تثبيت السحابة الخاصة الظاهرية لنقطة النهاية الآمنة وتكوينها

المحتويات

المقدمة

المتطلبات الأساسية

نشر VPC

تركيب الجهاز الظاهري

إعداد واجهة المستخدم الأولية

التهيئة الأولية للكمبيوتر vPC من خلال واجهة المستخدم الرسومية (GUI) عبر الويب

التكوين

الخدمات

حزمة تحديث AirGap

المشكلة رقم 1 - مساحة مستنفدة في مخزن البيانات

المشكلة رقم 2 - التحديث القديم

استكشاف الأخطاء وإصلاحها بشكل أساسي

المشكلة #1 - خادم FQDN و DNS

المشكلة رقم 2 - مشكلة مع المرجع المصدق الجذر

المقدمة

يصف هذا المستند كيفية نشر Virtual Private Cloud (VPC) على الخوادم في بيئة ESXi بنجاح ويركز على كيفية ذلك. بالنسبة للوثائق الأخرى مثل دليل البدء السريع واستراتيجية النشر ودليل الاستحقاق ووحدة التحكم ودليل المستخدم للمسؤول، يرجى زيارة وثائق هذا الموقع

تمت المساهمة بواسطة رومان فالنتا، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات:

برنامج VMware ESX 5 أو إصدار أحدث

- وضع وكيل الشبكة (فقط): ذاكرة وصول عشوائي سعة 128 جيجابايت و 8 مراكز لوحدة المعالجة المركزية (وحدات معالجة مركزية (CPU مع 4 مراكز موصى بها لكل منهما)، فضلاً عن مساحة قرص حرة تبلغ 1 تيرابايت كحد أدنى في مخزن بيانات VMware
- نوع محركات الأقراص: محركات أقراص مزودة بذاكرة مصنوعة من مكونات صلبة (SSD) مطلوبة لوضع الثغرات الهوائية وموصى بها للوكيل
- نوع RAID: مجموعة RAID 10 واحدة (مرآة مخططة)
- الحد الأدنى لحجم مخزن بيانات VMware: 2 تيرابايت
- الحد الأدنى للقراءات العشوائية لمخططات البيانات لمجموعة RAID 10 (4 كيلو): 60

كيلو عملية إدخال وإخراج في الثانية (IOPS)
- الحد الأدنى لكتابة Datastore Random لمجموعة RAID 10 (4K): 30 ألف عملية إدخال وإخراج في الثانية (IOPS)

cisco يوصي أن يتلقى أنت معرفة من هذا موضوع:

- معرفة أساسية بكيفية التعامل مع الشهادات.
- معرفة أساسية بكيفية إعداد DNS ضمن خادم DNS (Windows أو Linux)
- تثبيت قالب جهاز ظاهري مفتوح (OVA) في VMWare ESXi

مستخدم في هذا المختبر:

برنامج ESX 6.5 من VMware

- وضع وكيل الشبكة (فقط): ذاكرة وصول عشوائي سعة 48 جيجابايت و 8 مراكز لوحدة المعالجة المركزية (وحدات معالجة مركزية (CPU مع 4 مراكز موصى بها لكل منهما)، بالإضافة إلى مساحة حرة على القرص تبلغ 1 تيرابايت كحد أدنى في مركز بيانات VMware
- نوع محركات الأقراص: SATA
- نوع تقنية RAID: تقنية RAID 1 واحدة
- الحد الأدنى لحجم مجمع بيانات VMware: 1 تيرابايت
- MobaXterm 20.2 (برنامج متعدد المحطات مماثل لـ PuTTY)
- Cygwin64 (يستخدم لتنزيل تحديث AirGap)

بالإضافة إلى

- الشهادة التي قمت بإنشائها باستخدام OpenSSL أو XCA
- خادم DNS (Linux أو Windows) في مختبري أستخدمت نظام التشغيل Windows Server 2016 و CentOS-8
- Windows VM لنقطة نهاية الاختبار الخاصة بنا
- الترخيص

إذا كانت الذاكرة عبارة عن ذاكرة وصول عشوائي (RAM) سعة 48 جيجابايت منخفضة على الإصدار 3.2+ VPC تصبح غير قابلة للاستخدام.

ملاحظة: تقوم Private Cloud OVA بإنشاء أقسام محرك الأقراص لذلك لا حاجة لتعييننا في VMware. الخادم الذي يقوم بتحديد اسم مضيف الواجهة النظيفة. أفقن

ارجع إلى صفحة بيانات جهاز VPC للحصول على مزيد من المعلومات حول متطلبات الأجهزة الخاصة بالإصدار.

ملاحظة: تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر. أفقن

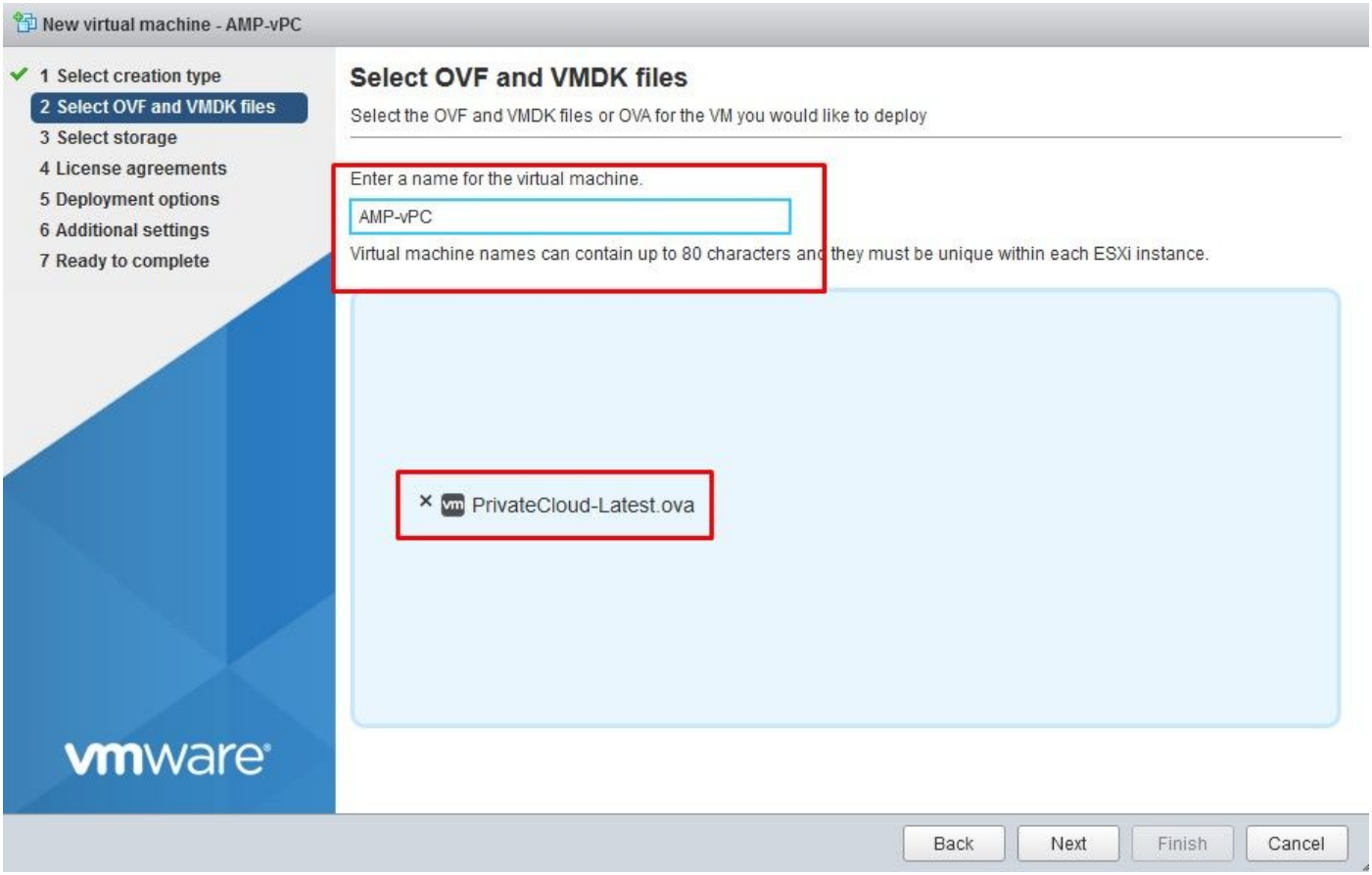
نشر VPC

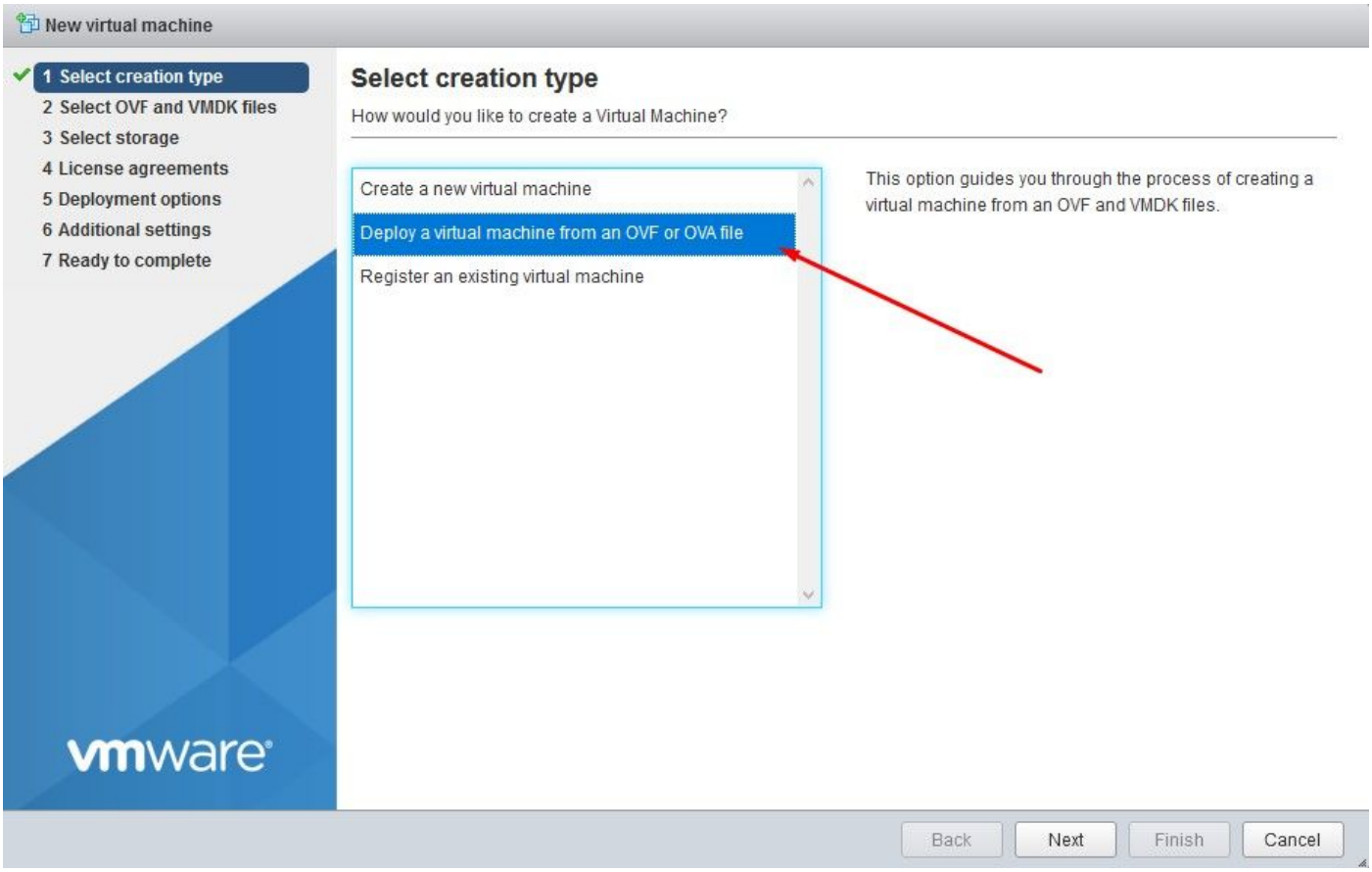
حدد عنوان URL المتوفر في البريد الإلكتروني للتسليم أو رسالة الاستحقاق. تنزيل ملف OVA ومتابعة التثبيت

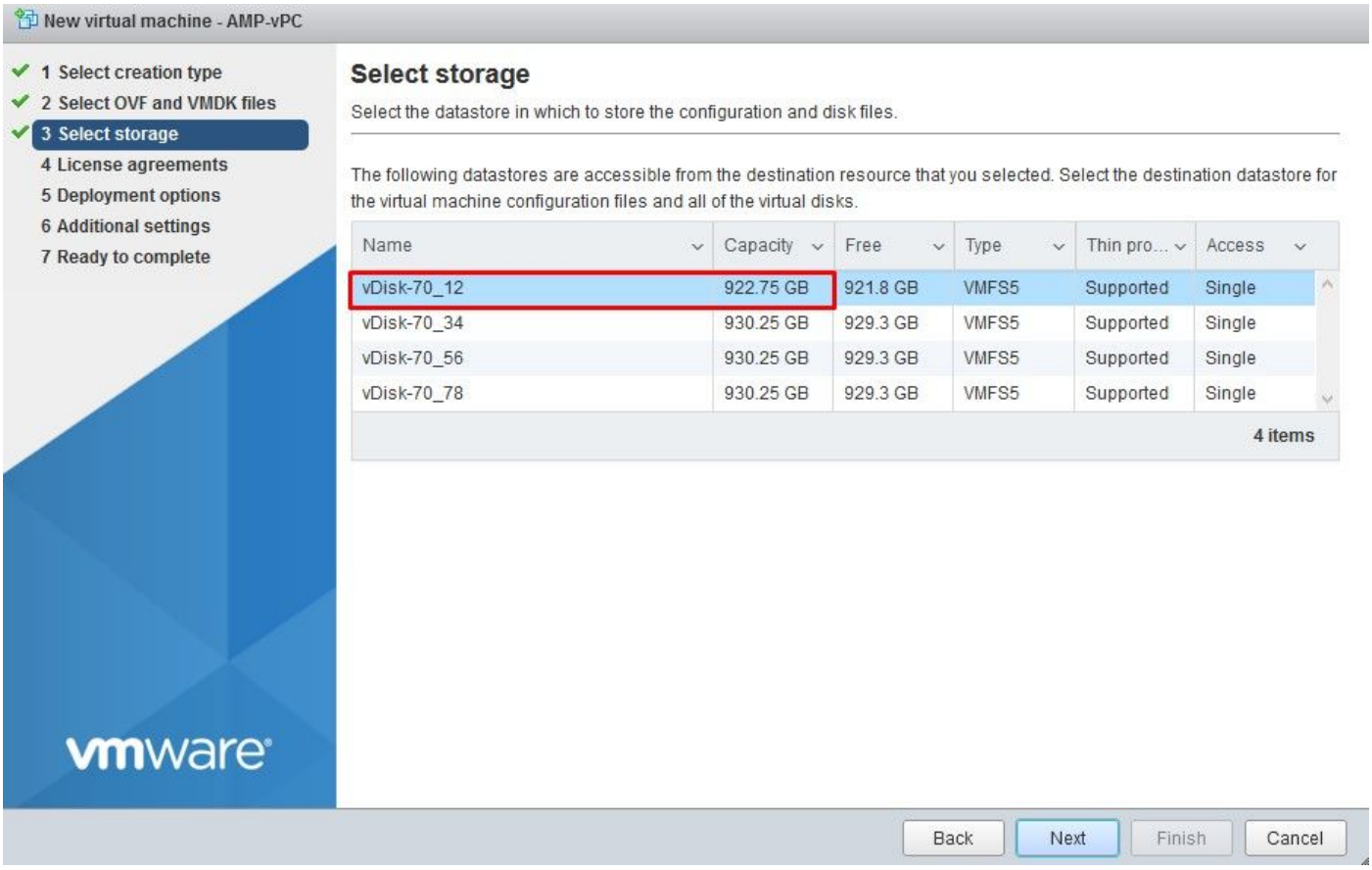
تركيب الجهاز الظاهري

الخطوة 1:

انتقل إلى ملف > نشر قالب OVF لفتح معالج نشر قالب OVF، كما هو موضح في الصورة.

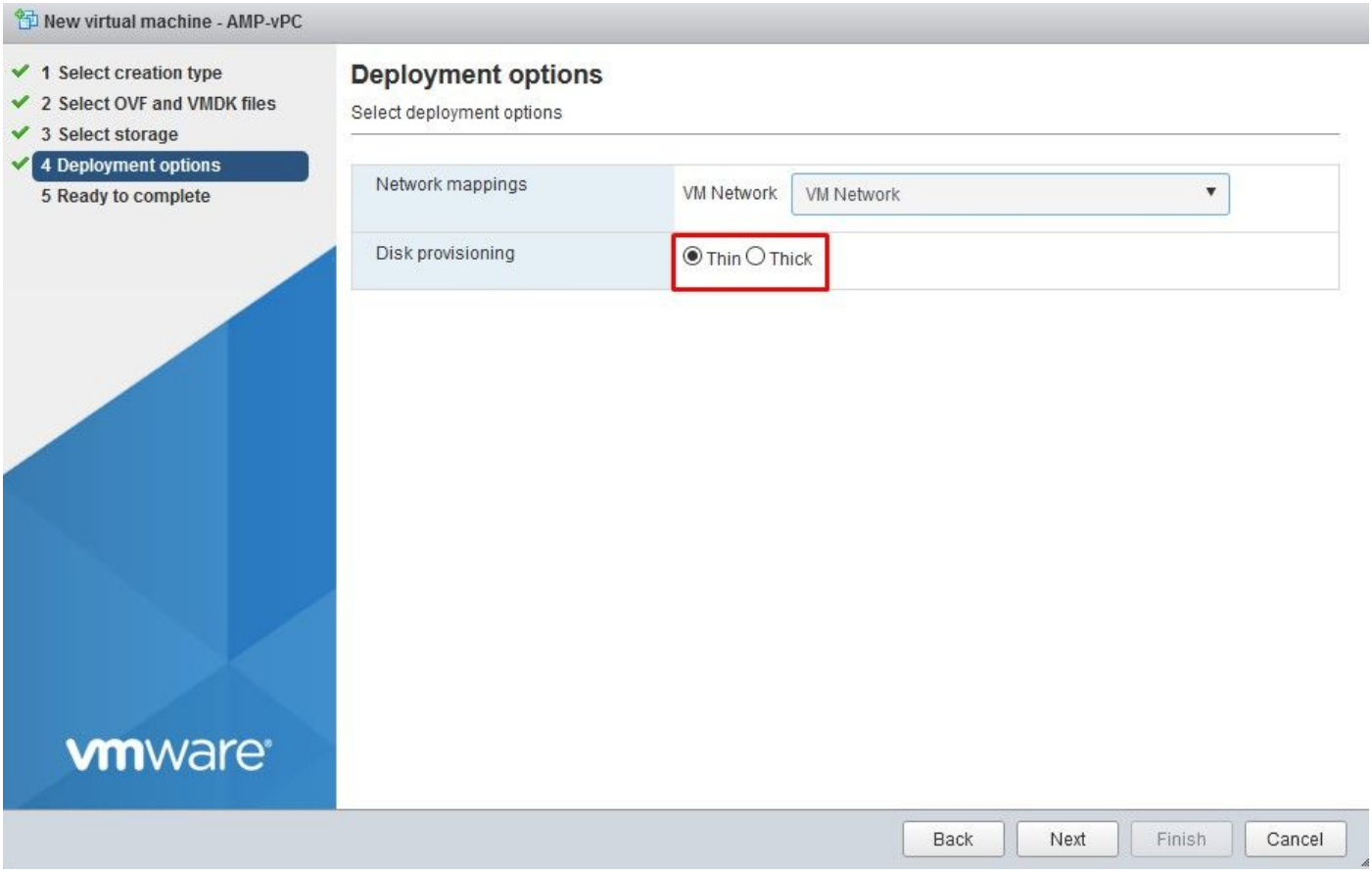






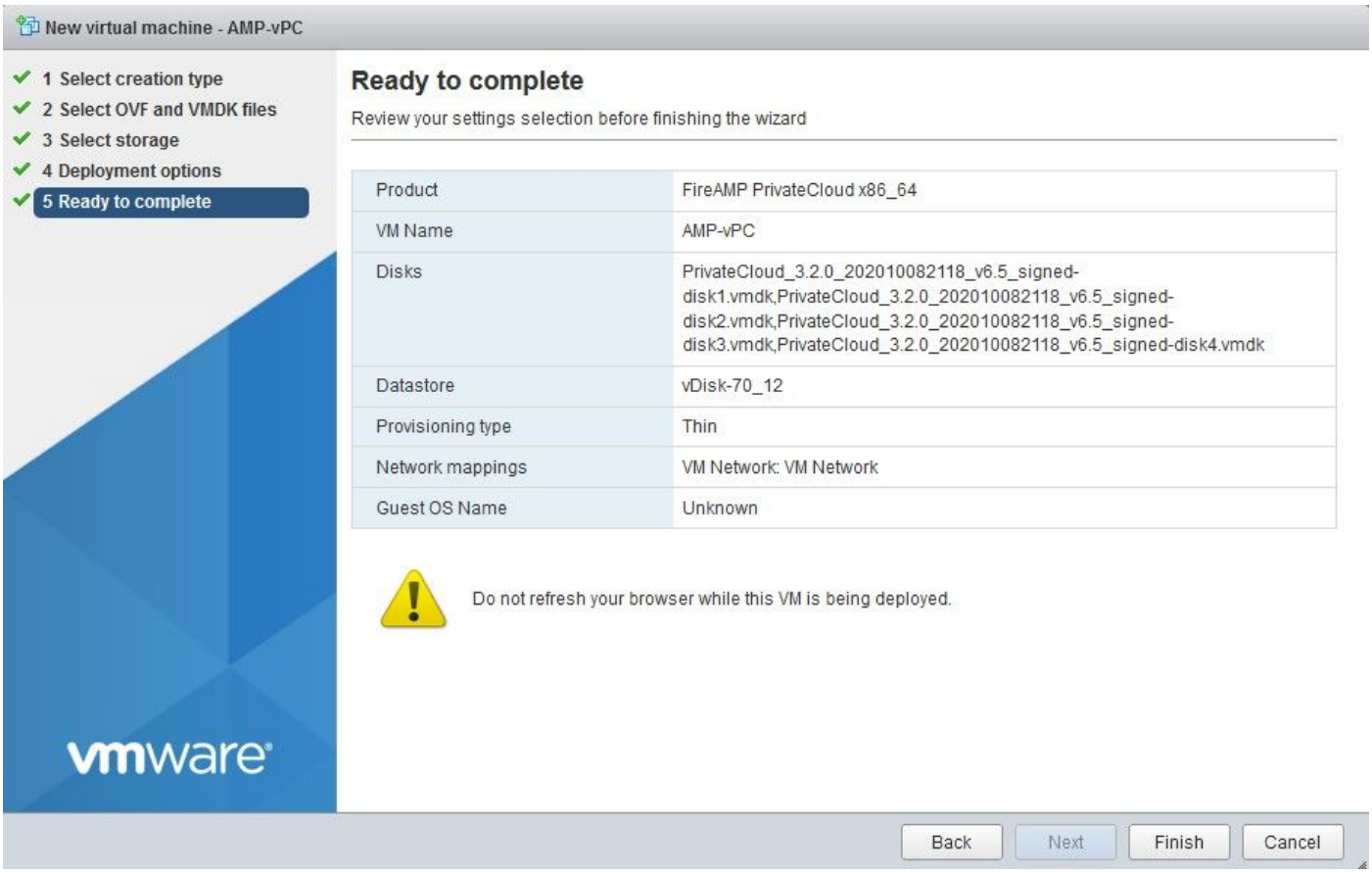
ملاحظة: يحتفظ الإعداد السميك بمساحة عند إنشاء قرص. إذا قمت بتحديد هذا الخيار، فيمكنه تحسين الأداء أكثر من رفيع المزود. ومع ذلك، فإن ذلك ليس إلزاميا. الآن حدد

على التالي، كما هو موضح في الصورة.

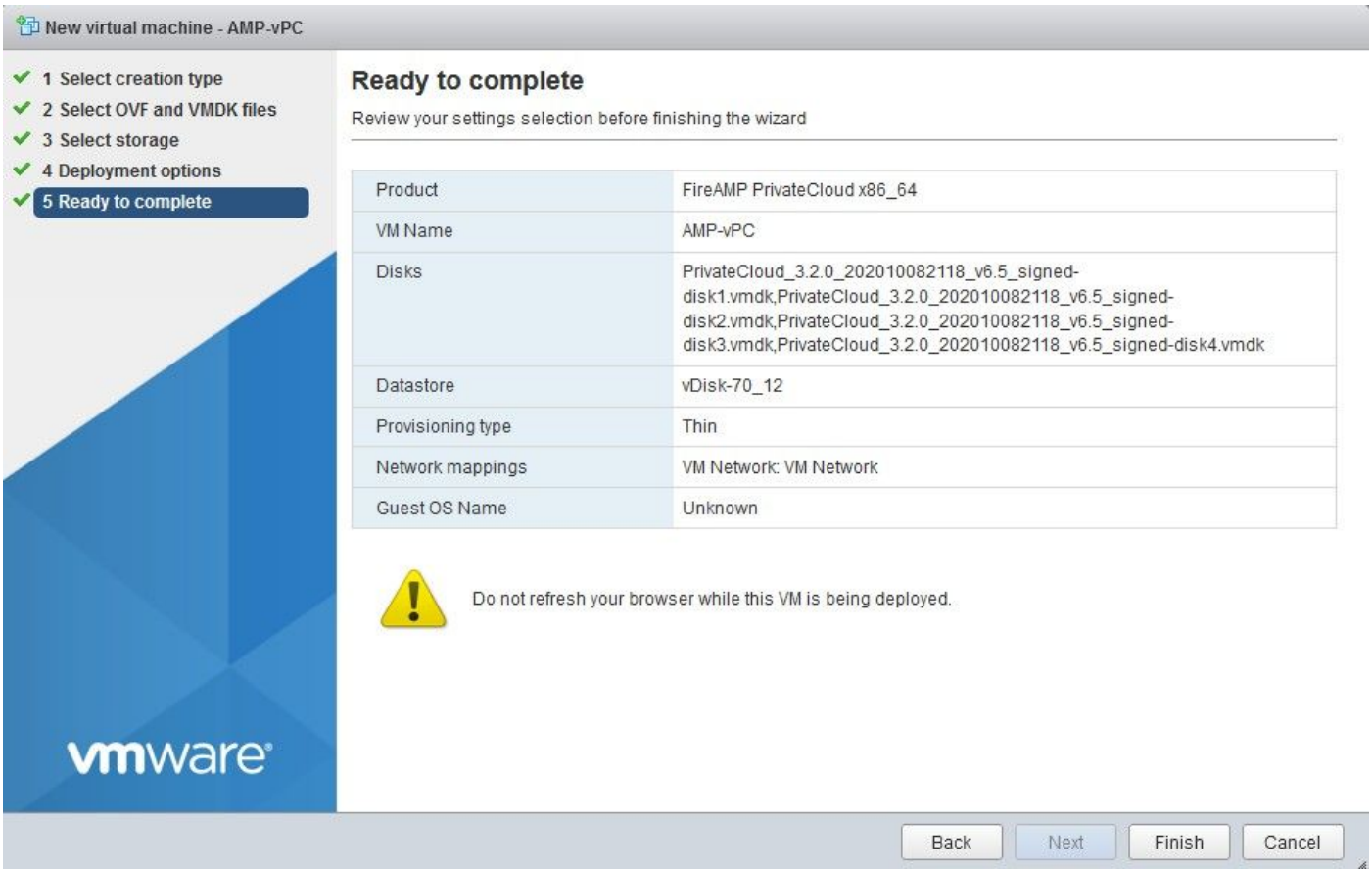


الخطوة 2:

حدد إستعراض.. لتحديد ملف OVA، ثم حدد على التالي. يمكنك مالحظة معلمات OVA الافتراضية في صفحة تفاصيل قالب OVF، كما هو موضح في الصورة. حدد في التالي.



إعداد واجهة المستخدم الأولية

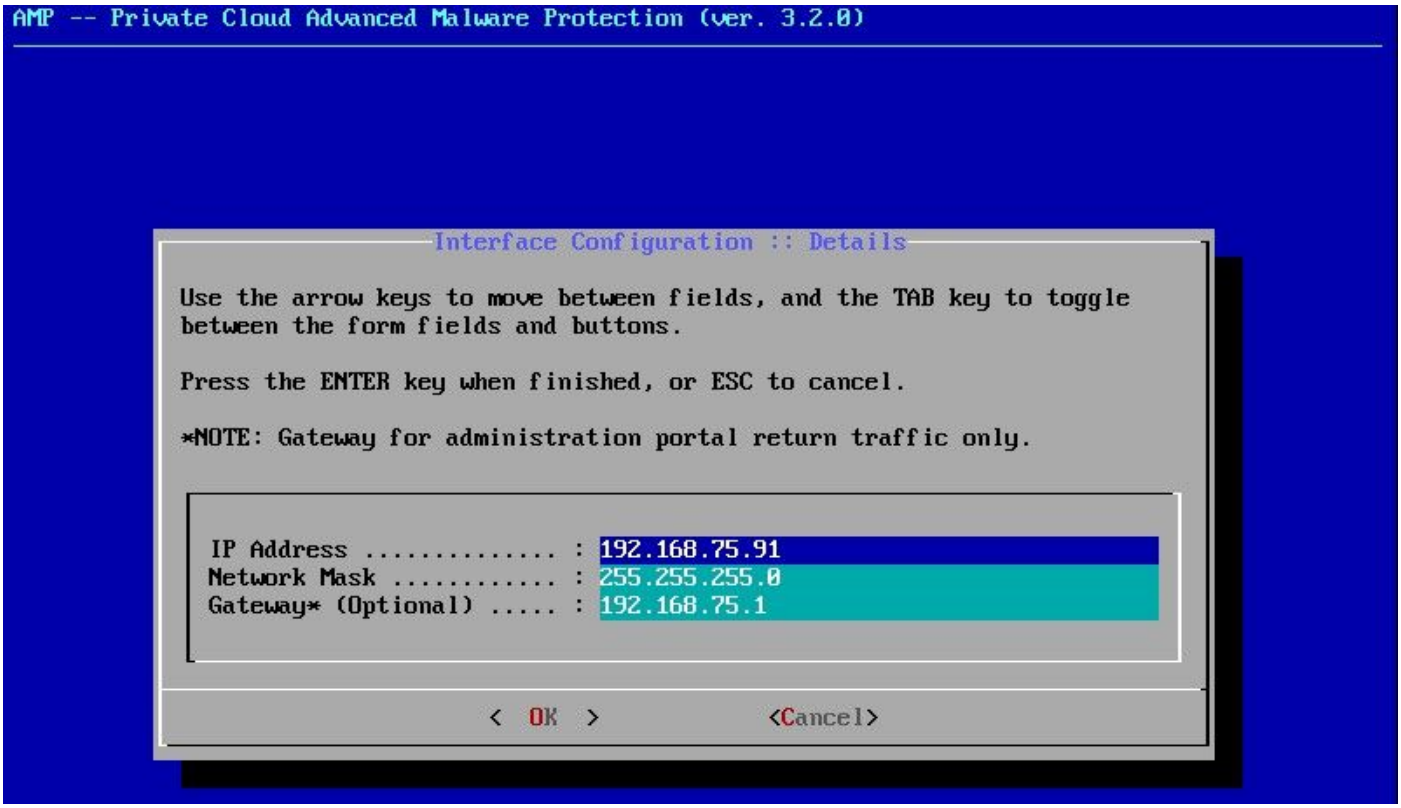


بمجرد تمهيد الأجهزة الافتراضية (VM)، يمكنك إجراء التكوين الأولي من خلال وحدة التحكم

في الأجهزة الافتراضية (VM).

الخطوة 1:

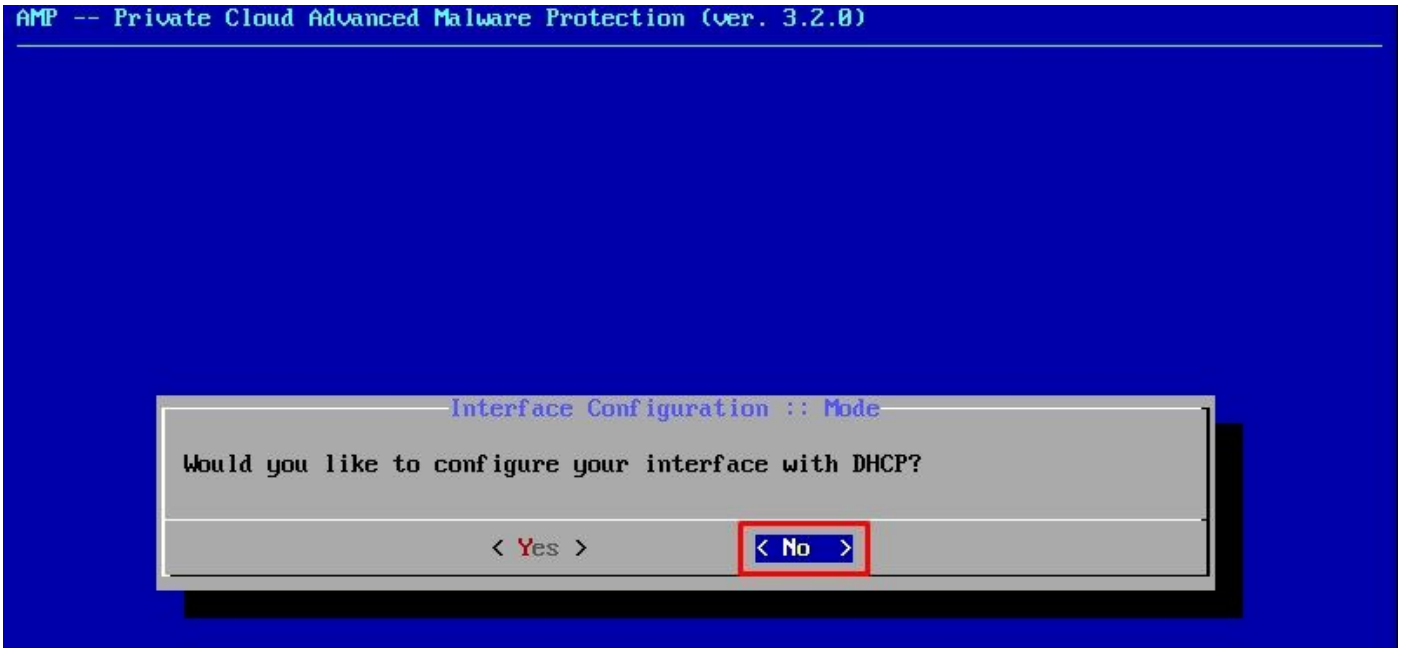
قد تلاحظ أن عنوان URL يظهر [غير مكون] إذا لم تتلق الواجهة عنوان IP من خادم DHCP. الرجاء ملاحظة أن هذه الواجهة هي واجهة الإدارة. هذه ليست واجهة الإنتاج.

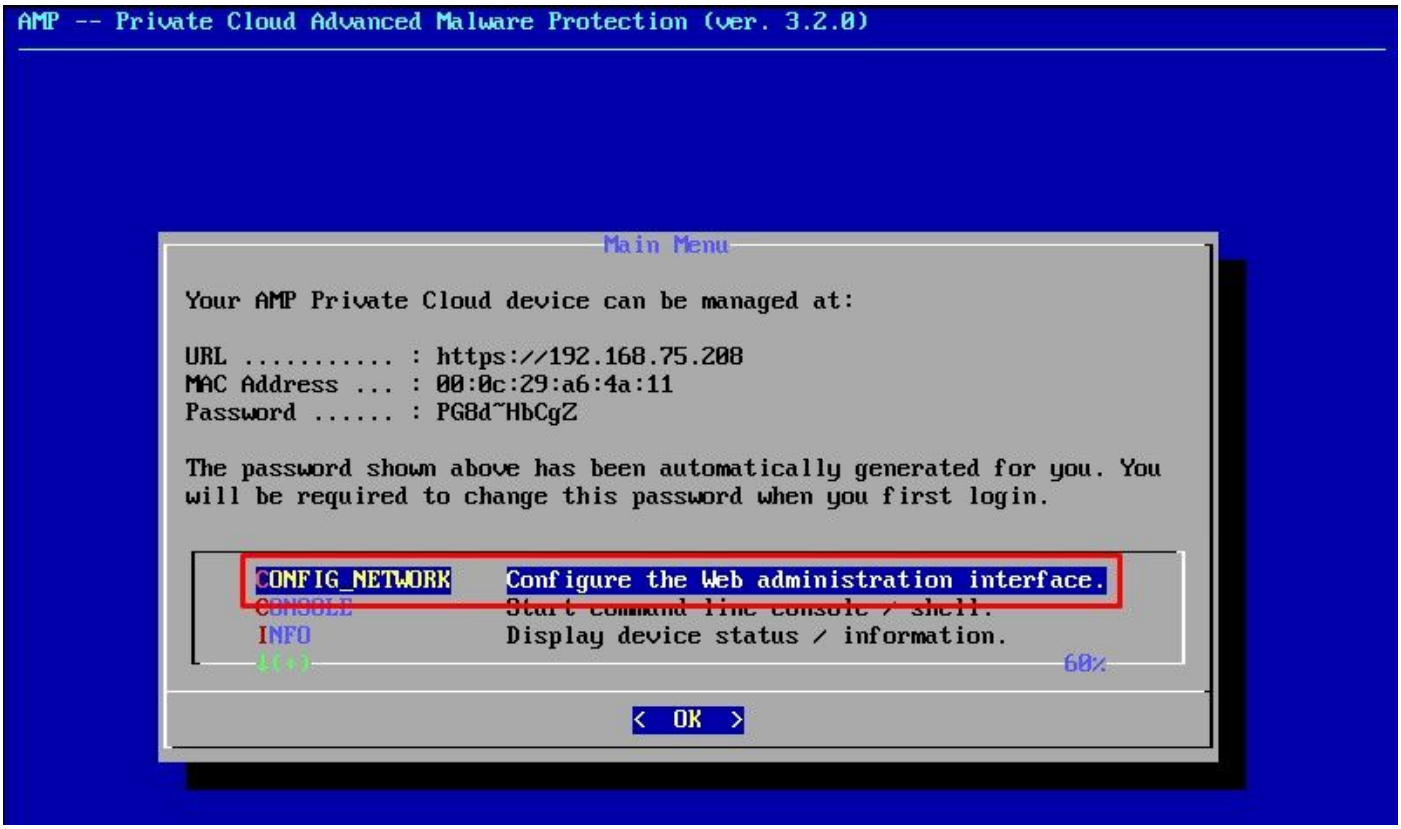


الخطوة 2:

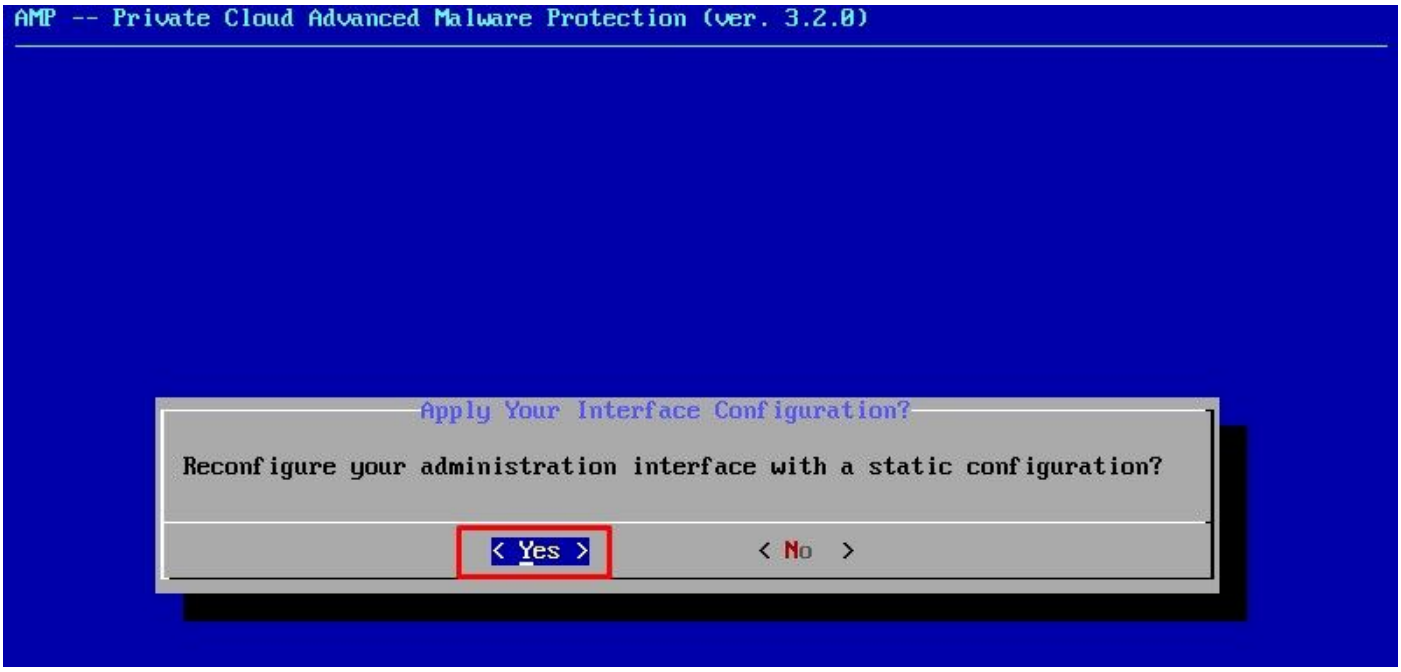
يمكنك التنقل خلال مفاتيح Tab وEnter والأسهم.

