إعداد وتصحيح CiscoSecure 2.x TACACS+

المحتويات

المقدمة

يهدف هذا المستند إلى مساعدة مستخدم Cisco Secure 2.x لأول مرة في إعداد تكوين Cisco Secure TACACS+ وتصحيح أخطائه. وهو ليس وصفا شاملا لقدرات Cisco الآمنة.

راجع وثائق Cisco Secure للحصول على مزيد من المعلومات الكاملة حول برنامج الخادم وإعداد المستخدم. راجع وثائق برنامج Cisco IOS للحصول على الإصدار المناسب للحصول على مزيد من المعلومات حول أوامر الموجه.

المتطلبات الأساسية

المتطلبات

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Secure ACS 2.x والإصدارات الأحدث
- برنامج Cisco IOS® الإصدار 11.3.3 والإصدارات الأحدث

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

إعداد Cisco Secure

أكمل الخطوات التالية:

1. تأكد من إستخدام التعليمات الواردة مع البرنامج لتثبيت رمز Cisco الآمن على خادم UNIX.
2. لتأكيد أن المنتج يتوقف ويبدأ، أدخل `etc/rc0.d/` وكجذر، قم بالتنفيذ `K80Cisco Secure/.` (لإيقاف التعليمات).أدخل `etc/rc2.d/` وكجذر، قم بالتنفيذ `S80.` من `Cisco Secure` (لبدء التعليمات).عند بدء التشغيل، يجب أن ترى رسائل مثل:
```
Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
DBServer, AAA Server
```
قم بتشغيل `$BASE/UTILS/PSG` للتأكد من تشغيل عملية واحدة على الأقل من العمليات الفردية، على سبيل المثال، SQLAnywhere أو محرك قاعدة بيانات آخر، أو عملية خادم قاعدة البيانات الآمن من Cisco، أو خادم ويب Netscape، أو Netscape Web Admin، أو خادم ويب Acme، أو عملية AAA الآمنة من Cisco، أو عملية إعادة التشغيل التلقائي.
3. للتأكد من أنك في الدلائل المناسبة، قم بإعداد المتغيرات والمسارات البيئية في بيئة الصدفة الخاصة بك. تستخدم C-Shell هنا.**BASE$** هو الدليل الذي يتم فيه تثبيت Cisco Secure، والذي يتم إختياره أثناء التثبيت. وهو يحتوي على أدلة مثل CSU، DBServer، DOCS، وهلم جرا.في هذا المثال، يتم افتراض التثبيت في opt/ciscoACS/، ولكن يمكن أن يختلف ذلك على النظام لديك:
```
setenv $BASE   /opt/CSCOacs
```
SQLany$ هو الدليل الذي يتم فيه تثبيت قاعدة بيانات Cisco Secure الافتراضية، والذي يتم إختياره أثناء التثبيت. إذا كانت قاعدة البيانات الافتراضية التي تأتي مع المنتج، SQLAnywhere، تم إستخدامها، فإنها تحتوي على أدلة مثل قاعدة البيانات، المستند، وهكذا دواليك.في هذا المثال، يتم افتراض التثبيت في opt/ciscoACS/SYBSsa50/، ولكن يمكن أن يختلف ذلك على النظام لديك.
```
setenv $SQLANY /opt/CSCOacs/SYBSsa50
```
إضافة مسارات في بيئة الهيكل إلى:
```
BASE/utils$
BASE/bin$
BASE/CSU$
BASE/ns-home/admserv$
BASE/Ns-home/bin/httpd$
SQLANY/bin$
```
4. قرص مضغوط إلى $base/config**CSU.cfg** هو ملف التحكم في خادم Cisco Secure. إجراء نسخة إحتياطية من هذا الملف.في هذا الملف، تعرض `LIST config_license_key` مفتاح الترخيص الذي إستلمته من خلال عملية الترخيص إذا قمت بشراء البرنامج؛ إذا كان هذا ترخيص تجريبي يحتوي على 4 منافذ، فيمكنك ترك هذا الخط.يمكن أن يحتوي قسم **NAS config_nas_config** على خادم وصول إلى الشبكة (NAS) أو موجه افتراضي، أو NAS الذي تقوم بإدخاله أثناء التثبيت. لأغراض تصحيح الأخطاء في هذا المثال، يمكنك السماح *لأي* وحدة تخزين متصلة بالشبكة (NAS) بالاتصال بخادم Cisco الآمن *دون* مفتاح. على سبيل المثال، يمكنك إزالة اسم NAS والمفتاح من الأسطر التي تحتوي على `/*  NAS  */` "*/* *NAS/Cisco Secure Secret*/. تقول *ستانزا* الوحيدة في تلك المنطقة:
```
} = NAS config_nas_config
                                        }
                                ,""     /* NAS name can go here */
                                ,""     /* NAS/Cisco Secure secret key */
                                ,""     /* message_catalogue_filename */
                                 ,1     /* username retries */
                                 ,2     /* password retries */
                                  1     /* trusted NAS for SENDPASS */
                                    {
                                     ;{

} = AUTHEN config_external_authen_symbols
```
عندما تقوم بذلك، تخبر Cisco Secure أنه مسموح به التحدث مع جميع وحدات التخزين المتصلة بالشبكة (NAS) بدون تبادل المفاتيح.

