配置 Cisco Secure UNIX 与安全 ID（SDI 客户端）

目录

简介

要实现在本文的配置，您需要所有Cisco Secure版本该支持Security Dynamics Incorporated (SDI) ‘s安全ID。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

在 Cisco Secure UNIX 机器上安装 SDI 客户端 (安全 ID)

注意： 安全ID通常安装，在Cisco Secure UNIX (CSUnix)前安装。在CSUnix安装后，这些说明描述如何安装SDI客户端。

1. 在SDI服务器上，请运行**sdadmin**。告诉SDI服务器CSUnix计算机是客户端并且指定有问题的SDI的用户在CSUnix客户端激活。
2. 请使用**nslookup #.#.#.#**或**nslookup <hostname>命令**确保CSUnix客户端和SDI服务器能执行转发和反向查找彼此。
3. 复制SDI服务器的/etc/sdace.txt文件到CSUnix客户端/etc/sdace.txt文件。
4. 复制SDI服务器的sdconf.rec文件给CSUnix客户端;此文件任何地方在CSUnix客户端可能驻留。然而，如果它在同一个目录结构安置在作为是在SDI服务器的CSUnix客户端，不必须修改sdace.txt。
5. /etc/sdace.txt或VAR_ACE必须指向sdconf.rec文件查找的路径。要验证此，请运行cat /etc/sdace.txt或者检查env输出肯定VAR_ACE在根的配置文件定义作为根开始。
6. 备份CSUnix客户端的CSU.cfg，然后修改AUTHEN config_external_authen_symbols部分用这些线路：
7. 由**K80CiscoSecure**和**S80CiscoSecure的**执行回收CSUnix。
8. 如果$BASE/utils/psg显示Cisco Secure AAA服务器进程进程是活跃的，在不之后前修改了CSU.cfg文件，但是，则错误在CSU.cfg文件的版本犯了。恢复原始CSU.cfg文件并且设法做再概述的变动在步骤6。

安全ID和CSUNIX的初始测试

要测试安全ID和CSUNIX，请执行这些步骤：

1. 确保非SDI用户可能远程登录到路由器和用CSUnix验证。如果这不工作， SDI不会工作。
2. 测试在路由器的基本SDI Authentication并且运行此命令：
   aaa new-model aaa authentication login default tacacs+ none **注意：** 这假设， **tacacs-server**命令已经是活跃的在路由器。
3. 从CSUnix line命令输入此命令添加一个SDI用户
   $BASE/CLI/AddProfile -p 9900 -u *sdi_user* **-pw sdi**
4. 设法验证作为用户。如果该用户工作， SDI isoperational和您能添加其他信息到用户配置文件。
5. SDI用户可以用在CSUnix的unknown_user配置文件测试。(用户在CSUnix不必须明确地列出，如果他们所有通过对SDI，并且所有有同一配置文件。)如果已经有未知用户配置文件请在此命令帮助下存在，删除它：
   $BASE/CLI/DeleteProfile -p 9900 -u unknown_user
6. 请使用此命令添加另一个未知用户配置文件：
   $BASE/CLI/AddProfile -p 9900 -u unknown_user -pw sdi 此命令通过所有未知用户对SDI。

