الإدارة القائمة على معيار VRF على أمثلة تكوين ASR

المحتويات

المقدمة

يصف هذا المستند إستخدام الإدارة الظاهرية القائمة على التوجيه وإعادة التوجيه (VRF-Aware) على السلسلة 1000 من موجه خدمات التجميع من Cisco (ASR1K) باستخدام واجهة الإدارة (**GigabitEthernet0**). المعلومات تنطبق أيضا على أي واجهة أخرى في التردد اللاسلكي (VRF)، ما لم يتم تحديدها بشكل صريح خلاف ذلك. يتم وصف العديد من بروتوكولات الوصول لسيناريوهات الاتصال **من** المربع **ومن المربع على** حد سواء.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- بروتوكولات الإدارة، مثل SSH و telnet و HTTP
- بروتوكولات نقل الملفات، مثل بروتوكول النسخ الآمن (SCP) و TFTP و FTP
- VRFs

المكونات المستخدمة

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

- Cisco IOS® XE الإصدار 15.2(1)S (3.5S) أو إصدارات Cisco IOS-XE الأحدث
ملاحظة: يتطلب بروتوكول SCP المتوافق مع معيار VRF هذا الإصدار على الأقل، في حين تعمل البروتوكولات الأخرى الموضحة في هذا المستند مع الإصدارات السابقة أيضا.
- ASR1K

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إن يكون شبكتك حي، تأكدت أنت تفهم الأثر المحتمل من أي أمر يستعمل.

معلومات أساسية

واجهة الإدارة: الغرض من واجهة الإدارة هو السماح للمستخدمين بتنفيذ مهام الإدارة على الموجه. إنها في الأساس واجهة لا يجب، وغالبا لا يمكن، إعادة توجيه حركة مرور مستوى البيانات. وإلا، يمكن إستخدامها للوصول عن بعد إلى الموجه، غالبا عبر برنامج Telnet و SSH (Secure Shell)، ولتنفيذ معظم مهام الإدارة على الموجه. تكون الواجهة مفيدة للغاية قبل أن يبدأ الموجه في التوجيه، أو في سيناريوهات أستكشاف الأخطاء وإصلاحها عندما تكون واجهات مهايئ المنفذ المشترك (SPA) غير نشطة. على ASR1K، الإدارة قارن في تقصير VRF يعين **Mgmt-intf**.

يتم إستخدام الأمر **ip *<protocol>*source-interface** في هذا المستند بشكل مكثف (حيث يمكن أن تكون الكلمة الأساسية *<protocol>*SSH و FTP و TFTP). يتم إستخدام هذا الأمر لتحديد عنوان IP الخاص بواجهة يتم إستخدامها كعنوان مصدر عندما يكون ASR هو جهاز العميل في اتصال (على سبيل المثال، يتم بدء الاتصال من ASR أو حركة مرور بيانات من المربع). وهذا يعني أيضا أنه إذا لم يكن ASR هو بادئ الاتصال، فإن أمر **ip *<protocol>*source-interface** غير قابل للتطبيق، ولا يستخدم ASR عنوان IP هذا لحركة مرور الرد؛ وبدلا من ذلك، فإنه يستخدم عنوان IP الخاص بالواجهة الأقرب إلى الوجهة. يسمح هذا الأمر لك بمصدر حركة مرور البيانات (للبروتوكولات المدعومة) من واجهة VRF-Aware.

بروتوكولات الإدارة

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

SCP

لاستخدام خدمة عميل SCP على ASR من واجهة تم تمكين VRF، أستخدم هذا التكوين.

التكوين

يتم إستخدام الأمر **ip ssh source-interface** لتوجيه واجهة الإدارة إلى **Mgmt-intf** VRF لكل من خدمات عميل SSH و SCP، نظرا لأن SCP يستخدم SSH. لا يوجد خيار آخر في الأمر **copy scp** لتحديد VRF. لذلك، يجب أن تستخدم أمر **ip ssh source-interface** هذا. وينطبق نفس المنطق على أي واجهة أخرى تدعم التردد اللاسلكي (VRF).

```
ASR(config)#ip ssh source-interface GigabitEthernet0
```

ملاحظة: على النظام الأساسي ASR1k، لا يعمل بروتوكول SCP الخاص بواجهة VRF حتى الإصدار XE3.5S (15.2(1)S).