5. إذا كنت ترغب في الحصول على معلومات تصحيح الأخطاء، فانتقل إلى /var/log/csuslog، يلزمك الحصول على سطر في القسم العلوي من CSU.cfg، يخبر الخادم عن كمية تصحيح الأخطاء المطلوب القيام بها. 0x7FFFFF يضيف كل التصحيح الممكن. إضافة هذا السطر أو تعديله وفقا لذلك:

```
;NUMBER config_logging_configuration = 0x7FFFFFFF
```

يرسل هذا السطر الإضافي معلومات تصحيح الأخطاء إلى محلي0:

```
;NUMBER config_system_logging_level = 0x80
```

أيضا، أضف هذا الإدخال لتعديل ملف /etc/syslog.conf:

```
local0.debug /var/log/csuslog
```

ثم أعد تدوير النظام لإعادة قراءته:

```
`kill -HUP `cat /etc/syslog.pid
```

إعادة تدوير خادم Cisco Secure:

```
etc/rc0.d/K80Cisco Secure/
etc/rc2.d/S80Cisco Secure/
```

ولا يزال ينبغي أن تبدأ.

6. قد ترغب في إستخدام المستعرض لإضافة مستخدمين أو مجموعات وما إلى ذلك أو أداة CSimport المساعدة. يمكن نقل المستخدمين العينة في الملف الثابت في نهاية هذا المستند بسهولة إلى قاعدة البيانات باستخدام CSimport. سيعمل هؤلاء المستخدمون لأغراض الاختبار وقد تقوم بحذفهم بمجرد إدخال المستخدمين الخاصين بك. بمجرد الاستيراد، يمكنك رؤية المستخدمين المستوردين من خلال واجهة المستخدم الرسومية (GUI).إذا قررت إستخدام CSimport:

```
CD $BASE/utils
```

ضع توصيفات المستخدم والمجموعة في نهاية هذا المستند في ملف مثل أي مكان في النظام، ثم من دليل $BASE/UTILS، مع تشغيل الأجهزة، على سبيل المثال، /etc/rc2.d/S80Cisco Secure وكجذر للمستخدم، قم بتشغيل CSimport باستخدام خيار الاختبار (-t):

```
<CSimport -t -p <path_to_file> -s <name_of_file/.
```

إختبار بناء الجملة هذا للمستخدمين؛ يجب أن تتلقى رسائل مثل:

```
Secure config home directory is: /opt/CSCOacs/config/CSConfig.ini
                hostname = berry and port = 9900 and clientid = 100
? 'home/ddunlap/csecure/upgrade.log exists, do you want to write over 'yes' or 'no/
                                                                          yes
                                                        ...Sorting profiles
                                                !Done sorting 21 profiles
                                        ...Running the database import test
```

يجب *ألا* تتلقى رسائل مثل:

```
"Error at line 2: password = "adminusr
   Couldn't repair and continue parse
```

ما إذا كانت هناك أخطاء أم لا، فتحقق من الترقية.log للتأكد من سحب ملفات التعريف. بمجرد تصحيح الأخطاء، من دليل $BASE/UTILS، مع تشغيل الأجهزة المساعدة (/etc/rc2.d/S80Cisco Secure)، وكجذر مستخدم، قم بتشغيل CSimport باستخدام خيار التأكيد (-c) لنقل المستخدمين إلى قاعدة البيانات:

```
<CSimport -c -p <path_to_file> -s <name_of_file/.
```

مرة أخرى، يجب ألا تكون هناك أخطاء على الشاشة أو في Upgrade.log.

