تكوين Cisco Secure UNIX و ID الآمن (SDI Client)

المحتويات

المقدمة

لتنفيذ التكوين في هذا المستند، يلزمك أي إصدار آمن من Cisco يدعم معرف Security Dynamics Incorporated (SDI)) الآمن.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

تثبيت عميل SDI (معرف آمن) على جهاز Cisco Secure UNIX

ملاحظة: يتم تثبيت المعرف الآمن عادة قبل تثبيت CSUnix (Cisco Secure Unix). تصف هذه التعليمات كيفية تثبيت عميل SDI بعد تثبيت CSUnix.

1. على خادم SDI، قم بتشغيل **sdadmin**. أخبر خادم SDI أن جهاز CSUnix هو عميل وحدد أن مستخدمي SDI المعنيين يتم تنشيطهم على عميل CSUnix.
2. أستخدم الأمر **nslookup** #.#.#.# أو hostname> **nslookup**> للتأكد من أنه يمكن لعميل CSUnix وخادم SDI إجراء بحث مسبق وعكسي عن بعضهما البعض.
3. انسخ ملف /etc/sdace.txt الخاص بخادم SDI إلى ملف /etc/sdace.txt الخاص بعميل CSUnix.
4. انسخ ملف sdconf.rec الخاص بخادم SDI إلى عميل CSUnix، قد يوجد هذا الملف في أي مكان على عميل CSUnix. ومع ذلك، إذا تم وضعها في نفس بنية الدليل على عميل CSUnix كما كانت على خادم SDI، فلا يجب تعديل sdace.txt.
5. يجب أن يشير إما /etc/sdace.txt أو VAR_ACE إلى المسار حيث يوجد ملف sdconf.rec. للتحقق من ذلك، قم بتشغيل cat /etc/sdace.txt، أو تحقق من إخراج env للتأكد من تعريف VAR_ACE في ملف تعريف الجذر مع بدء الجذر.
6. قم بإجراء نسخ إحتياطي لقسم CSU.cfg الخاص بعميل CSU.CFG، ثم قم بتعديل قسم AUTHEN config_external_authen_symbols باستخدام البنود التالية:

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

Note: A "," is required before and after these lines if preceeded or followed by another option "AUTHEN config_external_authen_symbols" section in the **CSU.cfg** file. The "," is *not* required when these lines appear as the last lines of the "AUTHEN config_external_authen_symbols" section of the **CSU.cfg** file.

7. إعادة تدوير CSUnix من خلال تنفيذ **K80CiscoSecure** و**S80CiscoSecure**.
8. إذا أظهرت $BASE/utils/PSG أن عملية خادم Cisco Secure AAA كانت نشطة قبل تعديل ملف CSU.cfg ولكن ليس بعد ذلك، بعد ذلك حدثت أخطاء في مراجعة ملف CSU.cfg. قم باستعادة ملف CSU.cfg الأصلي وحاول إجراء التغييرات المحددة في الخطوة 6 مرة أخرى.

الاختبار الأولي للمعرف الآمن و CSUnix

لاختبار معرف آمن و CSUnix، قم بإجراء الخطوات التالية:

1. تأكد من أنه يمكن لمستخدم بخلاف SDI إستخدام Telnet إلى الموجه وتتم مصادقته باستخدام CSUnix. إذا

لم ينجح ذلك، فلن يعمل SDI.
2. اختبر مصادقة SDI الأساسية في الموجه وشغل هذا أمر:

```
aaa new-model

aaa authentication login default tacacs+ none
```

ملاحظة: يفترض هذا أن أوامر **tacacs-server** نشطة بالفعل في الموجه.
3. إضافة مستخدم SDI من سطر أوامر CSUnix لإدخال هذا الأمر

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

4. حاول المصادقة كمستخدم. . إذا كان ذلك المستخدم يعمل، فإن SDI يكون في وضع التشغيل، ويمكنك إضافة معلومات إضافية إلى ملفات تعريف المستخدمين.
5. يمكن إختبار مستخدمي SDI باستخدام ملف تعريف مستخدم_غير معروف في CSUnix. (لا يجب إدراج المستخدمين بشكل صريح في CSUnix إذا تم نقلهم جميعا إلى SDI وكان لديهم جميعا نفس ملف التعريف.) إذا كان هناك ملف تعريف مستخدم غير معروف موجود بالفعل، فقم بحذفه باستخدام التعليمات الخاصة بهذا الأمر:

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

6. أستخدم هذا الأمر لإضافة ملف تعريف مستخدم آخر غير معروف:

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

يقوم هذا الأمر بتمرير جميع المستخدمين غير المعروفين إلى SDI.