التحقق من الصحة

استعملت هذا أمر in order to دققت التشكيل.

```
ASR#show vrf
Name Default RD Protocols Interfaces
   Mgmt-intf <not set> ipv4,ipv6 Gi0
#ASR
```

دخلت in order to نسخت مبرد من ASR إلى أداة بعيد مع SCP، هذا أمر:

```
ASR#copy running-config scp://guest@10.76.76.160/router.cfg
?[Address or name of remote host [10.76.76.160
?[Destination username [guest
?[Destination filename [router.cfg
:Writing router.cfg Password
!
Sink: C0644 2574 router.cfg
(bytes copied in 20.852 secs (123 bytes/sec 2574
#ASR
```

دخلت in order to نسخت مبرد من أداة بعيد إلى ASR مع SCP، هذا أمر:

```
:ASR#copy scp://guest@10.76.76.160/router.cfg bootflash
?[Destination filename [router.cfg
:Password
Sending file modes: C0644 2574 router.cfg
!
(bytes copied in 17.975 secs (143 bytes/sec 2574
```

TFTP

لاستخدام خدمة عميل TFTP على ASR1k من واجهة تم تمكين VRF بها، أستخدم هذا التكوين.

التكوين

يتم إستخدام خيار **ip tftp source-interface** من أجل توجيه واجهة الإدارة إلى **Mgmt-intf** VRF. لا يوجد خيار آخر في الأمر **copy tftp** لتحديد VRF. لذلك، يجب أن تستخدم أمر **ip tftp source-interface** هذا. وينطبق نفس المنطق على أي واجهة أخرى تدعم التردد اللاسلكي (VRF).

```
ASR(config)#ip tftp source-interface GigabitEthernet0
```

التحقق من الصحة

استعملت هذا أمر in order to دققت التشكيل.

```
ASR#show vrf
  Name Default RD Protocols Interfaces
     Mgmt-intf <not set> ipv4,ipv6 Gi0
#ASR
```

لنسخ ملف من ASR إلى خادم TFTP، أدخل هذا الأمر:

```
ASR#copy running-config tftp
?[Address or name of remote host [10.76.76.160
?[Destination filename [ASRconfig.cfg
!!
(bytes copied in 0.335 secs (7934 bytes/sec 2658
#ASR
```

دخلت in order to نسخت مبرد من ال TFTP نادل إلى ASR bootflash، هذا أمر:

```
:ASR#copy tftp://10.76.76.160/ASRconfig.cfg bootflash
?[Destination filename [ASRconfig.cfg
...Accessing tftp://10.76.76.160/ASRconfig.cfg
! :(Loading ASRconfig.cfg from 10.76.76.160 (via GigabitEthernet0
[OK - 2658 bytes]

(bytes copied in 0.064 secs (41531 bytes/sec 2658
#ASR
```

FTP

لاستخدام خدمة عميل FTP على ASR من واجهة تم تمكين VRF، أستخدم هذا التكوين.

التكوين

يتم إستخدام خيار **ip ftp source-interface** من أجل توجيه واجهة الإدارة إلى **Mgmt-intf** VRF. لا يوجد خيار آخر في الأمر **copy ftp** لتحديد VRF. لذلك، يجب أن تستخدم أمر **ip ftp source-interface**. وينطبق نفس المنطق على أي واجهة أخرى تدعم التردد اللاسلكي (VRF).

```
ASR(config)#ip ftp source-interface GigabitEthernet0
```

التحقق من الصحة

استعملت هذا أمر in order to دققت التشكيل.

```
ASR#show vrf
Name Default RD Protocols Interfaces
Mgmt-intf <not set> ipv4,ipv6 Gi0
```

دخلت in order to نسخت مبرد من ASR إلى FTP نادل، هذا أمر:

```
ASR#copy running-config ftp://username:password@10.76.76.160/ASRconfig.cfg
?[Address or name of remote host [10.76.76.160
?[Destination filename [ASRconfig.cfg
! Writing ASRconfig.cfg
(bytes copied in 0.576 secs (4542 bytes/sec 2616
#ASR
```