انتقل إلى config_network وحدد مفتاح enter على لوحة المفاتيح لبدء تكوين عنوان IP الخاص بإدارة السحابة الخاصة لنقطة النهاية الآمنة. إذا كنت لا تريد إستخدام DHCP، فحدد لا وحدد مفتاح إدخال.

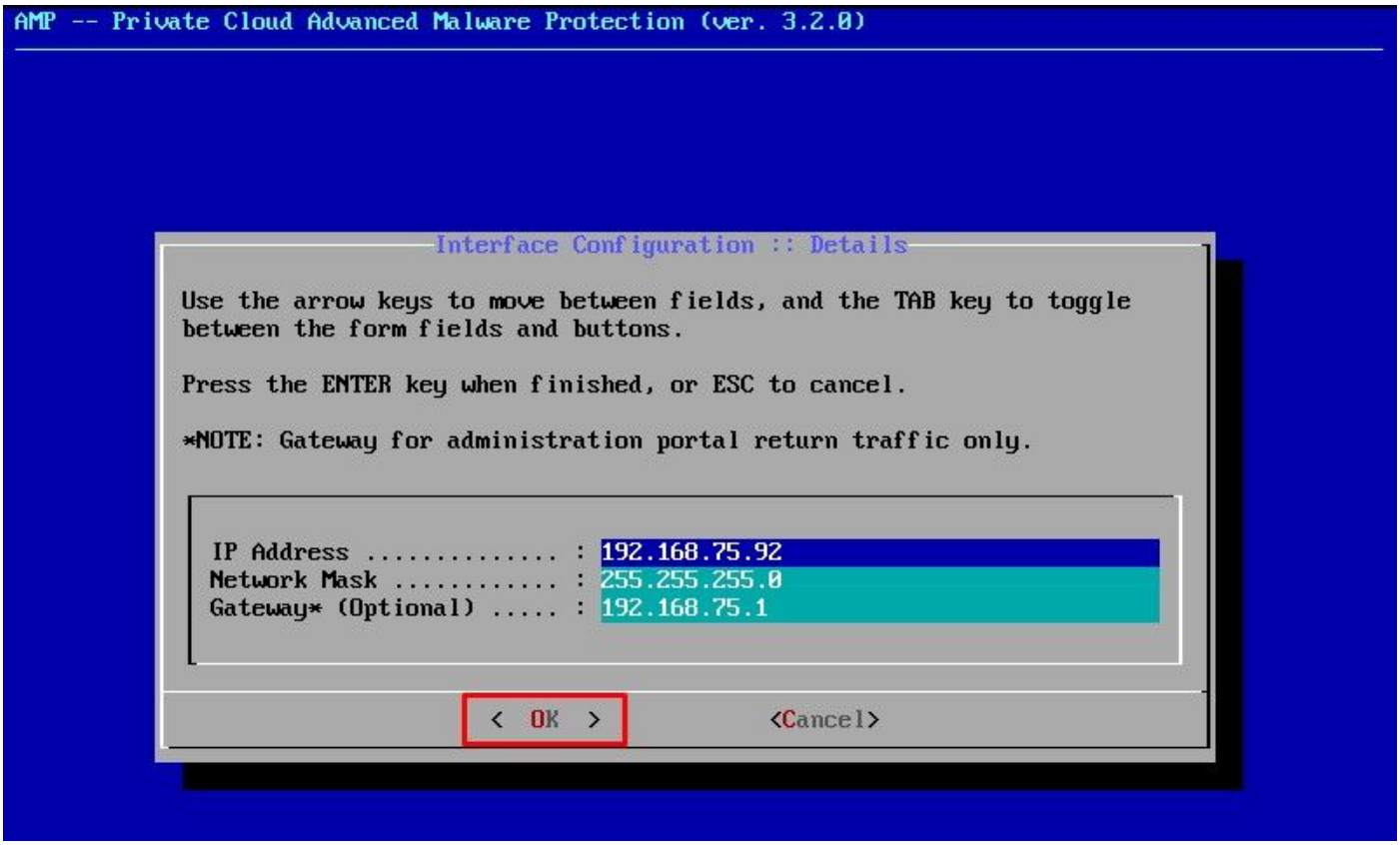




في النافذة التي تظهر، أختر نعم وحدد إدخال مفتاح.

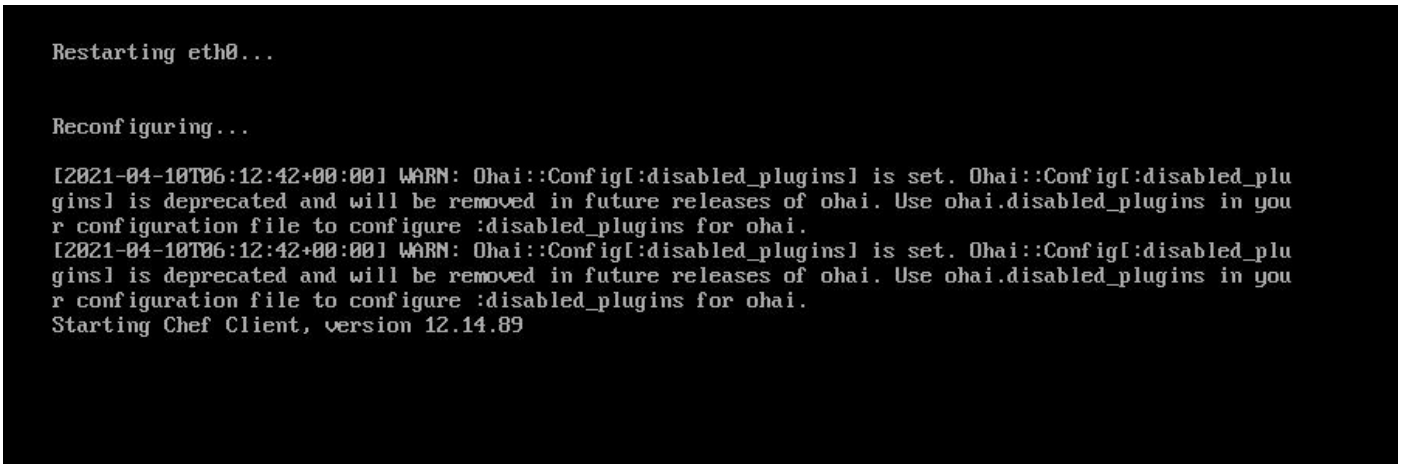


إذا كان IP قيد الاستخدام بالفعل، فسيتم التعامل معك مع سجل الأخطاء هذا. ببساطة عد واختر شيئا فريدا وليس قيد الاستخدام.



إذا سار كل شيء على ما يرام، سترى مخرجات تبدو هكذا

```
      - execute semanage fcontext --add --type var_log_t "/data/log(/.*)?"
    * execute[ConfigurePokedLogs] action run
      - execute semanage fcontext --add --type var_log_t "/data/poked(/.*)?"
    * execute[ConfigureCloudLogs] action run
      - execute semanage fcontext --add --type var_log_t "/data/cloud/log(/.*)?"
    * execute[ConfigureEventLogs] action run
      - execute semanage fcontext --add --type var_log_t "/data/event_log_store(/.*)?"
    * execute[RestoreSELinuxFileContextData] action run
      - execute restorecon -R /data
Recipe: base::ssh
  * template[/etc/ssh/sshd_config] action create
    - update content in file /etc/ssh/sshd_config from c85f41 to bad1ab
    --- /etc/ssh/sshd_config    2021-04-09 13:25:01.969995024 +0000
    +++ /etc/ssh/.chef-sshd_config20210410-8506-1ry0qx2 2021-04-10 06:13:11.889389544 +0000
    @@ -18,7 +18,7 @@
     #AddressFamily any
     #ListenAddress 0.0.0.0
     #ListenAddress ::
    -ListenAddress 192.168.75.208
    +ListenAddress 192.168.75.92

     # The default requires explicit activation of protocol 1
     Protocol 2
    - restore selinux security context
  * template[/etc/ssh/ssh_config] action create (up to date)
  * service[ssh_server] action enable (up to date)
  * service[ssh_server] action start (up to date)
Recipe: base::grub-conf
  * cookbook_file[/etc/default/grub] action create (up to date)
  * execute[Update grub if new kernel installed] action run (skipped due to only_if)
  * execute[Ensure grub menu displays Cisco not CentOS] action run (skipped due to only_if)
Recipe: base::transparent-hugepages
  * execute[disable transparent hugepage] action run
    - execute echo never > /sys/kernel/mm/transparent_hugepage/enabled
  * execute[disable transparent hugepage defrag] action run
    - execute echo never > /sys/kernel/mm/transparent_hugepage/defrag
  * execute[disable transparent hugepage for default kernel] action run
```



الخطوة 3:

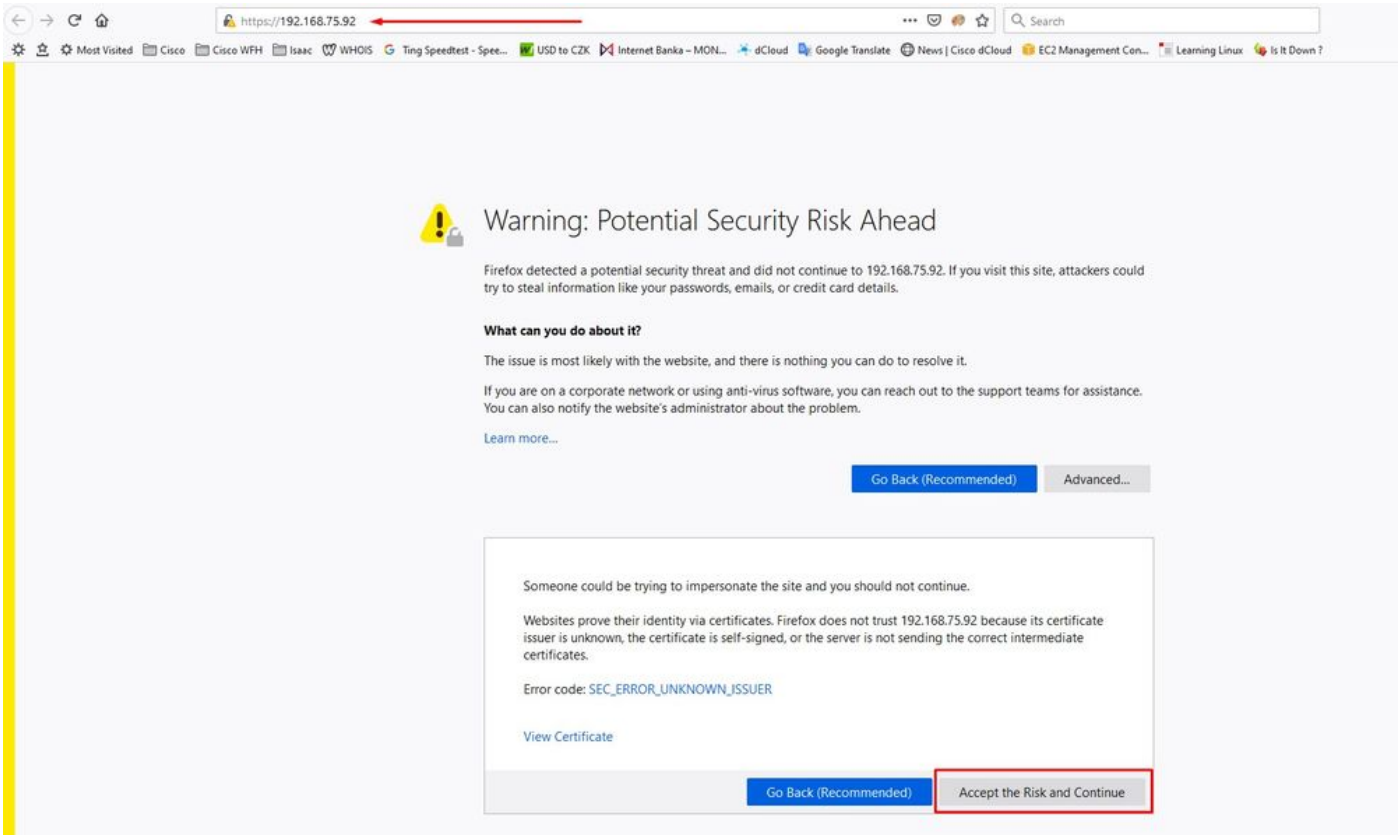
انتظر حتى تظهر الشاشة الزرقاء مرة أخرى مع IP الثابت الجديد لديك. الرجاء أيضا ملاحظة كلمة مرور المرة الواحدة. دون ملاحظة ودعونا نفتح المستعرض لدينا.

التكوين الأولي للكمبيوتر vPC عبر واجهة المستخدم الرسومية (GUI) عبر الويب

الخطوة 1:

افتح مستعرض ويب وانتقل إلى عنوان IP الخاص بإدارة الجهاز. يمكنك تلقي خطأ في الشهادة حيث تقوم سحابة Secure Endpoint Private بإنشاء شهادة HTTPS الخاصة بها مبدئيا، كما هو موضح في الصورة. قم بتكوين المستعرض ليثق في شهادة HTTPS الموقعة ذاتيا الخاصة بسحابة نقاط النهاية الآمنة.

في نوع المستعرض الخاص بك، IP الثابت الذي قمت بتكوينه مسبقا.

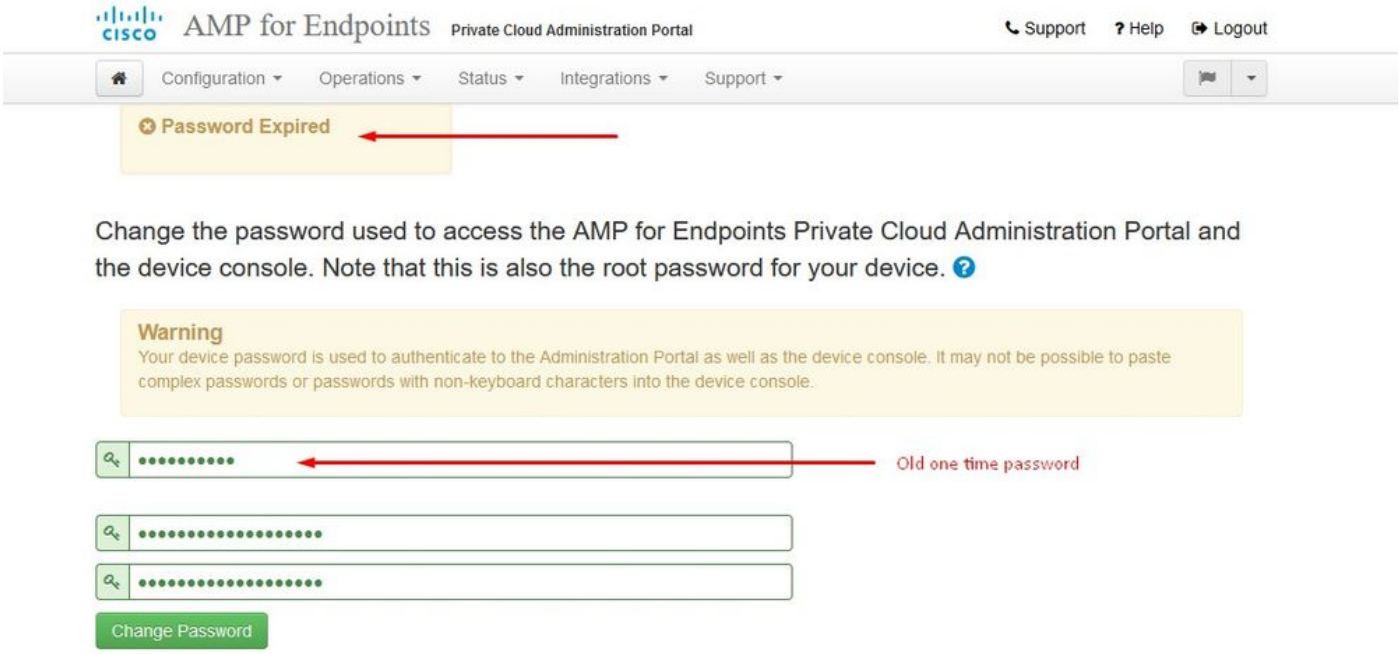


الخطوة 2:

بعد تسجيل الدخول، يجب عليك إعادة تعيين كلمة المرور. أستخدم كلمة المرور الأولية من وحدة التحكم في حقل كلمة المرور القديمة. أستخدم كلمة مرورك الجديدة في حقل كلمة المرور الجديدة. أعد إدخال كلمة المرور الجديدة في حقل كلمة المرور الجديدة. حدد على تغيير كلمة المرور.

الخطوة 3:

بعد تسجيل الدخول، يجب عليك إعادة تعيين كلمة المرور. أستخدم كلمة المرور الأولية من وحدة التحكم في حقل كلمة المرور القديمة. أستخدم كلمة مرورك الجديدة في حقل كلمة المرور الجديدة. أعد إدخال كلمة المرور الجديدة في حقل كلمة المرور الجديدة. حدد على تغيير كلمة المرور.

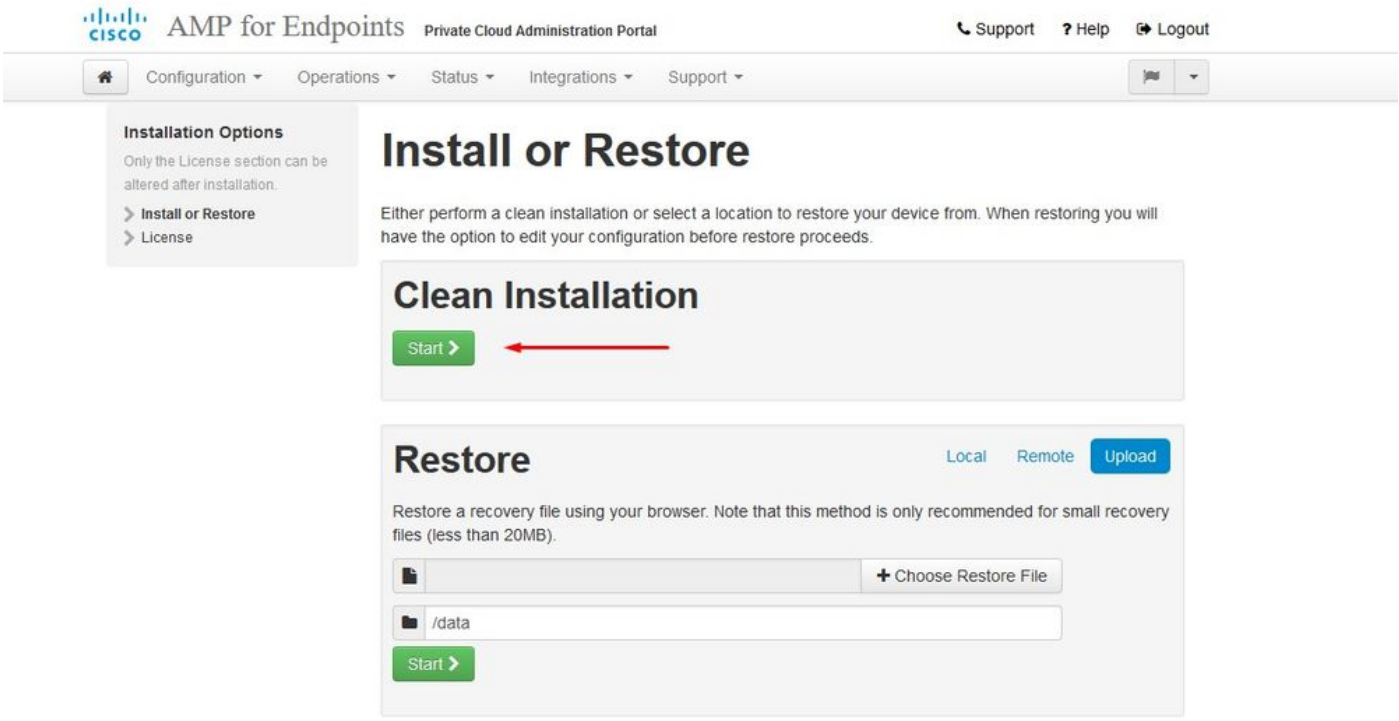


الخطوة 4:

في الصفحة التالية قم بالتمرير لأسفل إلى الأسفل لقبول إتفاقية الترخيص. حدد على الذي قمت بقراءته والموافقة عليه.

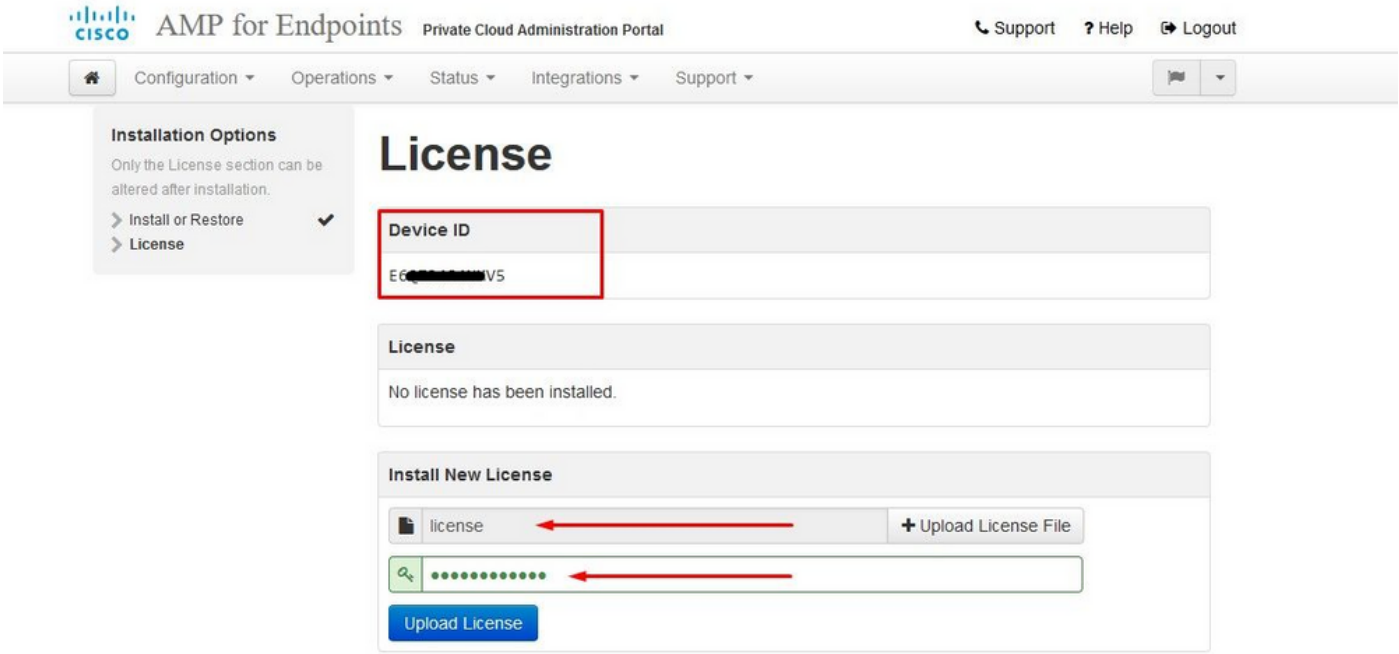
الخطوة 5:

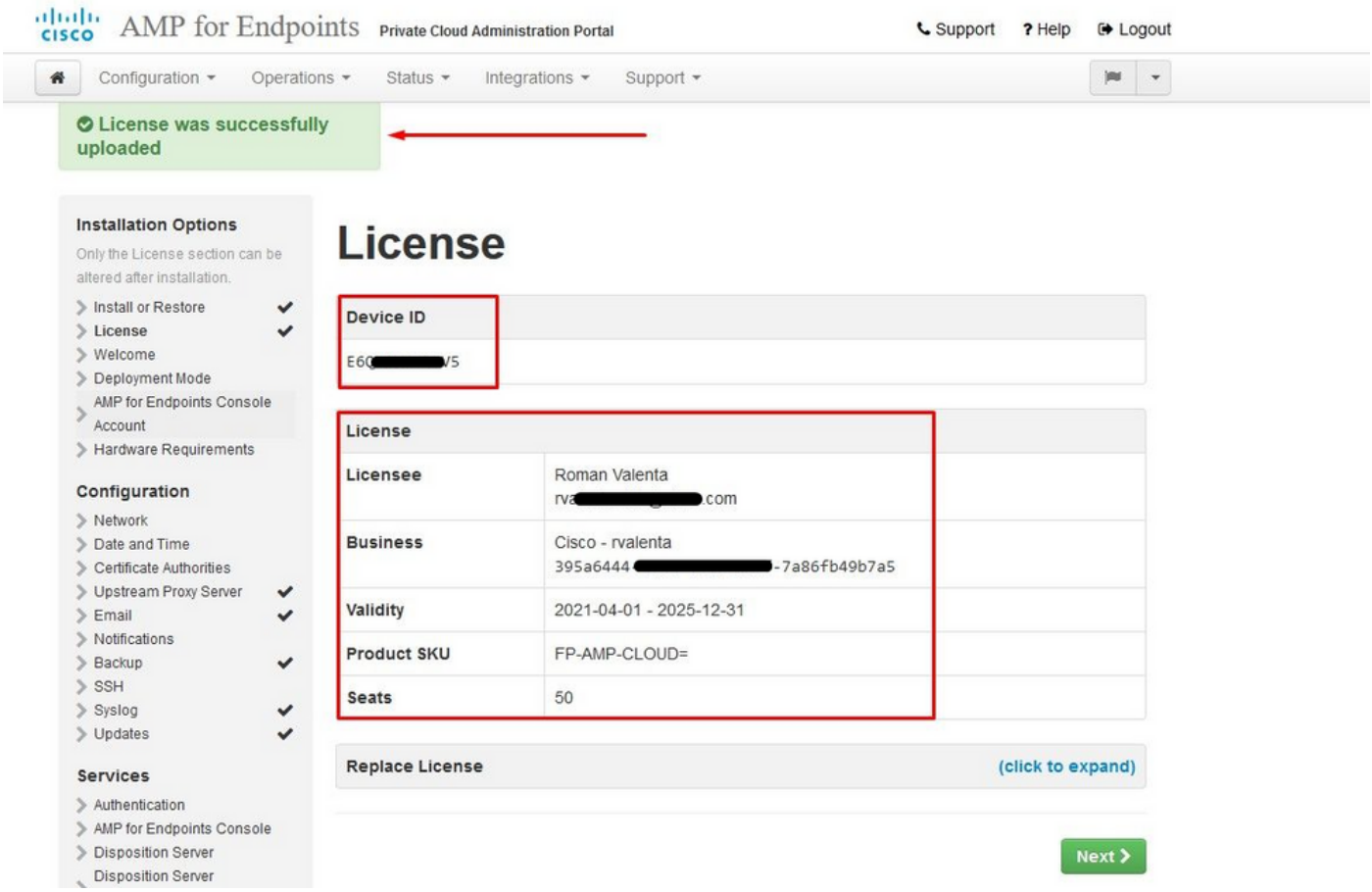
بعد قبول الاتفاقية، تحصل على شاشة التثبيت كما هو موضح في الصورة. إذا كنت تريد الاستعادة من نسخة إحتياطية، يمكنك القيام بذلك هنا، ومع ذلك، يستمر هذا الدليل مع خيار التثبيت النظيف. حدد في البدء في قسم التثبيت النظيف.



الخطوة 6:

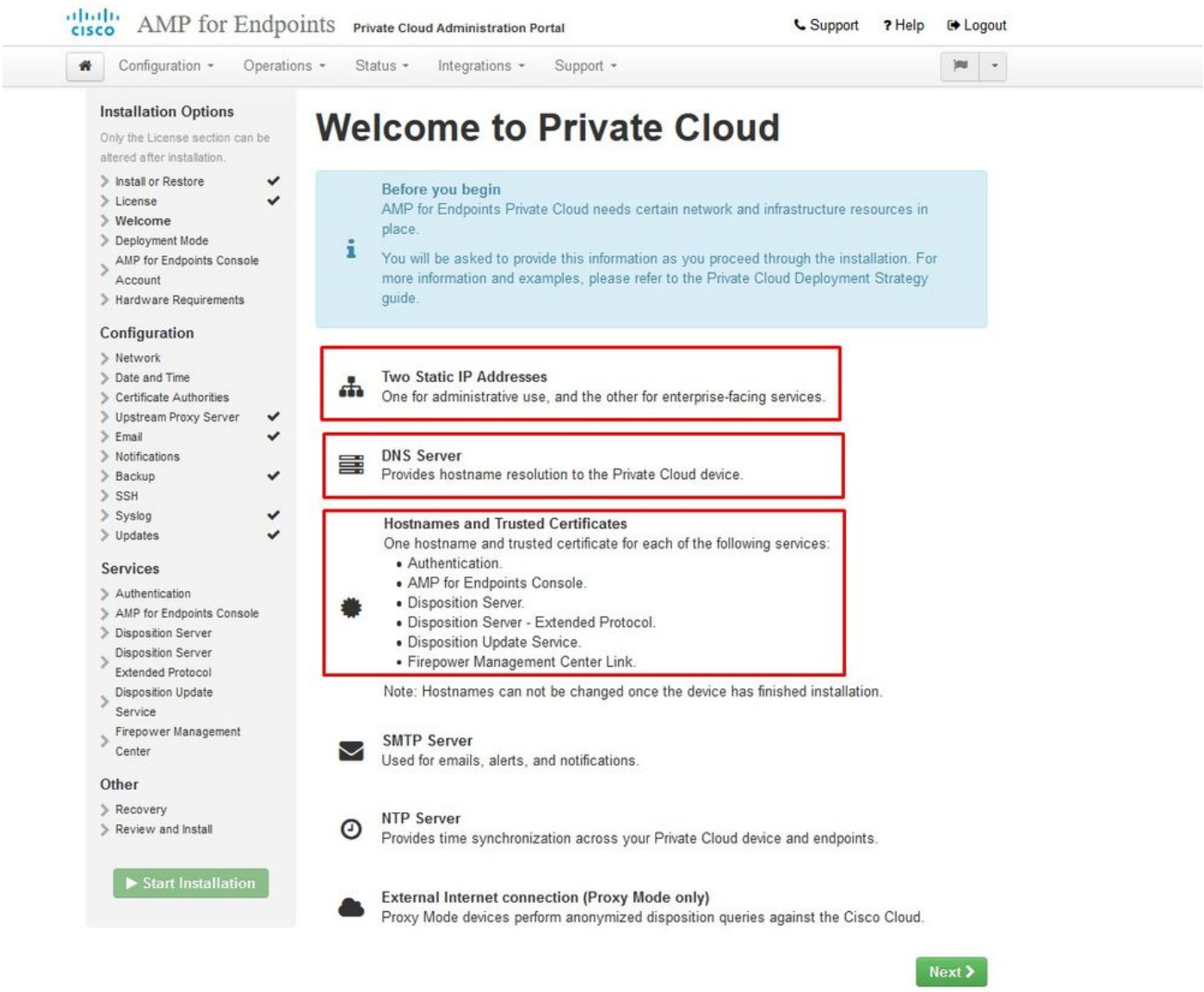
أول شيء تحتاجه هو رخصة للمضي قدما. تتلقى ترخيصا وعبارة مرور عند شراء المنتج. حدد على +ملف ترخيص التحميل. أختر ملف الترخيص وأدخل عبارة المرور. حدد على ترخيص التحميل. إذا لم ينجح التحميل، فالرجاء التحقق من صحة عبارة المرور. إذا نجح التحميل، يتم عرض شاشة تحتوي على معلومات ترخيص صالحة. تحديد في التالي. إذا لم تتمكن بعد من تثبيت الترخيص الخاص بك، فاتصل بدعم Cisco التقني.





الخطوة 7:

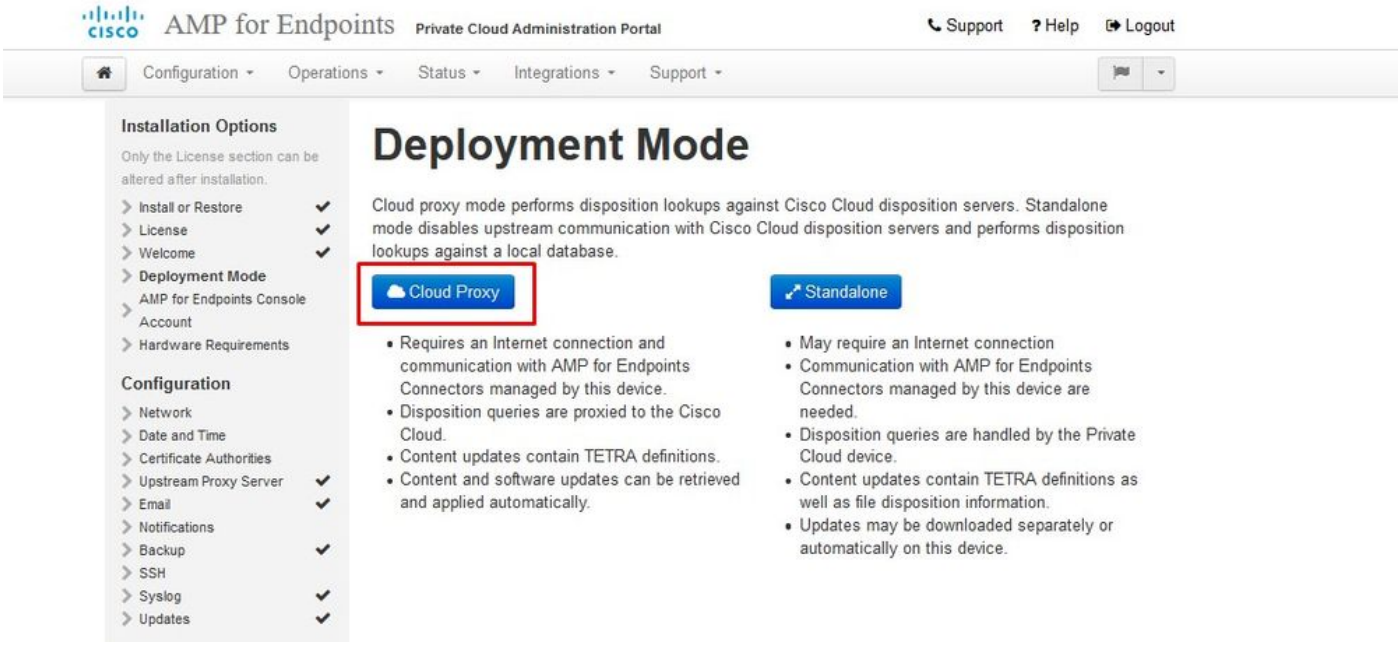
إنك تتلقى صفحة الترحيب، كما هو موضح في الصورة. تعرض هذه الصفحة المعلومات التي يجب أن تكون لديك قبل تكوين السحابة الخاصة. اقرأوا المتطلبات بانتباه. حدد في التالي لبدء تكوين التثبيت المسبق.



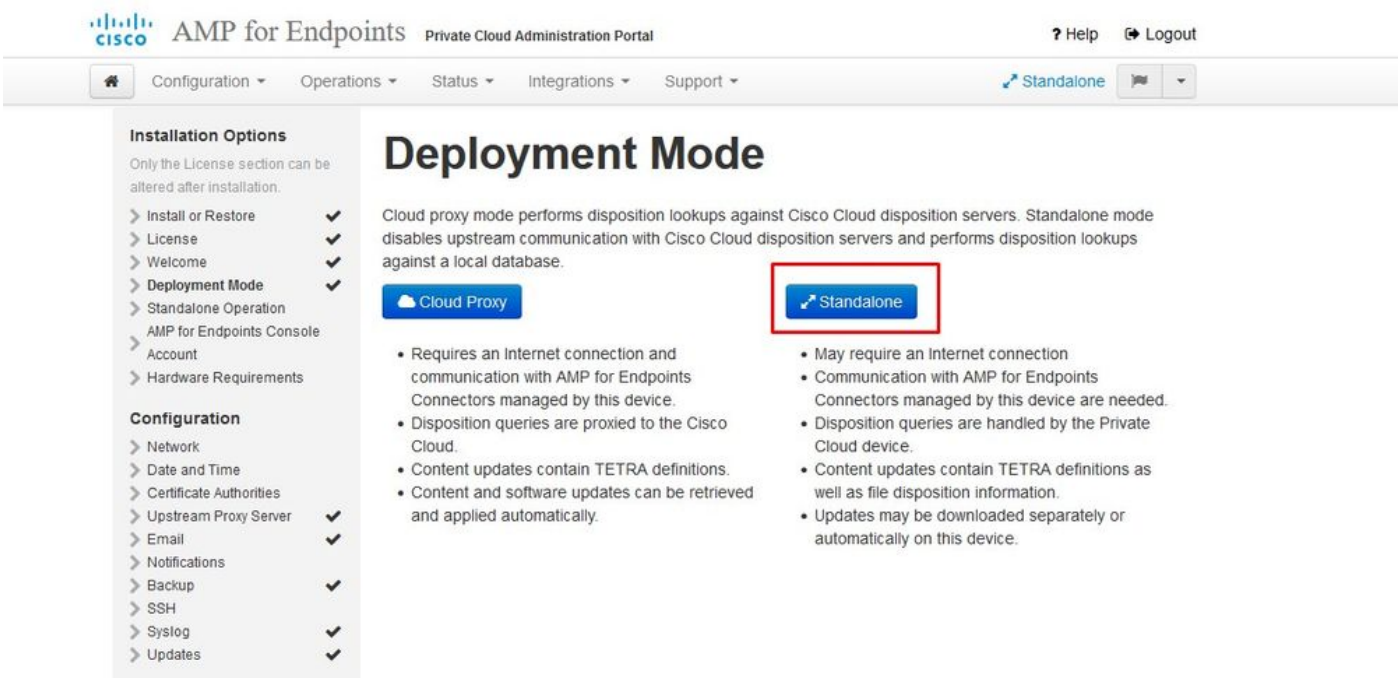
التكوين

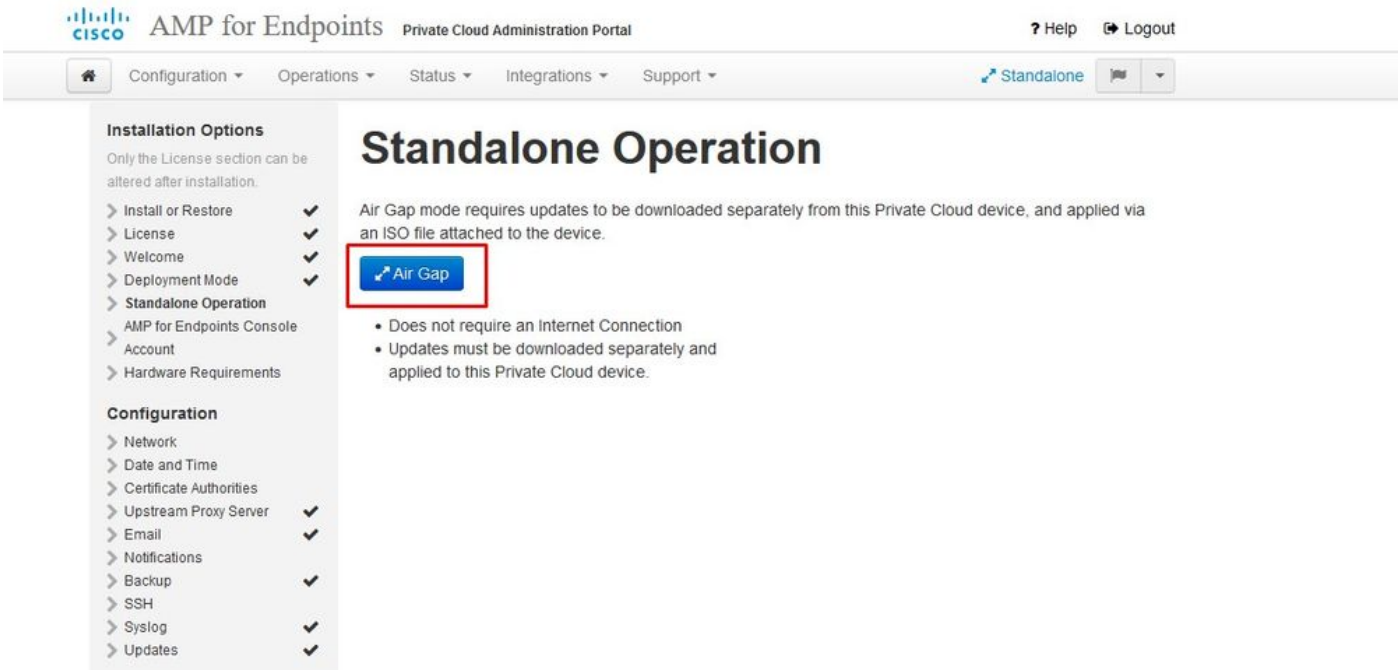
الخطوة 1:

ملاحظة: نلحظ أنه في المجموعات التالية من الشريحة، ندرج بعض العناصر الحصرية كما هو موضح في الصورة والتي تنفرد فقط بوضع فجوة الهواء، والتي يتم إرفاقها ووضع علامة عليها على أنها فجوة الهواء فقط


AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
AMP for Endpoints Console Account
Hardware Requirements
Configuration
Network
Date and Time
Certificate Authorities
Upstream Proxy Server
Email
Notifications
Backup
SSH
Syslog
Updates
Deployment Mode
Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.
Cloud Proxy
Standalone
Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
Disposition queries are proxied to the Cisco Cloud.
Content updates contain TETRA definitions.
Content and software updates can be retrieved and applied automatically.
May require an Internet connection
Communication with AMP for Endpoints Connectors managed by this device are needed.
Disposition queries are handled by the Private Cloud device.
Content updates contain TETRA definitions as well as file disposition information.
Updates may be downloaded separately or automatically on this device.