المعرف الآمن و CSUnix: ملف تعريف TACACS+

1. قم بإجراء إختبار أولي دون SDI. إذا لم يعمل ملف تعريف المستخدم هذا بدون كلمة مرور SDI لمصادقة تسجيل الدخول وبروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (CHAP) وبروتوكول مصادقة كلمة المرور (PAP)، فلن يعمل مع كلمة مرور SDI:

```
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. بمجرد أن يعمل التوصيف، أضف "sdi" إلى التوصيف بدلا من "clear" كما هو موضح في هذا المثال:

```
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
                  {
                  {

                  {
```

كيفية عمل ملف التعريف

يتيح ملف التعريف هذا للمستخدم تسجيل الدخول باستخدام هذه التركيبات:

- Telnet إلى الموجه واستخدام SDI. (يفترض هذا أنه تم تنفيذ الأمر **AAA authentication login default tacacs+** على الموجه.)
- اتصال PPP لشبكة الطلب الهاتفي و PAP. (يفترض هذا أن **مصادقة AAA** هي الأمر **tacacs الافتراضي إن** لزم **وPPP authen PAP** قد تم تنفيذه على الموجه).**ملاحظة:** في الكمبيوتر، في شبكة الطلب الهاتفي، تأكد من تحديد "قبول أي مصادقة بما في ذلك النص الواضح". قبل الطلب، أدخل إحدى مجموعات اسم المستخدم/كلمة المرور هذه في نافذة المحطة الطرفية:

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

username: cse
password: code+card
```

- اتصال PPP لشبكة الطلب الهاتفي وبروتوكول CHAP. (يفترض هذا أنه تم تنفيذ أوامر **مصادقة AAA الافتراضية ل PPP إذا لزم الأمر tacacs** و**ppp authen chap** على الموجه).**ملاحظة:** على الكمبيوتر، في شبكة الطلب الهاتفي، يجب التحقق من "قبول أي مصادقة بما في ذلك نص واضح" أو "قبول المصادقة المشفرة فقط". قبل الطلب، أدخل اسم المستخدم وكلمة المرور هذين في نافذة المحطة الطرفية:

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

مجموعات كلمة مرور CSUnix TACACS+ التي لا تعمل

ينتج عن هذه التركيبات أخطاء تصحيح أخطاء CSUnix هذه:

- CHAP وبدون كلمة مرور "النصوص غير المشفرة" في حقل كلمة المرور. يدخل المستخدم + بدلا من كلمة مرور "النصوص غير المشفرة". يتطلب RFC 1994 في بروتوكول CHAP تخزين كلمة مرور النص بوضوح.

```
username: cse
password: code+card

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

- كلمة مرور CHAP وكلمة مرور CHAP غير صحيحة.

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

(يمرر المستخدم إلى SDI، ويمرر SDI المستخدم، لكن CSUnix يفشل المستخدم لأن كلمة مرور CHAP سيئة.)

```
: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 وكلمة مرور PAP غير صحيحة.

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

(يمرر المستخدم إلى SDI، ويمرر SDI المستخدم، لكن CSUnix يفشل المستخدم لأن كلمة مرور CHAP سيئة.)

```
.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
```

ملفات تعريف نموذج CSUnix TACACS+ SDI للتصحيح

- يحتاج المستخدم إلى تنفيذ بروتوكول CHAP ومصادقة تسجيل الدخول، بينما يفشل بروتوكول PAP.

```
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
                   {
                   {
```

- يحتاج المستخدم إلى إجراء PAP ومصادقة تسجيل الدخول، ويفشل CHAP.

```
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
                   {
                   {
                   {
```

RADIUS CSUnix

تحتوي هذه الأقسام على إجراءات CSUnix RADIUS.