7. يتم سرد المستعرضات المدعومة في تلميح Cisco Secure Compatibility التقني. من مستعرض الكمبيوتر الشخصي الخاص بك، ارجع إلى مربع **http://#.#.#. #. #. #.#/cs** Cisco Secure/Solaris حيث **يكون #** هو عنوان IP الخاص بخادم Cisco Secure/Solaris.دخلت على الشاشة أن يظهر، للمستخدم **سوبر user** وكلمة، **تغيير**. لا تقم بتغيير كلمة المرور عند هذه النقطة. يجب أن ترى المستخدمين/المجموعات التي تمت إضافتها إذا كنت تستخدم CSimport في الخطوة السابقة أو يمكنك النقر فوق كتلة الاستعراض **إيقاف** التشغيل وإضافة مستخدمين ومجموعات يدويا من خلال واجهة المستخدم الرسومية (GUI).

إعداد المصادقة

ملاحظة: تم تطوير تكوين الموجه هذا على موجه يعمل ببرنامج Cisco IOS Software، الإصدار 11.3.3. يعرض برنامج Cisco IOS الإصدار T.12.0.5 والإصدارات الأحدث **بروتوكول المجموعة** بدلا من **tacacs**.

عند هذه النقطة، قم بتكوين الموجه.

1. قتل Cisco Secure أثناء تكوين الموجه.
```
.etc/rc0.d/K80Cisco Secure to stop the daemons/
```
2. على الموجه، ابدأ تكوين TACACS+. أدخل وضع التمكين واكتب `conf t` قبل مجموعة الأوامر. تضمن هذه الصياغة عدم إقفالك من الموجه *في البداية* مما يوفر ميزة Cisco Secure ليست قيد التشغيل. إدخال `ps -ef | GREP` للتحقق للتأكد من أن Cisco Secure لا يعمل، وقتل -9 العملية إذا كانت:

```
Turn on TACACS+ aaa new-model enable password whatever !--- These are lists of ---!
authentication methods, !--- that is, vtymethod and conmethod are !--- names of lists, and
the methods listed on the !--- same lines are the methods in the order to be !--- tried. As
used here, if authentication !--- fails due to Cisco Secure not being started, !--- the
enable password is accepted !--- because it is in each list. aaa authentication login
vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable !--- Point the
router to the server, that is, !--- #.#.#.# is the server IP address. tacacs-server host
#.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !---
during debugging. exec-timeout 0 0 login authentication conmethod line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0
0 login authentication vtymethod
```
3. قم بإجراء إختبار للتأكد من إستمرار إمكانية الوصول إلى الموجه باستخدام برنامج Telnet ومن خلال منفذ وحدة التحكم قبل المتابعة. لأن Cisco Secure لا يعمل، يجب قبول كلمة مرور enable.**تحذير:** الحفاظ على تنشيط جلسة عمل منفذ وحدة التحكم والبقاء في وضع التمكين؛ يجب ألا تنتهي مهلة هذه الجلسة. تبدأ في تقييد الوصول إلى الموجه عند هذه النقطة وتحتاج إلى أن تكون قادرا على إجراء تغييرات التكوين بدون قفل نفسك.أصدرت هذا أمر in order to رأيت نادل إلى مسحاج تخديد تفاعل في المسحاج تخديد:
```
terminal monitor
debug aaa authentication
```
4. كجذر، قم بتشغيل Cisco Secure على الخادم:
```
etc/rc2.d/S80Cisco Secure/
```
هذا يبدأ العملية، غير أن أنت تريد أن يمكن أكثر تصحيح مما يشكل في S80Cisco Secure، لذلك:
```
ps -ef | grep Cisco Secure
<kill -9 <pid_of CS_process
```

```
CD $BASE/CSU
Cisco Secure -cx -f $BASE/config/CSU.cfg to start the Cisco Secure process with debugging/.
```
مع خيار `-x`، تعمل Cisco بشكل آمن في المقدمة حتى يمكن ملاحظة تفاعل الموجه مع الخادم. يجب ألا ترى رسائل الخطأ. يجب أن تبدأ عملية Cisco الآمنة وتعلق هناك بسبب الخيار -x.
5. من نافذة أخرى، تحقق للتأكد من بدء تشغيل Cisco Secure. أدخل `ps -ef` وابحث عن عملية Cisco الآمنة.
6. يجب على مستخدمي vty) Telnet) الآن المصادقة من خلال Cisco Secure. مع تصحيح الأخطاء على الموجه، يدخل Telnet إلى الموجه من جزء آخر من الشبكة. يجب أن ينتج الموجه مطالبة باسم المستخدم وكلمة المرور. يجب أن تكون قادرا على الوصول إلى الموجه باستخدام مجموعات معرف المستخدم/كلمة المرور هذه:
```
adminusr/adminusr
operator/oper
desusr/encrypt
```
راقب الخادم والموجه حيث يجب أن ترى التفاعل، أي، ما يتم إرساله حيث، الاستجابات، والطلبات، وما إلى ذلك. قم بتصحيح أي مشاكل قبل المتابعة.
7. إن يريد أنت أيضا لمستخدميك أن يصدق من خلال cisco يأمن أن يدخل إلى enable أسلوب، تأكدت أن وحدة طرفية للتحكم ميناء جلسة لا يزال نشط وأضفت هذا أمر إلى المسحاج تخديد:

```
For enable mode, list 'default' looks to Cisco Secure !--- then enable password if ---!
Cisco Secure is not running. aaa authentication enable default tacacs+ enable
```
8. أنت سوفت الآن أن **يمكن** من خلال cisco يأمن. مع تصحيح الأخطاء على الموجه، يدخل Telnet إلى الموجه من جزء آخر من الشبكة. عندما يطلب الموجه اسم المستخدم/كلمة المرور، يتم الاستجابة باستخدام `oper/`.عندما يحاول المستخدم المشغل إدخال وضع التمكين (مستوى الامتياز 15)، تكون كلمة المرور "cisco" مطلوبة. لن يتمكن المستخدمون الآخرون من إدخال وضع التمكين بدون بيان مستوى الامتياز (أو مؤشر Cisco