⩔⩔ Airgap ⩔⩔ طق ف

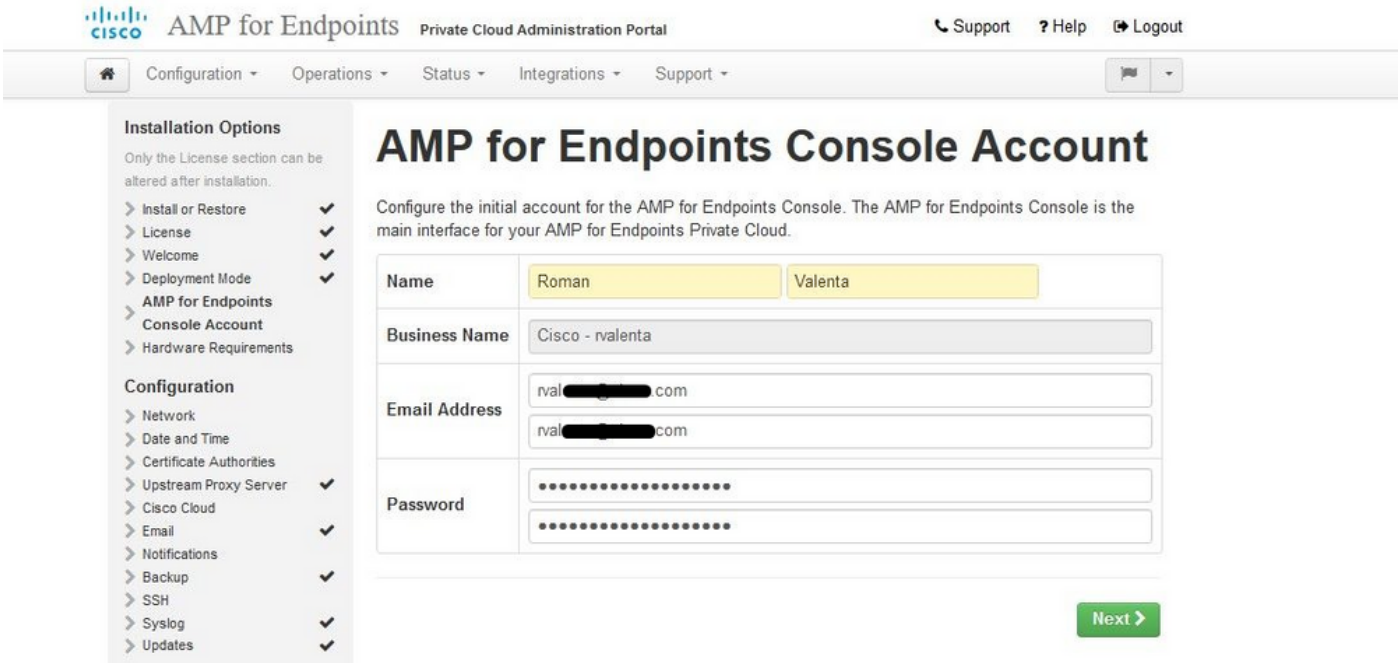

AMP for Endpoints
Private Cloud Administration Portal
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
Standalone Operation
AMP for Endpoints Console Account
Hardware Requirements
Configuration
Network
Date and Time
Certificate Authorities
Upstream Proxy Server
Email
Notifications
Backup
SSH
Syslog
Updates
Deployment Mode
Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.
Cloud Proxy
Standalone
Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
Disposition queries are proxied to the Cisco Cloud.
Content updates contain TETRA definitions.
Content and software updates can be retrieved and applied automatically.
May require an Internet connection
Communication with AMP for Endpoints Connectors managed by this device are needed.
Disposition queries are handled by the Private Cloud device.
Content updates contain TETRA definitions as well as file disposition information.
Updates may be downloaded separately or automatically on this device.



طقف ⩔⩔ Airgap ⩔⩔

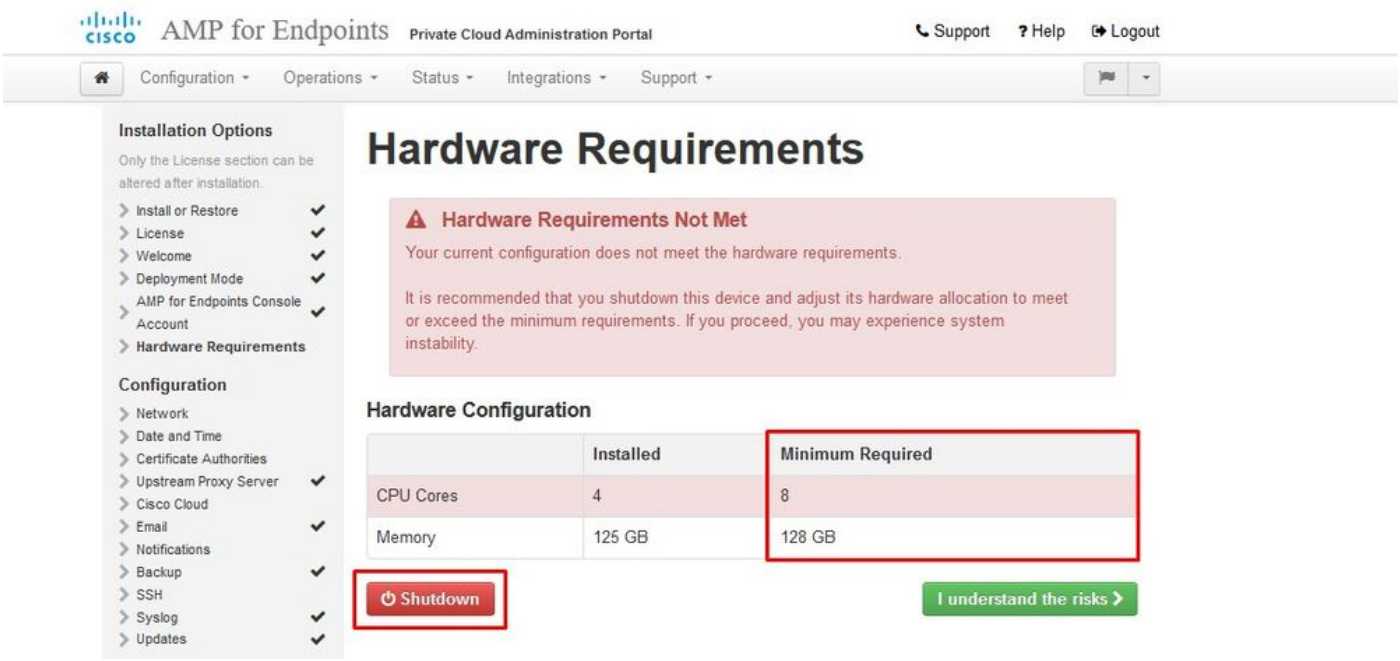
الخطوة 2:

انتقل إلى صفحة حساب وحدة تحكم نقطة النهاية الآمنة. يتم إستخدام مستخدم إداري لوحدة التحكم لإنشاء السياسات ومجموعات الكمبيوتر وإضافة مستخدمين إضافيين. أدخل الاسم وعنوان البريد الإلكتروني وكلمة المرور لحساب وحدة التحكم. حدد في التالي.

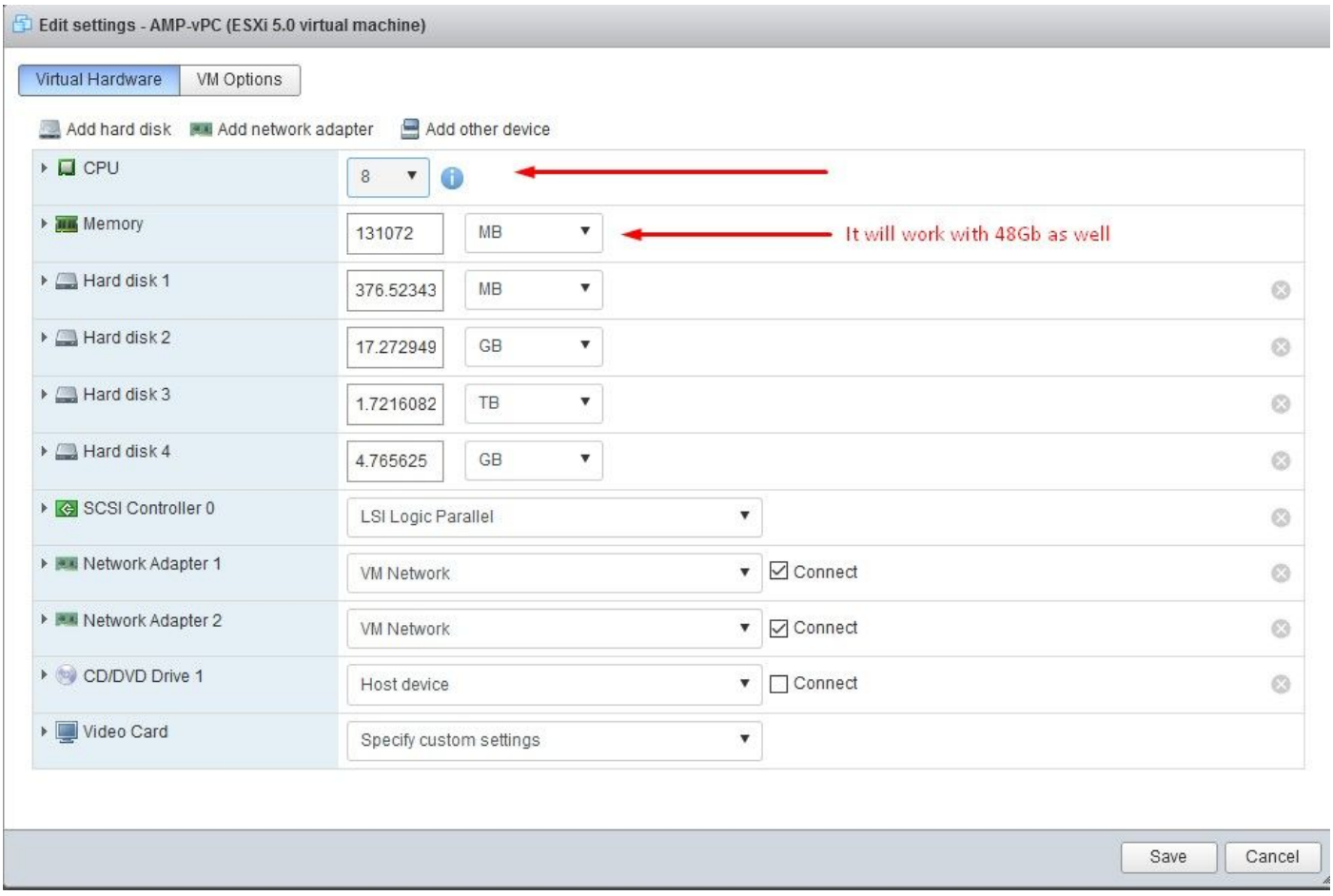


إن يركض أنت إلى هذا إصدار عندما يشر أنت من ال OVA مبرد بعد ذلك أنت تتلقى إثنان خيار إما، وتابعت وصحح هذا إصدار فيما بعد أو إيقاف عمل بعد ذلك in order to نشرت VM وطبقت وقفا لذلك. بعد إعادة التشغيل، استمر في المكان الذي غادرت فيه.

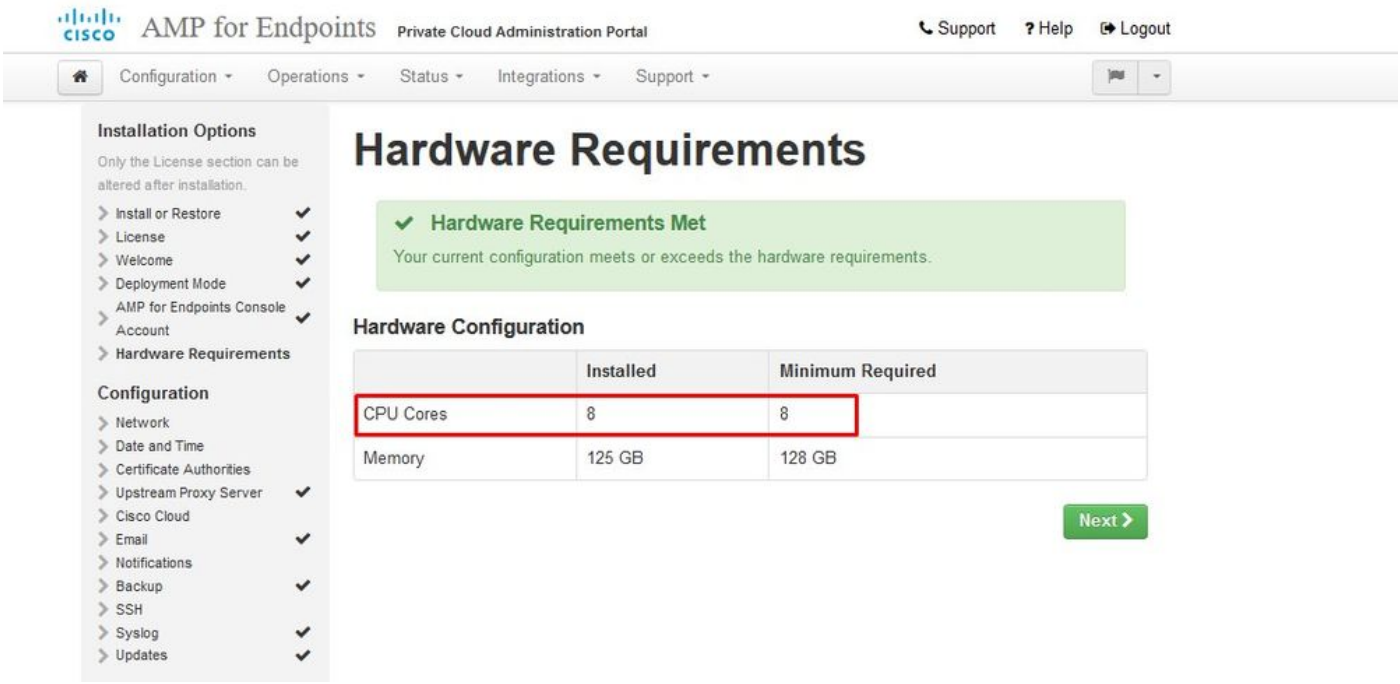
ملاحظة: تم إصلاح ذلك في ملف OVA للإصدار 3.5.2 الذي يتم تحميله بشكل صحيح مع ذاكرة وصول عشوائي سعة 128 جيجابايت ومراكز وحدة المعالجة المركزية (CPU) بسرعة 8.



ملاحظة: أستخدم القيم المستحسنة فقط إلا اذا كان ذلك لأغراض معملية



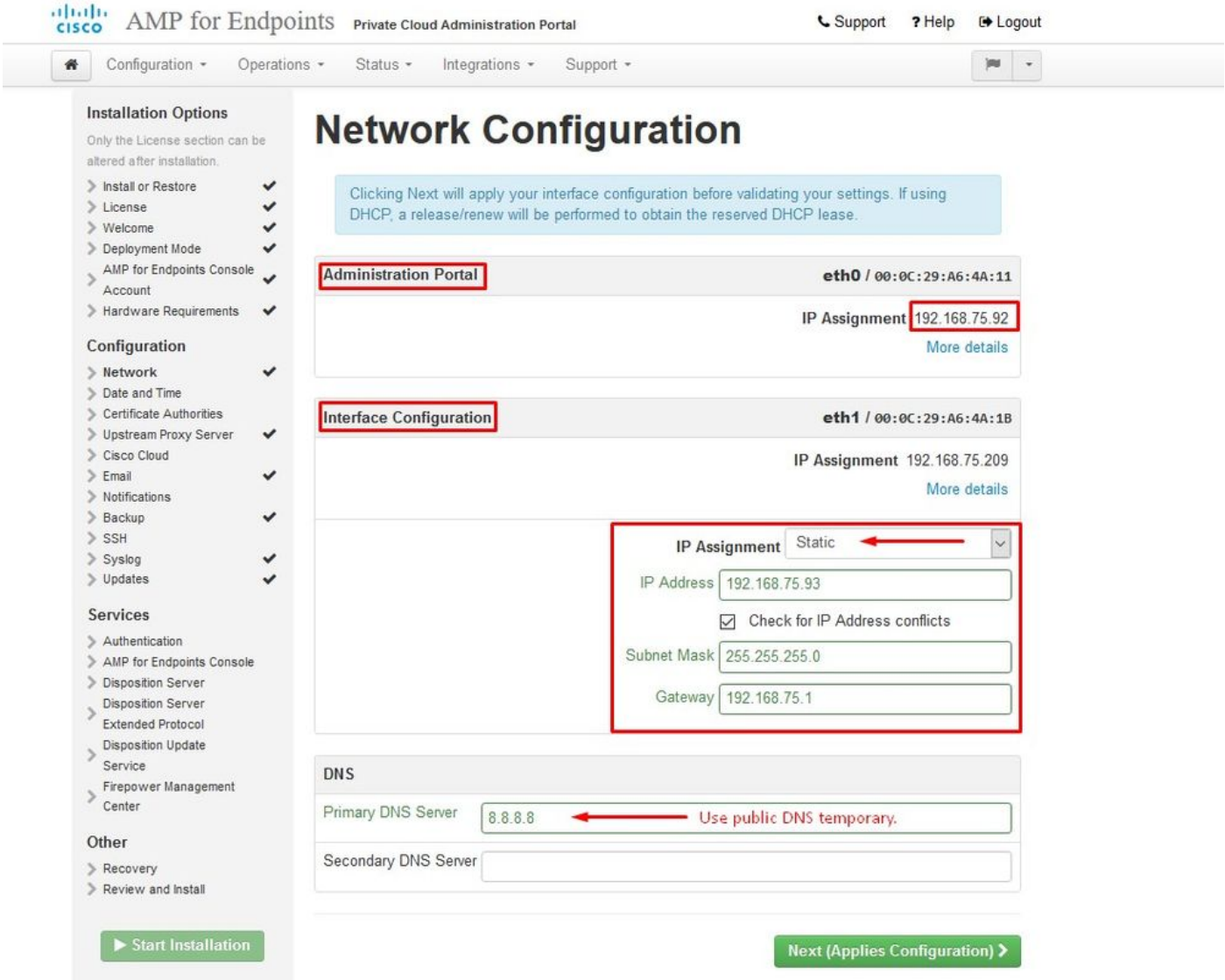
ام إن تم إعادة التشغيل حتى نتابع حيث غادرنا.



تأكد من تكوين ETH1 باستخدام IP الثابت أيضا.

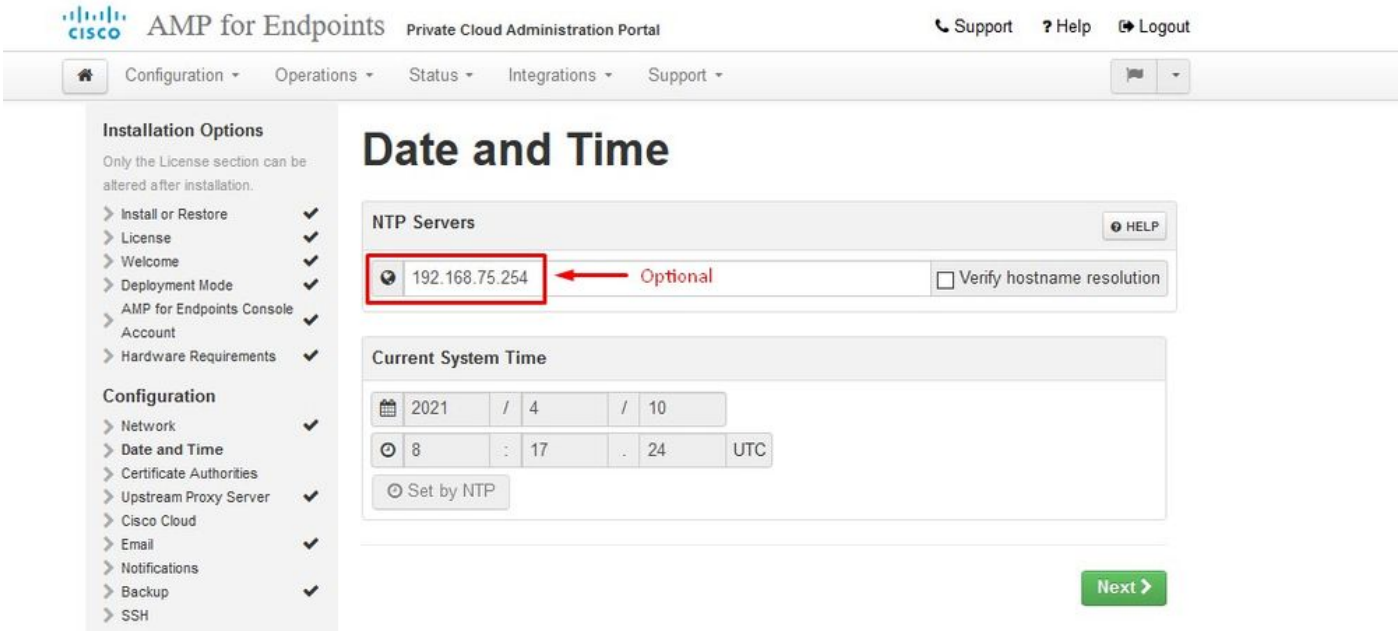
ملاحظة: يجب ألا تقوم أبدا بتكوين جهاز استخدام DHCP ما لم تقم بإنشاء حجوزات عنوان MAC للواجهات. إذا تم تغيير عناوين IP الخاصة بواجهات الاتصال، فقد يؤدي ذلك إلى حدوث مشاكل خطيرة في موصلات نقطة النهاية الآمنة التي تم نشرها. إذا لم يتم تكوين خادم DNS، يمكنك إستخدام DNS العام المؤقت لإنهاء التثبيت.

الخطوة 3:

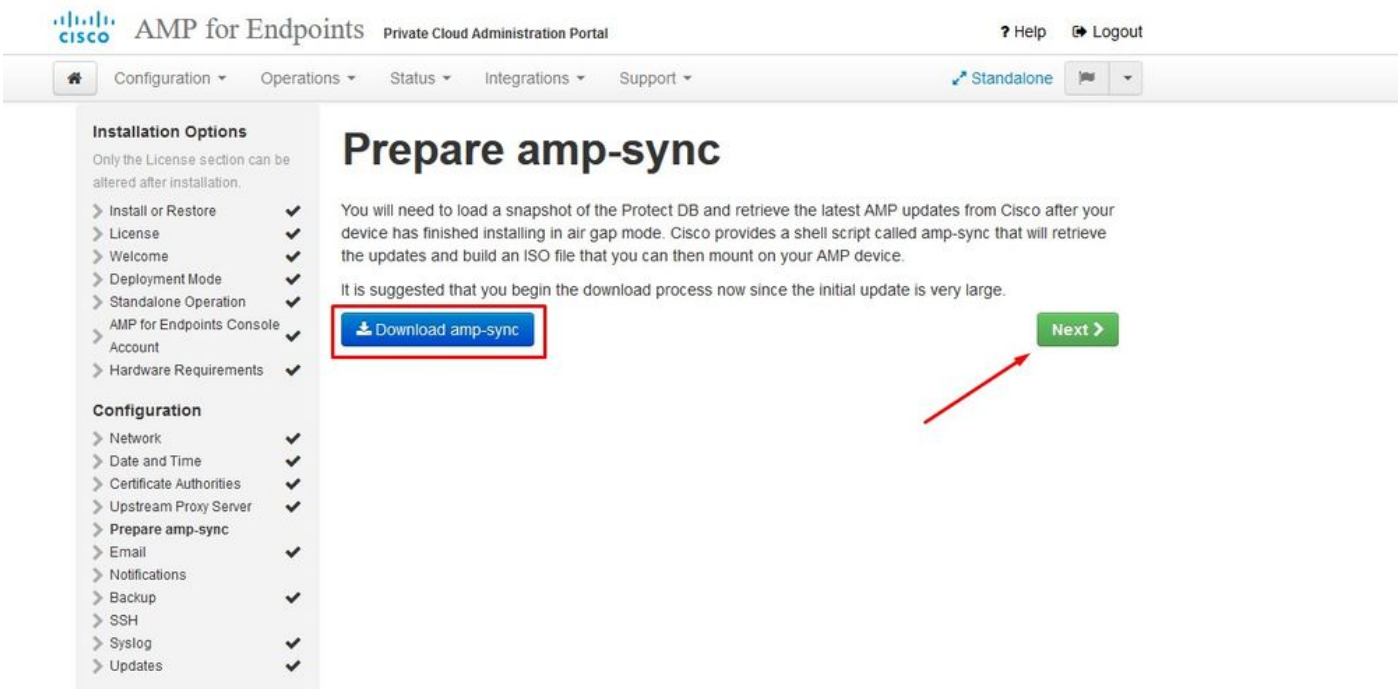


الخطوة 4:

يمكنك الحصول على صفحة التاريخ والوقت. أدخل عناوين خادم NTP واحد أو أكثر الذي تريد إستخدامه لمزامنة التاريخ والوقت. أنت يستطيع استعملت داخلي أو خارجي NTP دان ل وعينت أكثر من واحد من خالل فاصلة أو فارغ قائمة ميالن إلى جانب. قم بمزامنة الوقت مع الم ستعرض أو قم بتشغيل AMP-CTL NTPDATE من وحدة تحكم الجهاز لفرض مزامنة فوريه مع خوادم NTP. تحديد في التالي.



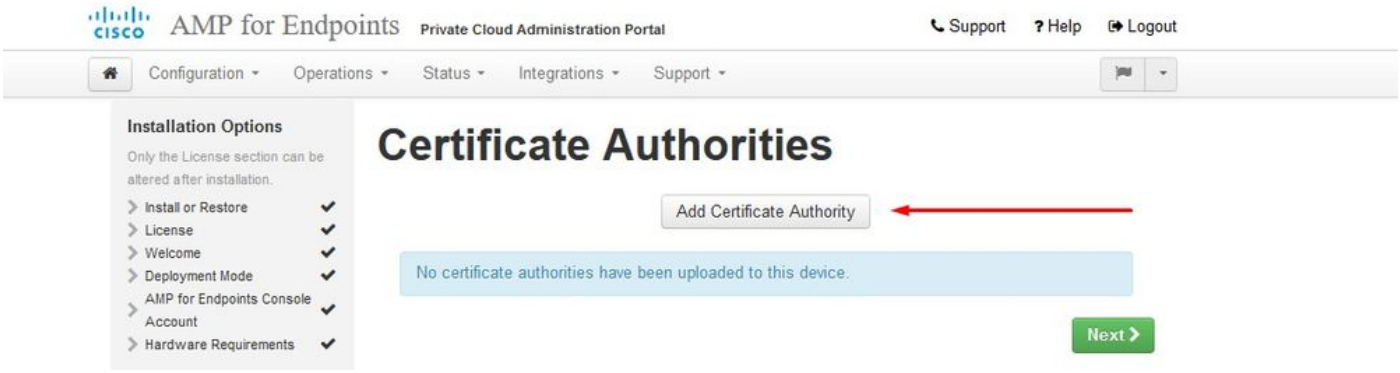
⩔⩔ Airgap ⩔⩔ فقط

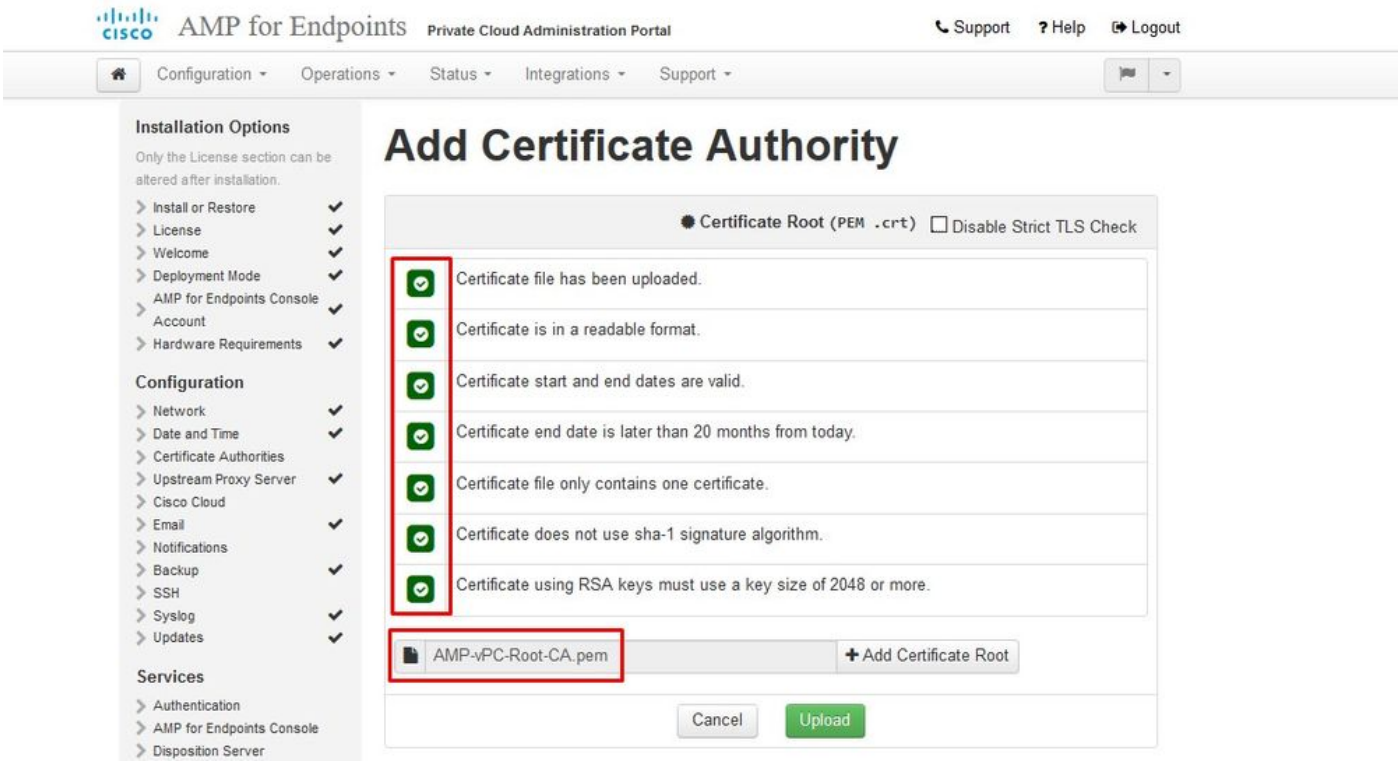


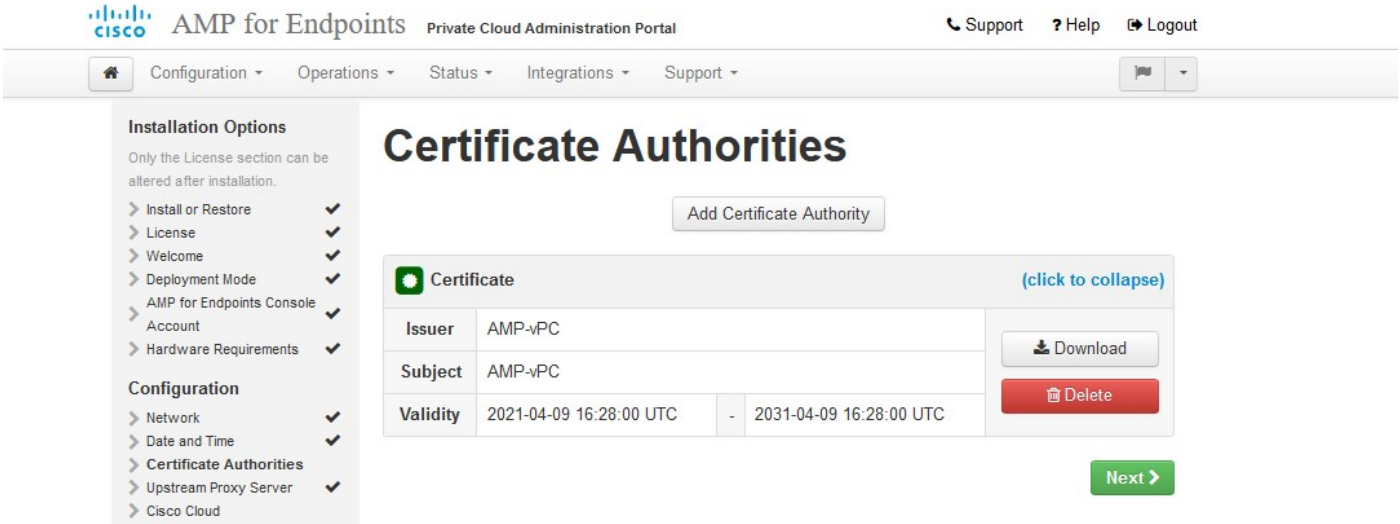
⩓⩓ Airgap ⩓⩓ فقط

الخطوة 5:

تحصل على صفحة المراجع المصدقة، كما هو موضح في الصورة. حدد على إضافة مرجع شهادات لإضافة شهادتك الجذر.



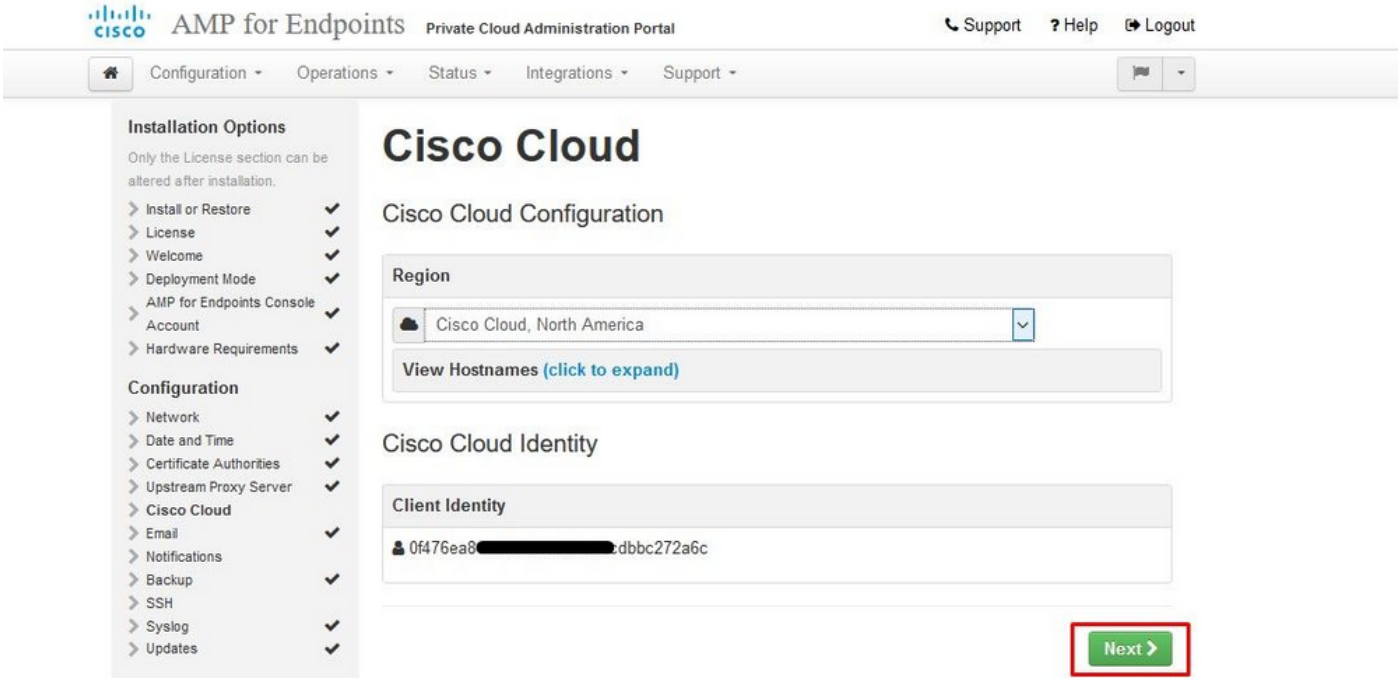




الخطوة 6:

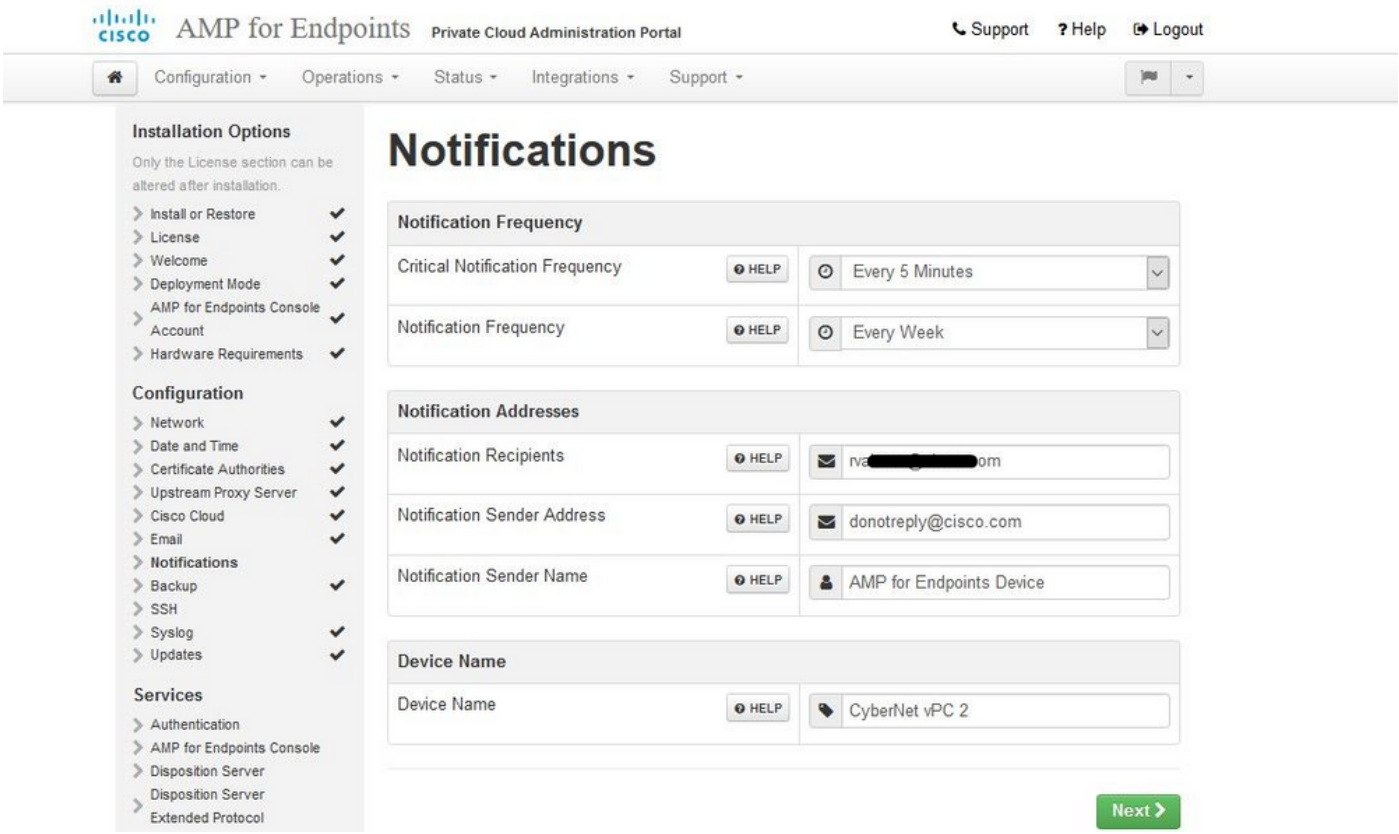
تتمثل الخطوة التالية في تكوين صفحة Cisco Cloud، كما هو موضح في الصورة. حدد منطقة سحابة Cisco المناسبة. قم بتوسيع عرض أسماء المضيف إذا كنت بحاجة إلى

إنشاء إستثناءات جدار الحماية لجهاز السحابة الخاص بنقطة النهاية الآمنة لديك للاتصال بسحابة Cisco لإجراء عمليات البحث عن الملفات وتحديثات الأجهزة. حدد في التالي.