مصادقة تسجيل الدخول باستخدام CSUnix و RADIUS

قم بإجراء هذه الخطوات لاختبار المصادقة:

1. قم بإجراء إختبار أولي دون SDI. إذا لم يعمل ملف تعريف المستخدم هذا بدون كلمة مرور SDI لمصادقة تسجيل الدخول، فلن يعمل مع كلمة مرور SDI:
```
ViewProfile -p 9900 -u cse/. #
      User Profile Information
                  }user = cse
               } radius=Cisco
               } =check_items
{ { { whatever" } reply_attributes= { 6=6"=2
```
2. بمجرد عمل ملف التعريف هذا، استبدل "أيا كان" ب "sdi" كما هو موضح في هذا المثال:
```
ViewProfile -p 9900 -u cse/. #
      User Profile Information
                  }user = cse
               } radius=Cisco
               } =check_items
{ { { sdi } reply_attributes= { 6=6=2
```

مصادقة PPP و PAP باستخدام CSUnix و RADIUS

قم بإجراء هذه الخطوات لاختبار المصادقة:

ملاحظة: مصادقة بروتوكول PPP CHAP باستخدام CSUnix و RADIUS غير مدعومة.

1. قم بإجراء إختبار أولي دون SDI. إذا لم يعمل ملف تعريف المستخدم هذا بدون كلمة مرور SDI لمصادقة PPP/PAP و"تخصيص الوضع غير المتزامن"، فلن يعمل مع كلمة مرور SDI:
```
ViewProfile -p 9900 -u cse/. #

                  } user = cse
"password = pap "pappass
               } radius=Cisco
            } = check_items
                        {
         } =reply_attributes
                       2=6
                       1=7
                         {
                         {
                         {
```
2. بمجرد عمل ملف التعريف المذكور أعلاه، أضف **كلمة المرور = sdi** إلى ملف التعريف وأضف السمة **1=200** كما هو موضح في هذا المثال (يعمل هذا على تعيين Cisco_Token_Immediate إلى نعم.):
```
ViewProfile -p 9900 -u cse/. #
                  } user = cse
"password = pap "pappass
              password = sdi
               } radius=Cisco
            } = check_items
                      1=200
                        {
         } =reply_attributes
                       2=6
                       1=7
                         {
                         {
                         {
```
3. في قسم **واجهة المستخدم الرسومية المتقدمة**، الخادم، **تأكد من تعيين تمكين التخزين المؤقت للرمز المميز**". يمكن تأكيد ذلك من واجهة سطر الأوامر (CLI) مع:
```
#.#.#.#.BASE/CLI/ViewProfile -p 9900 -u SERVER$
```

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

اتصال PPP الخاص بشبكة الطلب الهاتفي و PAP

يفترض أن **أوامر PPP authentication AAA الافتراضية إذا لزم الأمر tacacs** و**PPP authen PAP** قد تم تنفيذها على الموجه. أدخل اسم المستخدم وكلمة المرور هذه في نافذة المحطة الطرفية قبل أن تطلب.:

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

ملاحظة: في الكمبيوتر، في شبكة الطلب الهاتفي، تأكد من تحديد "قبول أي مصادقة بما في ذلك النص الواضح".

تلميحات تصحيح الأخطاء والتحقق

تحتوي هذه الأقسام على تلميحات لتصحيح الأخطاء وتلميحات التحقق من الصحة.

Cisco Secure RADIUS و PPP و PAP

هذا مثال على تصحيح أخطاء جيد:

```
(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 و CSUnix

يتم تخزين تصحيح الأخطاء في الملف المحدد في /etc/syslog.conf for local0.debug.

لا يمكن لأي مستخدم المصادقة - SDI أو أي طريقة أخرى:

بعد إضافة معرف آمن، تأكد من عدم حدوث أخطاء عند تعديل ملف CSU.cfg. قم بإصلاح ملف CSU.cfg أو قم بالرجوع إلى ملف Backup CSU.cfg.

هذا مثال على تصحيح أخطاء جيد:

```
: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
```

هذا مثال على تصحيح أخطاء غير صحيح:

يجد CSUnix ملف تعريف المستخدم ويرسله إلى خادم SDI، لكن خادم SDI يفشل في المستخدم لأن رمز المرور سيئ.

```
: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
```

هذا مثال يوضح أن خادم ACE معطل:

أدخل **./aceserver توقف** على خادم SDI. لم يحصل المستخدم على رسالة "إدخال رمز المرور".

```
: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
```

معلومات ذات صلة

- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم UNIX

- الإعلامات الميدانية ل Cisco Secure ACS ل UNIX
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).