الآمن أسفل).راقب الخادم والموجه حيث يجب أن ترى التفاعل الآمن من Cisco، على سبيل المثال، ما يتم إرساله حيث، والاستجابات، والطلبات، وما إلى ذلك. قم بتصحيح أي مشاكل قبل المتابعة.

9. قم بإسقاط عملية Cisco Secure على الخادم أثناء الاتصال بمنفذ وحدة التحكم للتأكد من أن المستخدمين لديك لا يزالون يستطيعون الوصول إلى الموجه إذا كان Cisco Secure معطلا:

```
ps -ef' and look for Cisco Secure process'
kill -9 pid_of_Cisco Secure
```

كرر Telnet وتمكين الخطوة السابقة. يجب أن يدرك الموجه أن عملية Cisco الآمنة لا تستجيب وتسمح للمستخدمين بتسجيل الدخول والتمكين باستخدام كلمات مرور التمكين الافتراضية.

10. أحضرت ال cisco يأمن نادل مرة أخرى وأنشأت جلسة Telnet إلى المسحاج تخديد، أي ينبغي صادقت من خلال cisco يأمن، مع مستعمل/**عامل**/oper username/password in order to فحصت لمصادقة من وحدة طرفية للتحكم ميناء مستعمل من خلال cisco يأمن. ابق متصلا في الموجه وفي وضع التمكين حتى تتأكد من إمكانية تسجيل الدخول إلى الموجه من خلال منفذ وحدة التحكم، على سبيل المثال، تسجيل الخروج من إتصالك الأصلي بالموجه من خلال منفذ وحدة التحكم، ثم إعادة الاتصال بمنفذ وحدة التحكم. يجب أن تكون مصادقة منفذ وحدة التحكم لتسجيل الدخول باستخدام مجموعات معرف المستخدم/كلمة المرور السابقة الآن من خلال Cisco Secure. على سبيل المثال، **يجب إستخدام operator/oper** userid/password ثم كلمة المرور **cisco** من أجل **التمكين**.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

إضافة التخويل

تعد إضافة التخويل أمرا إختياريا.

بشكل افتراضي، هناك ثلاثة مستويات أوامر على الموجه:

- مستوى الامتياز 0- الذي يتضمن تعطيل، تمكين الخروج، التعليمات، وتسجيل الخروج
- مستوى الامتياز 1—المستوى العادي على برنامج Telnet ونافذة مطالبة يقول >
- امتياز مستوى 15—enable مستوى ومطالبة يقول #

بما أن الأوامر المتاحة تعتمد على مجموعة ميزات Cisco IOS، إصدار برنامج Cisco IOS، طراز الموجه، وما إلى ذلك، فلا توجد قائمة شاملة لجميع الأوامر على المستويين 1 و 15. على سبيل المثال، **لا يكون show ipx route** موجودا في مجموعة ميزات IP فقط، و**show ip nat trans** ليس في برنامج Cisco IOS الإصدار x code.10.2 لأن NAT لم يتم تقديمه في ذلك الوقت، و**show environment** غير موجودة في نماذج الموجهات دون مصدر الطاقة ومراقبة درجة الحرارة.

