配置Cisco Secure UNIX和安全ID（SDI客戶端）

目錄

簡介

要實施本文檔中的配置，您需要支援Security Dynamics Incorporated(SDI)的安全ID的任何Cisco Secure版本。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

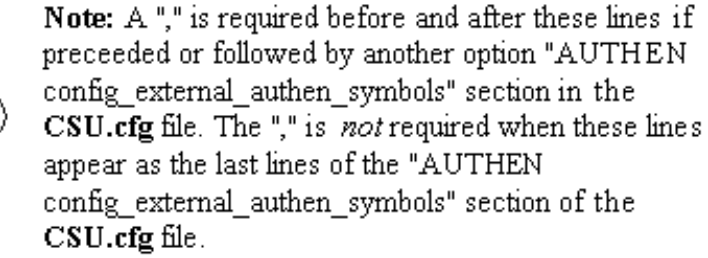
如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

在Cisco Secure UNIX電腦上安裝SDI客戶端（安全ID）

注意：安全ID通常在安裝思科安全UNIX(CSUnix)之前安裝。以下說明介紹了如何在安裝CSUnix之後安裝SDI客戶端。

1. 在SDI伺服器上，運行**sdadmin**。通知SDI伺服器該CSUnix電腦是一個客戶端，並指定在CSUnix客戶端上啟用相關的SDI使用者。
2. 使用**nslookup** #.#.#.#或**nslookup** <hostname>命令確保CSUnix客戶端和SDI伺服器可以相互執行正向和反向查詢。
3. 將SDI伺服器的/etc/sdace.txt檔案複製到CSUnix客戶端/etc/sdace.txt檔案。
4. 將SDI伺服器的sdconf.rec檔案複製到CSUnix客戶端；此檔案可能位於CSUnix客戶端上的任何位置。但是，如果它放置在CSUnix客戶端上與SDI伺服器相同的目錄結構中，則無需修改sdace.txt。
5. /etc/sdace.txt或VAR_ACE必須指向sdconf.rec檔案所在的路徑。要驗證這一點，請運行cat /etc/sdace.txt ，或檢查env的輸出，以確保根啟動時在根配置檔案中定義VAR_ACE。
6. 備份CSUnix客戶端的CSU.cfg，然後使用以下行修改AUTHEN config_external_authen_symbols部分

```
:
AUTHEN config_external_authen_symbols = {
  {
    "./libskey.so",
    "skey"
  }
        ,
  {
    "./libsdi.so",
    "sdi"
  }
        ,
  {
    "./libpap.so",
    "pap"
  }
        ,
  {
    "./libchap.so",
    "chap"
  }
```



7. 通過執行**K80CiscoSecure**和**S80CiscoSecure**可回收**CSUnix**。
8. 如果$BASE/utils/psg顯示Cisco Secure AAA Server Process進程在CSU.cfg檔案被修改之前處於活動狀態，但之後未處於活動狀態，則在CSU.cfg檔案的修訂版中出現錯誤。恢復原始CSU.cfg檔案，然後再次嘗試進行步驟6中概述的更改。

安全ID和CSUnix的初始測試

要測試安全ID和CSUnix，請執行以下步驟：

1. 確保非SDI使用者可以Telnet到路由器並使用CSUnix進行身份驗證。如果這不起作用，SDI將不起作用。

2. 在路由器中測試基本SDI身份驗證，然後運行以下命令：

```
aaa new-model

aaa authentication login default tacacs+ none
```

注意：此假設路由器中**的tacacs-server**命令已經處於活動狀態。

3. 從CSUnix命令列新增SDI使用者以輸入此命令

```
$BASE/CLI/AddProfile -p 9900 -u sdi_user -pw sdi
```

4. 嘗試以使用者身份進行身份驗證。.如果該使用者工作，則SDI是可操作的，並且您可以將其他資訊新增到使用者配置檔案中。
5. SDI使用者可以使用CSUnix中的unknown_user配置檔案進行測試。（如果所有使用者都傳遞到SDI且所有使用者都具有相同的配置檔案，則無需在CSUnix中明確列出。）如果已經存在未知的使用者配置檔案，請使用此命令的幫助將其刪除：

```
$BASE/CLI/DeleteProfile -p 9900 -u unknown_user
```

6. 使用以下命令新增另一個未知使用者配置檔案：

```
$BASE/CLI/AddProfile -p 9900 -u unknown_user -pw sdi
```

此命令將所有未知使用者傳遞給SDI。

安全ID和CSUnix:TACACS+設定檔

1. 不使用SDI執行初始測試。如果沒有SDI密碼進行登入身份驗證、Challenge Handshake身份驗證協定(CHAP)和密碼身份驗證協定(PAP)，此使用者配置檔案無法使用，它將不能使用SDI密碼：

```
# ./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. 配置檔案運行後，將「sdi」新增到配置檔案中，而不是「clear」，如下例所示：