دخلت in order to نسخت مبرد من ال FTP نادل إلى ASR bootflash، هذا أمر:

```
:ASR#copy ftp://username:password@10.76.76.160/ASRconfig.cfg bootflash
?[Destination filename [ASRconfig.cfg
...Accessing ftp://*****:*****@10.76.76.160/ASRconfig.cfg
! Loading ASRconfig.cfg
[OK - 2616/4096 bytes]

(bytes copied in 0.069 secs (37913 bytes/sec 2616
#ASR
```

بروتوكولات الوصول إلى الإدارة

وصول منتظم

بروتوكول النقل الآمن (SSH)

تحذير: هناك مشكلة مشتركة واحدة تتم رؤيتها مع ASR1ks هي أن بروتوكول SSH يفشل بسبب انخفاض الذاكرة. لمزيد من المعلومات حول هذه المشكلة، ارجع إلى فشل مصادقة SSH بسبب حالات انخفاض الذاكرة مقال Cisco.

هناك خياران يستخدمان لتشغيل خدمة عميل SSH على SSH) ASR من المربع). واحد خيار أن يعين ال VRF إسم في ال **ssh** أمر نفسه، لذلك أنت يستطيع أصدرت SSH حركة مرور من VRF خاص.

```
ASR#ssh -vrf Mgmt-intf -l cisco 10.76.76.161
:Password
Router>en
:Password
#Router
```

الخيار الآخر هو إستخدام خيار **ip ssh source-interface** من أجل مصدر حركة مرور SSH من واجهة معينة تم تمكين VRF بها.

```
ASR(config)#ip ssh source-interface GigabitEthernet0
#ASR
```

```
ASR#ssh -l cisco 10.76.76.161
:Password
Router>en
:Password
#Router
```

لاستخدام خدمة خادم SSH (SSH إلى المربع)، اتبع الإجراء لتمكين SSH على أي موجه CISCO IOS آخر. راجع نظرة عامة على Telnet و SSH لقسم موجهات سلسلة Cisco ASR 1000 من **دليل تكوين برنامج موجهات خدمات التجميع من السلسلة Cisco ASR 1000 Series** للحصول على مزيد من المعلومات.

Telnet

هناك خياران يستخدمان لتشغيل خدمة عميل Telnet على ASR (Telnet من المربع). واحد خيار أن يعين المصدر قارن أو ال VRF في **telnet** أمر نفسه كما هو موضح هنا:

```
ASR#telnet 10.76.76.160 /source-interface GigabitEthernet 0 /vrf Mgmt-intf
Trying 10.76.76.160 ... Open

User Access Verification

Username: cisco
:Password

Router>en
:Password
#Router
```

الآخر خيار أن يستعمل ال **ip telnet source-interface** أمر. أنت بعد ينبغي عينت ال VRF إسم في الخطوة التالية مع **ال telnet** أمر، كما هو موضح هنا:

```
ASR(config)#ip telnet source-interface GigabitEthernet0
#ASR
ASR#telnet 10.76.76.160 /vrf Mgmt-intf
Trying 50.50.50.3 ... Open

User Access Verification

Username: cisco
:Password

Router>en
:password
#Router
```

لاستخدام خدمة خادم Telnet (برنامج Telnet إلى المربع)، اتبع الإجراء لتمكين Telnet على أي موجه آخر. راجع نظرة عامة على Telnet و SSH لقسم موجهات سلسلة Cisco ASR 1000 من **دليل تكوين برنامج موجهات خدمات التجميع من السلسلة Cisco ASR 1000 Series** للحصول على مزيد من المعلومات.

HTTP

كما تتوفر واجهة مستخدم الويب القديمة التي تتوفر لجميع الموجهات ل ASR1K. قم بتمكين خادم HTTP أو خدمة العميل على ASR كما هو موضح في هذا القسم.