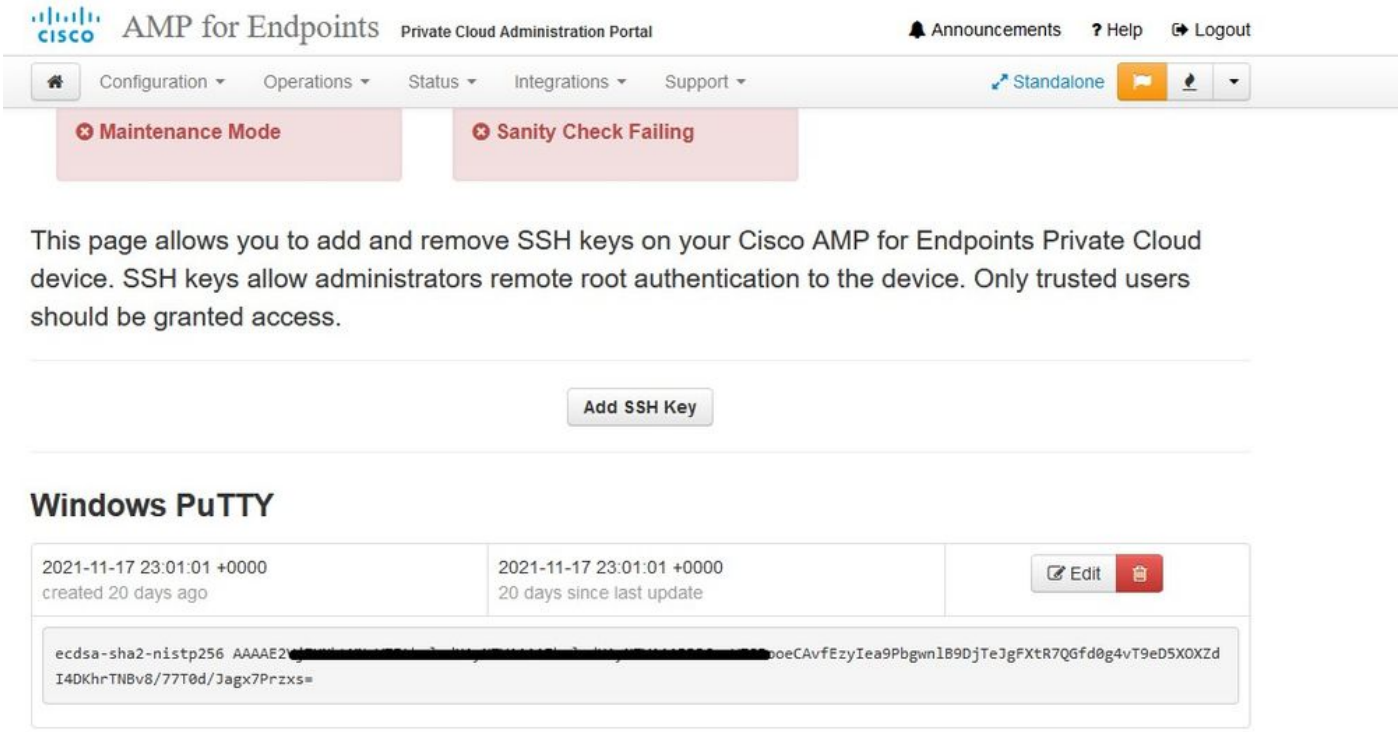
الخطوة 7:

انتقل إلى صفحة الإعدادات، كما هو موضح في الصورة. حدد التردد للإعدادات الهامة والمنتظمة. أدخل عناوين البريد الإلكتروني التي تريد تلقي إعدادات التنبيه لجهاز نقطة النهاية الآمنة. يمكنك إستخدام أسماء مستعارة للبريد الإلكتروني أو تحديد عناوين متعددة من خلال قائمة مفصولة بفاصلة. يمكنك أيضا تحديد اسم المرسل وعنوان البريد الإلكتروني المستخدم بواسطة الجهاز. هذه الإعدادات ليست نفس اشتراكات وحدة تحكم نقطة النهاية الآمنة. يمكنك أيضا تحديد اسم جهاز فريد إذا كان لديك العديد من أجهزة السحابة الخاصة لنقطة النهاية الآمنة. تحديد في التالي.



الخطوة 8:

بعد ذلك تقوم بالتنقل إلى صفحة مفاتيح SSH، كما هو موضح في الصورة. حدد على إضافة مفتاح SSH لإدخال أي مفاتيح عامة تريد إضافتها إلى الجهاز. تتيح لك مفاتيح SSH الوصول إلى الجهاز عبر طبقة بعيدة ذات امتيازات الجذر. يجب منح حق الوصول للمستخدمين الموثوق بهم فقط. يتطلب جهاز السحابة الخاص مفتاح RSA منسق ل OpenSSH. يمكنك إضافة المزيد من مفاتيح SSH الأقل من خلال التكوين > SSH في مدخل الإدارة لديك. حدد في التالي.



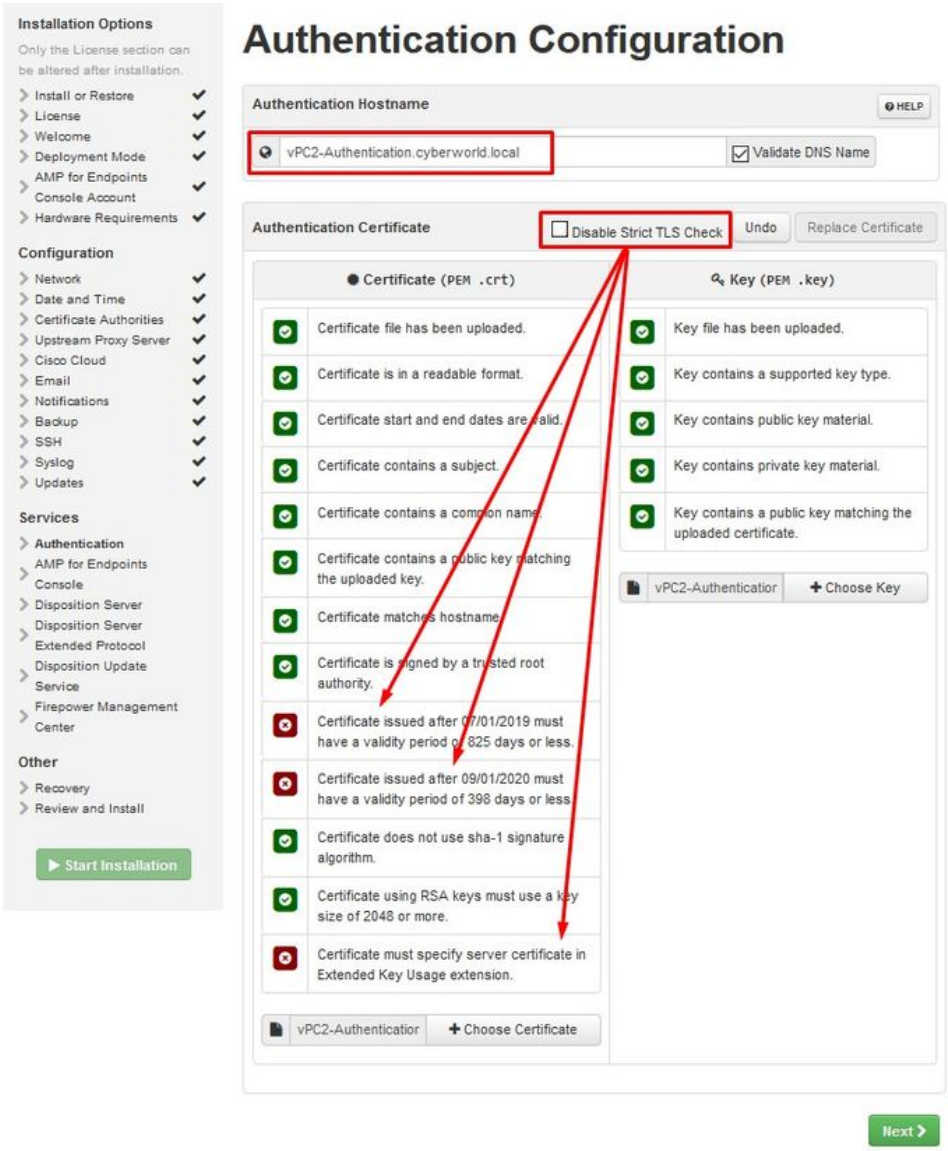
ثم تحصل على قسم الخدمات. في الصفحات التالية، يجب تعيين أسماء المضيف وتحميل أزواج الشهادات والمفاتيح المناسبة لخدمات الأجهزة هذه. في الشرائح القليلة التالية، يمكننا رؤية تهيئة إحدى الشهادات الست.

الخدمات

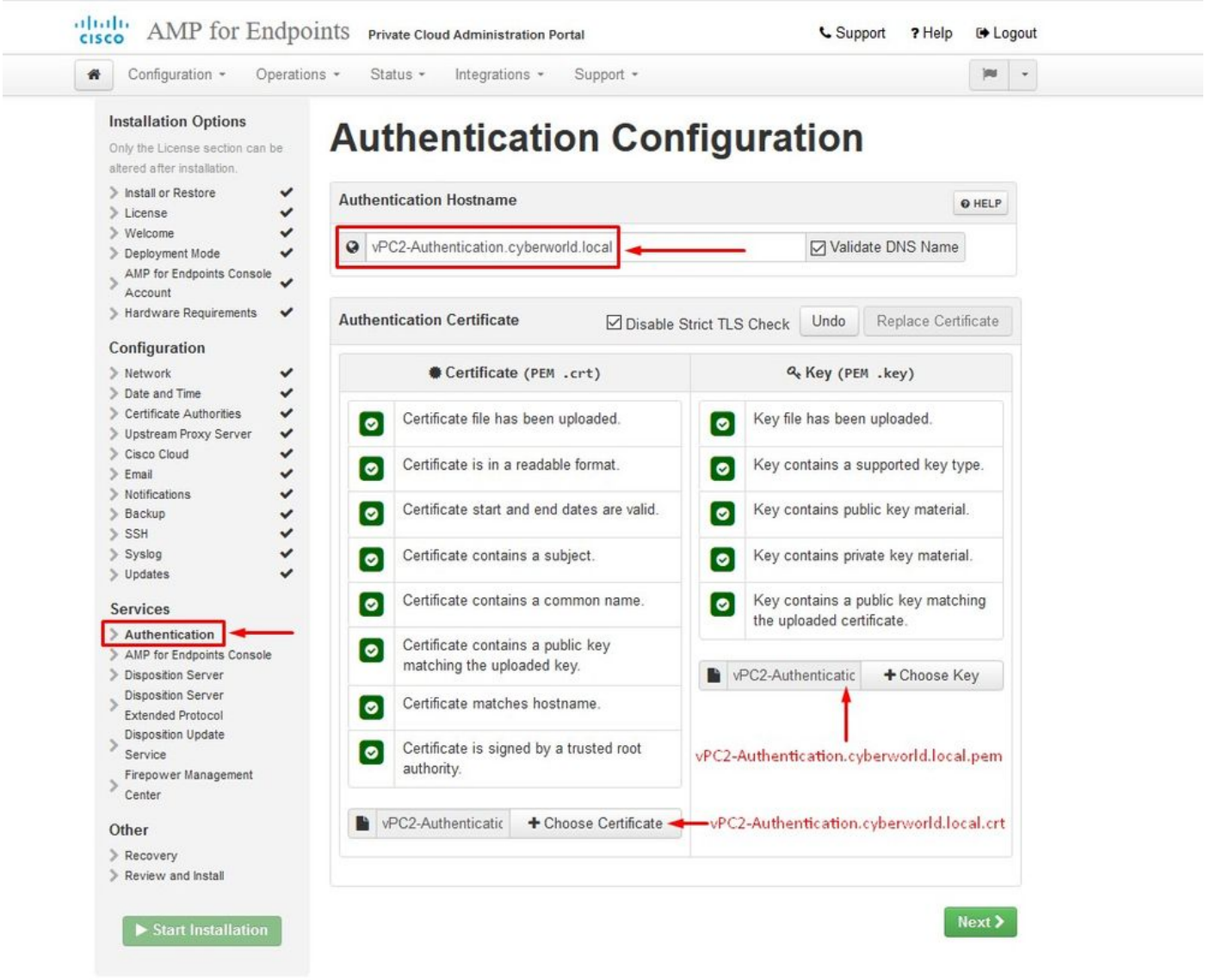
الخطوة 1:

أثناء عملية التكوين، قد يتم تشغيل هذه الأخطاء.

أول "خطأ" قد تلاحظه يتم إبرازه باللون الثالثة. لتجاوز هذا ببساطة إلغاء تحديد تعطيل التحقق الصارم من TLS"



بدون فحص TLS صارم

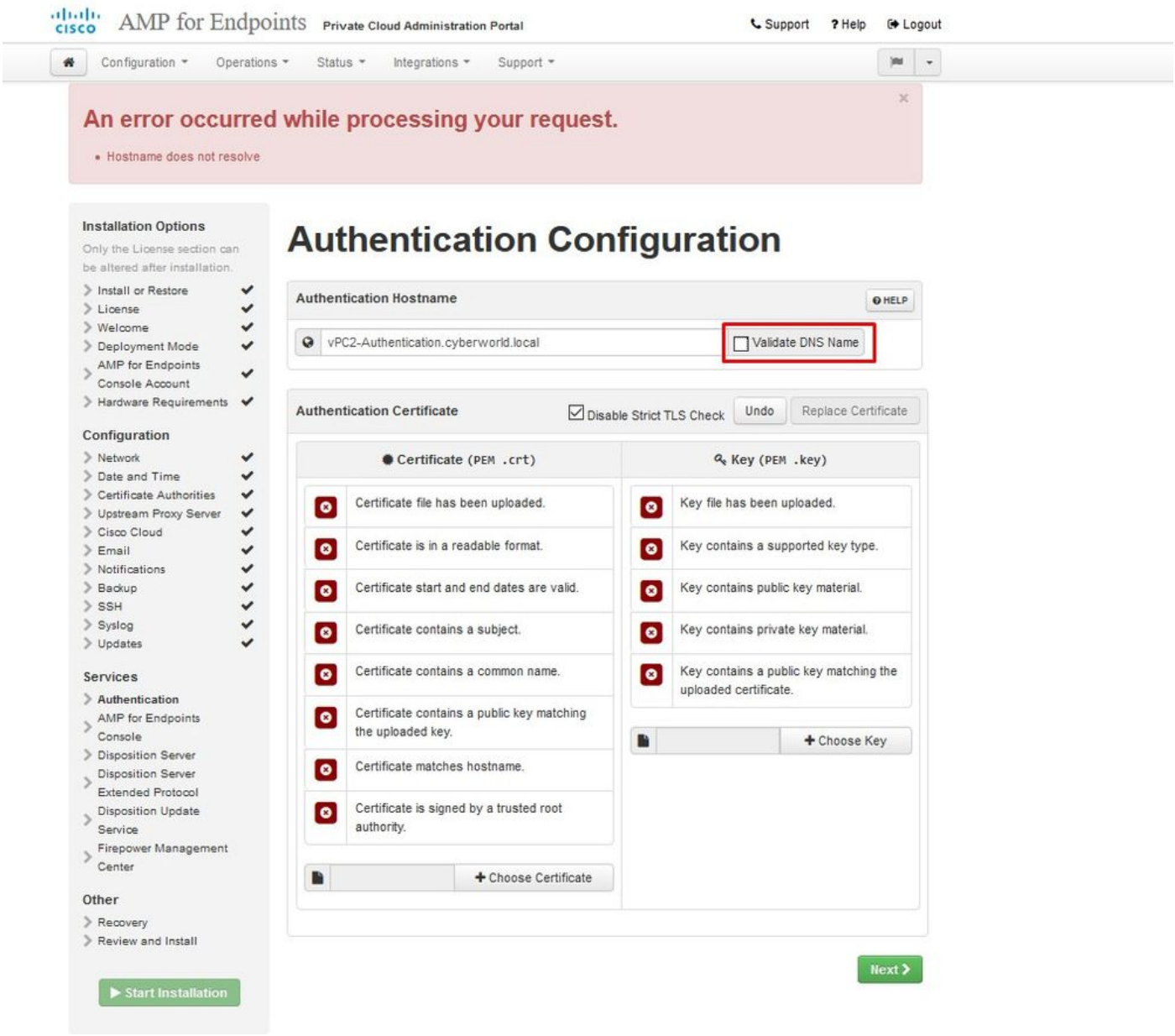


الخطوة 2:

الخطأ التالي الذي تحصل عليه وه إذا تركت التحقق من صحة اسم DNS" محدد. هنا لديك خيارين.

#1: إما أن تقوم بإلغاء تحديد علامة التحقق من صحة DNS

#2: ارجع إلى خادم DNS الخاص بك وقم بتكوين باقي سجلات المضيف الخاصة بك.



الآن كرر نفس العملية خمس مرات أخرى لبقية الشهادات.

المصادقة

- يتم إستخدام خدمة المصادقة في الإصدارات المستقبلية من Private Cloud لمعالجة مصادقة المستخدم.

وحدة التحكم في نقطة النهاية الآمنة

- وحدة التحكم هي اسم DNS حيث يمكن لمسؤول نقطة النهاية الآمنة الوصول إلى وحدة تحكم نقطة النهاية الآمنة ويتلقى موصلات نقطة النهاية الآمنة سياسات وتحديثات جديدة.

خادم المصير النهائي

- Disposition Server هو اسم DNS حيث تقوم موصلات نقطة النهاية الآمنة بإرسال معلومات البحث عن السحابة واستردادها.

خادم المصير النهائي - البروتوكول الموسع

- Disposition Server - البروتوكول الموسع هو اسم DNS حيث تقوم موصلات نقطة النهاية الآمنة الأحدث بإرسال معلومات البحث عن السحابة واستردادها.

خدمة تحديث المصير النهائي

- يتم إستخدام خدمة تحديث المصير النهائي عند ربط جهاز شبكة تهديدات الحماية من Cisco بجهاز الشبكة الخاص بك. يتم إستخدام جهاز شبكة التهديدات لإرسال الملفات للتحليل من وحدة تحكم النقطة الطرفية الآمنة ويتم إستخدام خدمة تحديث المصير النهائي للحصول على قرار (نظيف أو ضار) للملفات بعد تحليلها من قبل شبكة التهديدات لتحديث المصير النهائي.

مركز إدارة Firepower

- يسمح لك الارتباط الخاص بمركز إدارة Firepower بربط جهاز مركز إدارة FirePOWER (FMC) من Cisco بجهاز الشبكة الخاص بك. يتيح لك ذلك عرض بيانات نقطة النهاية الآمنة في FMC. لمزيد من المعلومات حول دمج FMC مع Secure Endpoint راجع وثائق FMC.

⚠ تحذير: لا يمكن تغيير أسماء المضيف بمجرد أن ينتهي الجهاز من التثبيت.

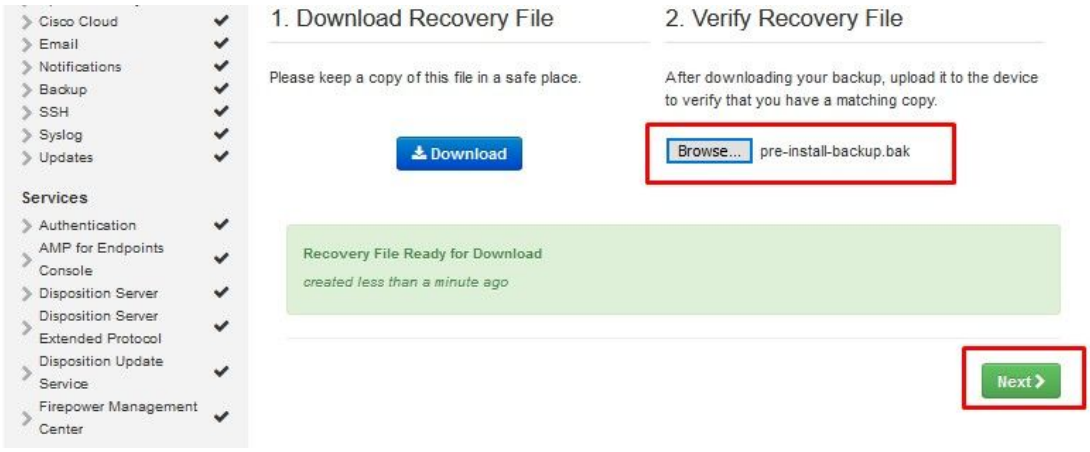
دون أسماء المضيف المطلوبة. يجب إنشاء ست سجلات DNS A فريدة للسحابة الخاصة بنقطة النهاية الآمنة. يشير كل سجل إلى نفس عنوان IP الخاص بواجهة وحدة تحكم النقطة الآمنة. يجب حل من قبل كل من السحابة الخاصة ونقطة السحابة الظاهرية (ETH1) النهاية الآمنة.

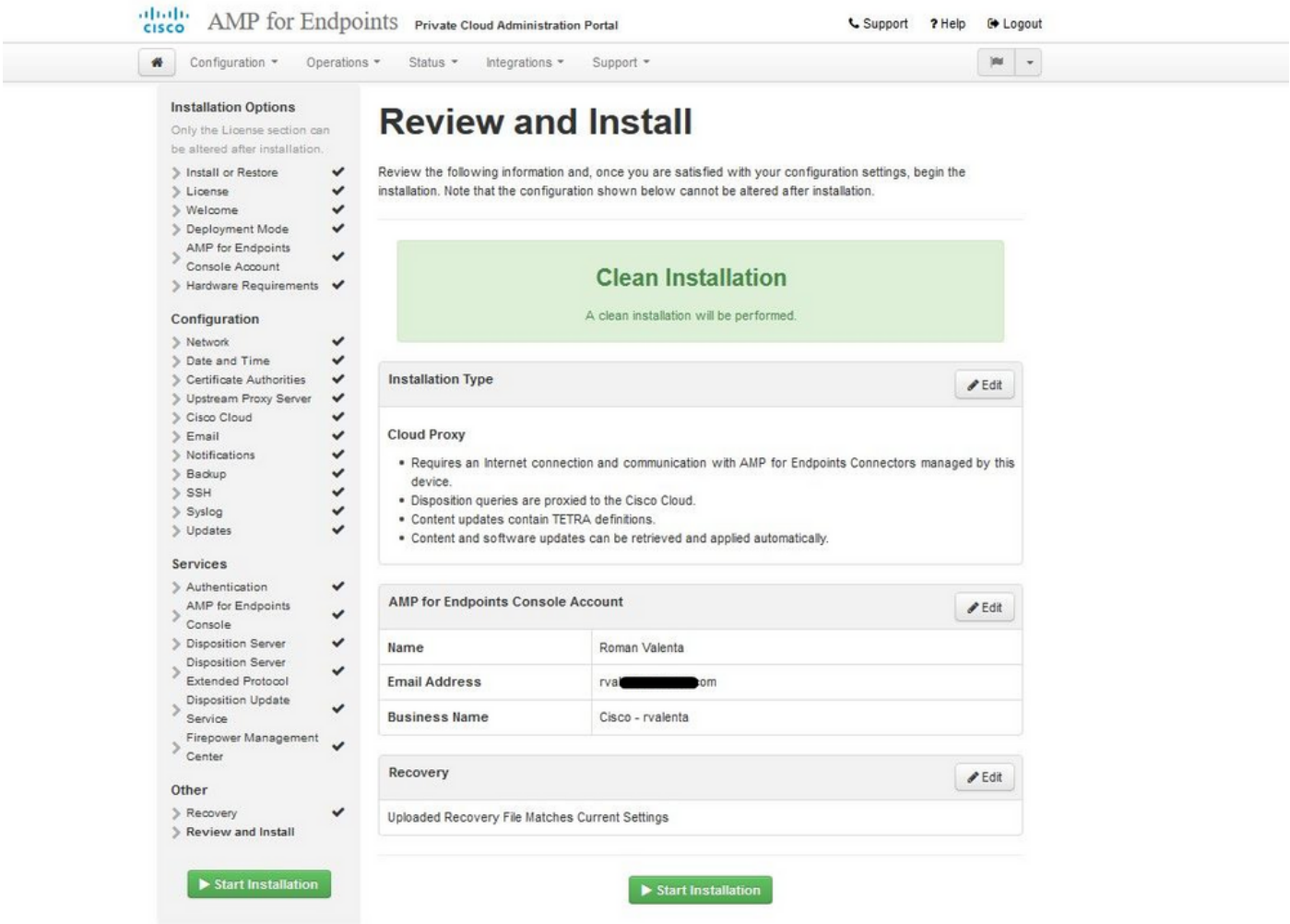
الخطوة 3:

في الصفحة التالية، قم بتنزيل ملف الاستدراد ثم التحقق منه.

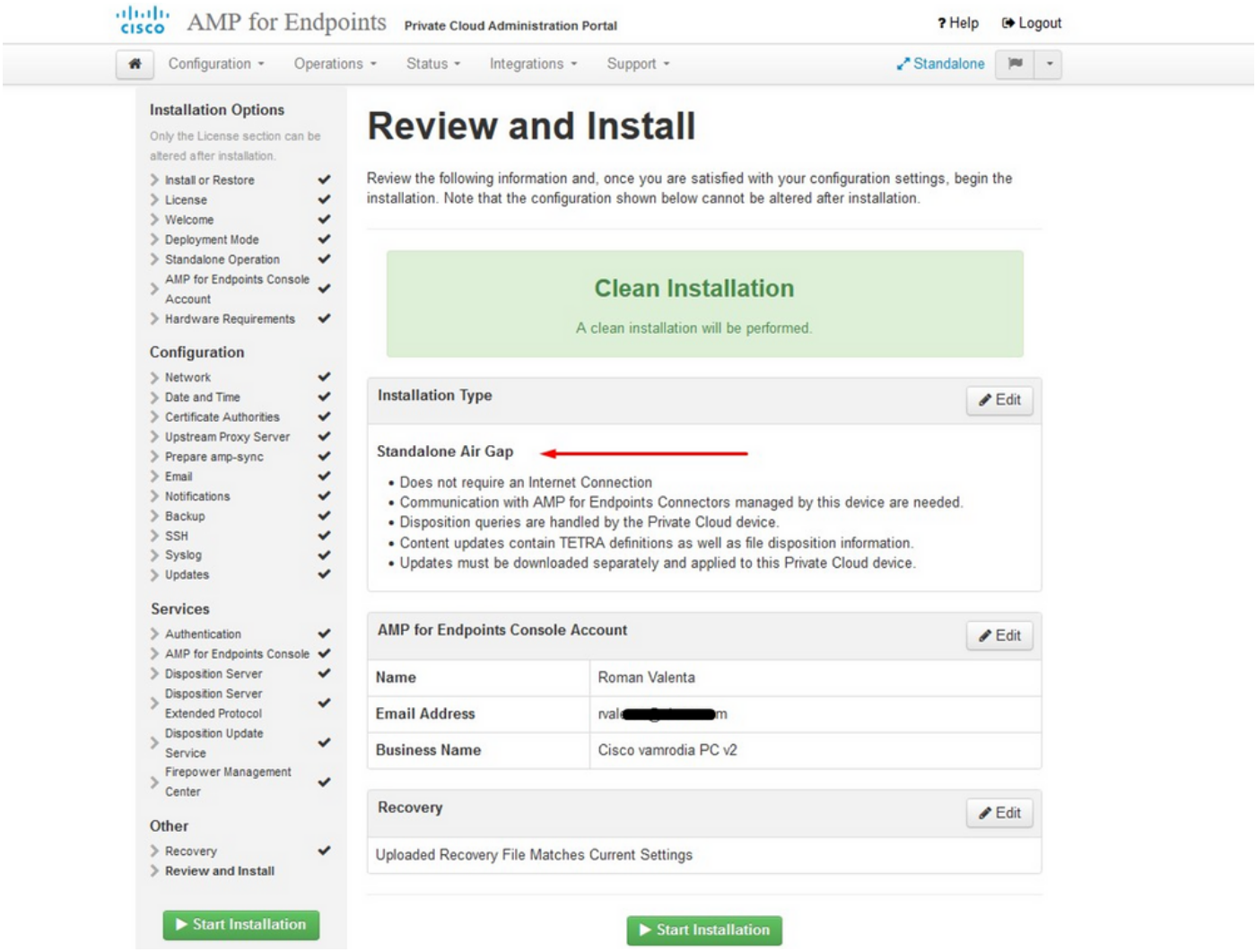
تحصل على صفحة الاستدراد، كما هو موضح في الصورة. يجب تنزيل نسخة إحتياطية من التكوين الخاص بك والتحقق من ذلك قبل بدء التثبيت. يحتوي ملف الاستدراد على جميع الخادم. إذا فقدت ملف إستدراد، فلن تتمكن من إستعادة التكوين بالإضافة إلى مفاتيح موصلات نقطة النهاية الآمنة. بدون مفاتيح التكوين الخاص بك ويجب إعادة تثبيت جميع الأساسية للسحابة الخاصة بالكامل باستخدام مفاتيح أصلي، يجب إعادة تكوين البنية جديدة. يحتوي ملف الاستدراد على جميع التكوينات المتعلقة بمدخل OpenAdmin. يحتوي ملف النسخ الاحتياطي على محتويات ملف الاستدراد بالإضافة إلى أي بيانات خاصة بوابات الحماية المعلومات مثل الأحداث ومحفوظات الموصل وما إلى ذلك. إذا كنت ترغب في إستعادة OpenAdmin فقط بدون بيانات الحدث وكل شيء، يمكنك إستخدام ملف الاستدراد. في حالة الاستعادة من ملف النسخة الاحتياطية، يتم بعد ذلك إستعادة بيانات مدخل الحماية المعلومات والمستخدمين.

حدد على التنزيل لحفظ النسخة الاحتياطية على الكمبيوتر المحلي. بمجرد تنزيل الملف، حدد على إختيار ملف لتحميل ملف النسخ الاحتياطي والتحقق من أنه غير تالف. حدد على التالي للتحقق من الملف ومتابعته.


Cisco Cloud
Email
Notifications
Backup
SSH
Syslog
Updates
Services
Authentication
AMP for Endpoints Console
Disposition Server
Disposition Server Extended Protocol
Disposition Update Service
Firepower Management Center
1. Download Recovery File
Please keep a copy of this file in a safe place.
Download
2. Verify Recovery File
After downloading your backup, upload it to the device to verify that you have a matching copy.
Browse...
pre-install-backup.bak
Recovery File Ready for Download
created less than a minute ago
Next


AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
AMP for Endpoints Console Account
Hardware Requirements
Configuration
Network
Date and Time
Certificate Authorities
Upstream Proxy Server
Cisco Cloud
Email
Notifications
Backup
SSH
Syslog
Updates
Services
Authentication
AMP for Endpoints Console
Disposition Server
Disposition Server Extended Protocol
Disposition Update Service
Firepower Management Center
Other
Recovery
Review and Install
Start Installation
Review and Install
Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.
Clean Installation
A clean installation will be performed.
Installation Type
Edit
Cloud Proxy
Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
Disposition queries are proxied to the Cisco Cloud.
Content updates contain TETRA definitions.
Content and software updates can be retrieved and applied automatically.
AMP for Endpoints Console Account
Edit
Name
Roman Valenta
Email Address
rva[redacted]om
Business Name
Cisco - rvalenta
Recovery
Edit
Uploaded Recovery File Matches Current Settings
Start Installation

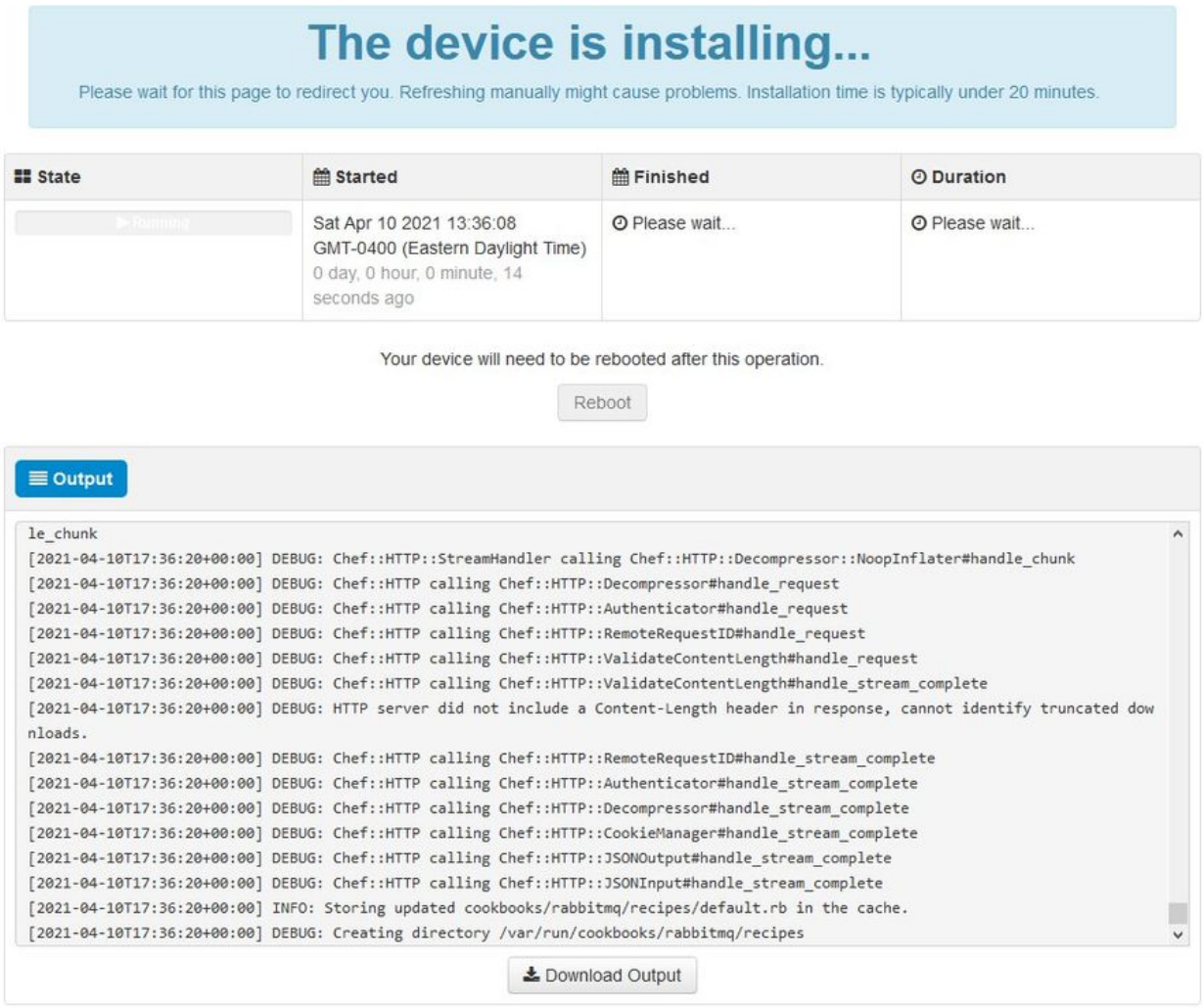
⩔⩔ Airgap ⩔⩔ طوق



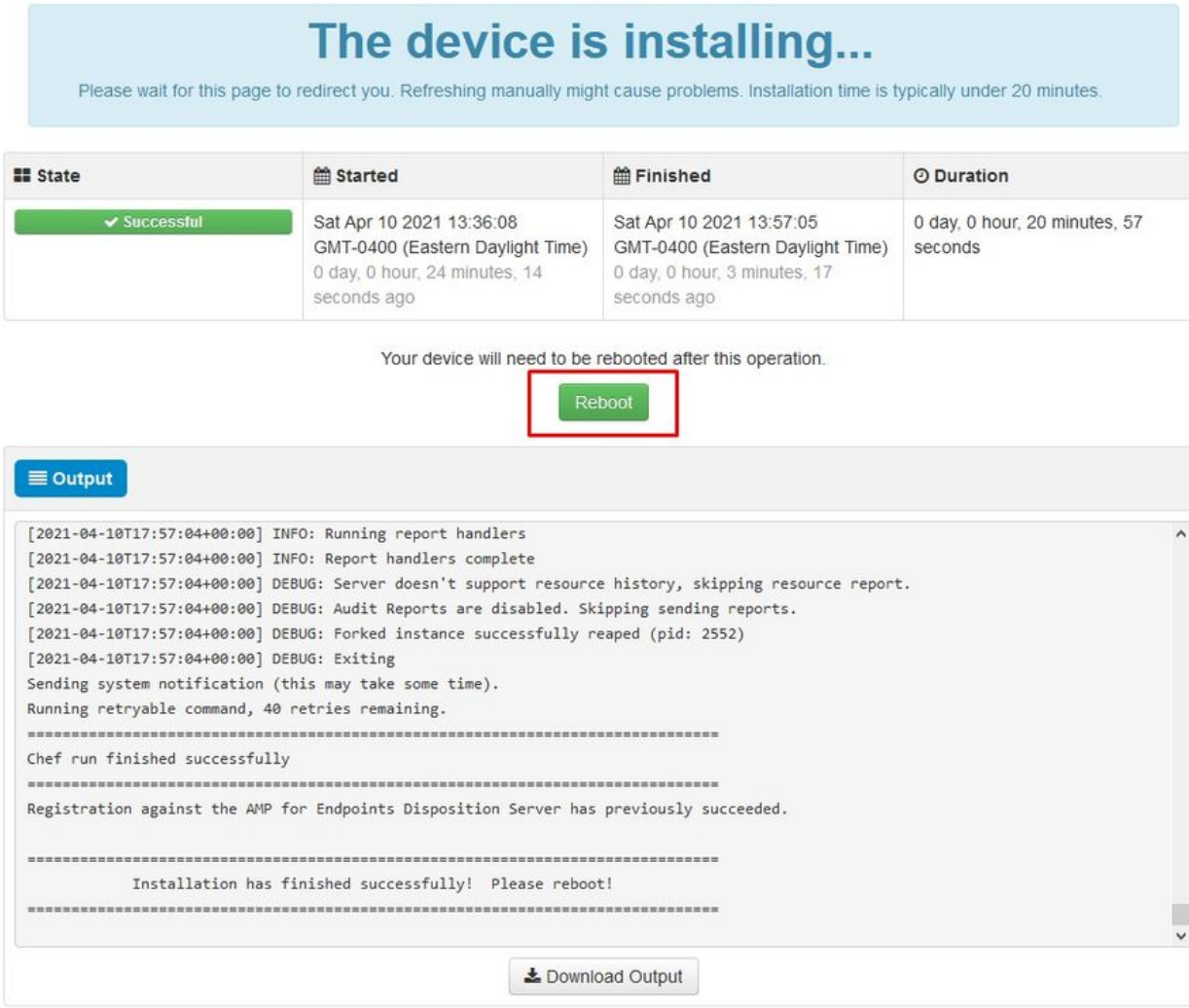
فقط ≪ ≪ Airgap ≪ ≪

ترى مدخلات مماثلة مثل هذه...

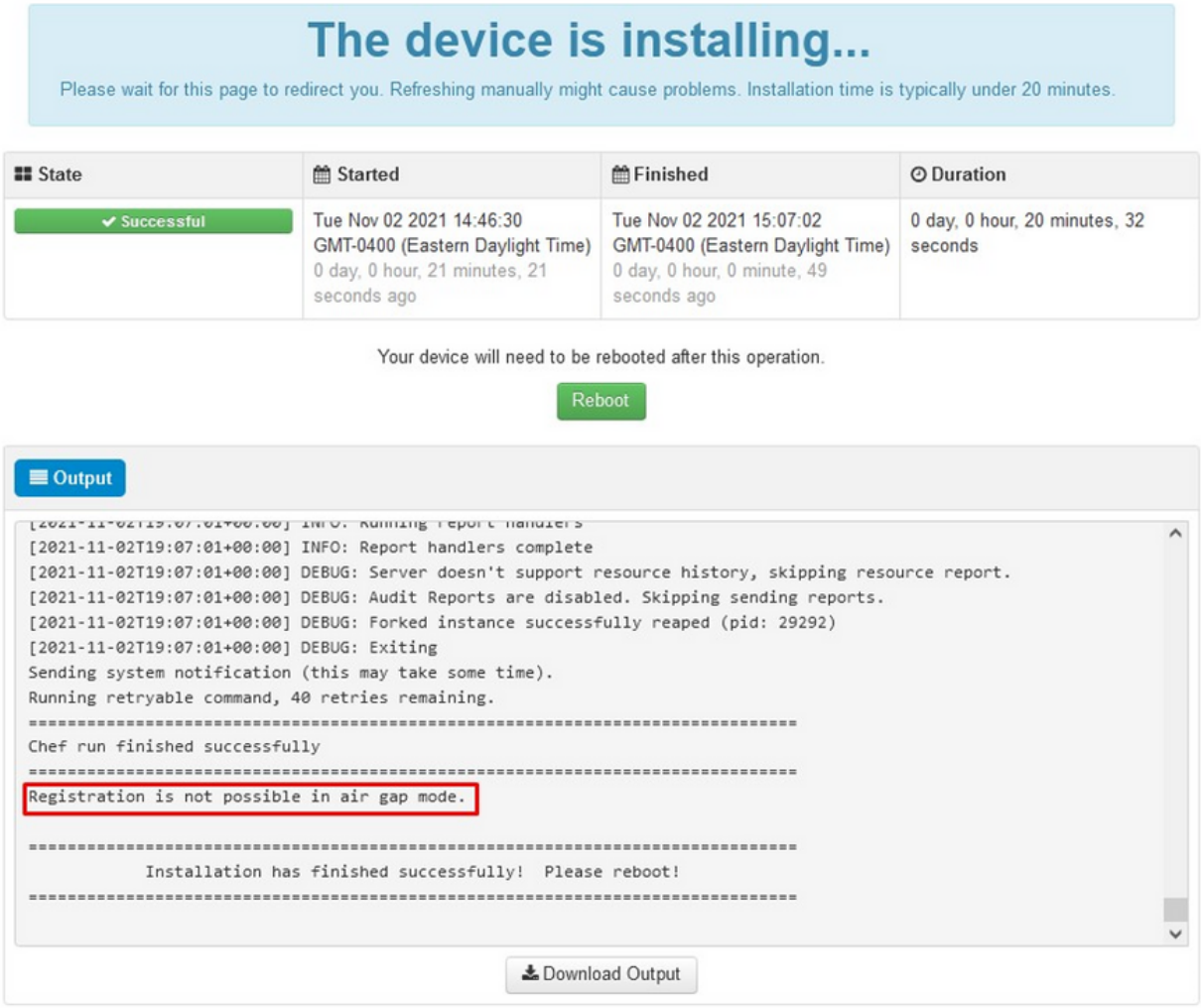
⚠ تحذير: عند وجودك في هذه الصفحة لا تقم بالتحديث لأنه قد يتسبب في حدوث مشاكل.