يمكن العثور على الأوامر المتوفرة في موجه معين على مستوى معين ؟ في موجه الأمر في الموجه عندما تكون على مستوى الامتياز هذا.

لم تتم إضافة تفويض منفذ وحدة التحكم كميزة حتى CSCdi82030. يكون تفويض منفذ وحدة التحكم قيد الإيقاف بشكل افتراضي لتقليل أحتمالية قفله من الموجه دون قصد. إذا كان للمستخدم وصول فعلي إلى الموجه من خلال وحدة التحكم، فإن تفويض منفذ وحدة التحكم ليس فعالا للغاية. ولكن، يمكن تشغيل تفويض منفذ وحدة التحكم تحت الأمر **line con 0** في صورة Cisco IOS حيث تم تنفيذ CSCdi82030 باستخدام الأمر **authorization exec default|word**.

أكمل الخطوات التالية:

1. يمكن تكوين الموجه لتخويل الأوامر من خلال Cisco Secure على جميع المستويات أو بعض المستويات. يتيح تكوين الموجه هذا لجميع المستخدمين إعداد التفويض لكل أمر على الخادم. يمكنك تخويل جميع الأوامر من خلال Cisco Secure ولكن إذا كان الخادم معطلا، فلن يكون هناك أي تفويض ضروري، وبالتالي فإن الأمر none.مع انخفاض خادم Cisco الآمن، أدخل الأوامر التالية:دخلت هذا أمر in order to أزلت المتطلب أن يمكن صحة هوية يكون من خلال cisco يؤمن:
```
no aaa authentication enable default tacacs+ none
```
دخلت هذا أمر in order to تطلبت أن يتم أمر تفويض من خلال cisco يأمن:
```
aaa authorization commands 0 default tacacs+ none
aaa authorization commands 1 default tacacs+ none
aaa authorization commands 15 default tacacs+ none
```
2. بينما يتم تشغيل خادم Cisco الآمن، يدخل Telnet إلى الموجه بمعرف المستخدم/كلمة المرور **loneusr/lonepwd**. يجب ألا يكون هذا المستخدم قادرا على تنفيذ أي أوامر أخرى غير:
```
show version
<ping <anything
logout
```
يجب أن يظل المستخدمون السابقون، **desusr/encrypt**، **operator/oper**، **admin/admin**، قادرين على تنفيذ جميع الأوامر بموجب = . إذا كانت هناك مشاكل في العملية، فأدخل وضع التمكين على الموجه وشغل تصحيح التخويل باستخدام هذا الأمر:
```
terminal monitor
debug aaa authorization
```
راقب الخادم والموجه حيث يجب أن ترى التفاعل الآمن من Cisco، على سبيل المثال، ما يتم إرساله حيث، والاستجابات، والطلبات، وما إلى ذلك. قم بتصحيح أي مشاكل قبل المتابعة.
3. يمكن تكوين الموجه لتخويل جلسات عمل EXEC من خلال Cisco Secure. يقوم الأمر AAA authorization exec default tacacs+ none بتعهد تفويض TACACS+ لجلسات عمل EXEC.إذا قمت بتطبيق هذا، فإنه يؤثر على وقت/وقت المستخدمين و**telnet/telnet** و**todam/todam** و**todpm/todpm** و**somerouters/somerouters**. بعد إضافة هذا الأمر إلى الموجه و Telnet إلى الموجه كوقت/**وقت** المستخدم، تظل جلسة EXEC مفتوحة لمدة دقيقة واحدة (تعيين المهلة = 1). يدخل المستخدم **telnet/telnet** الموجه ولكن يتم إرساله على الفور إلى العنوان الآخر (set autoCMD = "telnet 171.68.118.102"). من المحتمل أن يكون المستخدمون **Todam/Todam** و**TODPM/TODPM** قادرين أو غير قادرين على الوصول إلى الموجه، والذي يعتمد على الوقت من اليوم أثناء الاختبار. لا يمكن لمستخدم **Outlook** إلا إستخدام Telnet في الموجه koala.rtp.cisco.com من الشبكة x.10.31.1. يحاول Cisco Secure حل اسم الموجه. إذا كنت تستخدم عنوان IP 10.31.1.5، فإنه يكون صالحا إذا لم يتم الحل، وإذا كنت تستخدم الاسم كوالا، فإنه يكون صالحا إذا كان الحل قد تم.