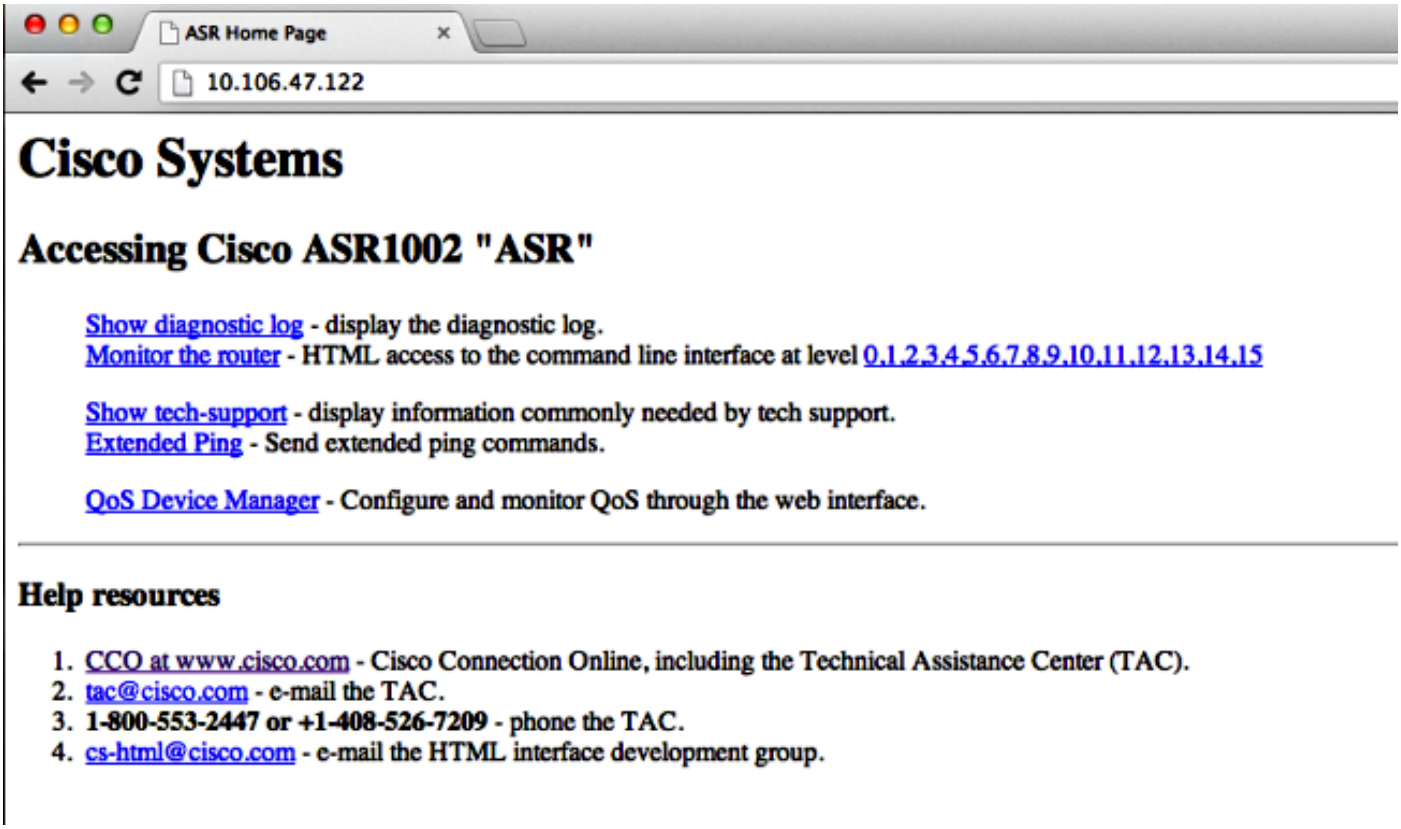
لتمكين وصول HTTP القديم إلى خدمة المربع (الخادم) واستخدام الوصول إلى واجهة المستخدم الرسومية (GUI) المستندة إلى الويب، أستخدم هذا التكوين الذي يستخدم المصادقة المحلية (يمكنك أيضا إستخدام خادم المصادقة والتفويض والمحاسبة (AAA) الخارجي).

```
ASR(config)#ip http
ASR(config)#ip http authentication local
<> ASR(config)#username <> password
```

فيما يلي التكوين لتمكين خادم HTTP الآمن (HTTPS):

```
ASR(config)#ip http secure-server
ASR(config)#ip http authentication local
<> ASR(config)#username <> password
```

تصفح إلى عنوان IP الخاص بواجهة على ASR، وسجل الدخول باستخدام حساب المستخدم الذي أنشأته. هنا لقطة شاشة:



دخلت in order to استعملت ال HTTP زبون خدمة، **ال ip http زبون interface name> source-interface <**أمر مصدر ل ال HTTP زبون حركة مرور من VRF يمكن قارن، كما هو موضح:

```
ASR(config)#ip http client source-interface GigabitEthernet0
```

هنا مثال يوضح إستخدام خدمة عميل HTTP لنسخ صورة من خادم HTTP بعيد إلى الذاكرة المؤقتة (flash):

```
#ASR
:ASR#copy http://username:password@10.76.76.160/image.bin flash
?[Destination filename [image.bin
...Accessing http://10.106.72.62/image.bin
Loading http://10.106.72.62/image.bin
(bytes copied in 20.038 secs (465819 bytes/sec 1778218
#ASR
```

وصول مستمر

لا ينطبق هذا القسم إلا على إتصالات Telnet/SSH/HTTP الخاصة بالمربع.