安全ID和CSUNIX ：TACACS+配置文件

1. 执行一最初的测验，不用SDI。如果此用户配置文件不工作没有登录认证的一个SDI密码，质询握手验证协议(CHAP)，和密码认证协议，不会与SDI密码一起使用：`# ./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. 一旦配置文件工作，如此示例所显示，请添加“sdi”到配置文件在“结算位置”：`# ./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 { } } }
```

配置文件如何工作

此配置文件允许用户登陆与这些组合：

- 对路由器和使用SDI的Telnet。(这假设， **aaa authentication login default tacacs+命令**在路由器被执行了。)
- 拨号网络PPP连接和PAP。(这假设， **aaa authentication ppp default if-needed tacacs和ppp验证pap**命令在路由器被执行了)。**注意：** 在PC上，在拨号网络，请确保“接受所有验证包括明文”被检查。在拨号前，请输入在终端窗口的这些用户名/密码组合之一：`username: cse*code+card password: pap (must agree with profile)`

  `username: cse password: code+card`
- 拨号网络PPP连接和CHAP。(这假设， **aaa authentication ppp default if-needed tacacs和ppp authen chap**命令在路由器被执行了)。**注意：** 在PC上，在拨号网络，或者“请接受所有验证包括明文”或“请接受仅加密的身份验证”必须检查。在拨号前，请输入在终端窗口的此用户名和密码：`username: cse*code+card password: chap (must agree with profile)`

CSUnix TACACS+不工作的密码组合

这些组合产生这些CSUnix调试错误：

- CHAP和不“明文”密码在密码字段。用户输入`code+card`而不是“明文”密码。在CHAP的RFC 1994要求明文密码存储设备。

  username: cse password: code+card `CiscoSecure INFO - User cse, No tokencard password received CiscoSecure NOTICE - Authentication - Incorrect password;`
- CHAP和一坏CHAP口令。

  username: cse*code+card password: wrong chap password (用户通过对SDI，并且SDI通过用户，但是CSUnix发生故障用户，因为CHAP口令是坏的。)`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和一坏PAP口令。

  username: cse*code+card password: wrong pap password (用户通过对SDI，并且SDI通过用户，但是CSUnix发生故障用户，因为CHAP口令是坏的。)
```
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;
```

调试CSUnix TACACS+ SDI示例配置文件

- 用户需要执行CHAP和登录认证;PAP发生故障。
```
# ./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 {
}
}
```

- 用户需要执行PAP和登录认证;CHAP发生故障。
```
# ./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

这些部分包含CSUnix RADIUS步骤。

与CSUnix和RADIUS的登录认证

执行这些步骤测试验证：

1. 执行一最初的测验，不用SDI。如果此用户配置文件不工作没有登录认证的一个SDI密码，不会与SDI密码一起使用：`# ./ViewProfile -p 9900 -u cse`
```
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }
```
2. 一旦此配置文件工作，请替换“什么”与“sdi”如此示例所显示：`# ./ViewProfile -p 9900 -u cse`
```
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }
```

PPP和PAP认证与CSUnix和RADIUS

执行这些步骤测试验证：

注意： 不支持与CSUnix和RADIUS的PPP CHAP认证。

1. 执行一最初的测验，不用SDI。如果此用户配置文件不工作没有PPP/PAP验证和“async mode dedicated的一个SDI密码”，不会与SDI密码一起使用：`# ./ViewProfile -p 9900 -u cse`

```
user = cse {
password = pap "pappass"
radius=Cisco {
check_items = {
}
reply_attributes= {
6=2
7=1
}
}
}
```
2. 一旦上述配置文件工作，请添加**密码= sdi**到配置文件并且添加属性**200=1**如此示例所显示(这设置Cisco_Token_Immediate为是。)：`# ./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“**高级GUI**，服务器部分”，**确保" Enable Token Caching "**设置。这可以从命令行界面(CLI)被确认与：`$BASE/CLI/ViewProfile -p 9900 -u SERVER.#.#.#.#`
```
!--- Where #.#.#.# is the IP address of the CSUnix server. TokenCachingEnabled="yes"
```

拨号联网 PPP 连接和 PAP

假设， **aaa authentication ppp default if-needed tacacs**和**PPP验证PAP**命令在路由器被执行了。在您拨号，请输入在终端窗口的此用户名和密码。前：

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

注意： 在PC上，在拨号网络，请确保“接受所有验证包括明文”被检查。

调试与验证提示

这些部分包含调试与验证提示的提示。

Cisco Secure RADIUS、PPP 和 PAP

这是成功调试的示例：

```
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

调试在local0.debug的/etc/syslog.conf指定的文件存储。

用户不能验证- SDI或：

在您添加安全ID后，请确保错误未犯，当您修改CSU.cfg文件时。修理CSU.cfg文件或恢复到备份CSU.cfg文件。

这是成功调试的示例：

```
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
```

这是错误Debug的示例：

CSUnix查找用户配置文件并且发送它到SDI服务器，但是SDI服务器发生故障用户，因为密码是坏的。

```
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;
```

这是示例显示ACE服务器发生故障：

回车在SDI服务器的./aceserver终止。用户没获得" Enter PASSCODE "消息。

```
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
```

相关信息

- Cisco Secure ACS for UNIX 支持页
- 用于UNIX的Cisco Secure ACS的问题信息通告(Field Notice)
- 技术支持 - Cisco Systems