إضافة محاسبة

إضافة المحاسبة أمر إختياري.

1. لا تتم المحاسبة ما لم يتم تكوينها في الموجه، إذا كان الموجه يشغل إصدار برنامج Cisco IOS Software لاحقا من برنامج Cisco IOS الإصدار 11.0. أنت يستطيع مكنت حساب على المسحاج تخديد:
```
+aaa accounting exec default start-stop tacacs
+aaa accounting connection default start-stop tacacs
+aaa accounting network default start-stop tacacs
+aaa accounting system default start-stop tacacs
```
ملاحظة: تم تعطيل محاسبة Command، في CSCdi44140 لمعرف تصحيح الأخطاء من Cisco، ولكن إذا كنت تستخدم صورة يكون هذا فيها ثابتا، يمكن أيضا تمكين حساب الأوامر.
2. إضافة تصحيح سجل المحاسبة على الموجه:
```
terminal monitor
debug aaa accounting
```
3. يجب أن يعرض تصحيح الأخطاء على وحدة التحكم سجلات المحاسبة التي تدخل الخادم أثناء تسجيل دخول المستخدمين.

4. لاسترداد سجلات المحاسبة، كجذر:

```
CD $BASE/utils/bin
AcctExport <filename> no_truncate/.
```

`no_truncate` يعني أن البيانات محتفظ بها في قاعدة البيانات.

إضافة مستخدمي الطلب الهاتفي

أكمل الخطوات التالية:

1. تأكد من أن الوظائف الأخرى لعمل Cisco الآمن قبل إضافة مستخدمي الطلب الهاتفي. إذا لم يعمل خادم Cisco Secure والمودم قبل هذه النقطة، فإنهما لا يعملان بعد هذه النقطة.
2. إضافة هذا الأمر إلى تكوين الموجه:

```
+aaa authentication ppp default if-needed tacacs
 aaa authentication login default tacacs+ enable
     +aaa authorization network default tacacs
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
```

تختلف تكوينات الواجهة، والتي تعتمد على كيفية إجراء المصادقة، ولكن يتم إستخدام خطوط الطلب الهاتفي في هذا المثال، مع التكوينات التالية:

```
                                                interface Ethernet 0
                                              ip address 10.6.1.200 255.255.255.0
CHAP/PPP authentication user: interface Async1 ip unnumbered Ethernet0 encapsulation ---! !
                ppp async mode dedicated peer default ip address pool async no cdp enable ppp
     authentication chap ! !--- PAP/PPP authentication user: interface Async2 ip unnumbered
 Ethernet0 encapsulation ppp async mode dedicated peer default ip address pool async no cdp
       enable ppp authentication pap ! !--- login authentication user with autocommand PPP:
     interface Async3 ip unnumbered Ethernet0 encapsulation ppp async mode interactive peer
  default ip address pool async no cdp enable ip local pool async 10.6.100.101 10.6.100.103
line 1 session-timeout 20 exec-timeout 120 0 autoselect during-login script startup default
    script reset default modem Dialin transport input all stopbits 1 rxspeed 115200 txspeed
      115200 flowcontrol hardware ! line 2 session-timeout 20 exec-timeout 120 0 autoselect
  during-login script startup default script reset default modem Dialin transport input all
  stopbits 1 rxspeed 115200 txspeed 115200 flowcontrol hardware ! line 3 session-timeout 20
    exec-timeout 120 0 autoselect during-login autoselect ppp script startup default script
   reset default modem Dialin autocommand ppp transport input all stopbits 1 rxspeed 115200
                txspeed 115200 flowcontrol hardware ! access-list 101 deny icmp any any
```