بمجرد الانتهاء من التثبيت اضغط على زر إعادة التشغيل

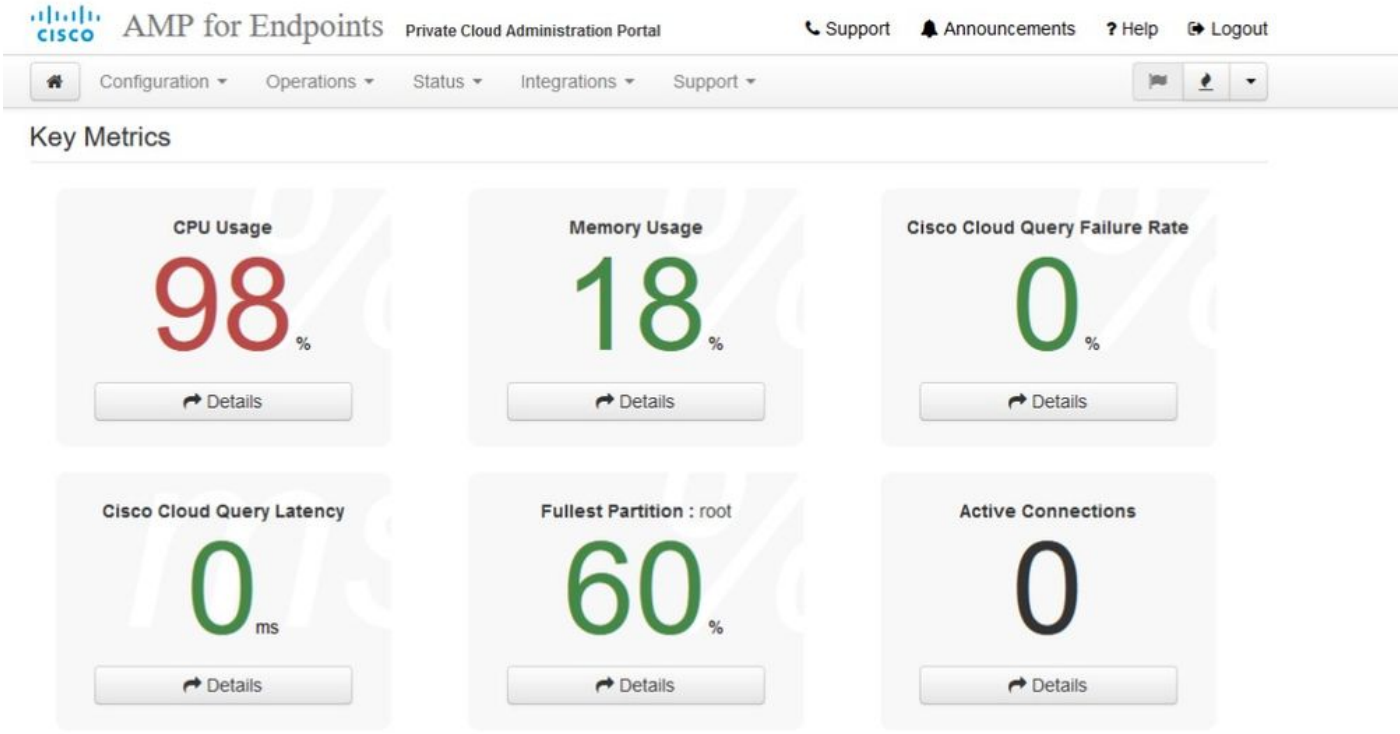

The device is installing...
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.
State
Started
Finished
Duration
Successful
Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time)
0 day, 0 hour, 24 minutes, 14 seconds ago
Sat Apr 10 2021 13:57:05 GMT-0400 (Eastern Daylight Time)
0 day, 0 hour, 3 minutes, 17 seconds ago
0 day, 0 hour, 20 minutes, 57 seconds
Your device will need to be rebooted after this operation.
Reboot
Output
[2021-04-10T17:57:04+00:00] INFO: Running report handlers
[2021-04-10T17:57:04+00:00] INFO: Report handlers complete
[2021-04-10T17:57:04+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-04-10T17:57:04+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-04-10T17:57:04+00:00] DEBUG: Forked instance successfully reaped (pid: 2552)
[2021-04-10T17:57:04+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
Chef run finished successfully
Registration against the AMP for Endpoints Disposition Server has previously succeeded.
Installation has finished successfully! Please reboot!
Download Output

⩔⩔ Airgap ⩔⩔ طق ف

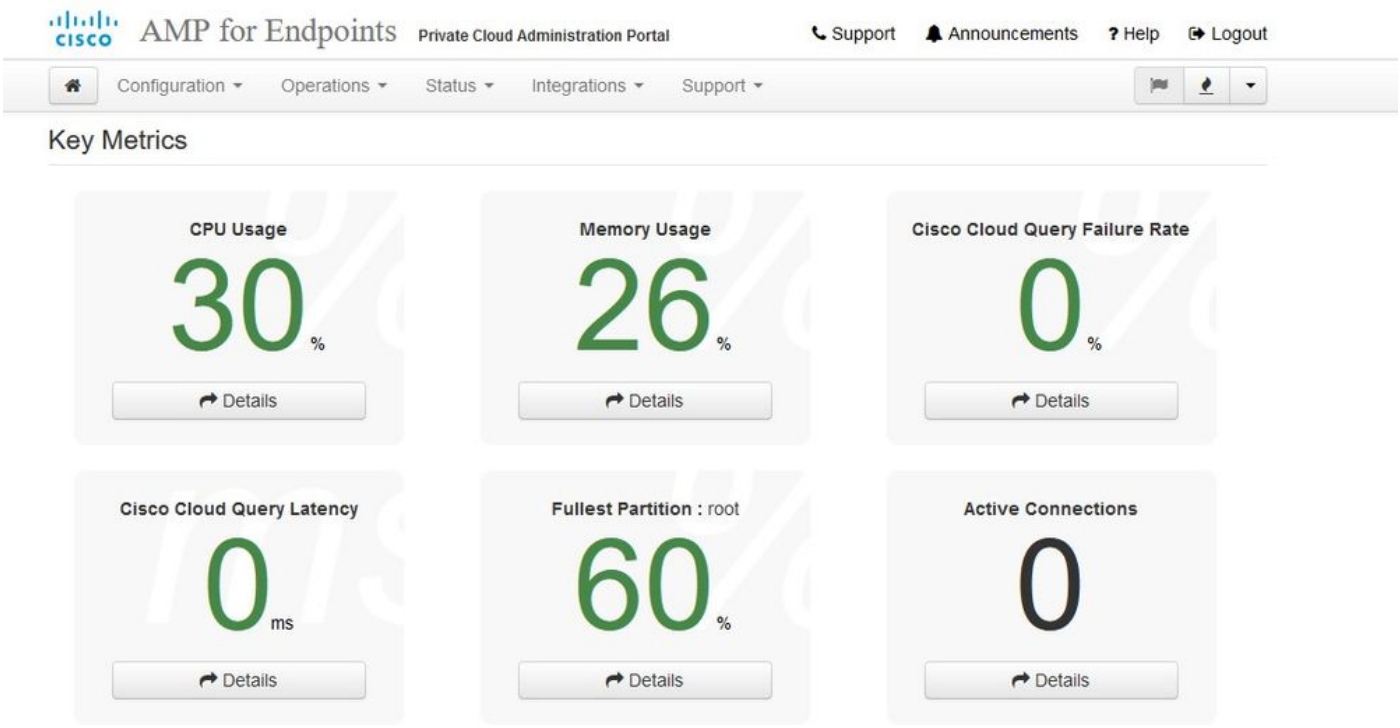


فقط Airgap

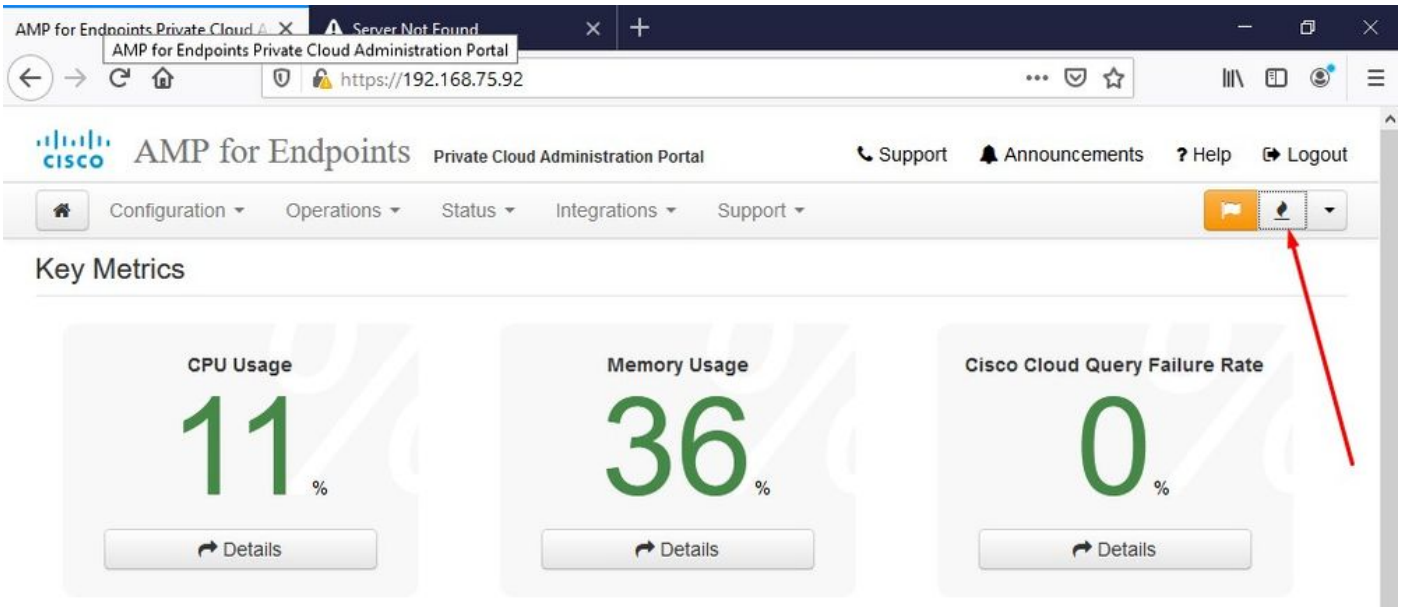
بمجرد تمهيد الجهاز بالكامل، يتم تقديم لوحة المعلومات هذه في المرة التالية التي تقوم فيها بتسجيل الدخول باستخدام واجهة المسؤول الخاصة بك. قد تلاحظ إرتفاع في المعالج في البداية، لكن إذا أعطيت بضع دقائق، فإنه يستقر.



بعد دقائق قليلة...

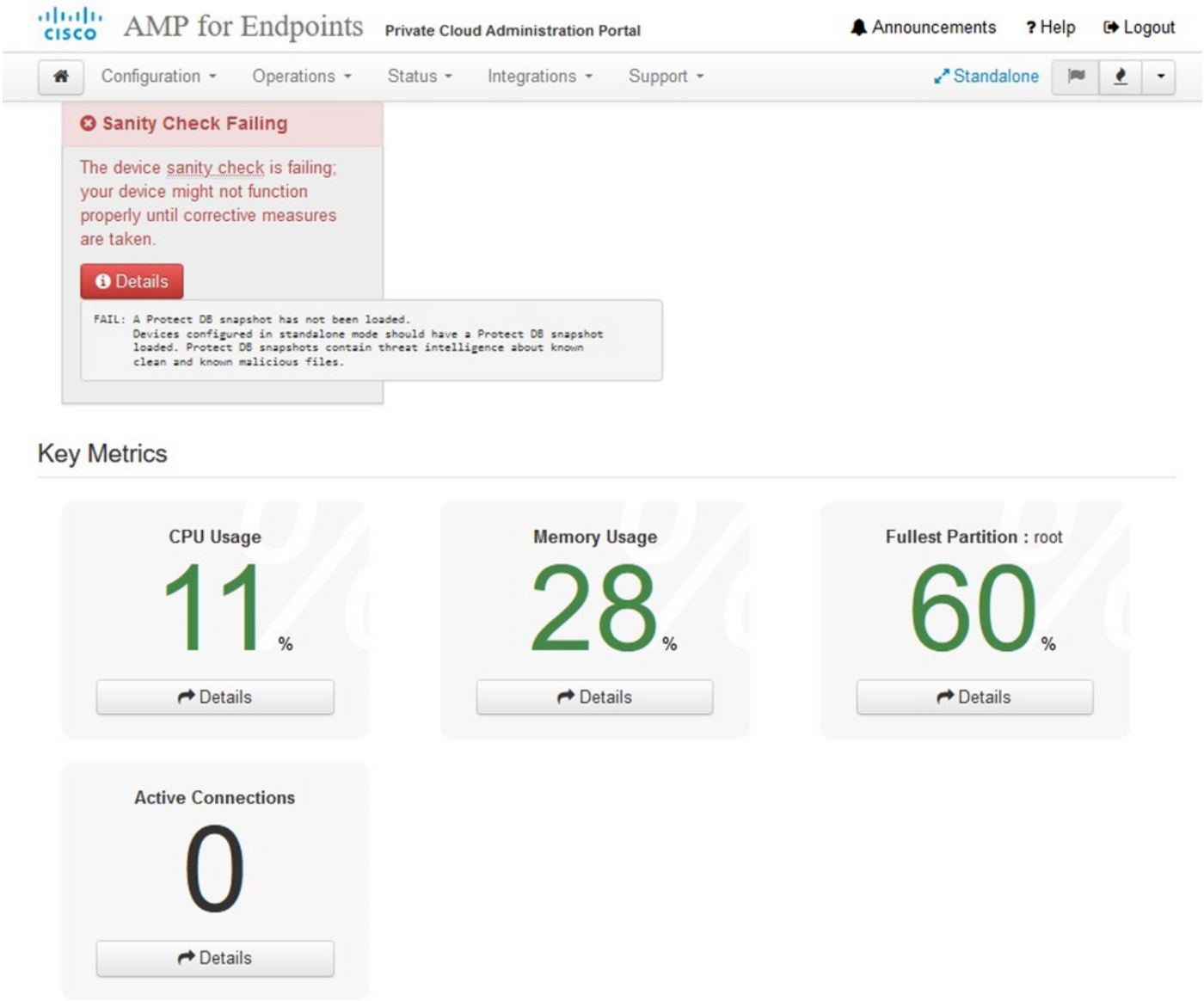


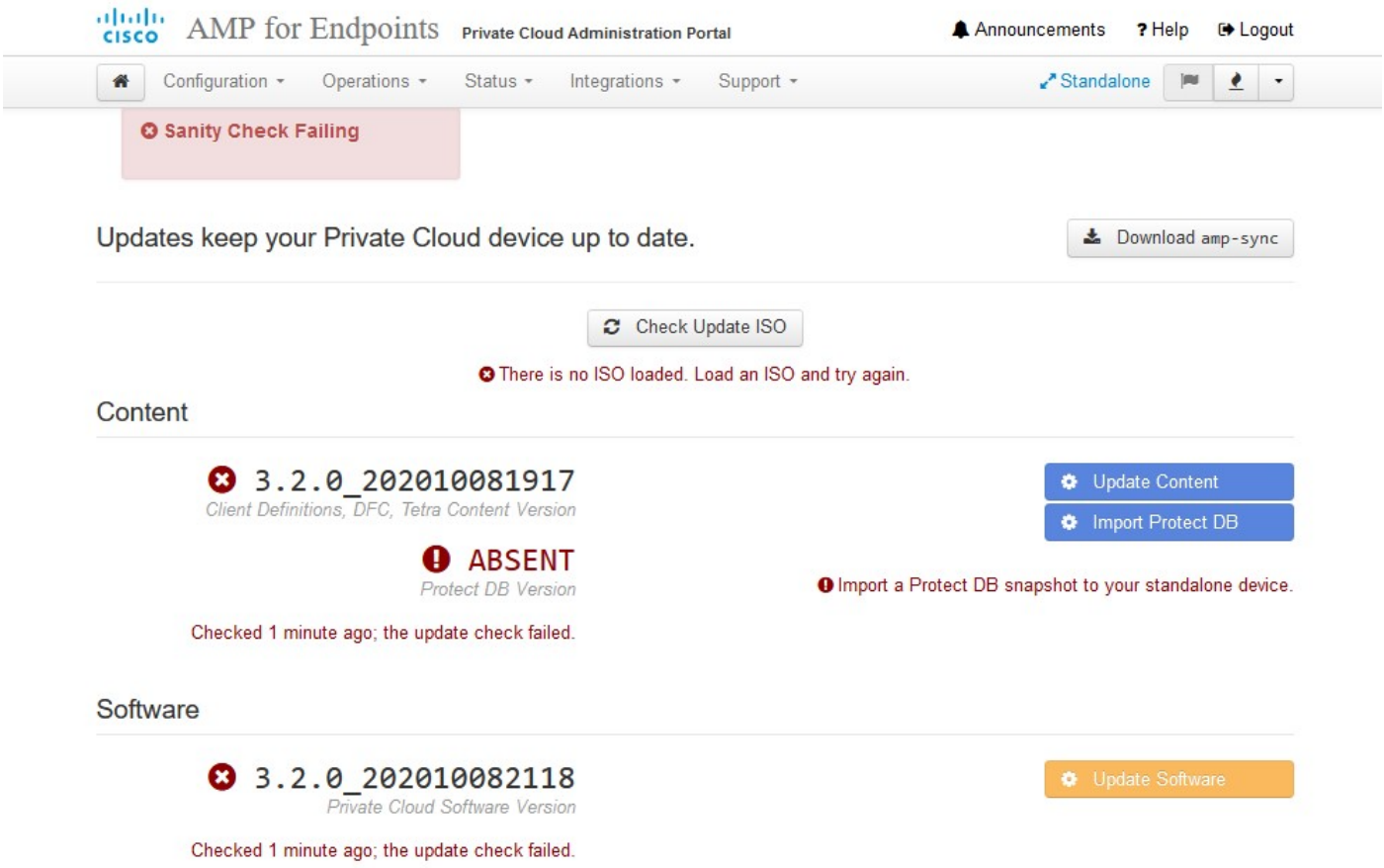
من هنا تقوم بالتنقل إلى وحدة تحكم نقطة النهاية الآمنة. انقر على الأيقونة الصغيرة التي تبدو مثل النار في الزاوية اليمنى بجوار العلم.



⩔⩔ Airgap ⩔⩔ فقط

كما ترى، فشلنا في التحقق من الصحة بسبب حماية لقطة DB، وأيضا بسبب تعريفات العميل و DFC و Tetra. يجب القيام بذلك عن طريق التحديث دون اتصال بالإنترنت عبر ملف ISO الذي تم تنزيله وتم إعداده مسبقا من خلال AMP-Sync وتحميله إلى الجهاز الظاهري (VM) وأ تخزينه في موقع NFS.


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
Sanity Check Failing
The device sanity check is failing; your device might not function properly until corrective measures are taken.
Details
FAIL: A Protect DB snapshot has not been loaded.
Devices configured in standalone mode should have a Protect DB snapshot loaded. Protect DB snapshots contain threat intelligence about known clean and known malicious files.
Key Metrics
CPU Usage
11 %
Details
Memory Usage
28 %
Details
Fullest Partition : root
60 %
Details
Active Connections
0
Details



حزمة تحديث AirGap

للمرة الأولى علينا إستخدام هذا الأمر لاستلام قاعدة بيانات الحماية

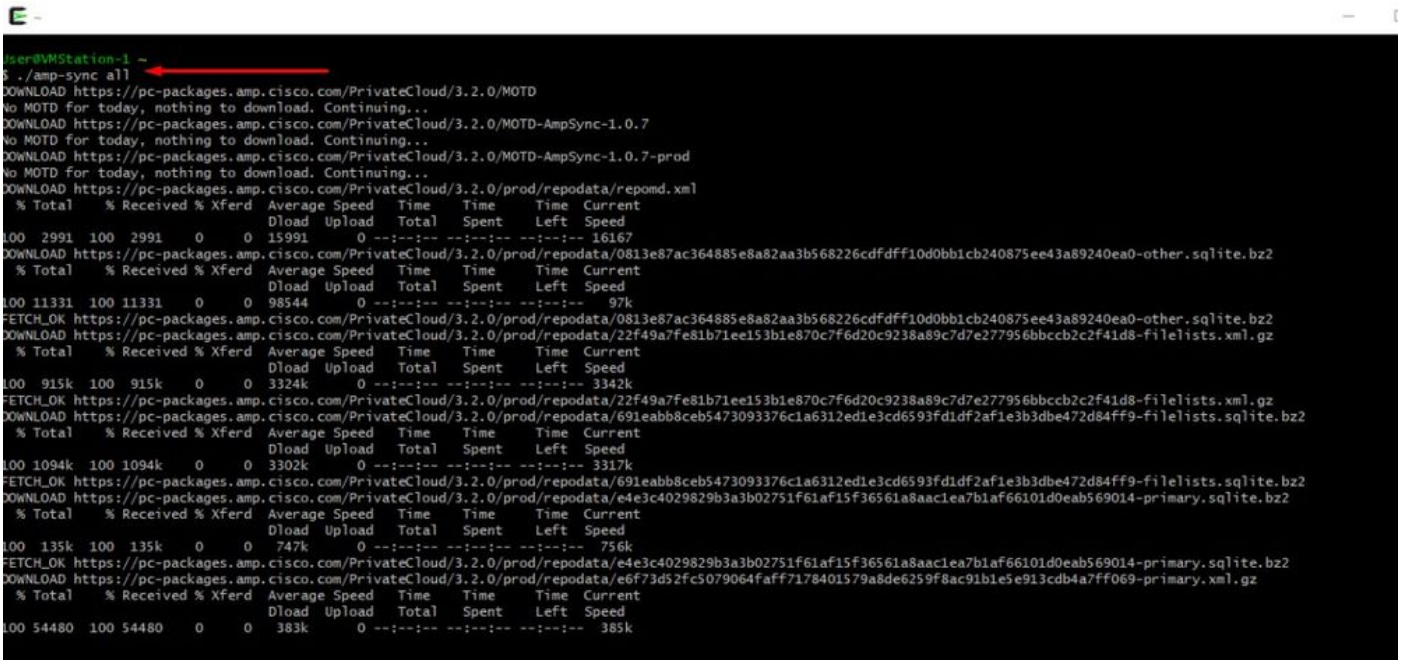
```
./amp-sync all
```

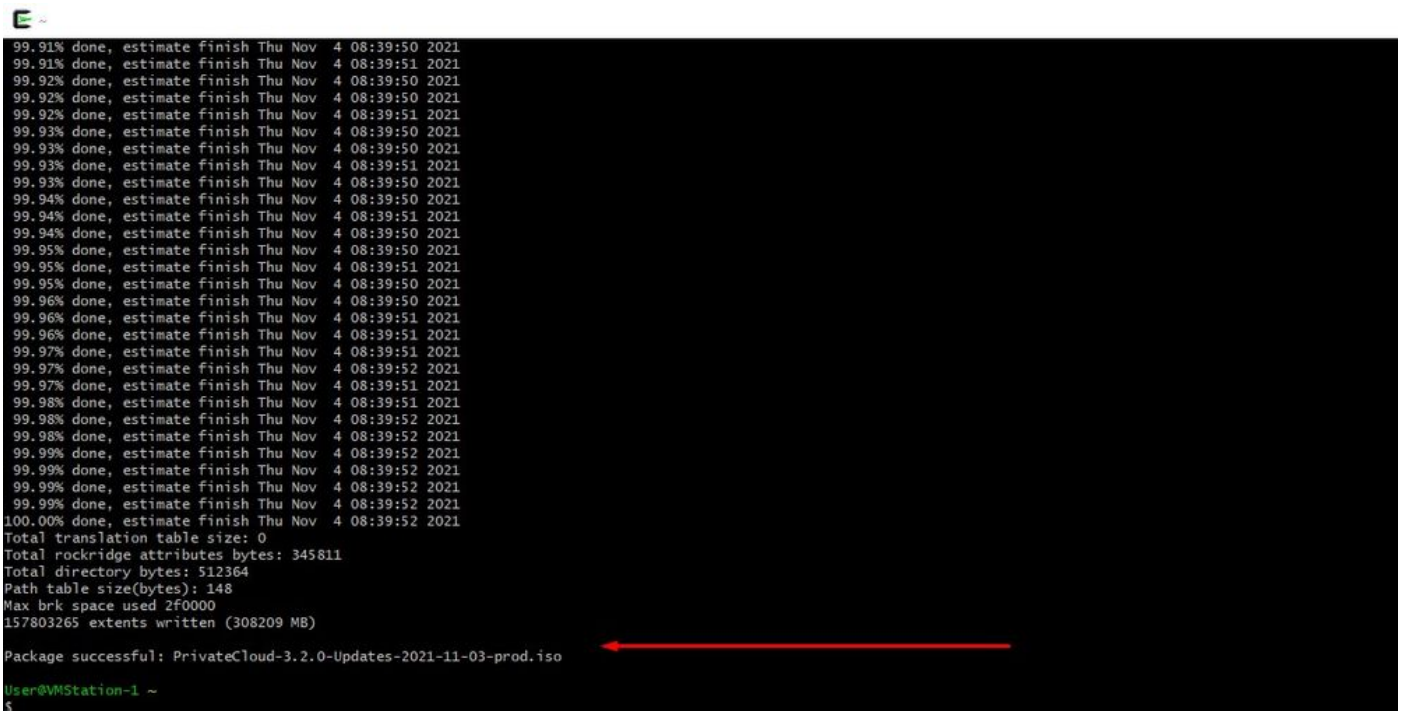
ملاحظة: قم بتنزيل جميع الحزم عبر هذا الأمر ثم تحقق من أنه يمكن أن يستغرق أكثر من 24 ساعة. تعتمد على السرعة وجودة الارتباط. في حالتي مع ألياف 1Gig الى الأمر يستغرق 25 ساعة تقريبا للاكتمال. ويرجع هذا أيضا جزئيا إلى حقيقة أن هذا التنزيل يتم مباشرة من AWS وبالتالي يتم تخريبه. أخيرا لاحظ أن هذا التحميل كبير. كان الملف الذي تم تنزيله في حالتي تبلغ سعته 323 جيجابايت. صفر

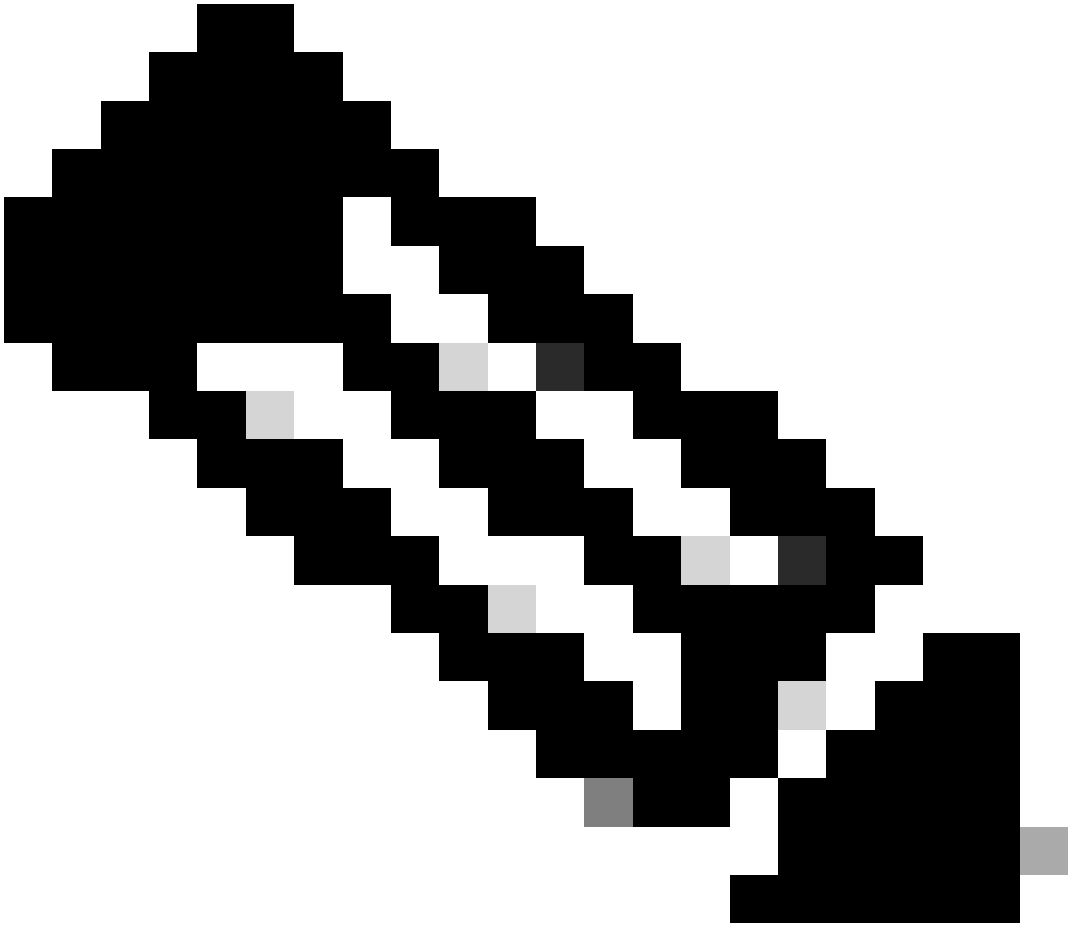
في هذا المثال إستخدمنا CygWin64

1. تنزيل الإصدار x64 من Cygwin وتثبيته.
2. قم بتشغيل setup-x86_64.exe وانتقل خلال عملية التثبيت أختر جميع الإعدادات الافتراضية.
3. أختر مرآة للتنزيل.
4. حدد حزم لتثبيتها:

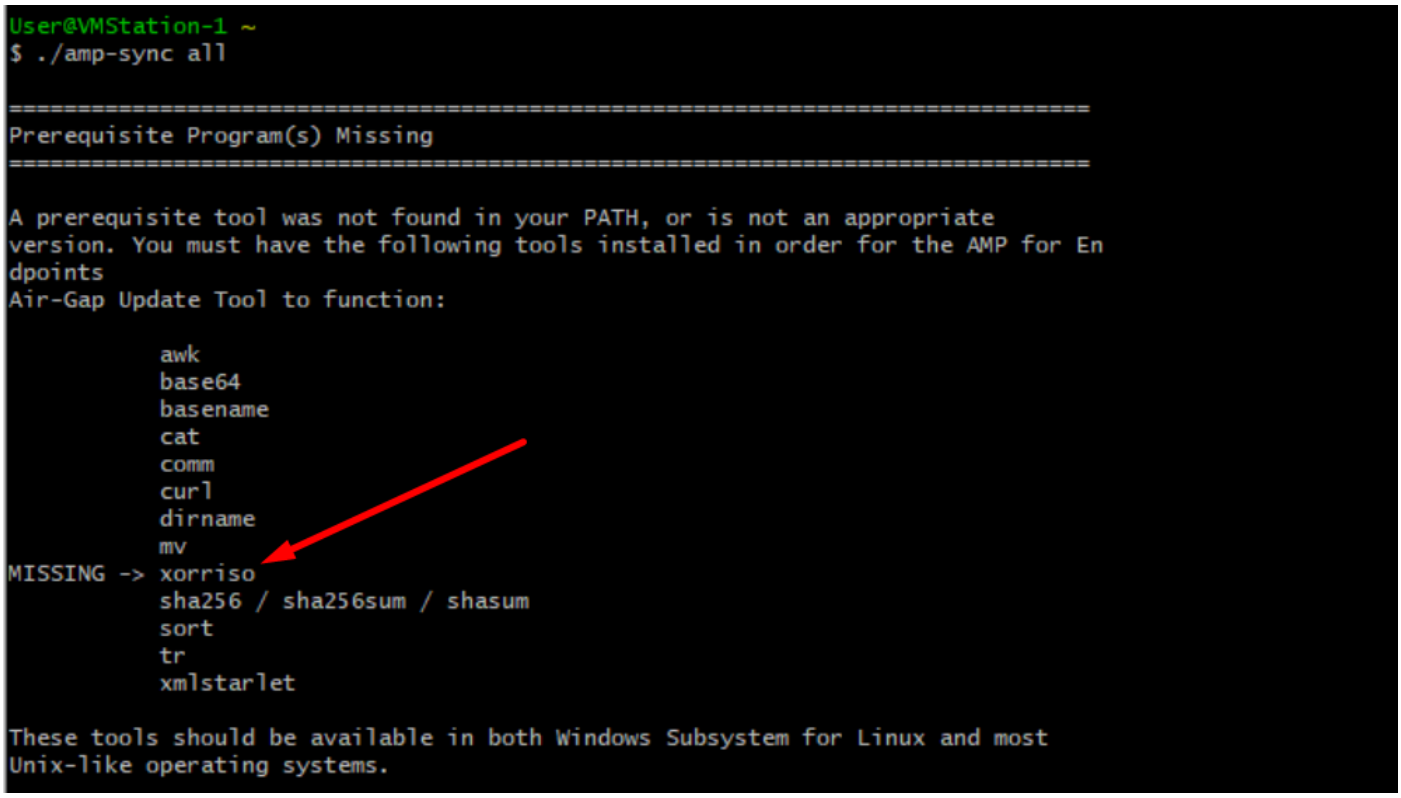
all -> Net -> Curl
All -> Utils -> Genisoimage
all -> utils -> xmlstarlet
* VPC 3.8.x up - > xorriso







ملاحظة: في أحدث تحديث VPC 3.8.x مع CygWin64 كأداة التنزيل الرئيسية يمكنك مواجهة هذه المشكلة الموضحة أدناه.



ملاحظة الإصدار الصفحة رقم 58. وكما ترون الآن فإن الكسوريس" مطلوبة. غيرنا تنسيق ISO إلى ISO 9660 وأن التبعية هي ما يحول الصورة إلى التنسيق المناسب حتى يمكن إكمال التحديث. ولسوء الحظ، لا يقدم CygWin64 xorriso في أي من المستودعات المدمجة الخاصة به. ومع ذلك، فبالنسبة لأولئك الذين ما زالوا يرغبون في إستخدام CygWin64، هناك طريقة للتغلب على هذه المسألة.

Installing dependencies

CentOS

To run amp-sync you will first have to install EPEL, xorriso, and xmlstarlet.

1. Enable the EPEL repo.

```
> sudo yum install epel-release
```

2. Install dependencies via yum.

```
> sudo yum install xorriso
> sudo yum install xmlstarlet
```

Ubuntu

To run amp-sync you will first have to install xorriso and xmlstarlet.

- Install dependencies via apt.

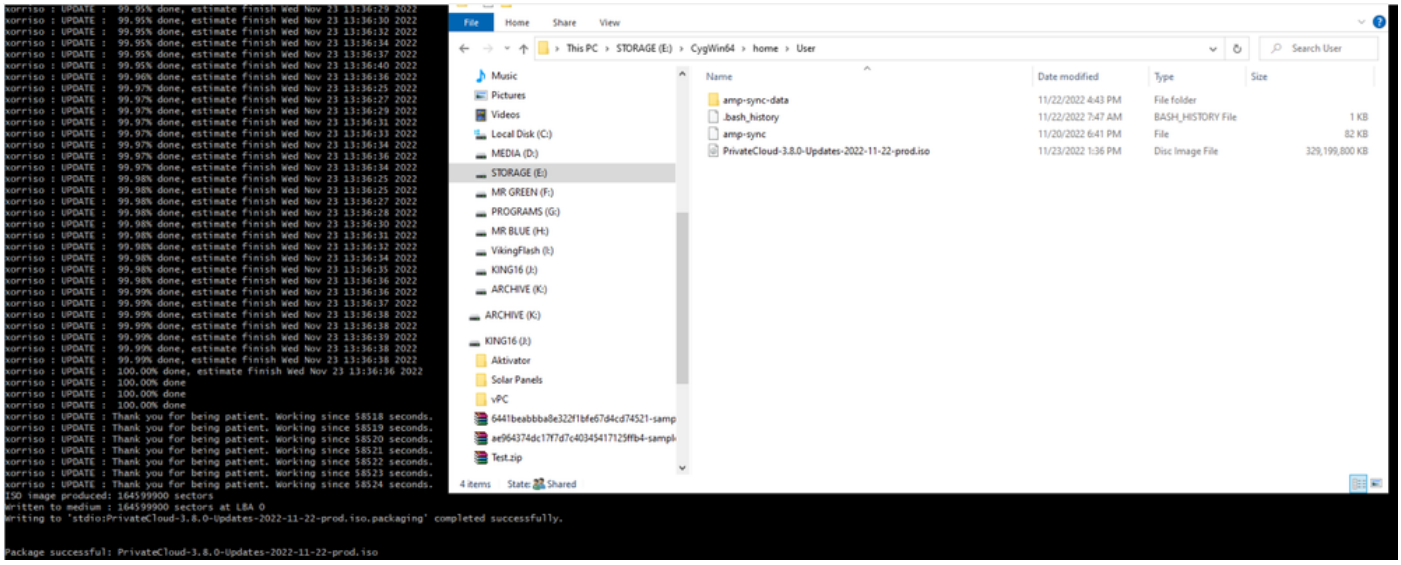
```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

Windows

1. Set up Windows Subsystem for Linux (WSL) with the Ubuntu distribution. See the Microsoft documentation for details.
2. Expand the WSL virtual hard disk size to comply with minimum free disk space. See the Microsoft documentation for details.
3. Install xorriso and xmlstarlet dependencies via apt.

```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

لتتمكن من إستخدام CygWin مرة أخرى، يجب تنزيل xorriso يدويا من مستودع GitHub. افتح المستعرض واكتب <Latest xorriso.exe 1.5.2 بناء مسبق ل Windows> يجب أن يظهر كأول إرتباط يسمى <PeyTy/xorriso-exe-for-windows - GitHub> انتقل إلى صفحة GitHub هذه وقم بتنزيل ملف <xorriso-exe-for-windows-master.zip> داخل ملف zip الذي تجده بين ملفات أخرى قليلة تسمى <xorriso.exe> انسخ هذا الملف والصقه إلى <CygWin64\bin مسار تثبيت Cyg المحلي. حاول مرة أخرى تشغيل الأمر <amp-sync>. يجب أن لا ترى رسالة الخطأ بعد الآن وتنزيل البدء والانتهاء كما هو موضح في الصورة.

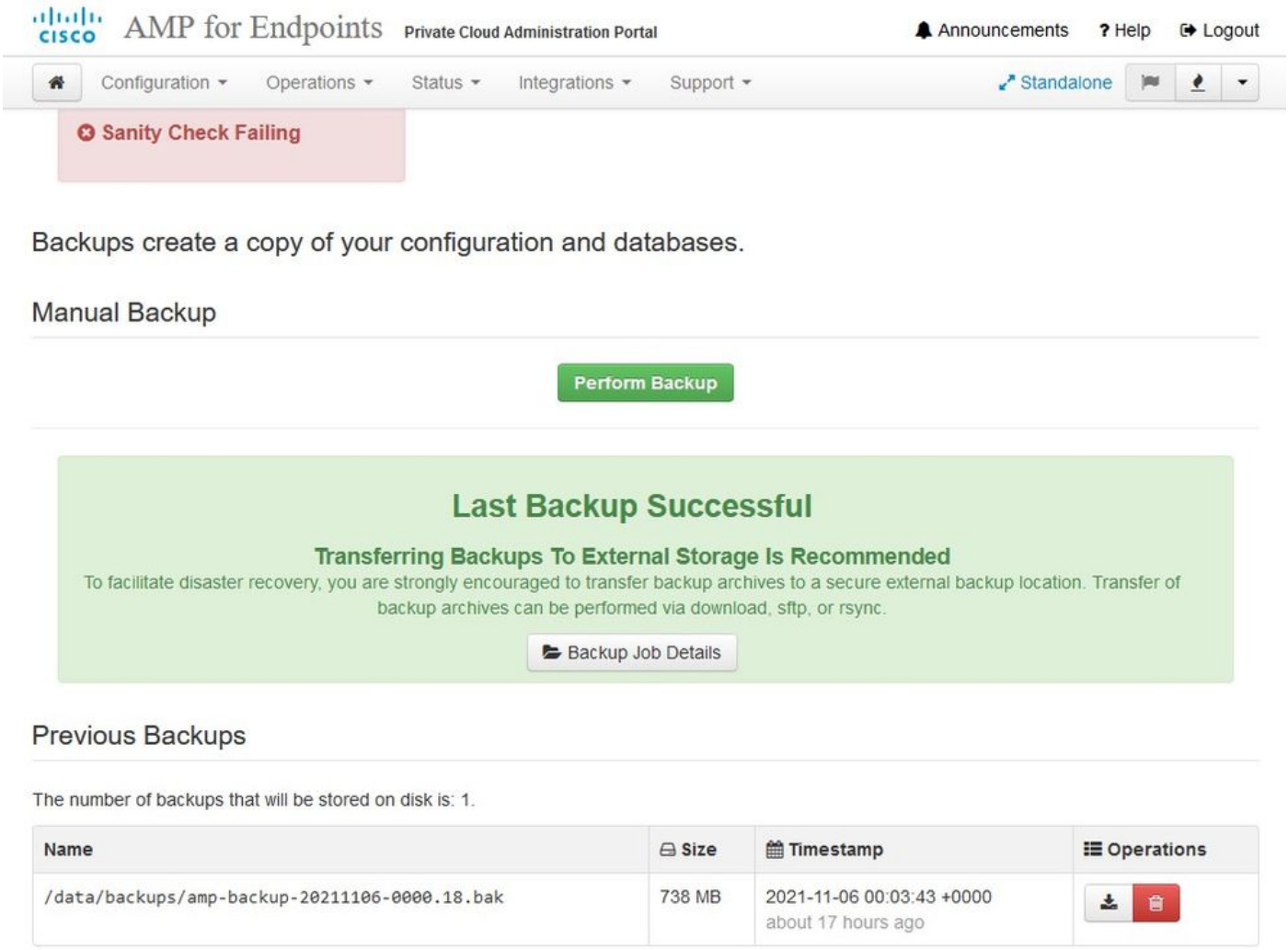


قم بإجراء النسخ الاحتياطي للتيار (في هذه الحالة) 3.2.0 VPC في وضع Airgap.