باستخدام بروتوكول SSH المستمر وبرنامج Telnet المستمر، يمكنك تكوين خريطة نقل تحدد معالجة حركة مرور SSH أو Telnet الواردة على واجهة إيثرنت الإدارة. وبالتالي، يؤدي هذا إلى إنشاء القدرة على الوصول إلى الموجه عبر وضع التشخيص حتى عندما تكون عملية Cisco IOS غير نشطة. لمزيد من المعلومات حول وضع التشخيص، ارجع إلى قسم فهم وضع التشخيص في دليل تكوين البرنامج Cisco ASR 1000 Series Aggregation Services Routers Software.

ملاحظة: يمكن تكوين SSH الدائم أو برنامج Telnet الثابت فقط على واجهة الإدارة، **GigabitEthernet0**.

ملاحظة: في الإصدارات التي لا تحتوي على الإصلاح لمعرف تصحيح الأخطاء من Cisco CSCuj37515، تعتمد طريقة المصادقة للوصول الدائم على الطريقة التي يتم إستخدامها تحت سطر **VTY**. يتطلب الوصول المستمر أن تكون المصادقة محلية، حتى يظل الوصول إلى وضع التشخيص يعمل عند فشل المصادقة الخارجية. هذا يعني أن أي وصول SSH و telnet عادي يتطلب أيضا إستخدام المصادقة المحلية.

تحذير: في الإصدارات التي لا تحتوي على الإصلاح لمعرف تصحيح الأخطاء من Cisco CSCug77654، يحد إستخدام طريقة AAA الافتراضية من قدرة المستخدم على إدخال موجه أمر SSH عند إستخدام بروتوكول SSH الدائم. يتم إجبار المستخدم دائما على إدخال المطالبة التشخيصية. بالنسبة لهذه الإصدارات، توصي Cisco باستخدام طريقة مصادقة الاسم، أو ضمان تمكين SSH و telnet العاديين.

SSH المستمر

قم بإنشاء خريطة نقل للسماح ببروتوكول SSH الدائم كما هو موضح في القسم التالي:

التكوين

```
ASR(config)#crypto key generate rsa label ssh-keys modulus 1024
The name for the keys will be: ssh-keys

The key modulus size is 1024 bits %
...Generating 1024 bit RSA keys, keys will be non-exportable %
(OK] (elapsed time was 1 seconds]

#ASR
ASR(config)#transport-map type persistent ssh
persistent-ssh-map
ASR(config-tmap)#rsa keypair-name ssh-keys
ASR(config-tmap)#transport interface GigabitEthernet0
ASR(config-tmap)#banner wait X
.'Enter TEXT message. End with the character 'X
--Waiting for vty line--
X
#(ASR(config-tmap
ASR(config-tmap)# banner diagnostic X
.'Enter TEXT message. End with the character 'X
--Welcome to Diagnostic Mode--
c
ASR(config-tmap)#connection wait allow interruptible
ASR(config-tmap)#exit
ASR(config)#transport type persistent ssh input persistent-ssh
:Jul 10 15:31:57.102: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd*
Server persistent ssh has been notified to start
```

يجب الآن تمكين المصادقة المحلية ل SSH الدائم. ويمكن القيام بذلك إما باستخدام أمر **AAA new-model** أو بدونه. وقد تم وصف كلا السيناريوهين هنا. (في أي من الحالتين، تأكد من أن لديك حساب اسم مستخدم/كلمة مرور محلي

على الموجه).

يمكنك إختيار التكوين الذي يستند إلى ما إذا تم تمكين AAA على ASR أم لا.