3. من مستعمل مبرد من ال cisco يأمن:chapUser-CHAP/PPP-user dials في السطر 1؛ تم تعيين العنوان بواسطة **مجموعة عناوين IP الافتراضية للنظير async وتجمع IP المحلي async 10.6.100.101 10.6.100.103** على الموجهعنوان 10. 29. 1.99 معين بواسطة الخادمCHAP/PPP—chpacl-رسائل المستخدم في السطر 1؛ تم تعيين العنوان 10.29.1.100 بواسطة الخادم وتم تطبيق قائمة الوصول الواردة 101 (والتي يجب تعريفها على الموجه)PAP/PPP—Papuser— رسائل المستخدم في السطر 2؛ تم تعيين العنوان بواسطة **تجمع عناوين IP الافتراضي للنظير غير متزامن وتجمع IP المحلي غير متزامن 10.6.100.101 10.6.100.103** على الموجهالورق—PAP/PPP—رسائل المستخدم في السطر 2، العنوان 10.29.1.98 يتم تعيينه بواسطة الخادمPAP/PPP—PAPACL—رسائل المستخدم في السطر 2؛ تم تعيين العنوان 10.29.1.100 بواسطة الخادم وتم تطبيق قائمة الوصول الواردة 101، والتي يجب تعريفها على الموجهالدخول تلقائيا—المستخدم في السطر 3؛ مصادقة الدخول باستخدام الأمر التلقائي على الخط تجبر المستخدم على الاتصال ب PPP وتعين العنوان من المجموعة
4. إعداد Microsoft Windows لكافة المستخدمين باستثناء تسجيل دخول المستخدم تلقائياأختر **ابدأ > البرامج > الملحقات > شبكات الطلب الهاتفي**.أختر **إتصالات > إجراء توصيل جديد**. اكتب اسما للاتصال الخاص بك.أدخل المعلومات الخاصة للمودم. في **تكوين > عام**، أختر أعلى سرعة للمودم الخاص بك، ولكن لا تقم بتحديد المربع أدناه.في **تكوين > اتصال**، أستخدم 8 وحدات بت بيانات، بدون تماثل، و 1 وحدة بت إيقاف. تفضيلات الاتصال هي **انتظار نغمة الطلب قبل الطلب وإلغاء المكالمة إذا لم تكن متصلة بعد 200 ثانية**.في الخيارات المتقدمة، أختر فقط **التحكم في تدفق الأجهزة** و**نوع التعديل القياسي**.في **تكوين > خيارات**، لا يجب التحقق من أي شيء إلا تحت التحكم في الحالة. وانقر فوق **OK**.في الإطار التالي، أدخل رقم هاتف الوجهة، ثم انقر **بعد ذلك**، ثم

انقر **إنهاء**.بمجرد ظهور رمز الاتصال الجديد، انقر بزر الماوس الأيمن عليه واختر **خصائص**، ثم انقر على **نوع الخادم**.أختر **PPP:Windows 95، Windows NT 3.5، إنترنت** ولا تحقق من أي خيارات متقدمة.في بروتوكولات الشبكة المسموح بها، تحقق على الأقل من **TCP/IP**.تحت إعدادات TCP/IP، أختر **عنوان IP المعين للخادم**، **وعناوين خادم الأسماء المعينة للخادم**، و**أستخدم البوابة الافتراضية على الشبكة البعيدة**. وانقر فوق **OK**.عندما تنقر نقرا مزدوجا على الرمز لإظهار نافذة "الاتصال ب" للطلب، يجب عليك تعبئة حقلي اسم المستخدم وكلمة المرور، ثم انقر على **الاتصال**.

5. إعداد Microsoft Windows 95 لتسجيل دخول المستخدم تلقائياتكوين تسجيل دخول المستخدم، مستخدم المصادقة باستخدام الأمر التلقائي PPP، هو نفسه كما هو الحال بالنسبة للمستخدمين الآخرين باستثناء الموجود في نافذة **تكوين > خيارات**. تحقق من **إحضار نافذة المحطة الطرفية بعد الطلب**.عندما تقوم بالنقر المزدوج على الأيقونة لعرض نافذة "الاتصال ب" للطلب، فإنك لا تملأ حقلي اسم المستخدم وكلمة المرور. انقر على **توصيل** وبعد إجراء الاتصال بالموجه، اكتب اسم المستخدم وكلمة المرور في الإطار الأسود الذي يظهر.بعد المصادقة، انقر على **متابعة(F7)**.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

الخادم

```
Cisco Secure -cx -f $BASE/CSU$BASE/config/CSU.cfg/.
```

الموجّه

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**. للحصول على مزيد من المعلومات حول أوامر معينة، يرجى مراجعة مرجع أوامر تصحيح أخطاء Cisco IOS.

- **terminal monitor** —عرض الأمر **debug** ورسائل خطأ النظام للمحطة الطرفية والجلسة الحالية.
- **debug ppp negotiation**—عرض حزم PPP المرسلة أثناء بدء تشغيل PPP، حيث يتم التفاوض حول خيارات PPP.
- **debug ppp packet**—عرض حزم PPP التي يتم إرسالها واستقبالها. يعرض هذا الأمر مكبات حزم منخفضة المستوى.
- **debug ppp chap**—عرض معلومات عن حركة مرور البيانات وتبادلها في شبكة داخلية تنفذ بروتوكول مصادقة التحدي (CHAP).
- **debug aaa authentication** — راجع ما هي طرق المصادقة الجاري إستخدامها وما هي نتائج هذه الطرق.
- **debug aaa authorization**—راجع أساليب التفويض المستخدمة ونتائج هذه الطرق.