أنت يستطيع استعملت هذا أمر من CLI

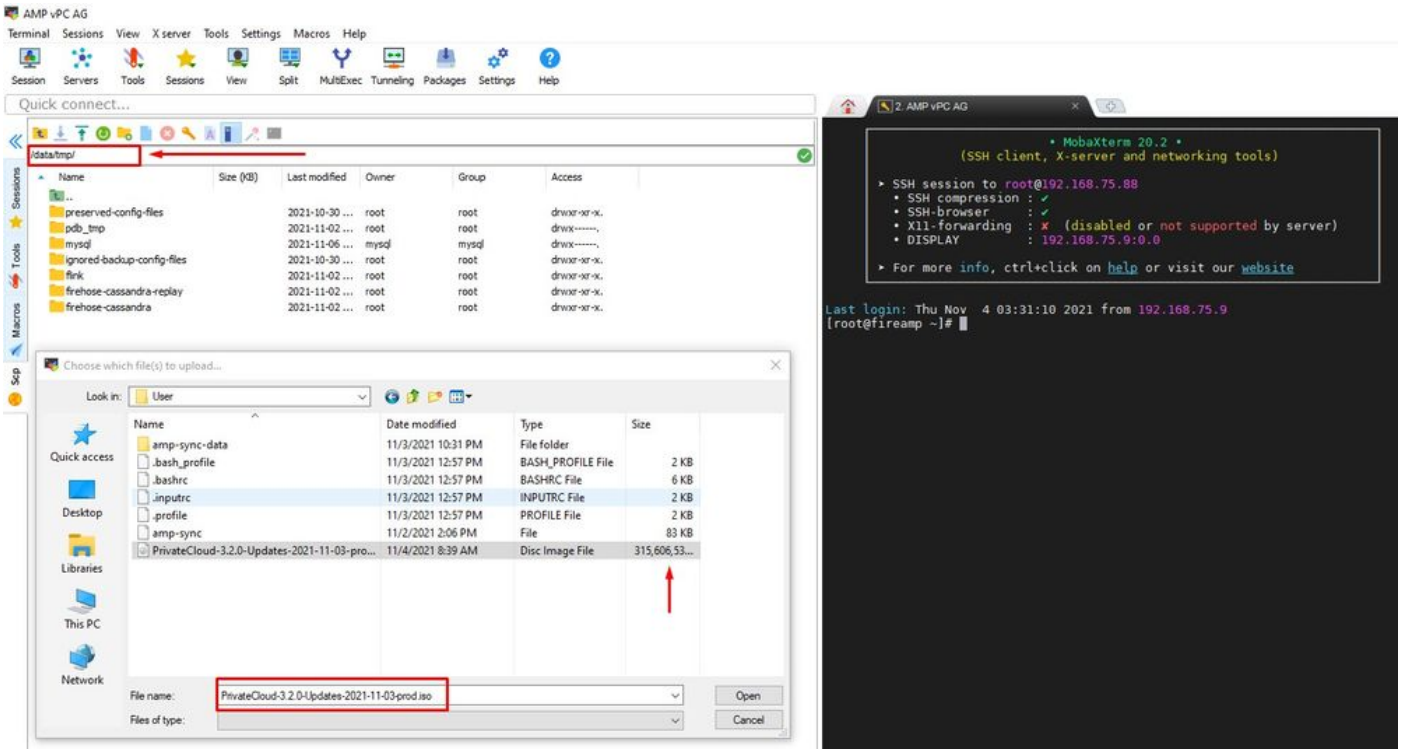
```
rpm -qa | grep Pri
```

أو يمكنك أيضا التنقل إلى العمليات > النسخ الاحتياطية، كما هو موضح في الصورة وإجراء النسخ الاحتياطي هناك.



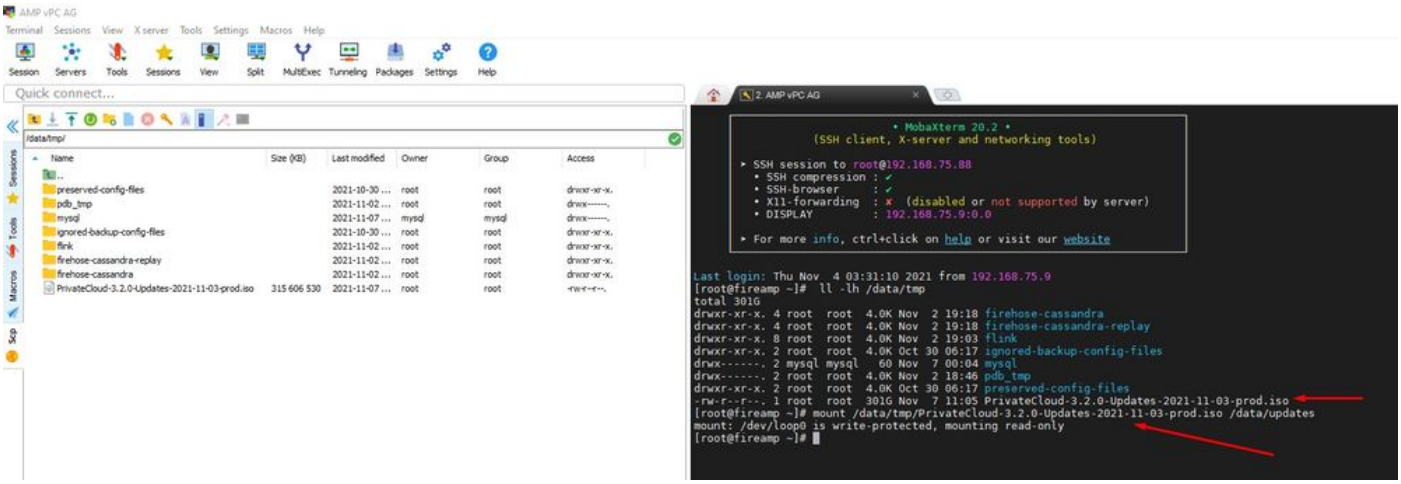
قم بنقل أحدث ISO الذي تم إنشاؤه باستخدام AMP-sync إلى VPC. قد يستغرق هذا الأمر عدة ساعات أيضا استنادا إلى سرعتك. في هذه الحالة، استغرق النقل أكثر من 16 ساعة

```
/data/tmp
```



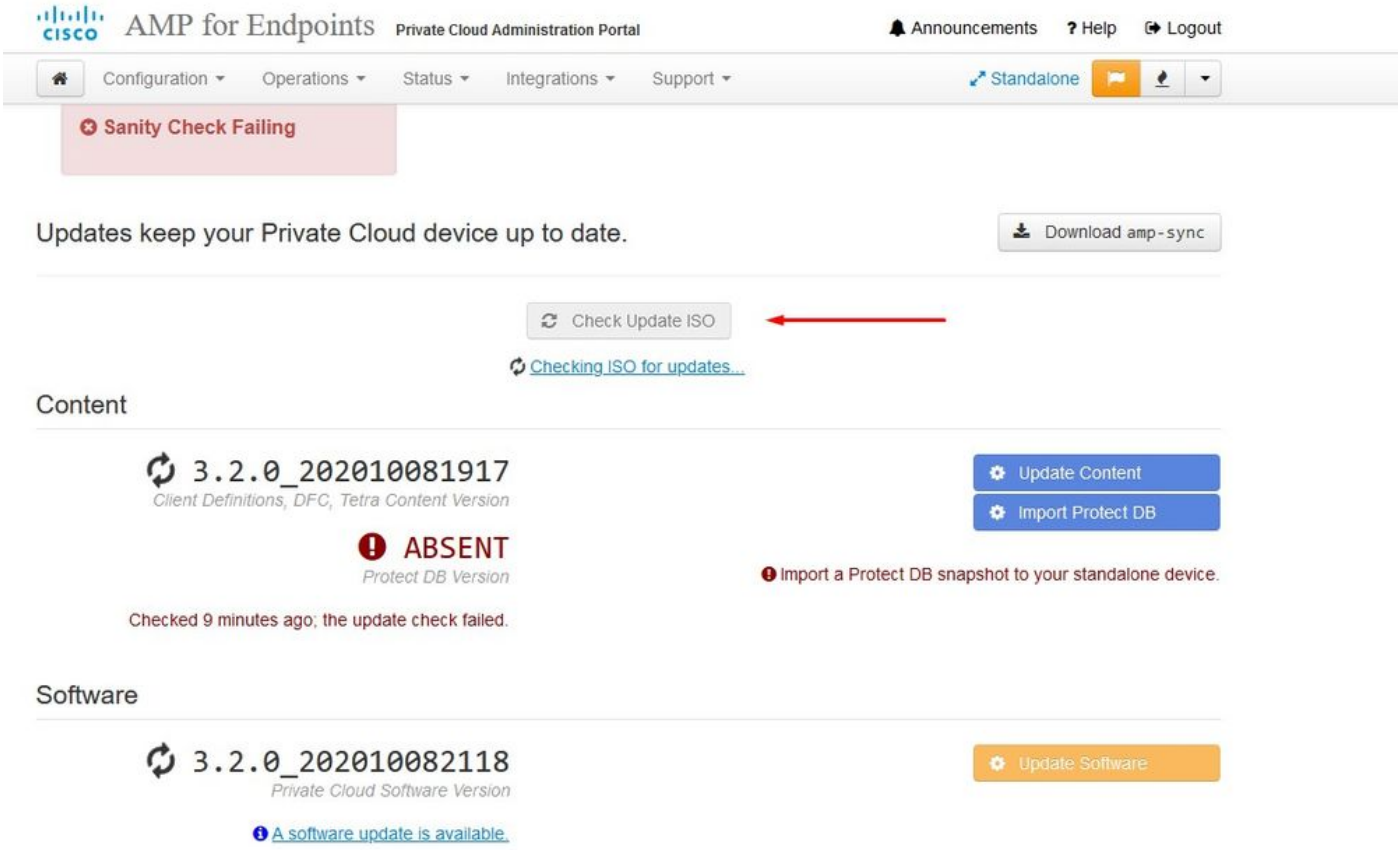
بعد الانتهاء من التحميل، قم بتحميل ISO

```
mount /data/tmp/PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso /data/updates/
```

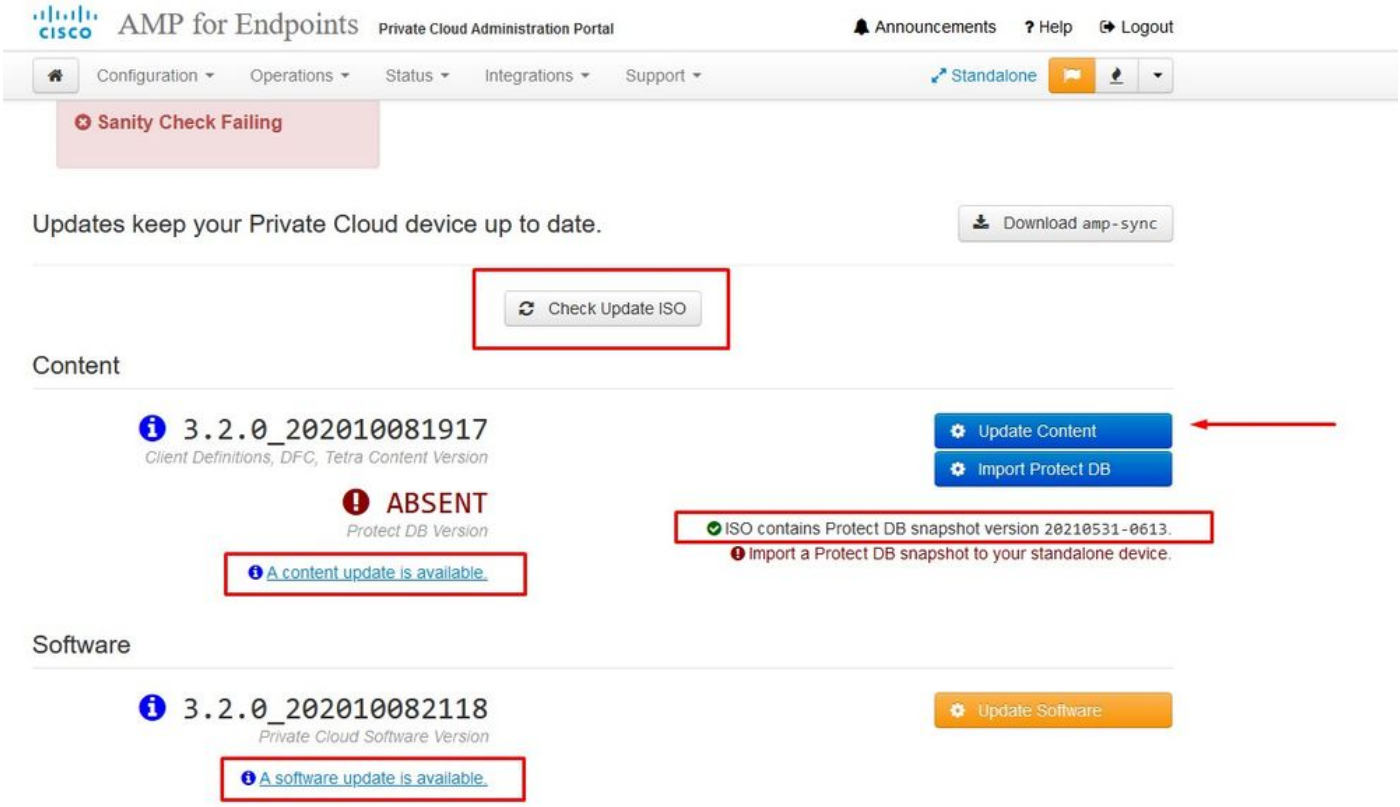


انتقل إلى واجهة مستخدم Opdamin لإجراء التحديث عمليات > تحديث الجهاز > تحديد التحقق

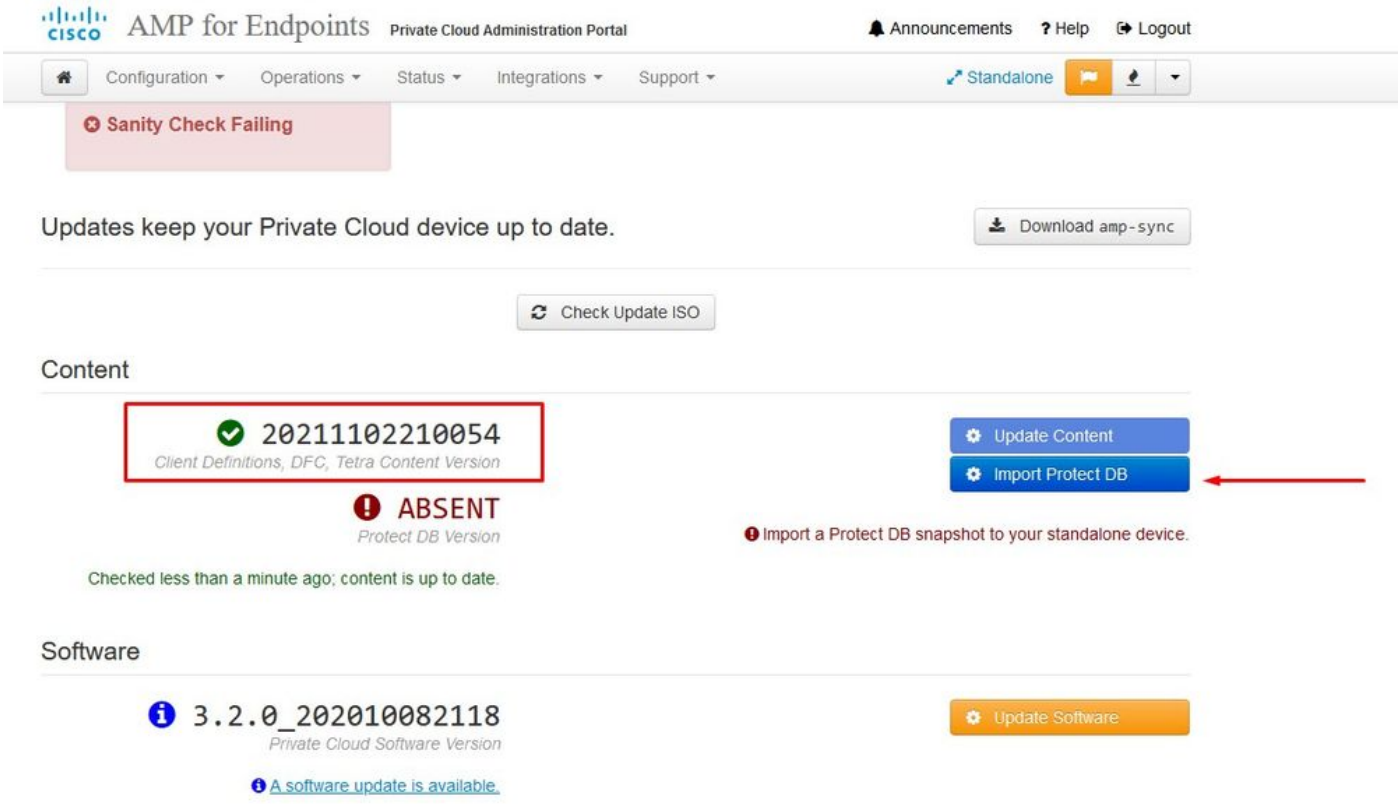
من تحديث ISO.



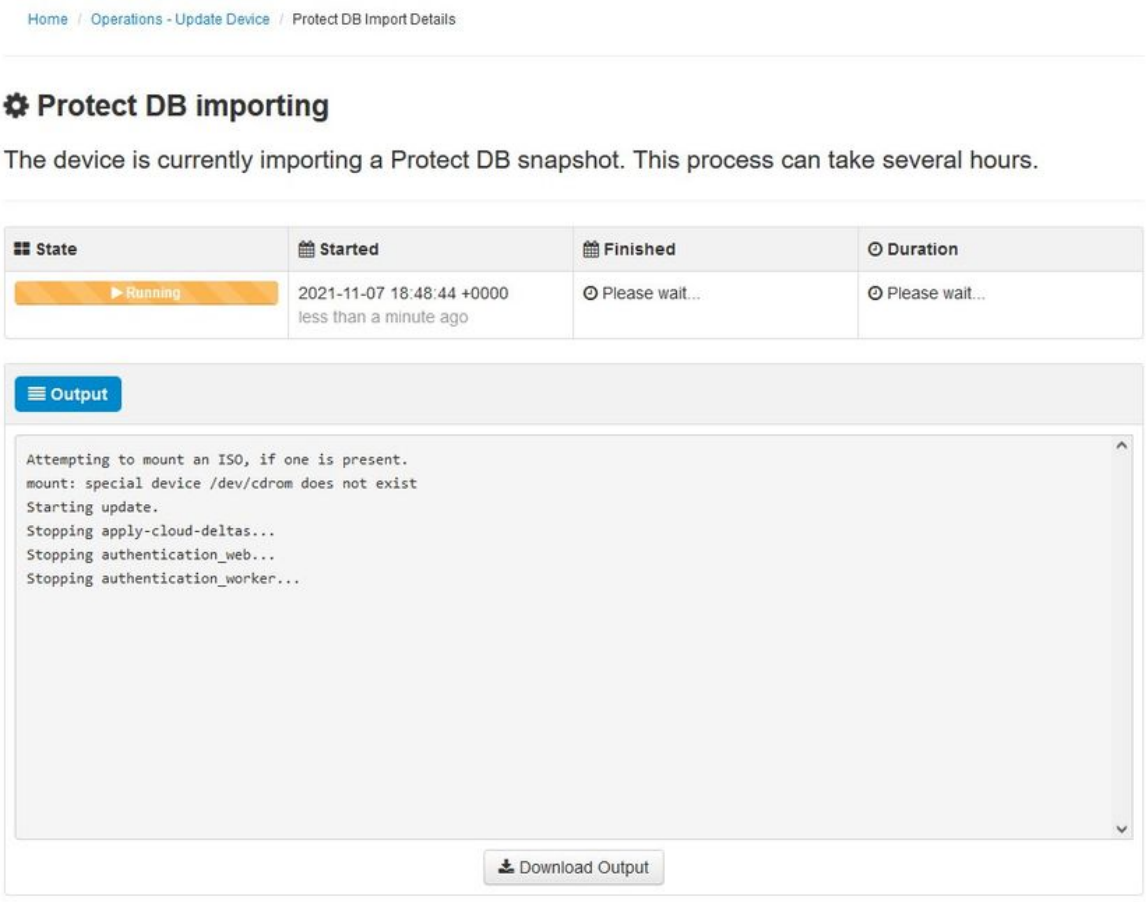
في هذا المثال، أتابع تحديث المحتوى أولا



ثم حدد قاعدة بيانات حماية الاستيراد.



وكما ترون فإن هذه عملية طويلة جدا قد تستغرق وقتا طويلا حتى تكتمل.



Home / Operations - Update Device / Protect DB Import Details

Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
Running	2021-11-07 18:48:44 +0000 42 minutes ago	Please wait...	Please wait...

Output

```
Extraction   14.9GB at    6.6MB/s  eta:   9:28:21    6% [==                  ]
Extraction   14.9GB at    6.6MB/s  eta:   9:28:27    6% [==                  ]
Extraction   14.9GB at    6.5MB/s  eta:   9:28:40    6% [==                  ]
Extraction   14.9GB at    6.5MB/s  eta:   9:28:46    6% [==                  ]
Extraction   14.9GB at    6.5MB/s  eta:   9:28:58    6% [==                  ]
Extraction   14.9GB at    6.5MB/s  eta:   9:29:12    6% [==                  ]
Extraction   14.9GB at    6.5MB/s  eta:   9:29:26    6% [==                  ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:56    6% [==                  ]
Extraction   15.0GB at    6.6MB/s  eta:   9:28:20    6% [==                  ]
Extraction   15.0GB at    6.6MB/s  eta:   9:28:28    6% [==                  ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:44    6% [==                  ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:51    6% [==                  ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:48    6% [==                  ]
Extraction   15.0GB at    6.5MB/s  eta:   9:28:56    6% [==                  ]
Extraction   15.0GB at    6.5MB/s  eta:   9:29:10    6% [==                  ]
Extraction   15.0GB at    6.5MB/s  eta:   9:29:23    6% [==                  ]
```

Download Output

Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
Running	2021-11-19 17:04:05 +0000 about 20 hours ago	Please wait...	Please wait...

Output

```
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00   99% [====================]
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00  100% [====================]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```

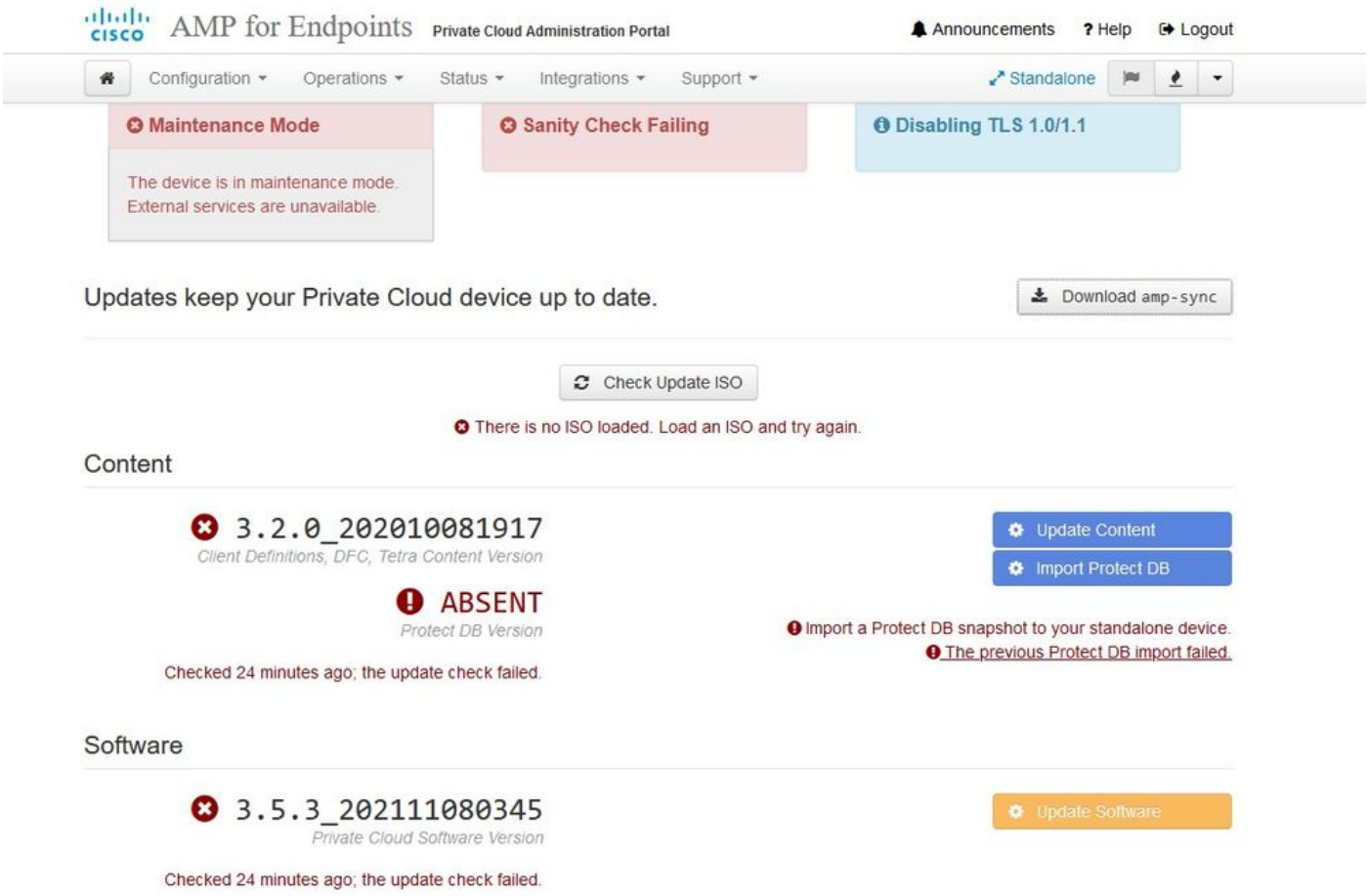
المشككلة رقم 1 - مساحة مستنفدة في نزخم البيانات

هنا يمكنك الحصول على مسألتين. امب أن vPC قبل 3.5.2 ال يملك القدرة على تحميل تخزين NFS الخارجي، يجب عليك تحميل تحديث ملف ISO إلى الدليل /data/temp. في حالتي، امب أن مكنسة البيانات كانت سعة 1 تيرابايت فقط، ركضت من الغرفة وتحطم الجهاز الظاهري. بمعنى آخر، تحتاج إلى مساحة ال تقل عن 2 تيرابايت على "نزخم البيانات" لديك لنشر VPC AirGap وهو حاجب الإصدار 3.5.2 منخفض القيمة

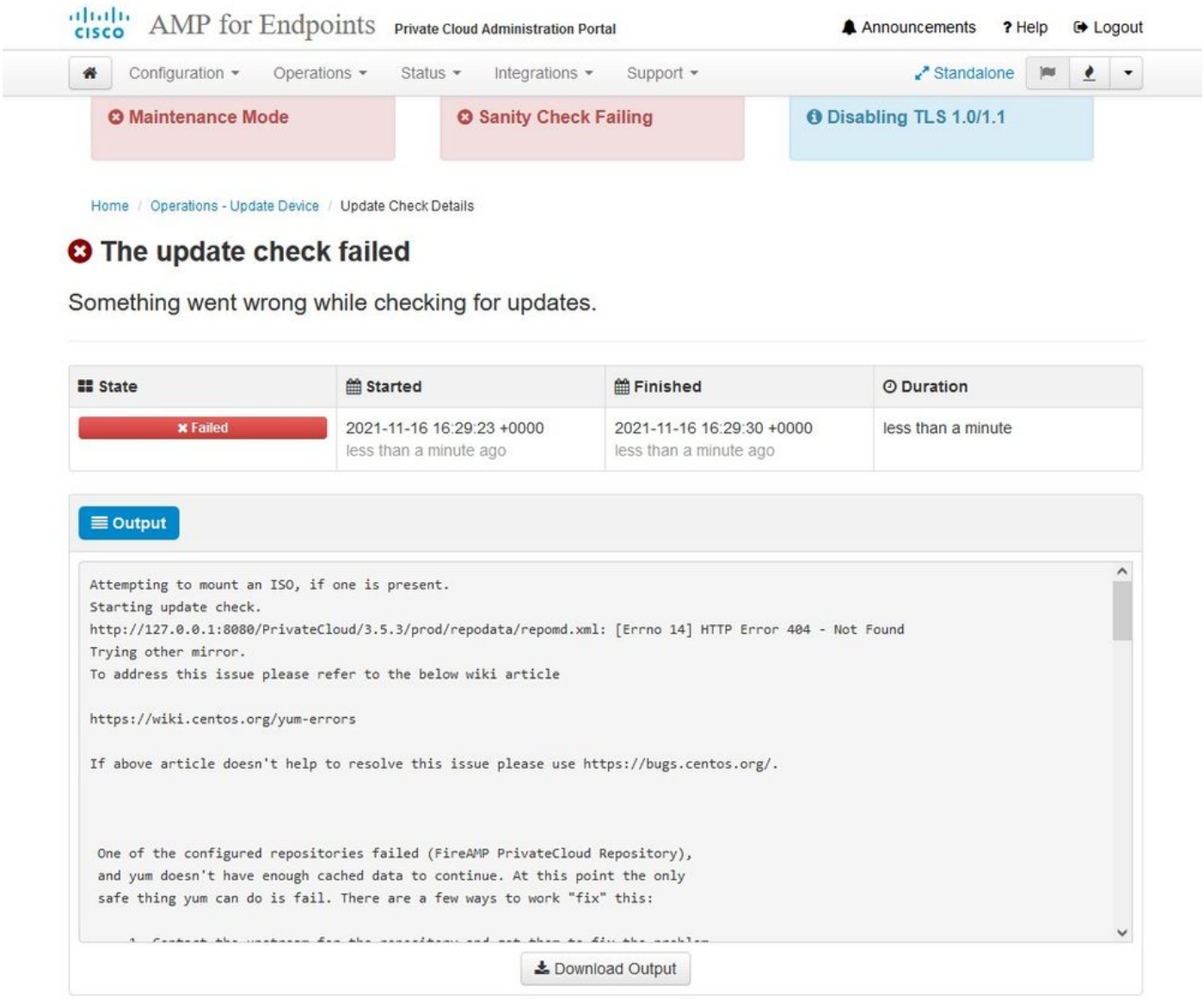
هذه الصورة الموجودة في مداخ ESXi الذي يظهر الخطأ المتمثل في عدم توفر مساحة إضافية على محرك الأقراص الثابتة عند محاولة تمهيد جهاز VM. تمكنت من إستعادة اذه الخطأ من اللخ التحويل المؤقت لذاكرة الوصول العشوائي (RAM) سعة 128 جيجابايت إلى 64 جيجابايت. مث تمكنت من التمهيد مرة أخرى. تذكر أيضا أنك إذا قمت بتوفير الجهاز الافتراضي (VM) اذه كجهاز عميل قليل السمك، فإن الجانب السلبي لنشر الجهاز العميل قليل السمك يتمثل في إمكانية زيادة حجم القرص، ولكنه لن يتقلص حتى إذا قمت بتوفير بعض المساحة. بمعنى آخر، دعنا نفترض أنك قمت بتحميل الملف سعة 300 جيجابايت إلى دليل vPC مث قمت بحذفه. ال يزال القرص الموجود في ESXi يظهر مساحة أقل تبلغ 300 جيجابايت على محرك الأقراص الثابتة لديك

المشككلة رقم 2 - التحديث القديم

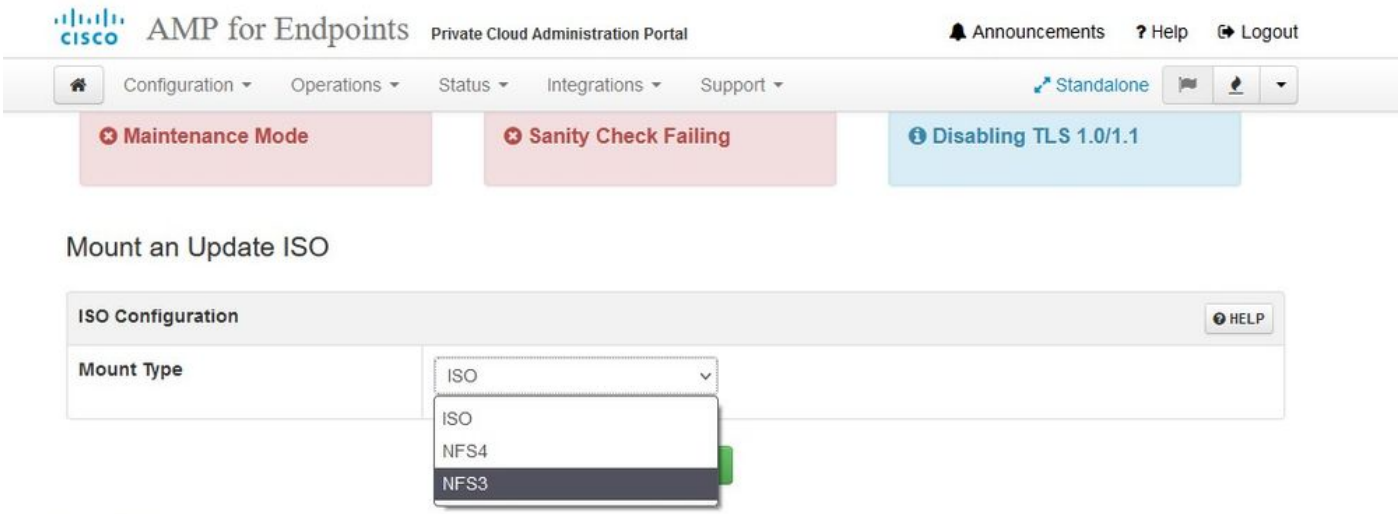
المشككلة الثانية هي إذا قمت بتشغيل تحديث البرنامج أولا كما فعلت في الإصدار الثاني من إصداري 3.2.0 وم انتهى بي الأمر مع VPC للترقية إلى 3.5.2 وبسبب ذلك اضطررت إلى تنزيل ملف تحديث ISO الجديد لأن الإصدار 3.2.0 أصبح غير صالح بسبب حقيقة أنني لم أعد على الإصدار 3.2.0 الأصلي.

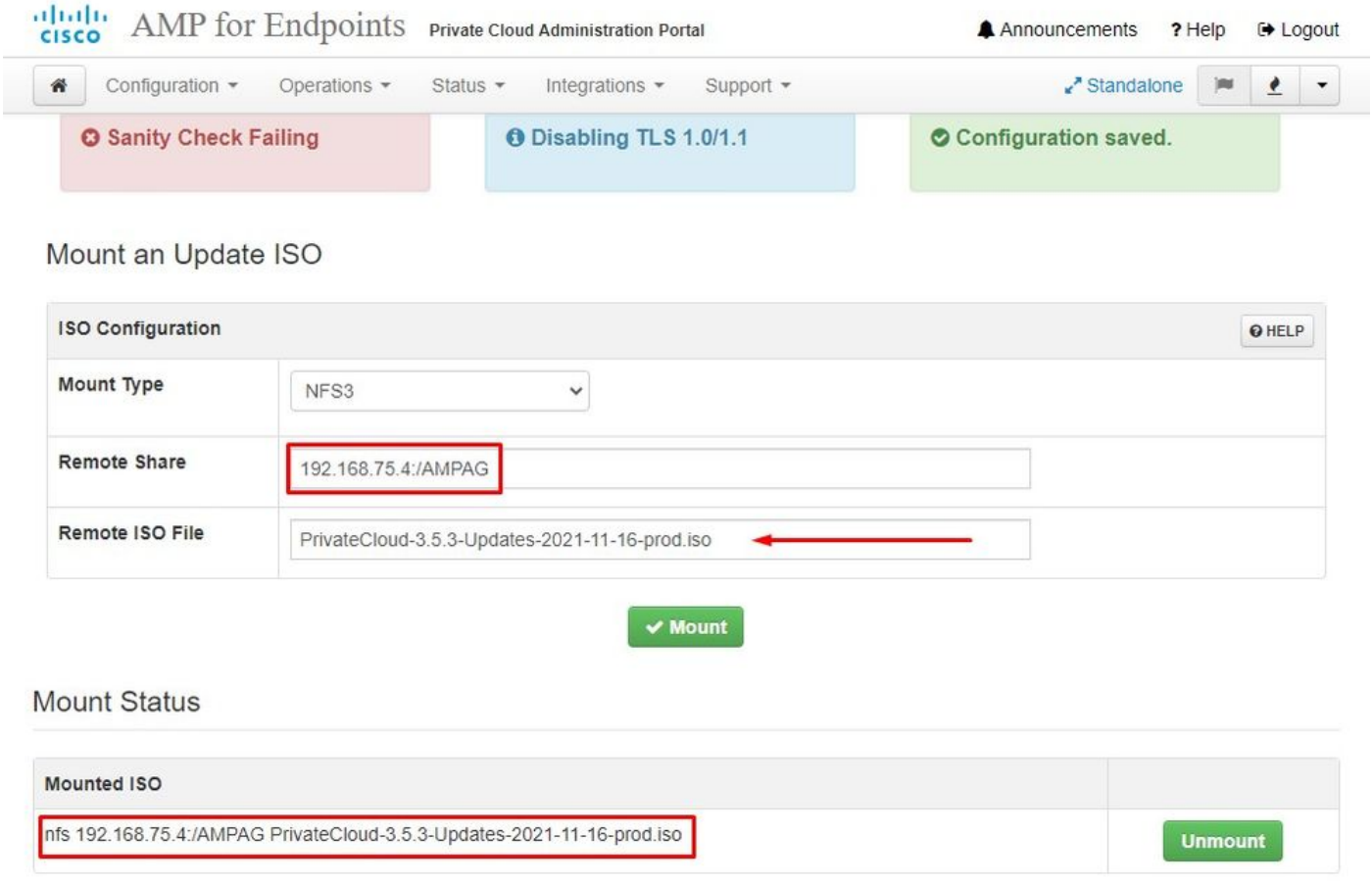


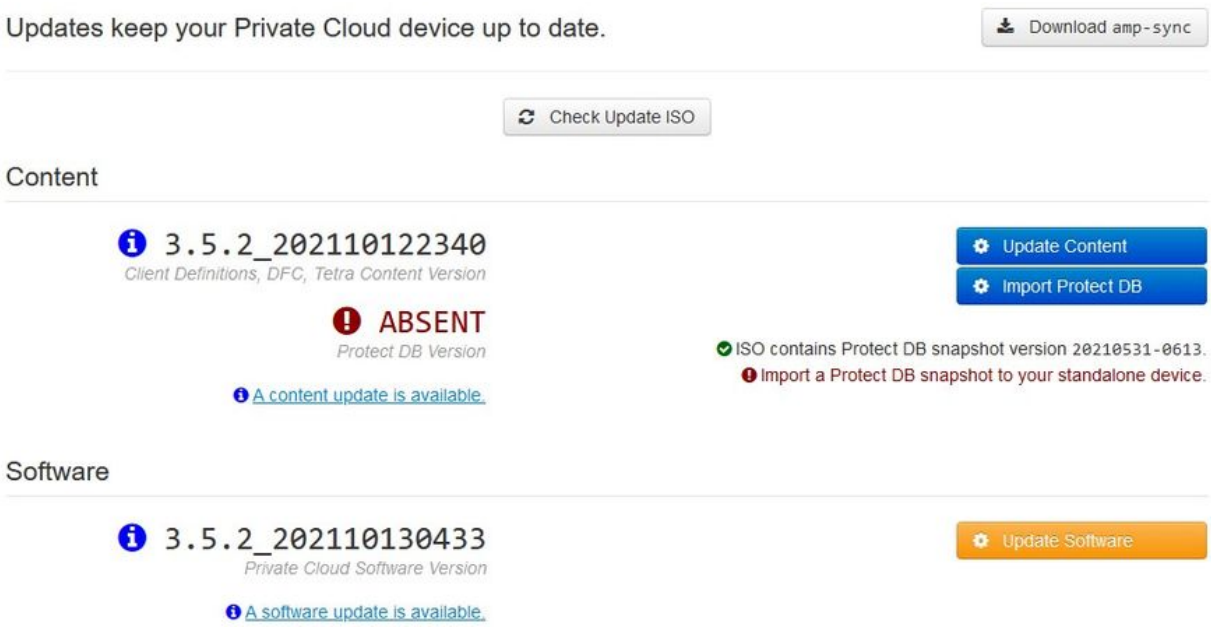
هذا هو الخطأ الذي ترى إذا حاولت تحميل ملف تحديث ISO مرة أخرى.



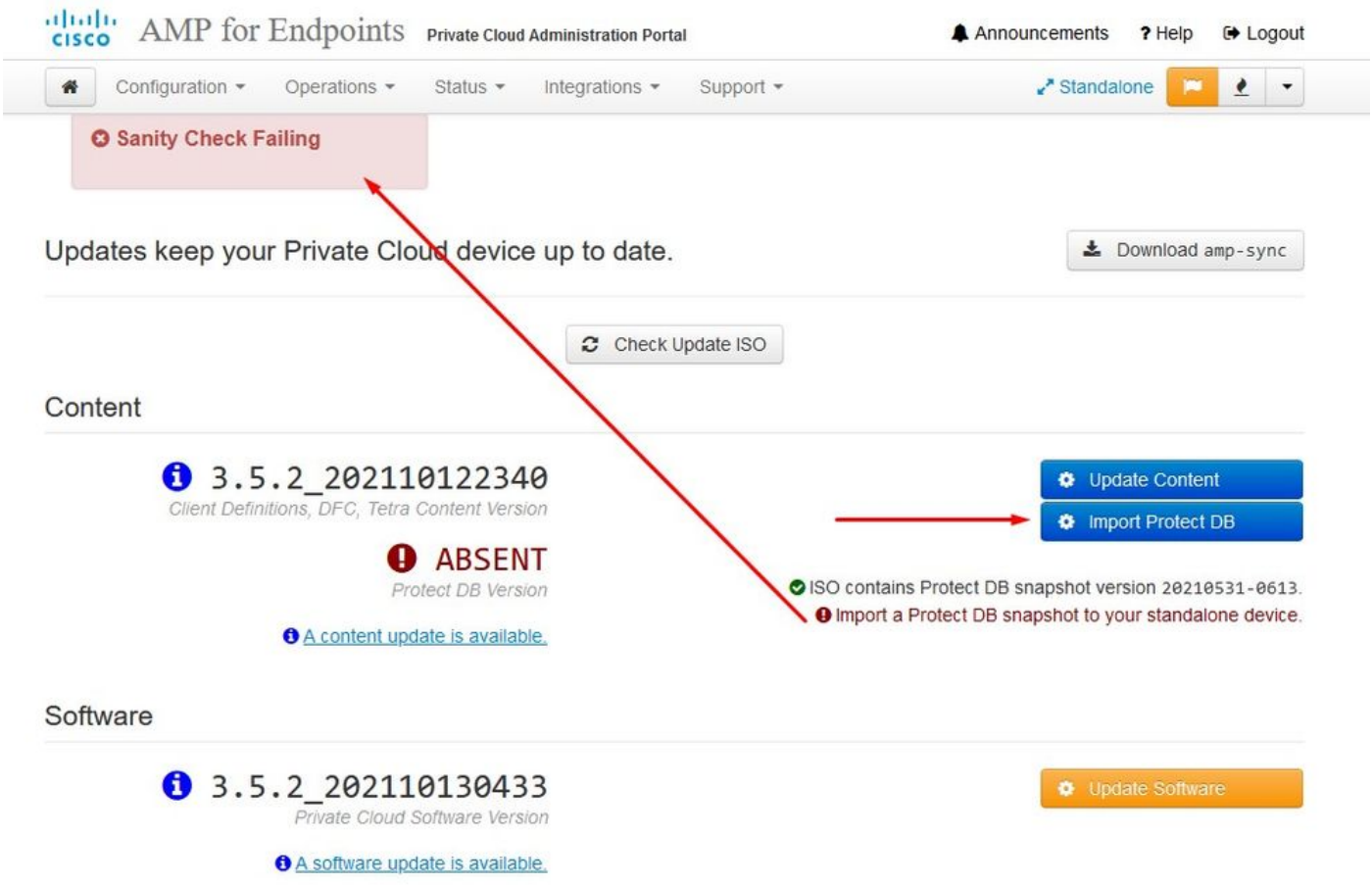
تظهر هذه الصورة طريقة بديلة لتحميل صورة التحديث إلى VPC الخاص بك. في الإصدار 3.5.x، يمكنك إستخدام موقع بعيد مثل تخزين NFS لمشاركة ملف التحديث مع جهاز VPC الخاص بك.


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
Maintenance Mode
Sanity Check Failing
Disabling TLS 1.0/1.1
Mount an Update ISO
ISO Configuration
HELP
Mount Type
ISO
ISO
NFS4
NFS3
Mount Status
No ISO mounted


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
Sanity Check Failing
Disabling TLS 1.0/1.1
Configuration saved.
Mount an Update ISO
ISO Configuration
HELP
Mount Type
NFS3
Remote Share
192.168.75.4:/AMPAG
Remote ISO File
PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso
Mount
Mount Status
Mounted ISO
nfs 192.168.75.4:/AMPAG PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso
Unmount



فشل التحقق من سلامة النظام مرتبط بحماية قاعدة بيانات المحول (DB) غير متوفر حاليا على الكمبيوتر الشخصي (VPC)



Protect DB importing

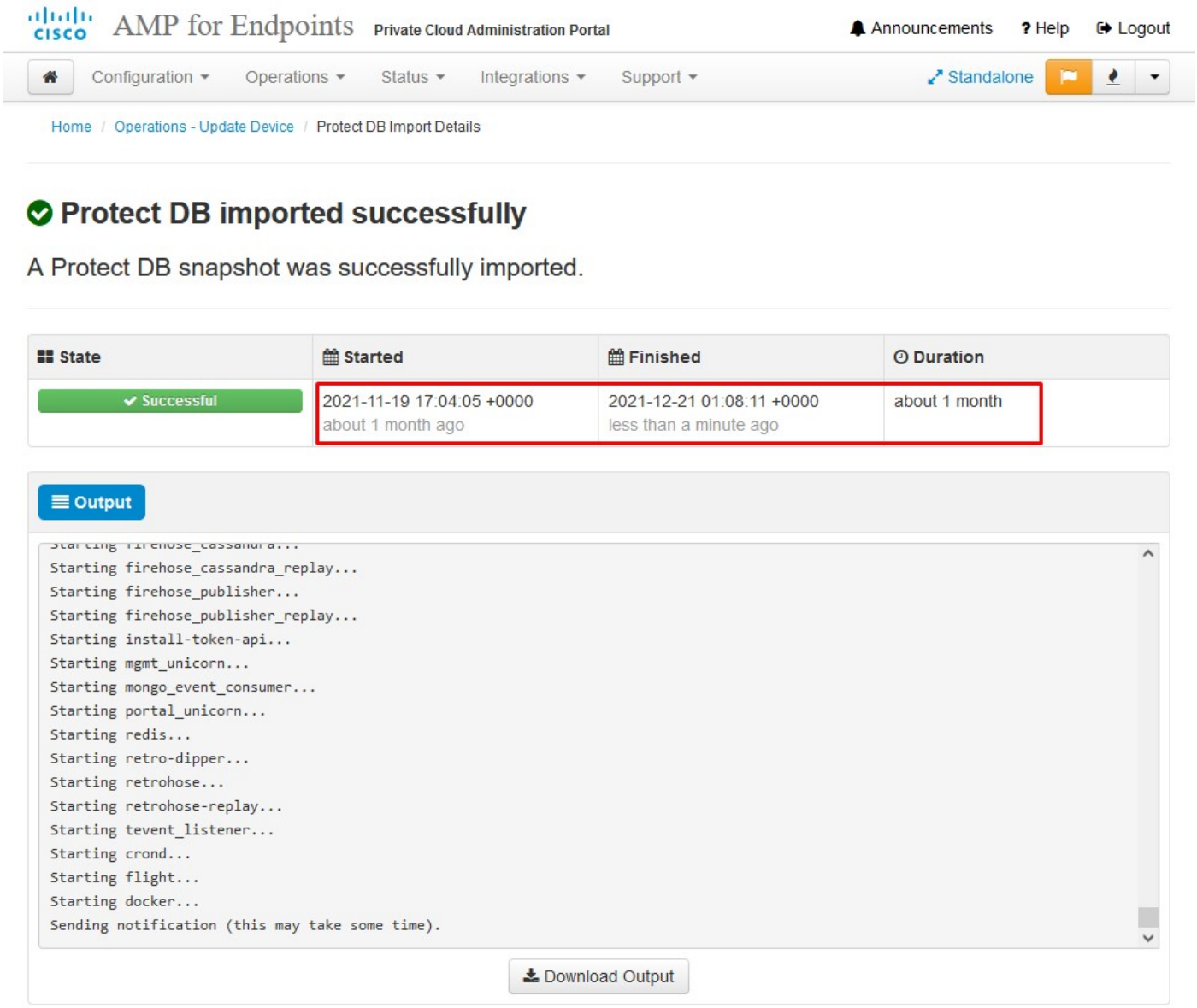
The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
Running	2021-11-19 17:04:05 +0000 about 20 hours ago	Please wait...	Please wait...

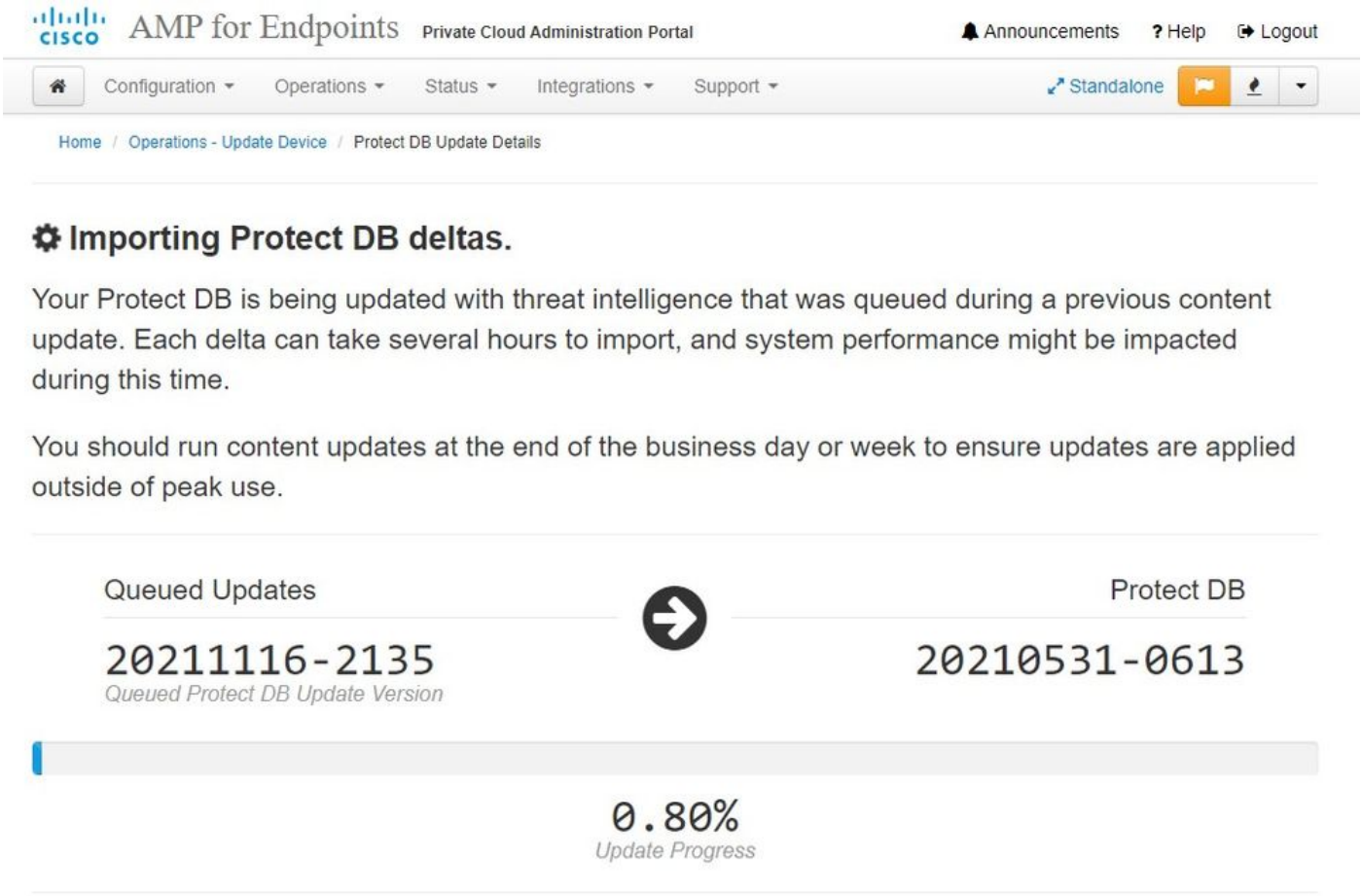
Output