1. مع تمكين AAA:

```
ASR(config)#aaa new-model
ASR(config)#aaa authentication login default local
ASR(config)#line vty 0 4
ASR(config-line)#login authentication default
```

2. دون تمكين AAA:

```
ASR(config)#line vty 0 4
ASR(config-line)#login local
```

التحقق من الصحة

SSH إلى ASR باستخدام عنوان IP الخاص بواجهة **GigabitEthernet0** التي تم تمكين VRF بها. ما إن دخلت الكلمة يكون، أنت ينبغي دخلت الفصل تسلسل (**Ctrl-C** أو **Ctrl-shift-6**).

```
management-station$ ssh -l cisco 10.106.47.139
:cisco@10.106.47.139's password

--Waiting for vty line--

--Welcome to Diagnostic Mode--
#(ASR(diag
```

ملاحظة: أدخل تسلسل الفاصل (**Ctrl-C** أو **Ctrl-shift-6**) عندما يعرض **—في انتظار سطر vty-** على المحطة الطرفية لإدخال وضع التشخيص.

برنامج Telnet مستمر

التكوين

باستخدام منطق مماثل كما هو موضح في القسم السابق لبروتوكول طبقة الأمان (SSH)، قم بإنشاء خريطة نقل لبروتوكول Telnet الدائم كما هو موضح هنا:

```
ASR(config)#transport-map type persistent telnet persistent-telnet
ASR(config-tmap)#banner diagnostic X
.'Enter TEXT message. End with the character 'X
--Welcome to Diagnostic Mode--
X
ASR(config-tmap)#banner wait X
.'Enter TEXT message. End with the character 'X
--Waiting for IOS Process--
X
ASR(config-tmap)#connection wait allow interruptible
ASR(config-tmap)#transport interface gigabitEthernet 0
ASR(config-tmap)#exit
ASR(config)#transport type persistent telnet input persistent-telnet
:Jul 10 15:26:56.441: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd*
Server persistent telnet has been notified to start
```

وكما تمت مناقشة ذلك في القسم الأخير من بروتوكول SSH، هناك طريقتان لتكوين المصادقة المحلية كما هو موضح هنا:

1. مع تمكين AAA:

```
ASR(config)#aaa new-model
ASR(config)#aaa authentication login default local
ASR(config)#line vty 0 4
ASR(config-line)#login authentication default
```

2. دون المصادقة والتفويض والمحاسبة (AAA):

```
ASR(config)#line vty 0 4
ASR(config-line)#login local
```

التحقق من الصحة

Telnet إلى عنوان IP الخاص بواجهة **GigabitEthernet0**. بعد إدخال بيانات الاعتماد، أدخل تسلسل الفاصل ثم انتظر لبضع ثوان (قد يستغرق ذلك بعض الوقت في بعض الأحيان) قبل تسجيل الدخول إلى وضع التشخيص.

```
Management-station$ telnet 10.106.47.139
...Trying 10.106.47.139
.Connected to 10.106.47.139
.'[^' Escape character is
Username: cisco
:Password

--Waiting for IOS Process--


--Welcome to Diagnostic Mode--
#(ASR(diag
```

ملاحظة: أدخل تسلسل الفاصل **Ctrl+C** أو **Ctrl+العالي+6**، وانتظر لبضع ثوان. عندما **—في انتظار عملية IOS—** يتم العرض على المحطة الطرفية، يمكنك إدخال وضع التشخيص.

HTTP الدائم

لتمكين وصول HTTP المستمر إلى المربع (لا تتوفر خدمة HTTP من المربع أو خدمة عميل HTTP) واستخدام وصول GUI المستند إلى الويب الجديد، أستخدم هذا التكوين الذي يستخدم المصادقة المحلية (يمكنك أيضا إستخدام خادم AAA خارجي).

التكوين

في هذه التكوينات، يكون **http-webui** و**https-webui** أسماء خرائط النقل.

```
ASR(config)#ip http serverASR(config)#ip http authentication local
<> ASR(config)#username <> password
ASR(config)#transport-map type persistent webui http-webui
ASR(config-tmap)#server
ASR(config-tmap)#exit
ASR(config)#transport type persistent webui input http-webui
```

فيما يلي التكوين المستخدم لتمكين خادم HTTP الآمن (HTTPS).

```
ASR(config)#ip http secure-serverASR(config)#ip http authentication local
<> ASR(config)#username <> password
ASR(config)#transport-map type persistent webui https-webui
```

```
ASR(config-tmap)#secure-server
ASR(config-tmap)#exit
ASR(config)#transport type persistent webui input https-webui
```