ملف تأمين المستخدمين من Cisco

```
                                                } group = admin
                                "password = clear "adminpwd
```

```
                                } service = shell
                      default cmd = permit
                default attribute = permit
                                                {
                                                        {

                                             } group = oper
                           "password = clear "oper
                      privilege = clear "cisco" 15
                                } service = shell
                      default cmd = permit
                default attribute = permit
                                                {
                                                        {

                                          } user = adminusr
                       "password = clear "adminusr
                          default service = permit
                                                {

                                           } user = desusr
                    "password = des "QjnXYd1kd7ePk
                          default service = permit
                                                {

                                          } user = operator
                                  member = oper
                          default service = permit
                                                {

                                           } user = time
                          default service = permit
                           "password = clear "time
                                }  service = shell
                           set timeout = 1
                      default cmd = permit
                default attribute = permit
                                                {
                                                        {

                                          } user = todam
                          "password = clear "todam
                                }  service = shell
                      default cmd = permit
                default attribute = permit
                    time = Any 0600 - 1200
                                                {
                                                {

                                          } user = todpm
                          "password = clear "todpm
                                }  service = shell
                      default cmd = permit
                default attribute = permit
                    time = Any 1200 - 2359
                                                {
                                                {

                                         } user = telnet
                             "password = clear "telnet
                                }  service = shell
           "set autocmd = "telnet 171.68.118.102
                                        {
                                                {
```

```
                                } user = limit_lifetime
                        password = clear "cisco" from
                                  may 2001" until 2"
                                        "may 2001 4"
                                                   {

                                         } user = loneusr
                           "password = clear "lonepwd
                                  }  service = shell
                                } cmd = show
                                "permit "ver
                                           {
                                } cmd = ping
                                  "." permit
                                           {
                                } cmd = logout
                                  "." permit
                                           {
                                                   {
                                                           {

                                         } user = chapuser
                             default service = permit
                           "password = chap "chapuser
                                     } service = ppp
                             } protocol = lcp
                                    {
                              } protocol = ip
                                           {
                                                   {
                                                           {

                                         } user = chapaddr
                           "password = chap "chapaddr
                                     } service = ppp
                             } protocol = lcp
                                    {
                              } protocol = ip
                       set addr = 10.29.1.99
                                           {
                                                   {
                                                           {

                                          } user = chapacl
                             default service = permit
                            "password = chap "chapacl
                                     } service = ppp
                             } protocol = lcp
                                    {
                              } protocol = ip
                             set inacl = 101
                       set addr = 10.29.1.100
                                           {
                                                   {
                                                           {

                                         } user = papuser
                             default service = permit
                             "password = pap "papuser
                                     } service = ppp
                             } protocol = lcp
                                    {
                              } protocol = ip
```

```
                                        {
                                                {
                                                        {

                                         } user = papaddr
                                default service = permit
                                "password = pap "papaddr
                                        } service = ppp
                                } protocol = lcp
                                        {
                                 } protocol = ip
                        set addr = 10.29.1.98
                                        {
                                                {
                                                        {

                                          } user = papacl
                                default service = permit
                                "password = chap "papacl
                                        } service = ppp
                                } protocol = lcp
                                        {
                                 } protocol = ip
                               set inacl = 101
                          set addr = 10.29.1.100
                                        {
                                                {
                                                        {

                                       } user = loginauto
                                   default service = permit
                                "password = clear "loginauto
                                        } service = ppp
                                   } protocol = lcp
                                        {
                                    } protocol = ip
                                        {
                                                        {
                                                               {

                                     } user = somerouters
                                "password = clear "somerouters
                               "*.\allow koala ".*" "10\.31\.1
                        "*.\allow koala.rtp.cisco.com ".*" "10\.31\.1
                                "*.\allow 10.31.1.5 ".*" "10\.31\.1
                                        "*." "*." "*." refuse
                                        } service=shell
                                    default cmd=permit
                                default attribute=permit
                                                        {
                                                        {
```

معلومات ذات صلة

- مصدر المحتوى الإضافي الآمن من Cisco لدعم منتجات UNIX
- الإعلامات الميدانية لمنتجات الأمان (بما في ذلك Cisco Secure UNIX)

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).