```
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00   99% [====================]
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00  100% [====================]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```

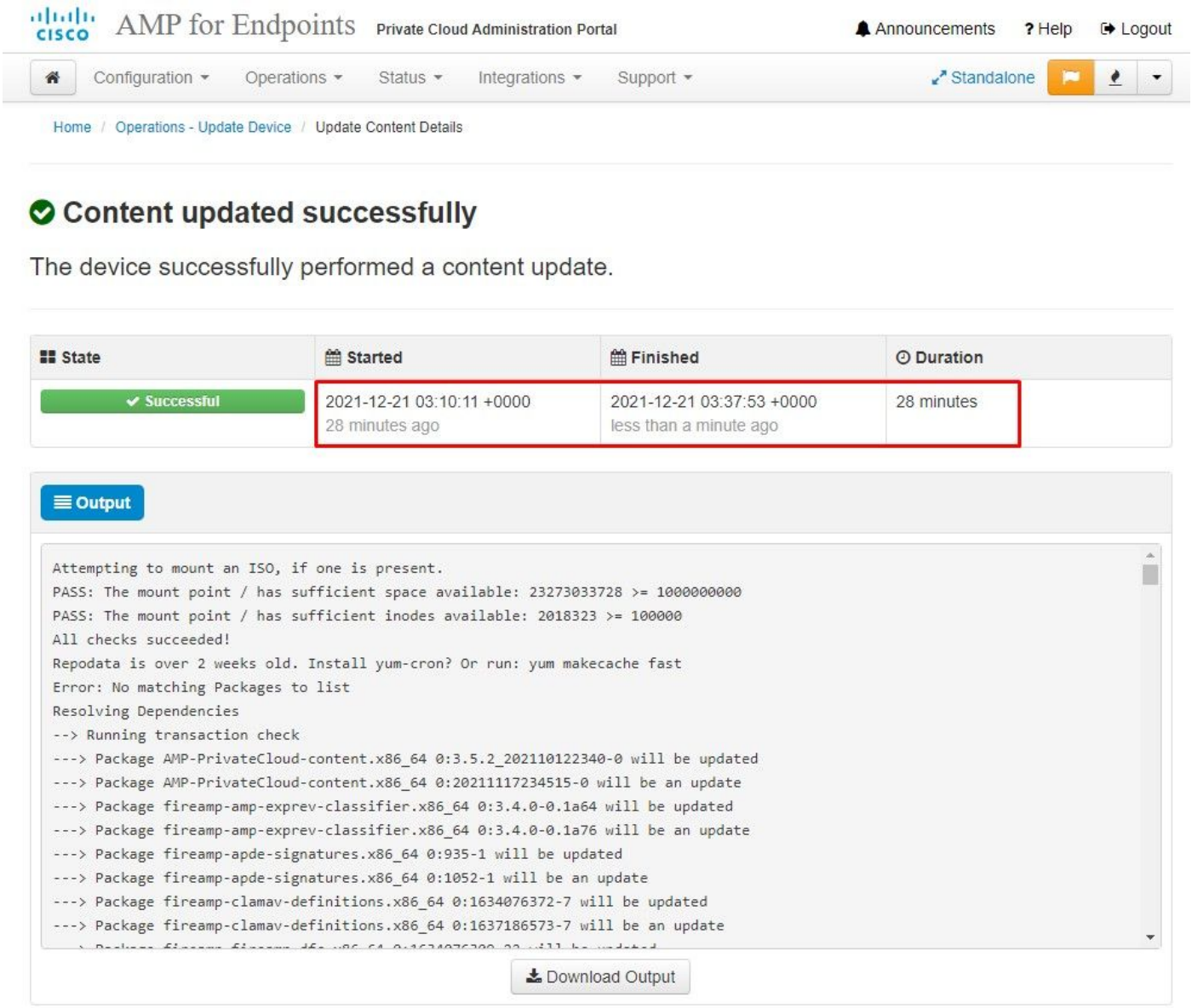
Download Output



يبدأ التحديث التالي تلقائيا



بعد هذه العملية الطويلة جدا لقاعدة بيانات قاعدة بيانات حماية الاستيراد، يمكنك نقل وتحديث تعريف العميل والبرامج التي يمكنها تقريبا أن تتطلب أكثر من 3 ساعات إضافية.



و أخيرا تم، من فضلكم لاحظوا أن هذه العملية ستستغرق وقتا طويلا جدا.

بالنسبة لجهاز VPC، تفضل بزيارة هذا الجهاز الذي يحتوي على طرق أخرى لتحديث جهاز الأجهزة وتثبيت ملف ISO والتمهيد من جهاز USB.

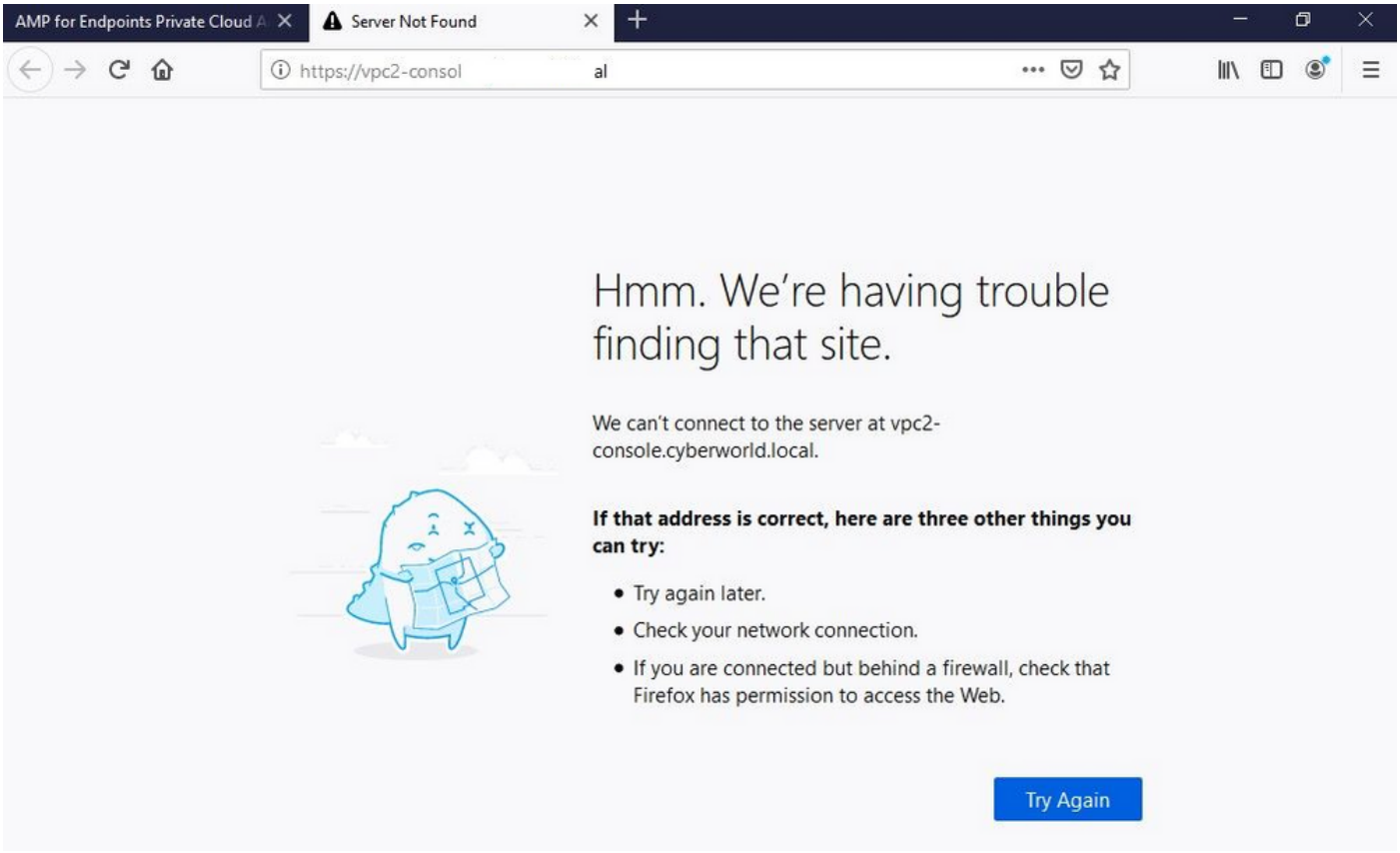
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5

طقف ≪≪ Airgap ≪≪

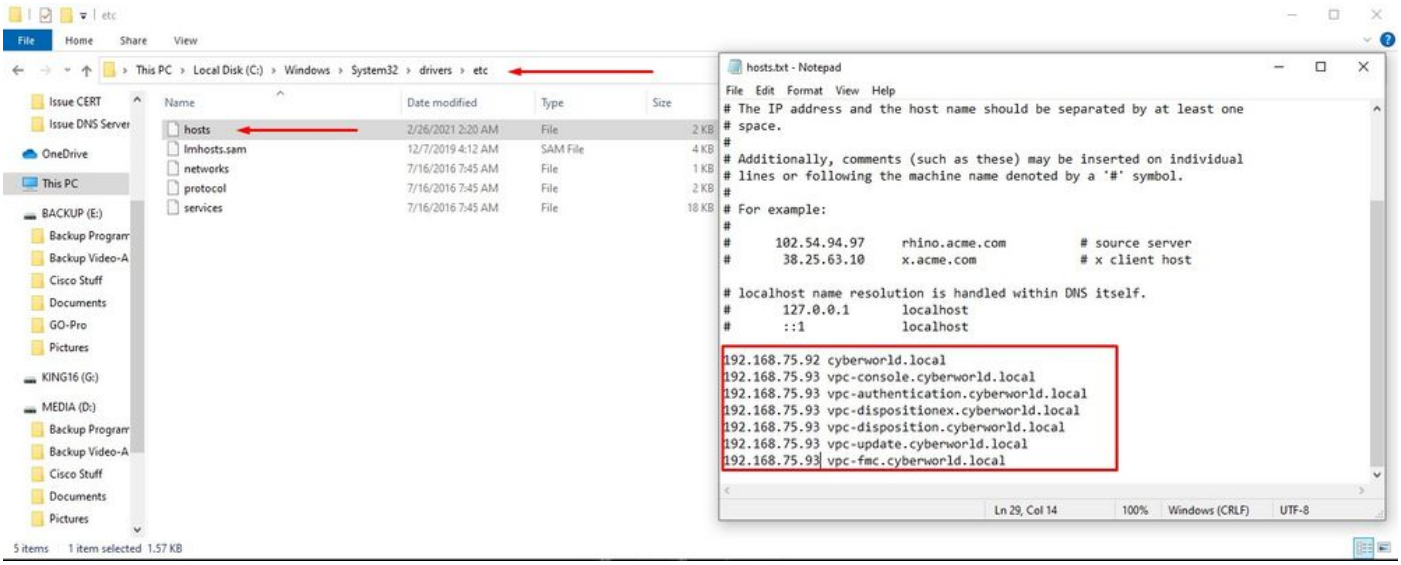
أستكشاف الأخطاء وإصلاحها بشكل أساسي

المشكلة #1 - خادم FQDN و DNS

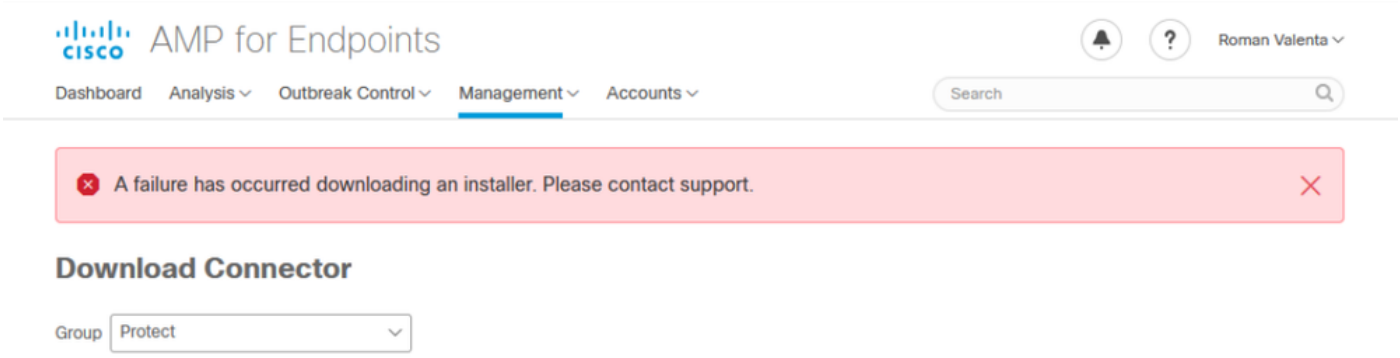
المشكلة الأولى التي يمكن أن تواجهها هي إذا لم يتم إنشاء خادم DNS الخاص بك ولم يتم تسجيل جميع FQDN وحلها بشكل صحيح. قد تبدو المشكلة بهذا الشكل عندما تحاول الاتصال إلى وحدة تحكم نقطة النهاية الآمنة من خلال رمز "fire" لنقطة النهاية الآمنة. إذا كنت تستخدم عنوان IP فقط، فهذا يعمل، ولكن لا يمكنك تنزيل الموصل. كما ترى في مخاوف الصور [3].



إذا قمت بتعديل Host File (مضيف) على جهازك المحلي كما هو موضح في الصورة قم بحل المشكلة وتنتهي بأخطاء.



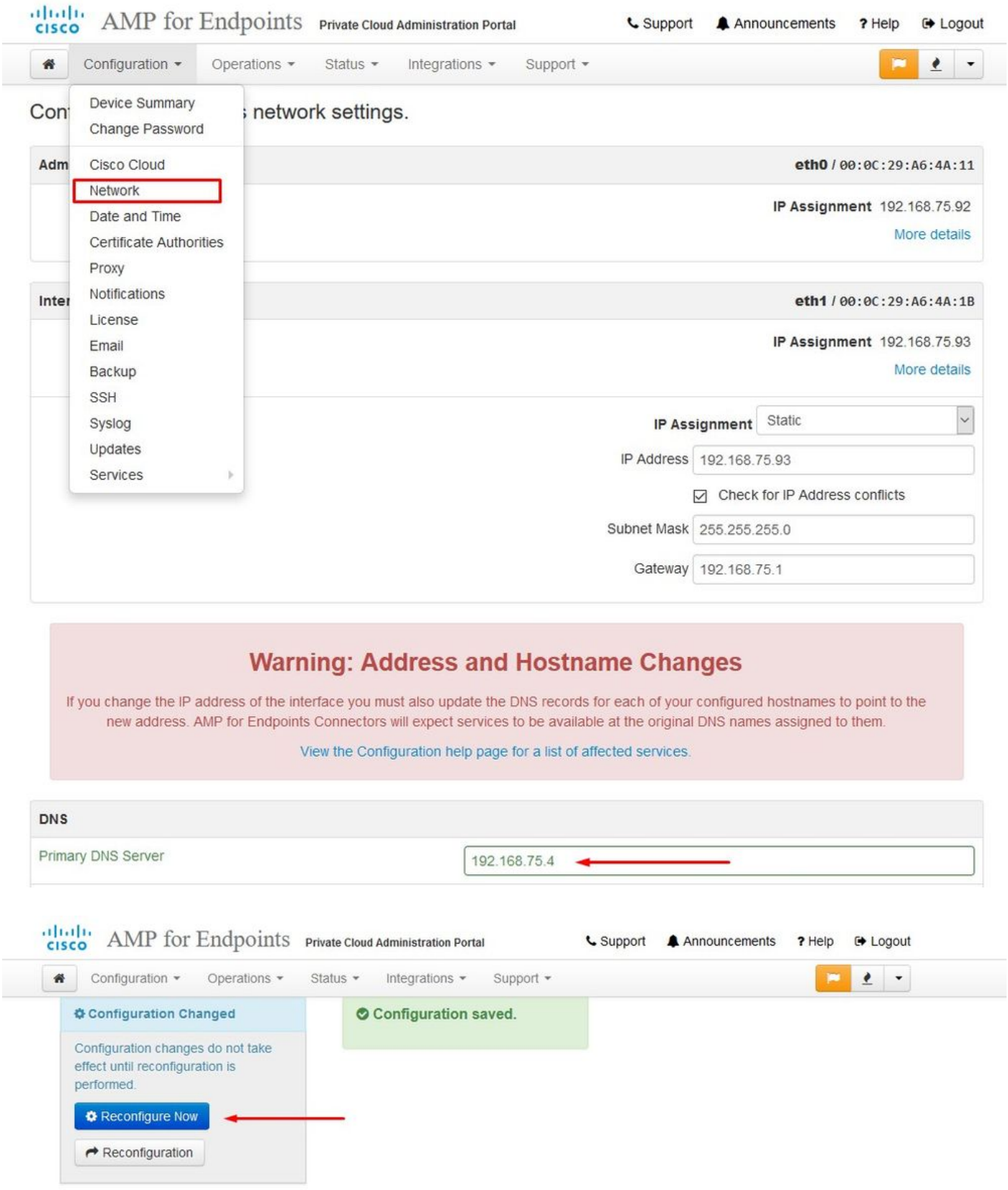
تتلقى رسالة الخطأ هذه أثناء محاولة تنزيل أداة تثبيت موصل نقطة النهاية الآمنة.



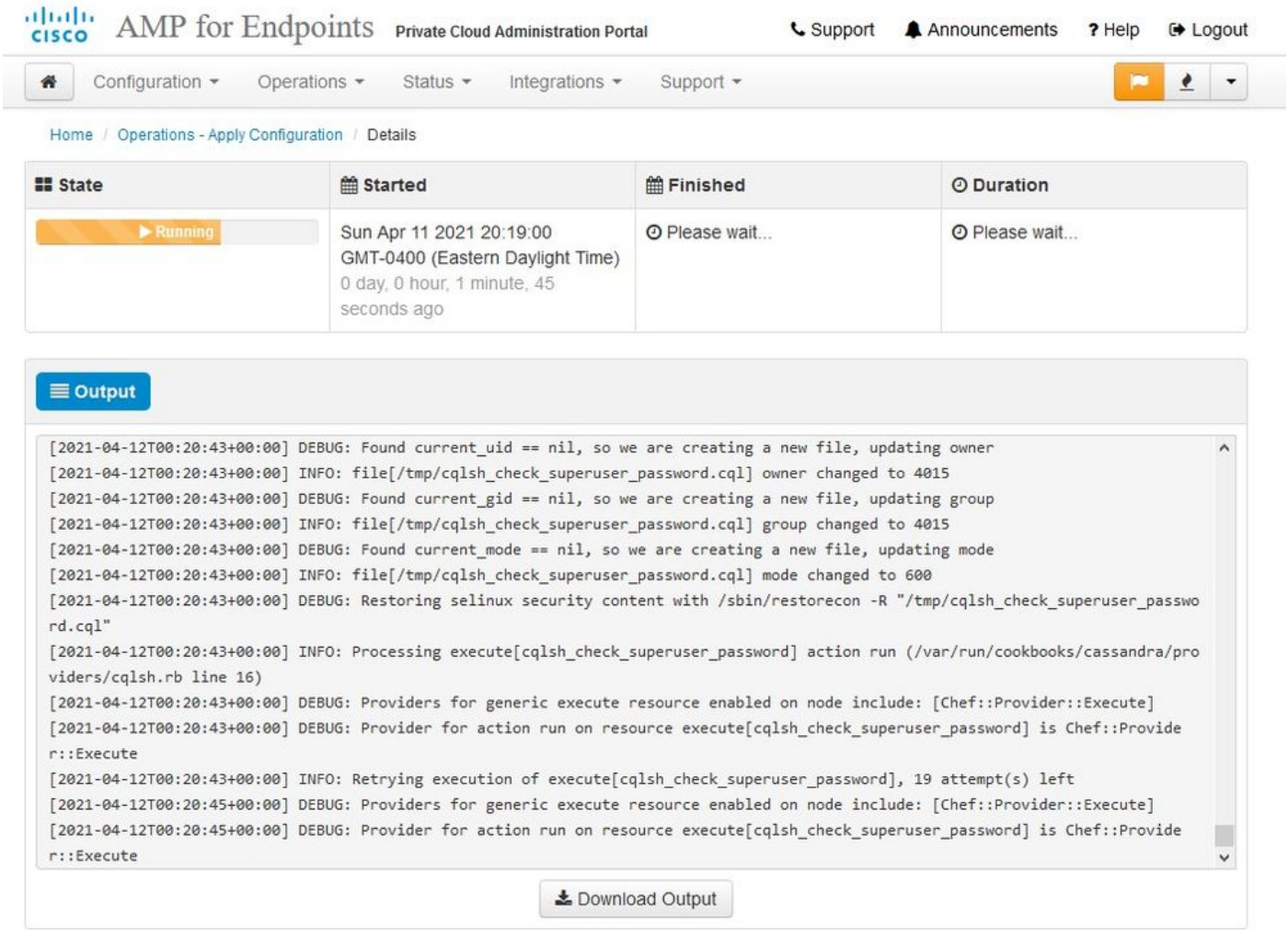
بعد أستكشاف بعض المشاكل وإصلاحها، كان الحل الوحيد الصحيح هو إعداد خادم DNS.

```
DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0

================================================================================

Server:         8.8.8.x
Address:        8.8.8.x#53

** server can't find vPC-Console.cyberworld.local: NXDOMAIN
```

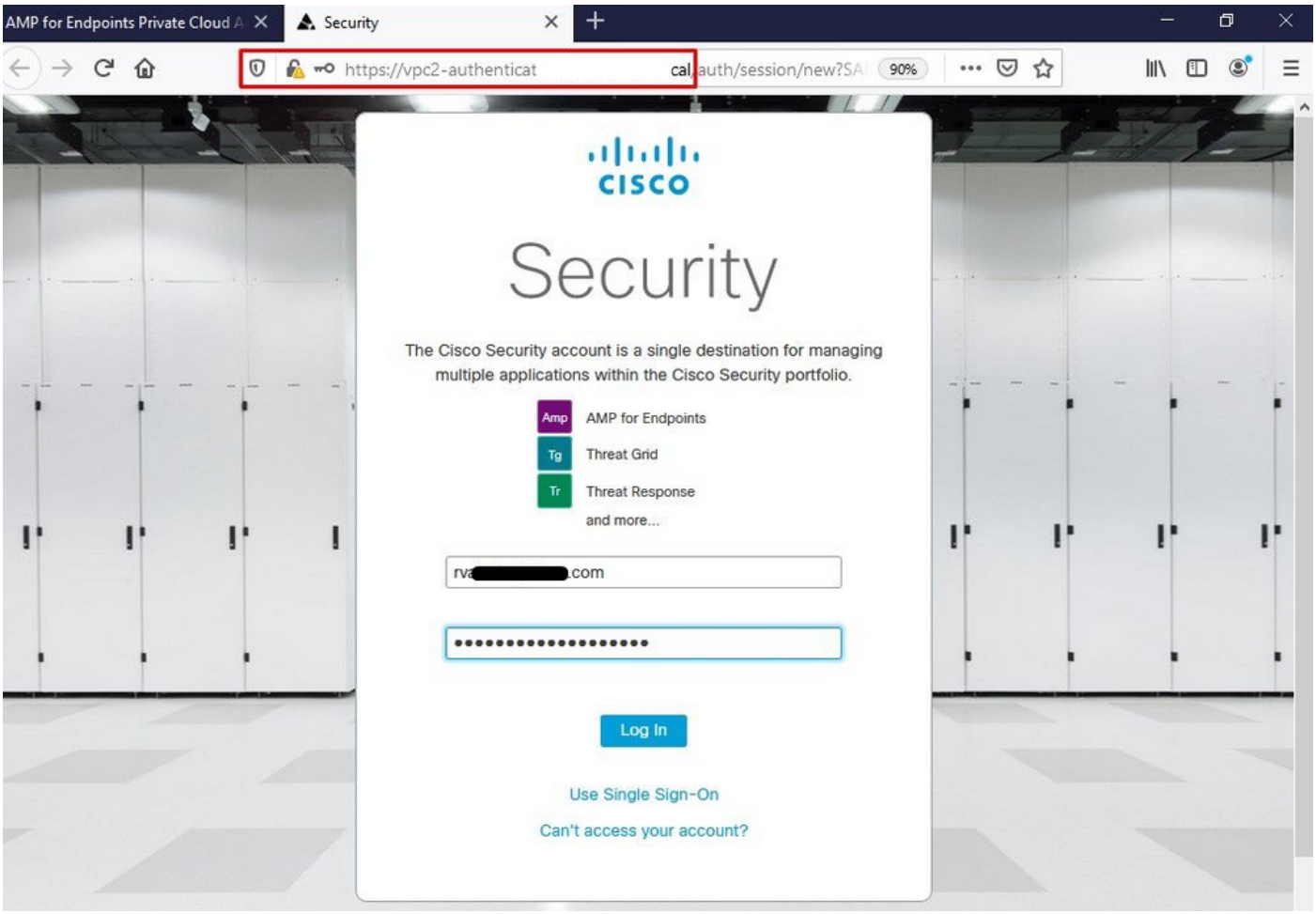
بمجرد تسجيل كافة FQDN في خادم DNS لديك وتغيير السجل في Virtual Private Cloud من DNS العام إلى خادم DNS، يجب أن كل شيء يعمل كما هو مفترض.


AMP for Endpoints
Private Cloud Administration Portal
Support
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Device Summary
Change Password
Cisco Cloud
Network
Date and Time
Certificate Authorities
Proxy
Notifications
License
Email
Backup
SSH
Syslog
Updates
Services
network settings.
eth0 / 00:0C:29:A6:4A:11
IP Assignment 192.168.75.92
More details
eth1 / 00:0C:29:A6:4A:1B
IP Assignment 192.168.75.93
More details
IP Assignment Static
IP Address 192.168.75.93
Check for IP Address conflicts
Subnet Mask 255.255.255.0
Gateway 192.168.75.1
Warning: Address and Hostname Changes
If you change the IP address of the interface you must also update the DNS records for each of your configured hostnames to point to the new address. AMP for Endpoints Connectors will expect services to be available at the original DNS names assigned to them.
View the Configuration help page for a list of affected services.
DNS
Primary DNS Server
192.168.75.4

AMP for Endpoints
Private Cloud Administration Portal
Support
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Configuration Changed
Configuration changes do not take effect until reconfiguration is performed.
Reconfigure Now
Reconfiguration
Configuration saved.

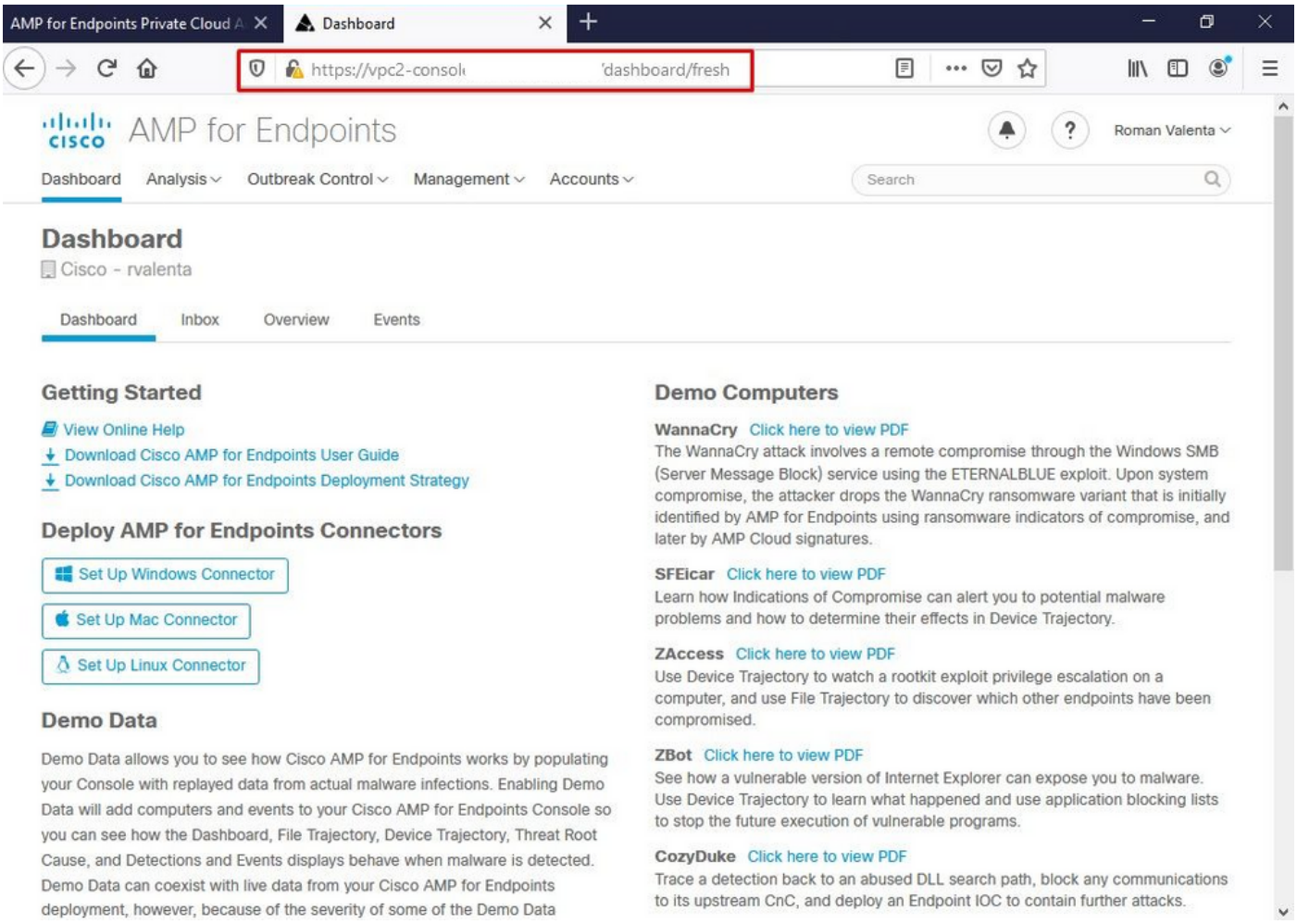


في هذه المرحلة يمكنك تسجيل الدخول وتنزيل الموصل

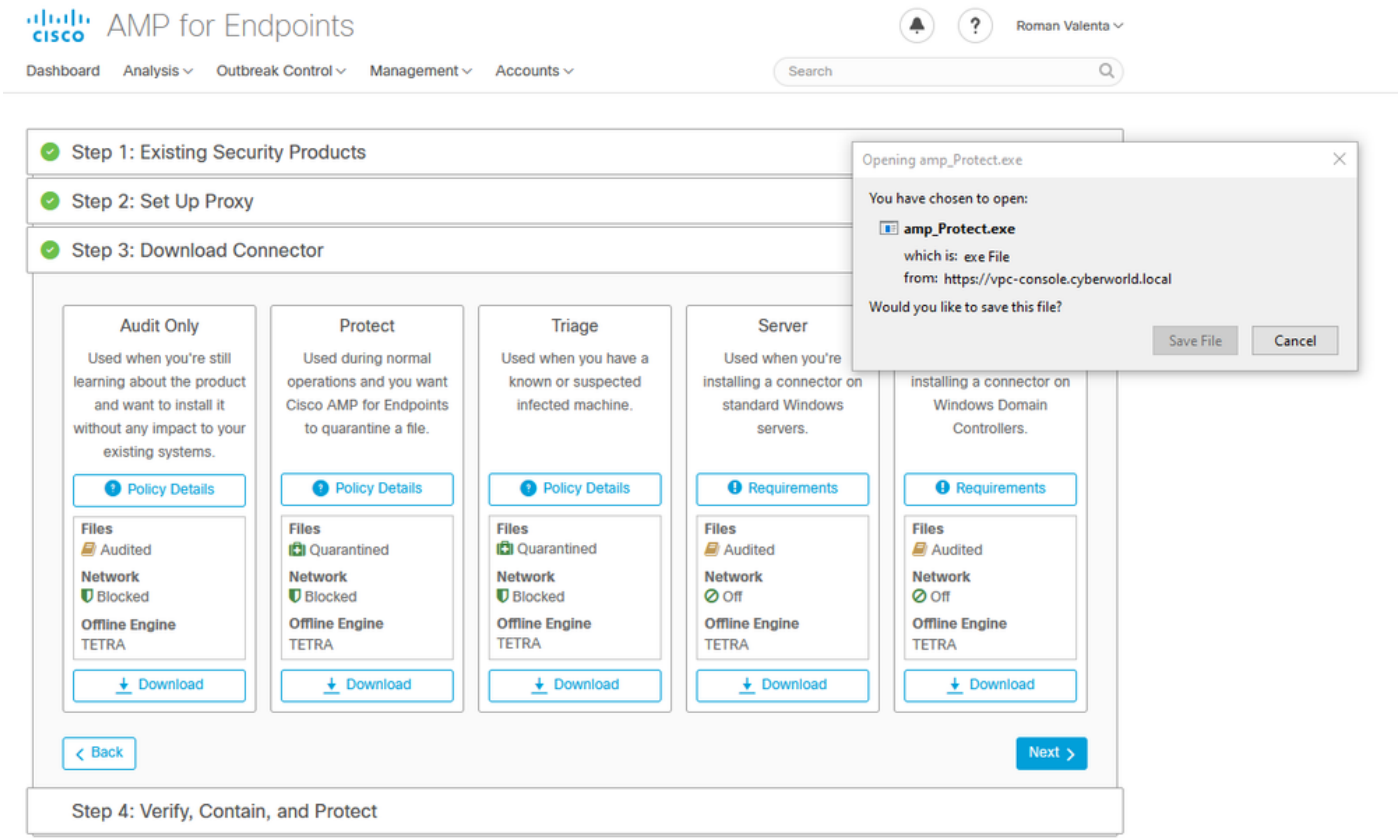


يمكنك الحصول على معالج نهج "نقطة النهاية الآمنة" الأولي لبيئتك. يساعدك البرنامج في إختيار منتج مكافحة الفيروسات الذي تستخدمه، إن كان له وجود، بالإضافة إلى التعامل مع البروكسي، وأنواع السياسات التي ترغب في نشرها. تحديد الزر "إعداد منا سب"... يعتمد على نظام تشغيل الموصل.