التحقق من الصحة

إستعراض إلى عنوان IP الخاص بواجهة على ASR. قم بتسجيل الدخول باستخدام اسم المستخدم/كلمة المرور التي قمت بإنشائها لتشغيل الصفحة الرئيسية. يتم عرض المعلومات المتعلقة بالصحة والمراقبة، بالإضافة إلى **IOS WebUI** حيث يمكنك تطبيق الأوامر. وفيما يلي لقطة من الصفحة الرئيسية:

استكشاف الأخطاء وإصلاحها

إذا لم تكن WebUI متوفرة عبر HTTPS، فتحقق من وجود مفتاح الشهادة و RSA (Rivest-Shamir-Adleman) وتشغيلهما. يمكنك إستخدام الأمر **debug** هذا لتحديد سبب عدم بدء تشغيل WebUI بشكل صحيح:

```
ASR#debug platform software configuration notify webui
ASR#config t
ASR(config)#no transport type persistent webui input https-webui
UICFGEXP-6-SERVER_NOTIFIED_STOP: SIP0: psd: Server wui has been notified to stop%
ASR(config)#transport type persistent webui input https-webui

CNOTIFY-UI: Setting transport map
CNOTIFY-UI: Transport map https-webui input being processed
CNOTIFY-UI: Processing map association
CNOTIFY-UI: Attempting to send config
CNOTIFY-UI: Preparing to send config
CNOTIFY-UI: server cache: false, tm: false
CNOTIFY-UI: secure-server cache: true, tm: true
CNOTIFY-UI: Validating server config
CNOTIFY-UI: Validating secure server config
CNOTIFY-UI: Checking if secure server config is ok
CNOTIFY-UI: Secure server is enabled in map
CNOTIFY-UI: Getting trust point
CNOTIFY-UI: Getting self-signed trust point
CNOTIFY-UI: Could not get self-signed trustpoint
CNOTIFY-UI: A certificate for does not exist
CNOTIFY-UI: Getting rsa key-pair name
CNOTIFY-UI: Failed to get rsa key pair name
CNOTIFY-UI: Key needed to generate the pem file
CNOTIFY-UI: Secure-server config invalid
CNOTIFY-UI: Config analysis indicates no change
CNOTIFY-UI: Failed to prepare config
```

مفتاح RSA

دخلت in order to دققت الوجود من ال RSA مفتاح، هذا أمر:

```
ASR#show crypto key mypubkey rsa
Key pair was generated at: XX:XX:XX XXX XXX XX XXXX %
Key name: ASR.ASR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
.Key is not exportable. Redundancy enabled
;Key Data&colon
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXX
Key pair was generated at: XX:XX:XX XXX XXX XX XXXX %
Key name: ASR.ASR.server
Key type: RSA KEYS
```

```
Temporary key
Usage: Encryption Key
.Key is not exportable. Redundancy enabled
;Key Data&colon
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXX
#ASR
```

لاحظ اسم المفتاح، كما هو مطلوب لإنشاء الشهادة. إذا لم يكن أحد المفاتيح موجودا، فيمكنك إنشاء مفتاح باستخدام الأوامر التالية:

```
ASR(config)#ip domain-name Router
ASR(config)#crypto key generate rsa
The name for the keys will be: Router.Router
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
.a few minutes

How many bits in the modulus [512]: 2048
...Generating 2048 bit RSA keys, keys will be non-exportable %
(OK] (elapsed time was 1 seconds]

#(ASR(config
Dec 22 10:57:11.453: %SSH-5-ENABLED: SSH 1.99 has been enabled*
```

شهادة

ما إن يكون المفتاح حاضر، أنت يستطيع دخلت هذا أمر in order to دققت الشهادة:

```
ASR#show crypto pki certificates
ASR Self-Signed Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: General Purpose
:Issuer
serialNumber=XXXXXXXXXXX+ipaddress=XXX.XXX.XXX.XXX+hostname=ASR
cn=XXX.XXX.XXX.XXX
c=US
st=NC
l=Raleigh
:Subject
Name: Router
IP Address: XXX.XXX.XXX.XXX
Serial Number: XXXXXXXXXXX
serialNumber=XXXXXXXXXXX+ipaddress=XXX.XXX.XXX.XXX+hostname=aSR
cn=XXX.XXX.XXX.XXX
c=US
st=NC
l=Raleigh
:Validity Date
start date: XX:XX:XX XXX XXX XX XXXX
end date: XX:XX:XX XXX XXX XX XXXX
Associated Trustpoints: local
```

