルが、ログイン認証用 SDI パスワード、Challenge Handshake Authentication Protocol（CHAP）、およびパスワード認証プロトコル（PAP）なしで機能しない場合は、SDI パスワードで機能しません。
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
password = chap "chappwd"
password = pap "pappwd"
password = clear,"clearpwd"
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
}
protocol=ip {
}
}
}
```
2. プロファイルが機能したら、次の例に示すように、「clear」の代わりに「sdi」をプロファイルに追加します。
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
password = chap "chappwd"
password = pap "pappwd"
password = sdi default service=permit service=shell { } service=ppp { protocol=lcp { }
protocol=ip { } } }
```

プロファイルの仕組み

このプロファイルでは、次の組み合わせでユーザがログインできます。

- ルータへの Telnet 接続と SDI の使用（ここでは、**aaa authentication login default tacacs+** コマンドがルータ上で実行されたことを想定しています）。
- ダイヤルアップ ネットワーキング PPP 接続および PAP（ここでは、**aaa authentication ppp default if-needed tacacs** および **ppp authen pap** コマンドがルータで実行されたことを想定しています）。**注:** PC のダイヤルアップ ネットワークで、「Accept any authentication including clear text」がオンであることを確認します。 ダイヤルする前にターミナル ウィンドウで、次のユーザ名とパスワードの組み合わせのいずれかを入力します。
```
username: cse*code+card
password: pap (must agree with profile)

username: cse
```

```
password: code+card
```

- ダイヤルアップ ネットワーキング PPP 接続および CHAP（ここでは、**aaa authentication ppp default if-needed tacacs** および **ppp authen chap** コマンドがルータで実行されたことを想定しています）。**注:** PC のダイヤルアップ ネットワークで、「Accept any authentication including clear text」または「Accept only encrypted authentication」がオンであることが必要です。 ダイヤルする前にターミナル ウィンドウで、次のユーザ名とパスワードを入力します。
```
username: cse*code+card
password: chap (must agree with profile)
```

機能しない CSUnix TACACS+ パスワードの組み合わせ

次の組み合わせにより、次の CSUnix デバッグ エラーが発生します。

- CHAP と、パスワード フィールドの「クリアテキスト」ではないパスワード。 ユーザは、「クリアテキスト」パスワードではなく、code+card を入力します。 RFC 1994 on CHAP では、クリアテキストのパスワードの保存が要求されます。
```
username: cse password: code+card CiscoSecure INFO - User cse, No tokencard password
received CiscoSecure NOTICE - Authentication - Incorrect password;
```
- CHAP と不正な CHAP パスワード。

  username: cse*code+card password: wrong chap password（ユーザが SDI に渡し、SDI はユーザに渡しますが、CHAP パスワードが正しくないため、CSUnix はユーザにエラーを表示します。）
```
CiscoSecure INFO - The character * was found in username:
   username=cse,passcode=1234755962
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
CiscoSecure INFO - sdi_verify: rtn 1
CiscoSecure NOTICE - Authentication - Incorrect password;
```
- PAP と不正な PAP パスワード。

  username: cse*code+card password: wrong pap password（ユーザが SDI に渡し、SDI はユーザに渡しますが、CHAP パスワードが正しくないため、CSUnix はユーザにエラーを表示します。）
```
CiscoSecure INFO - 52 User Profiles and 8 Group Profiles loaded into Cache.
CiscoSecure INFO - The character * was found in username:
   username=cse,passcode=1234651500
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
CiscoSecure INFO - sdi_verify: rtn 1
CiscoSecure NOTICE - Authentication - Incorrect password;
```

CSUnix TACACS+ SDI のサンプル プロファイルのデバッグ

- ユーザは、CHAP および ログイン認証を行う必要があります。 PAP が失敗します。
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
password = chap "********"
password = sdi
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
}
protocol=ip {
```

```
}
}
```

- ユーザは、PAP およびログイン認証を行う必要があります。 CHAP が失敗します。
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
member = admin
password = pap "********"
password = sdi
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
}
protocol=ip {
}
}
}
```

CSUnix RADIUS

以降のセクションでは、CSUNIX RADIUS の手順を説明します。

CSUnix および RADIUS によるログイン認証

次の手順を実行して認証をテストします。

1. SDI を使用せずに初期テストを実行します。 このユーザ プロファイルがログイン認証用 SDI パスワードなしで機能しない場合は、SDI パスワードで機能しません。
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```
2. このプロファイルが機能したら、次の例に示すように「whatever」を「sdi」に置き換えます。
```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

CSUnix および RADIUS による PPP および PAP 認証

次の手順を実行して認証をテストします。

注: CSUnix と RADIUS での PPP CHAP 認証はサポートされていません。

1. SDI を使用せずに初期テストを実行します。 このユーザ プロファイルが、PPP/PAP 認証用 SDI パスワードおよび「async mode dedicated」なしで機能しない場合は、SDI パスワードで機能しません。
```
# ./ViewProfile -p 9900 -u cse

user = cse {
password = pap "pappass"
```

```
radius=Cisco {
check_items = {
}
reply_attributes= {
6=2
7=1
}
}
}
```

2. 上記のプロファイルが機能したら、次に示すように、プロファイルに **password = sdi** を追加し、属性 **200=1** を追加します（これで、Cisco_Token_Immediate が yes に設定されます）。`# ./ViewProfile -p 9900 -u cse`