يمكنك الحصول على صفحة منتجات الأمان الموجودة، كما هو موضح في الصورة. أختر منتجات الأمان التي تستخدمها. فهو يقوم تلقائيا بإنشاء استبعادات قابلة للتطبيق لمنع حدوث مشاكل في الأداء على نقاط النهاية الخاصة بك. تحديد في التالي.

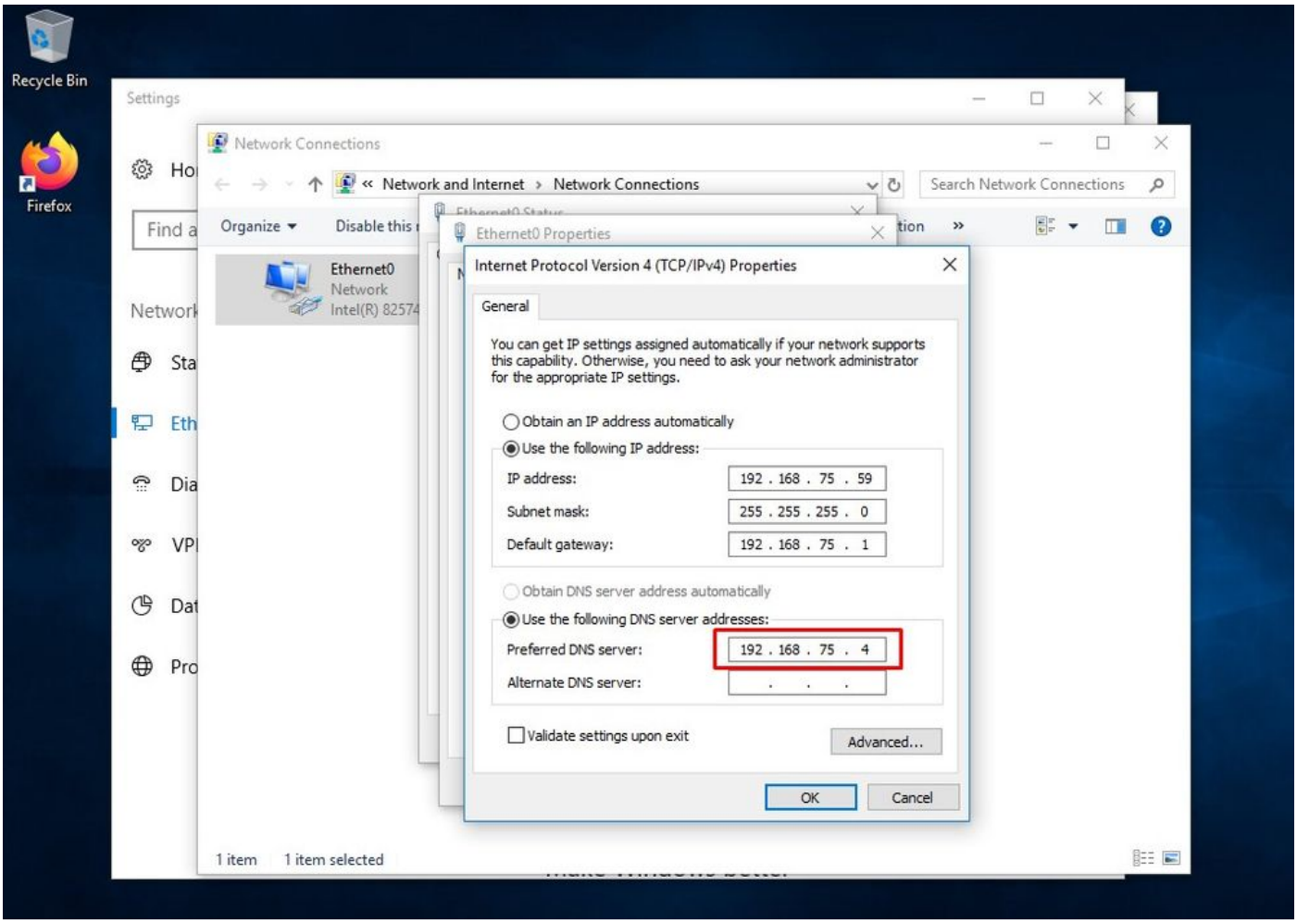


تنزيل الموصل.

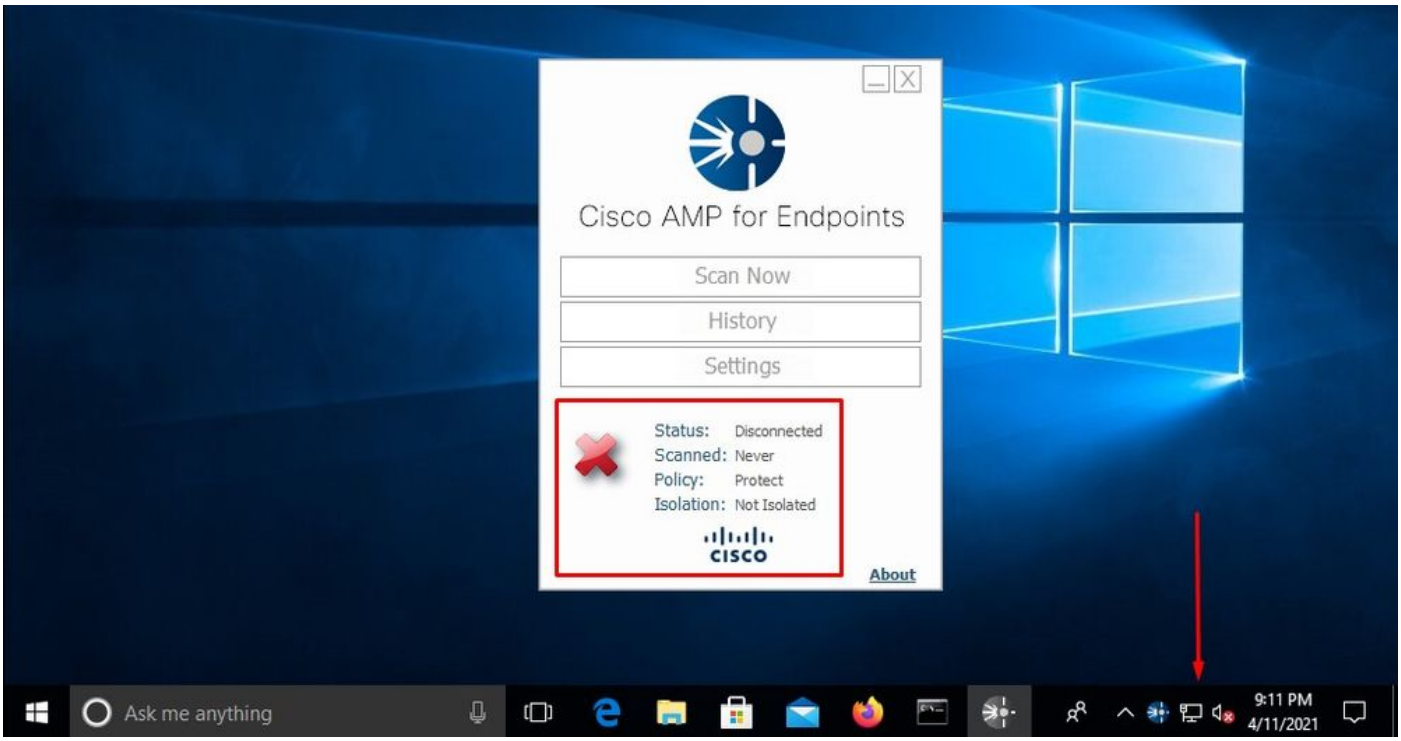


المشكلة رقم 2 - مشكلة مع المرجع المصدق الجذر

المشكلة التالية التي يمكن أن تواجهها هي إذا كنت تستخدم الشهادات الداخلية الخاصة بك هي أنه بعد التثبيت الأولي، يمكن أن يظهر الموصل على أنه غير متصل.



بمجرد تثبيت نقطة النهاية الآمنة للموصل يمكن رؤيتها على أنها غير متصلة. شوط تشخيص حزمة وانظر خلال الـ log، أنت يستطيع حددت الإصدار.

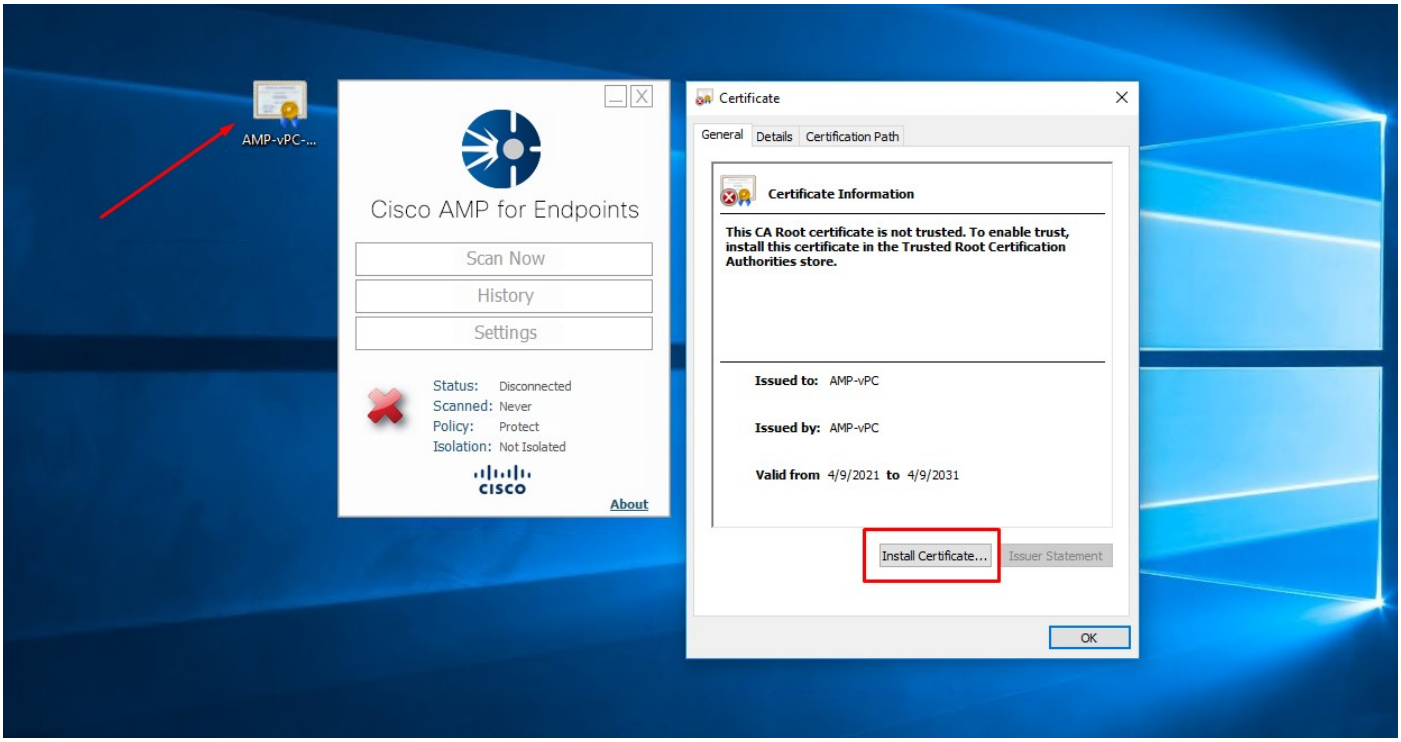


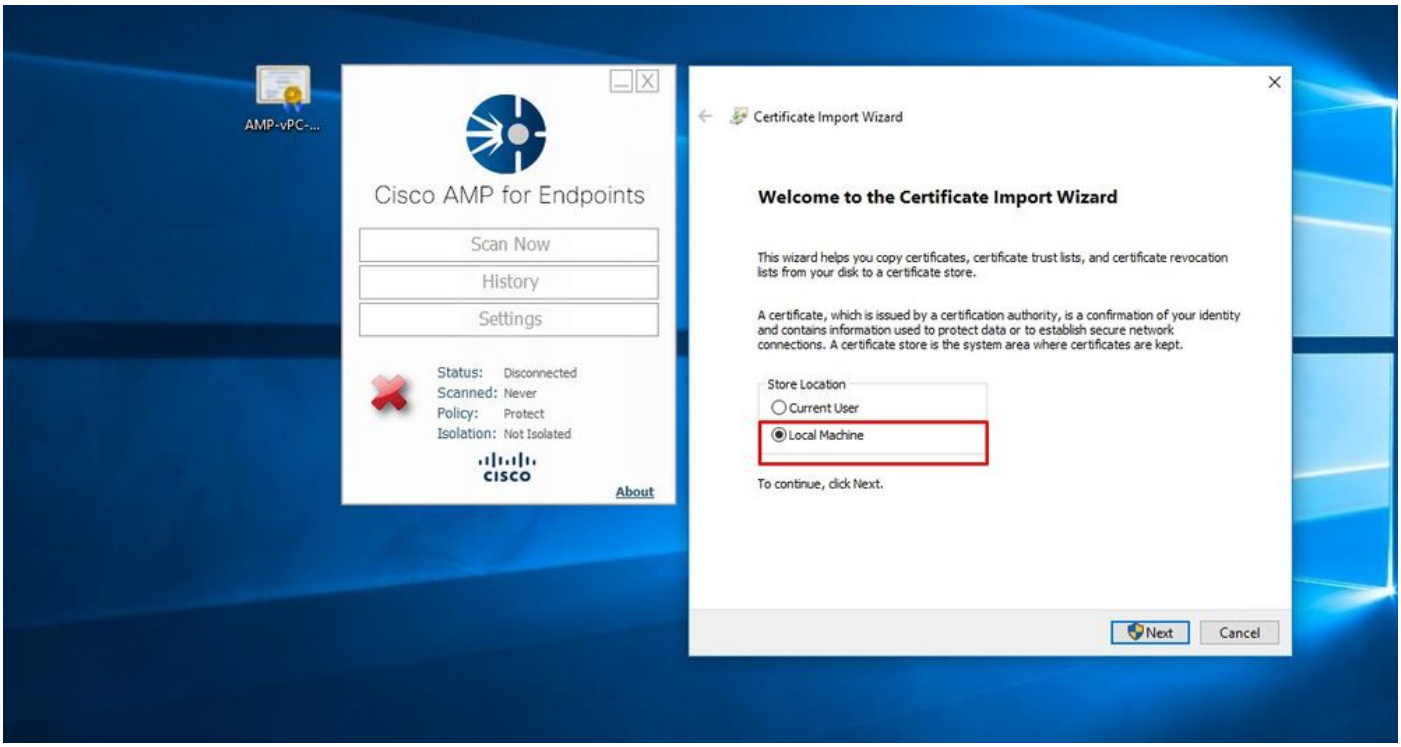
استنادا إلى هذا الإخراج الذي تم تجميعه من الحزمة التشخيصية، يمكنك رؤية خطأ المرجع

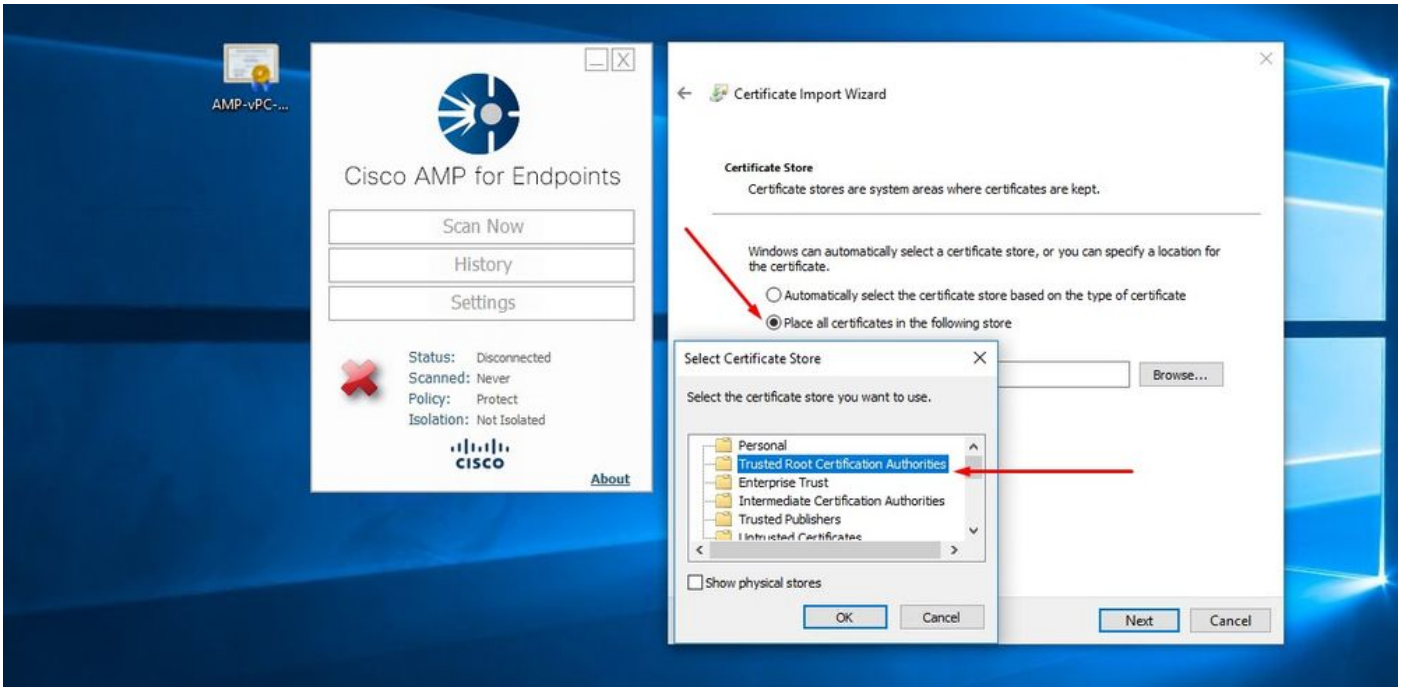
المصدق الجذر

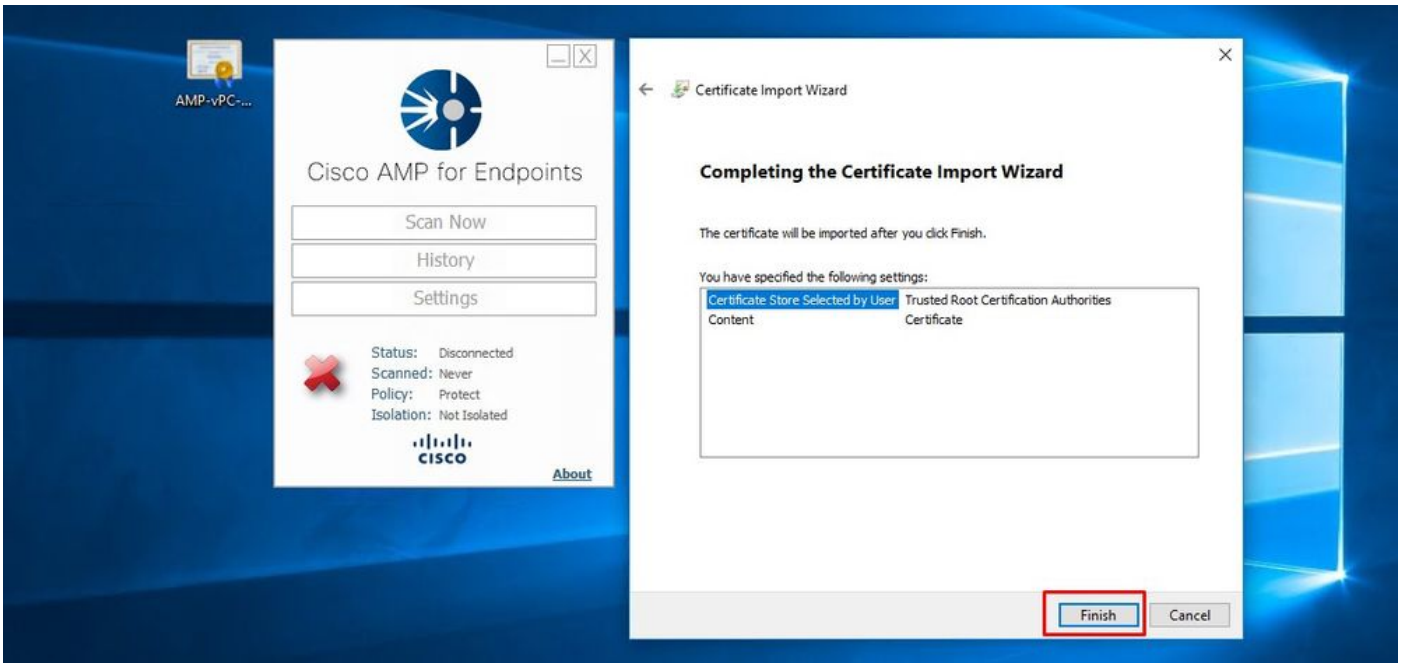
```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60
```

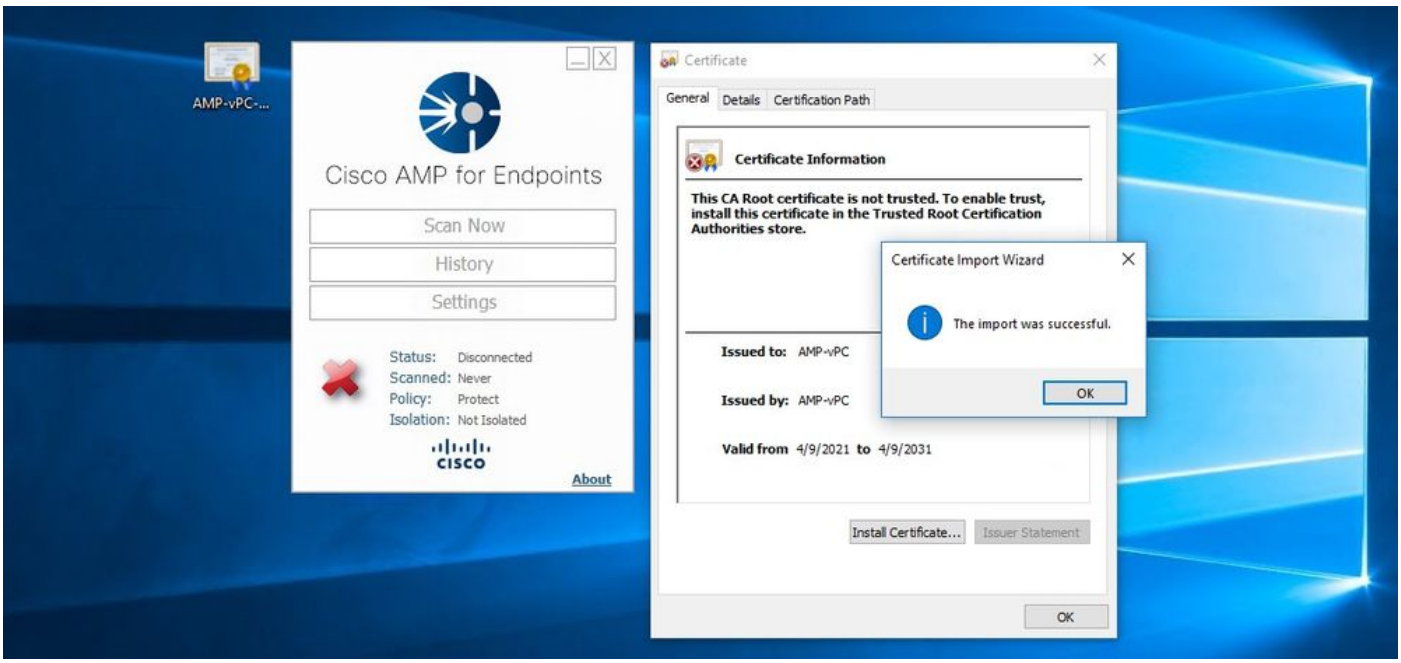
بمجرد تحميل المرجع المصدق الجذر في مخزن المرجع المصدق الجذر الموثوق به وإعادة تشغيل خدمة نقطة النهاية الآمنة. كل شيء يبدأ بالعمل كما هو متوقع.

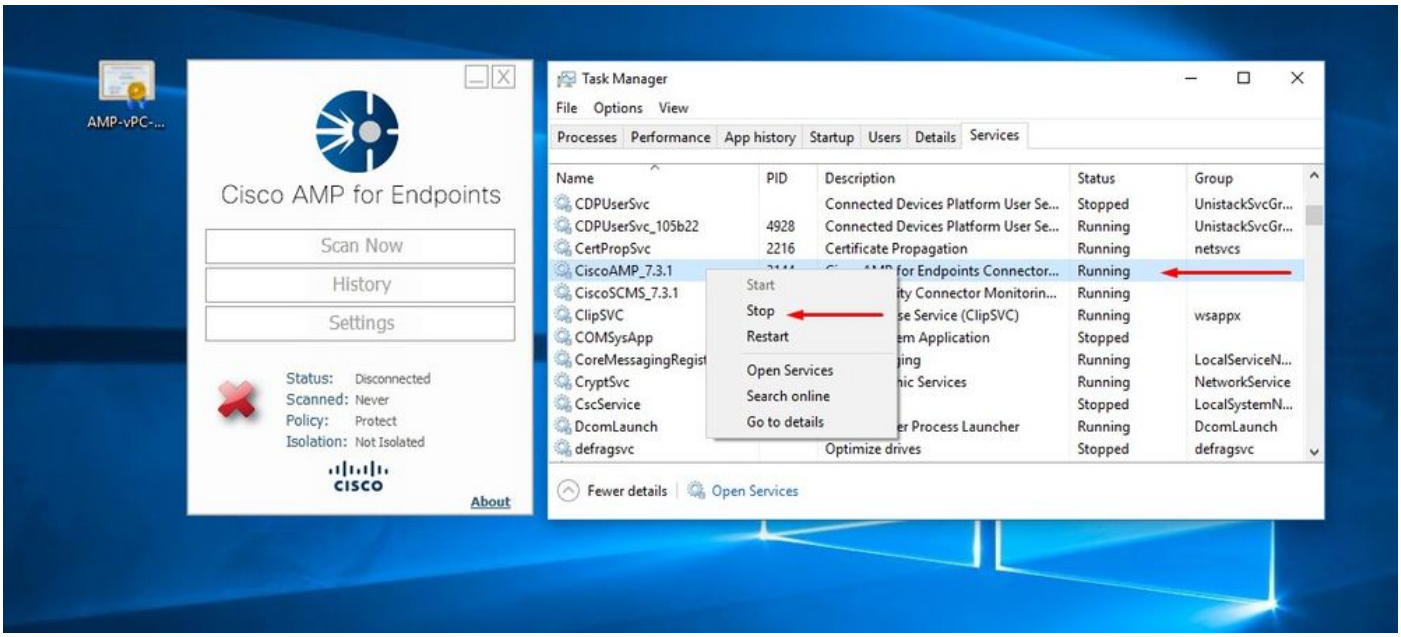



AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel

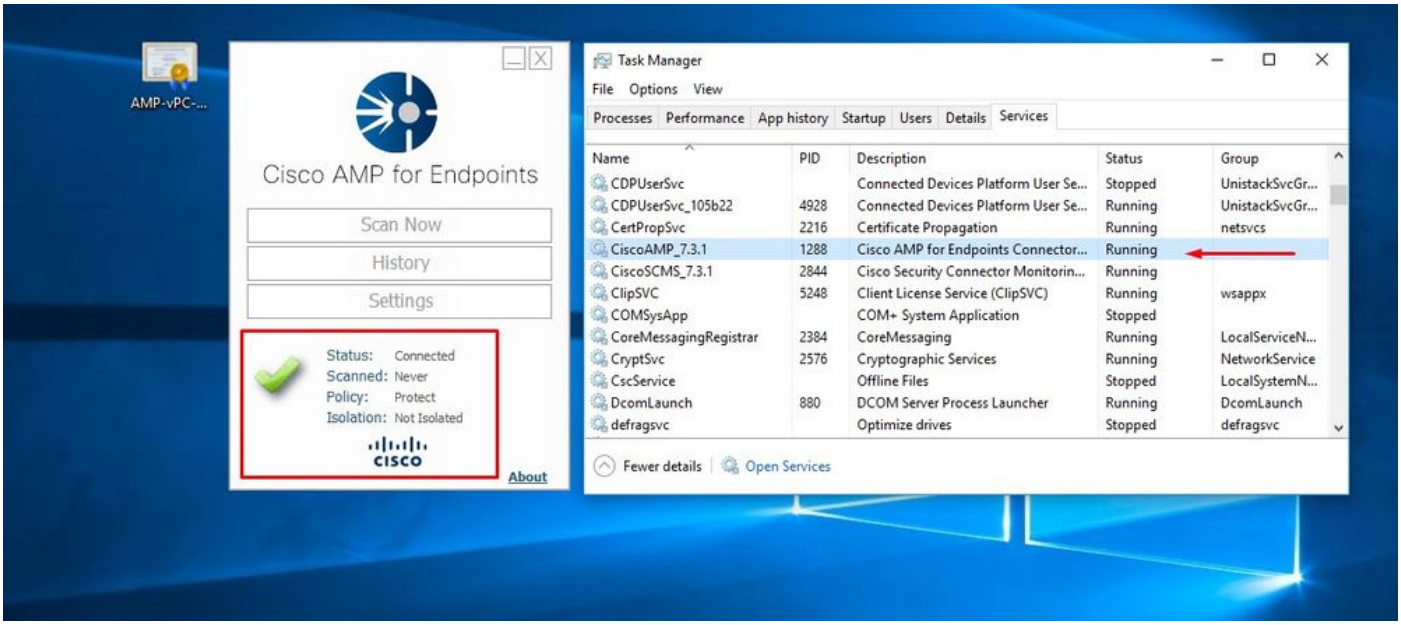

AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Browse...
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Show physical stores
OK
Cancel
Next
Cancel

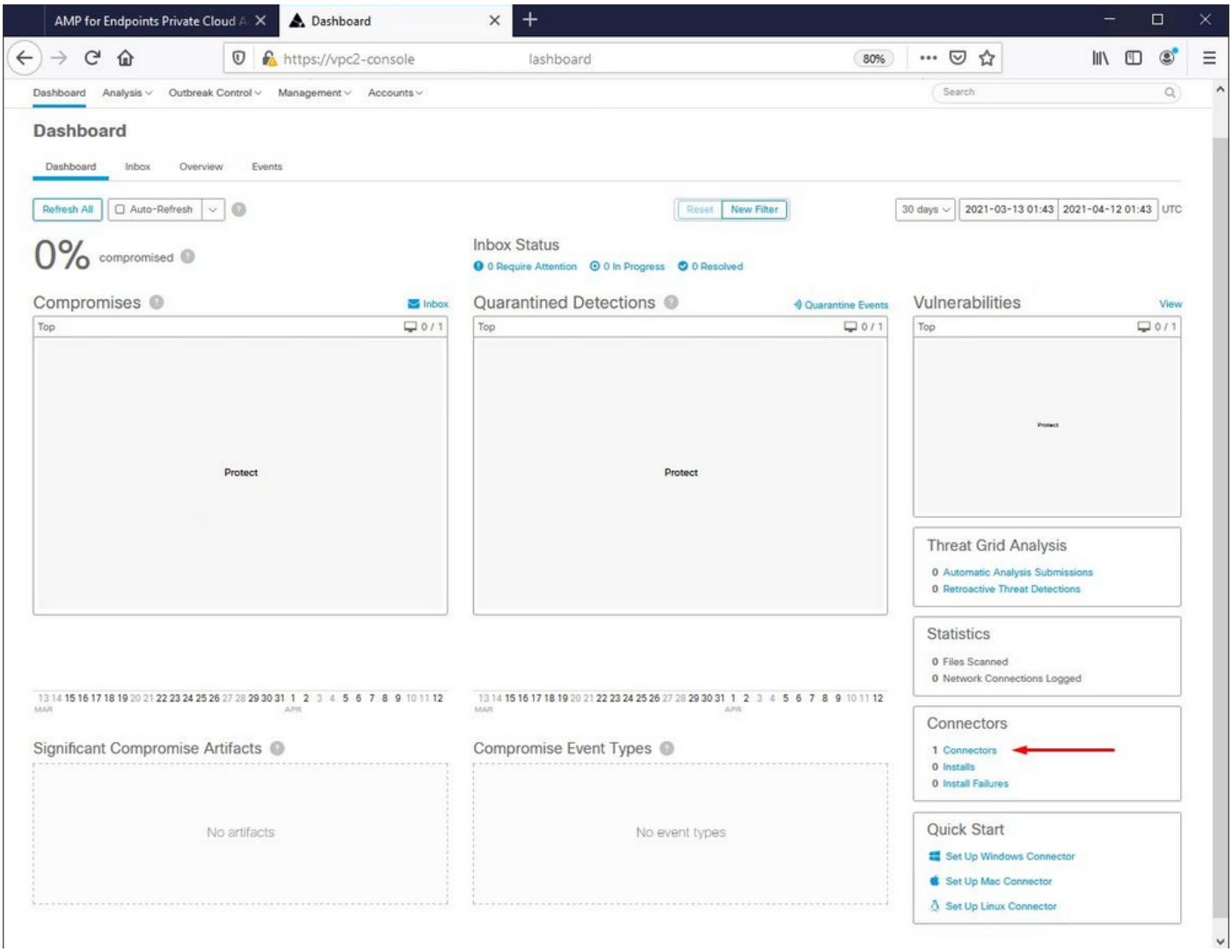

AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
Finish
Cancel


AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: AMP-vPC
Issued by: AMP-vPC
Valid from 4/9/2021 to 4/9/2031
Install Certificate...
Issuer Statement
OK
Certificate Import Wizard
The import was successful.
OK

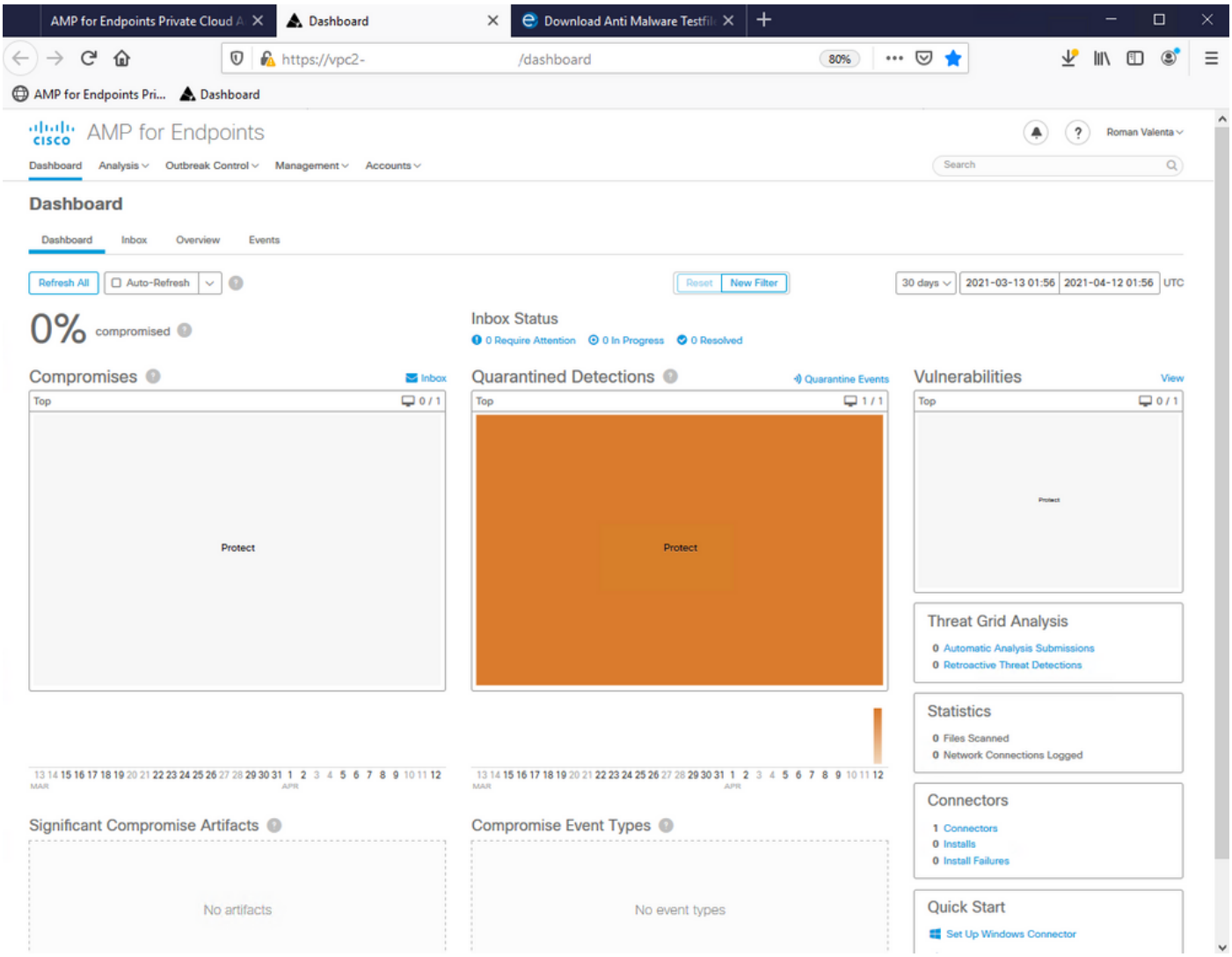


بمجرد إرتداد موصل خدمة نقطة النهاية الآمنة يصبح متصل كما هو متوقع.





نشاط ضار تم إختباره


AMP for Endpoints Private Cloud A
Dashboard
Download Anti Malware Testfil
https://vpc2-
/dashboard
80%
AMP for Endpoints Pri...
Dashboard
AMP for Endpoints
Roman Valenta
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
Refresh All
Auto-Refresh
Reset
New Filter
30 days
2021-03-13 01:56
2021-04-12 01:56
UTC
0%
compromised
Inbox Status
0 Require Attention
0 In Progress
0 Resolved
Compromises
Inbox
Top
0 / 1
Protect
Quarantined Detections
Quarantine Events
Top
1 / 1
Protect
Vulnerabilities
View
Top
0 / 1
Protect
Threat Grid Analysis
0 Automatic Analysis Submissions
0 Retroactive Threat Detections
Statistics
0 Files Scanned
0 Network Connections Logged
Connectors
1 Connectors
0 Installs
0 Install Failures
Quick Start
Set Up Windows Connector
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR
APR
Significant Compromise Artifacts
No artifacts
Compromise Event Types
No event types

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).