```
# ./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 {
}
}

}
```

配置檔案的工作原理

此配置檔案允許使用者使用以下組合登入：

- Telnet至路由器並使用SDI。(這假設已在路由器上執行**aaa authentication login default tacacs+**命令。)
- 撥號網路PPP連線和PAP。(此假設路由器上已執行**aaa authentication ppp default if-needed tacacs**和**ppp authen pap**命令)。**附註：** 在PC的撥號網路中，確保選中「接受包括明文在內的任何身份驗證」。撥號之前，在終端視窗中輸入以下使用者名稱/密碼組合之一：

```
username: cse*code+card
password: pap (must agree with profile)

username: cse
password: code+card
```

- 撥號網路PPP連線和CHAP。(此假設路由器上已執行**aaa authentication ppp default if-needed tacacs**和**ppp authen chap**命令)。**注意：**在PC上的撥號網路中，必須選中「接受包括明文在內的任何身份驗證」或「僅接受加密身份驗證」。撥號之前，請在終端視窗中輸入此使用者名稱和密碼：

```
username: cse*code+card
password: chap (must agree with profile)
```

無法正常工作的CSUnix TACACS+密碼組合

這些組合會產生以下CSUnix調試錯誤：

- CHAP，並且密碼欄位中沒有「明文」密碼。使用者輸入`code+card`而不是「cleartext」密碼。CHAP上的RFC 1994需要 「明文密碼」儲存。

```
username: cse
password: code+card

CiscoSecure INFO - User cse, No tokencard password received
CiscoSecure NOTICE - Authentication - Incorrect password;
```

- CHAP和錯誤的CHAP密碼。

```
username: cse*code+card
password: wrong chap password
```

（使用者會傳遞到SDI，SDI傳遞使用者，但CSUnix會因為CHAP密碼錯誤而使使用者失敗。）

```
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和錯誤的PAP密碼。

```
username: cse*code+card
password: wrong pap password
```

（使用者會傳遞到SDI，SDI傳遞使用者，但CSUnix會因為CHAP密碼錯誤而使使用者失敗。）

```
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;
```

調試CSUnix TACACS+ SDI示例配置檔案

- 使用者需要執行CHAP和登入驗證；PAP失敗。

```
# ./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 {
}
}
```

- 使用者需要執行PAP和登入驗證；CHAP失敗。

```
# ./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

這些部分包含CSUnix RADIUS過程。

使用CSUnix和RADIUS的登入身份驗證

執行以下步驟測試身份驗證：

1. 不使用SDI執行初始測試。如果沒有用於登入身份驗證的SDI密碼，此使用者配置檔案無法正常工作，它將不能使用SDI密碼：

```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```

2. 一旦此配置檔案生效，請將「whatever」替換為「sdi」，如以下示例所示：

```
# ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

使用CSUnix和RADIUS的PPP和PAP身份驗證

執行以下步驟測試身份驗證：

注意：不支援使用CSUnix和RADIUS進行PPP CHAP身份驗證。

1. 不使用SDI執行初始測試。如果沒有用於PPP/PAP身份驗證的SDI口令和「專用非同步模式」，如果此使用者配置檔案無法使用，它將不能使用SDI口令：

```
# ./ViewProfile -p 9900 -u cse

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

2. 上述設定檔運作後，將**password = sdi**新增至設定檔並新增屬性**200=1**，如以下範例所示（這會將Cisco_Token_Immediate設定為yes。）：

```
# ./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. 在「**Advanced GUI， server**」部分，確保**已設定「Enable Token Caching」**。這可透過以下方式透過指令行介面(CLI)確認：

```
$BASE/CLI/ViewProfile -p 9900 -u SERVER.#.#.#.#
!--- Where #.#.#.# is the IP address of the CSUnix server. TokenCachingEnabled="yes"
```

撥號網路PPP連線和PAP

假設路由器上已執行**aaa authentication ppp default if-needed tacacs**和**PPP auth PAP**命令。在撥號之前在終端視窗中輸入此使用者名稱和密碼：

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

注意：在PC的撥號網路中，確保選中「接受包括明文在內的任何身份驗證」。

偵錯和驗證提示

這些部分包含調試和驗證提示的提示。

Cisco安全RADIUS、PPP和PAP

以下是偵錯範例：

```
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)
```

安全ID和CSUnix

調試儲存在/etc/syslog.conf為local0.debug指定的檔案中。

沒有使用者能夠進行身份驗證 — SDI或其他：

新增安全ID後，請確保修改CSU.cfg檔案時未出現錯誤。修復CSU.cfg檔案或恢復到備份CSU.cfg檔案。

以下是偵錯範例：

```
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
```

以下是錯誤偵錯的範例：

CSUnix查詢使用者配置檔案並將其傳送到SDI伺服器，但SDI伺服器因密碼錯誤而使使用者失敗。

```
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;
```

以下範例顯示Ace伺服器已關閉：

在SDI伺服器上輸入**./aceserver stop**。使用者未收到「Enter PASSCODE」訊息。

```
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
```

相關資訊

- Cisco Secure ACS for UNIX支援頁
- 適用於UNIX的Cisco Secure ACS的現場通知
- 技術支援 - Cisco Systems