```
user = cse {
password = pap "pappass"
password = sdi
radius=Cisco {
check_items = {
200=1
}
reply_attributes= {
6=2
7=1
}
}
}
```

3. 「**Advanced GUI サーバ セクション**」で、「**Enable Token Caching**」が設定されていることを確認します。 これは、コマンドライン インターフェイス（CLI）で、次のように確認できます。`$BASE/CLI/ViewProfile -p 9900 -u SERVER.#.#.#.#`

```
!--- Where #.#.#.# is the IP address of the CSUnix server. TokenCachingEnabled="yes"
```

ダイヤルアップ ネットワーキング PPP 接続および PAP

ここでは、**aaa authentication ppp default if-needed tacacs** および **PPP authen PAP** コマンドがルータで実行されたことを想定しています。 ダイヤルする前にターミナル ウィンドウで、次のユーザ名とパスワードを入力します。

```
username: cse
password: code+card
```

注: PC のダイヤルアップ ネットワークで、「Accept any authentication including clear text」がオンであることを確認します。

デバッグと検証のヒント

以降のセクションには、デバッグと検証のヒントが含まれています。

Cisco Secure RADIUS、PPP および PAP

次に示すのは、正しいデバッグの例です。

```
CiscoSecure DEBUG - RADIUS ; Outgoing Accept Packet id=133 (10.31.1.6)
    User-Service-Type = Framed-User
    Framed-Protocol = PPP
CiscoSecure DEBUG - RADIUS ; Request from host a1f0106 nas (10.31.1.6)
    code=1 id=134 length=73
CiscoSecure DEBUG - RADIUS ; Incoming Packet id=134 (10.31.1.6)
    Client-Id = 10.31.1.6
```

```
    Client-Port-Id = 1
    NAS-Port-Type = Async
    User-Name = "cse"
    Password = "?\235\306"
    User-Service-Type = Framed-User
    Framed-Protocol = PPP
CiscoSecure DEBUG - RADIUS ; Authenticate (10.31.1.6)
CiscoSecure DEBUG - RADIUS ; checkList: ASCEND_TOKEN_IMMEDIATE = 1
CiscoSecure DEBUG - RADIUS ; User PASSWORD type is Special
CiscoSecure DEBUG - RADIUS ; authPapPwd (10.31.1.6)
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
CiscoSecure DEBUG - profile_valid_tcaching FALSE ending.
CiscoSecure DEBUG - Token Caching.  IGNORE.
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
CiscoSecure INFO - sdi_verify: rtn 1
CiscoSecure DEBUG - RADIUS ; Sending Ack of id 134 to a1f0106 (10.31.1.6)
```

Secure ID および CSUNIX

デバッグは、local0.debug の /etc/syslog.conf で指定されたファイルに保存されます。

SDI でも、その他の方法でもユーザを認証できない：

Secure ID を追加した後、CSU.cfg ファイルの変更時にエラーがなかったことを確認します。CSU.cfg ファイルを修正するか、バックアップの CSU.cfg ファイルに戻します。

次に示すのは、正しいデバッグの例です。

```
Dec 13 11:24:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:24:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: cse authenticated by ACE Srvr
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: cse authenticated by ACE Srvr
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 1
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 1
```

次に示すのは、正しくないデバッグの例です。

CSUnix がユーザ プロファイルを見つけ、SDI サーバに送信しますが、パスコードが正しくないため、SDI サーバがユーザにエラーを表示します。

```
Dec 13 11:26:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:26:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   WARNING - sdi_verify: cse denied access by ACE Srvr
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   WARNING - sdi_verify: cse denied access by ACE Srvr
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
```

```
   INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 0
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi_verify: rtn 0
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   NOTICE - Authentication - Incorrect password;
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
   NOTICE - Authentication - Incorrect password;
```

次の例は、ACE サーバがダウンしていることを示しています。

SDI サーバで **./aceserver stop** を入力します。 ユーザには「Enter PASSCODE」メッセージが表示されません。

```
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   ERROR - sdi_challenge error: sd_init failed cli/srvr comm init (cse)
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   ERROR - sdi_challenge error: sd_init failed cli/srvr comm init (cse)
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=RESET
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:
   INFO - sdi: cse free external_data memory,state=RESET
```

関連情報

- Cisco Secure ACS for UNIX に関するサポート ページ
- Cisco Secure ACS for UNIX に関する Field Notice
- テクニカルサポート - Cisco Systems