إذا كانت الشهادة غير صحيحة أو غير موجودة، يمكنك إنشاء الشهادة باستخدام الأوامر التالية:

```
ASR(config)#crypto pki trustpoint local
ASR(ca-trustpoint)#enrollment selfsigned
ASR(ca-trustpoint)#subject-name CN=XXX.XXX.XXX.XXX; C=US; ST=NC; L=Raleigh
ASR(ca-trustpoint)#rsakeypair ASR.ASR 2048
```

```
ASR(ca-trustpoint)#crypto pki enroll local
Include the router serial number in the subject name? [yes/no]: yes %
Include an IP address in the subject name? [no]: yes %
 Enter Interface name or IP Address[]: XXX.XXX.XXX.XXX
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

بمجرد تحديث مفتاح RSA والشهادة وصالتهما، يمكن إقران الشهادة بتكوين HTTPS:

```
ASR(config)#ip http secure-trustpoint local
```

يمكنك بعد ذلك تعطيل WebUI وإعادة تمكينه لضمان أنه يعمل:

```
ASR#conf t
.Enter configuration commands, one per line. End with CNTL/Z
ASR(config)#no transport type persistent webui input https-webui
#(ASR(config
CNOTIFY-UI: Setting transport map
CNOTIFY-UI: Transport map usage being disabled
CNOTIFY-UI: Processing map association
CNOTIFY-UI: Attempting to send config
CNOTIFY-UI: Preparing to send config
CNOTIFY-UI: Persistent webui will be shutdown if running
CNOTIFY-UI: Creating config message
CNOTIFY-UI: Secure-server state actually being set to: disabled
CNOTIFY-UI: Webui server information: changed: true, status: disabled, port: 80
CNOTIFY-UI: Webui secure server information: changed: true, status: disabled, port: 443
CNOTIFY-UI: Webui service (re)start: false. Sending all config
#(ASR(config
ASR(config)#transport type persistent webui input https-webui
#(ASR(config
CNOTIFY-UI: Setting transport map
CNOTIFY-UI: Transport map https-webui input being processed
CNOTIFY-UI: Processing map association
CNOTIFY-UI: Attempting to send config
CNOTIFY-UI: Preparing to send config
CNOTIFY-UI: server cache: false, tm: false
CNOTIFY-UI: secure-server cache: true, tm: true
CNOTIFY-UI: Validating server config
CNOTIFY-UI: Validating secure server config
CNOTIFY-UI: Checking if secure server config is ok
CNOTIFY-UI: Secure server is enabled in map
CNOTIFY-UI: Getting trust point
CNOTIFY-UI: Using issued certificate for identification
CNOTIFY-UI: Getting rsa key-pair name
CNOTIFY-UI: Getting private key
CNOTIFY-UI: Getting certificate
CNOTIFY-UI: Secure server config is ok
CNOTIFY-UI: Secure-server config is valid
CNOTIFY-UI: Creating config message
CNOTIFY-UI: Secure-server state actually being set to: enabled
CNOTIFY-UI: Adding rsa key pair
CNOTIFY-UI: Getting base64 encoded rsa key
CNOTIFY-UI: Getting rsa key-pair name
CNOTIFY-UI: Getting private key
CNOTIFY-UI: Added rsa key
CNOTIFY-UI: Adding certificate
CNOTIFY-UI: Getting base64 encoded certificate
CNOTIFY-UI: Getting certificate
CNOTIFY-UI: Getting certificate for local
CNOTIFY-UI: Certificate added
```

```
CNOTIFY-UI: Webui server information: changed: false, status: disabled, port: 80
CNOTIFY-UI: Webui secure server information: changed: true, status: enabled, port: 443
CNOTIFY-UI: Webui service (re)start: true. Sending all config
```

UICFGEXP-6-SERVER_NOTIFIED_START: SIP0: psd: Server wui has been notified to start%

معلومات ذات صلة

- معالجة منفذ وحدة التحكم وبرنامج Telnet و SSH
- فهم وضع التشخيص
- الدعم التقني والمستندات - 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).