بناء الوحدات النمطية لنواة نقطة النهاية الآمنة Cisco Secure Endpoint Connector Linux Kernel Modules

المحتويات

المقدمة

يشرح هذا المقال كيفية تحديد وقت عدم توفر وحدات kernel النمطية المحولة مسبقا والمطلوبة لنظام الملفات الخاص بموصل Cisco Secure Endpoint Linux ومراقبة الشبكة لنواة النظام التي تعمل حاليا، والإجراء الخاص بتجميع وحدات kernel يدويا حتى يمكن تشغيل نظام الملفات ومراقبة الشبكة.

لغرض هذه المقالة، فإن "kernel غير المدعوم" هو إصدار kernel مدعوم من قبل موصل Linux ولكن وحدات kernel المحددة المحولة مسبقا والمطلوبة لإصدار kernel غير متضمنة في حزمة تثبيت الموصل وبالتالي يجب تحويلها برمجيا يدويا. يمكن أن تكون هذه هي الحال مع إصدار محدد من موصل ليونكس يعمل على نظام تشغيل يستخدم تحديث إصدار متدحرج، مثل Amazon Linux 2.

ليست جميع برامج ليونكس ودعم إصدارات kernel التي تشغل وحدات kernel المجمعة. ستساعد هذه المقالة في تحديد الوقت الذي يمكن فيه إستخدام تحويل وحدات kernel يدويا.

المتطلبات الأساسية

المتطلبات

- بالنسبة للأنظمة التي تعتمد على RHEL، يتم تركيب مجلس التعاون الخليجي الموفر للتوزيع مع دعم Kernel المثبت للعنصر الأساسي الجاري تشغيله حاليا.
- بالنسبة للأنظمة التي تستخدم برنامج Enterprise Kernel غير القابل للكسر (UEK) الذي يتم تركيبه عبر دول مجلس التعاون (GCC) الموفر للتوزيع والذي يتم تثبيته على kernel-uek-devel ليتم تشغيله حاليا على kernel.

قابلية التطبيق

نظام تشغيل

- نظام التشغيل RHEL/CentOS 7
- نواة Oracle Linux 7 المتوافقة مع Red Hat (RHCK)
- نظام التشغيل Oracle Linux 7 UEK 5 والإصدارات الأحدث
- أمازون لينكس 2

إصدارات Kernel

- يمكن تجميع وحدة kernel الخاصة بمراقبة الشبكة للإصدارات من 2.6 إلى 4.14 الشاملة.
- يمكن تجميع وحدة kernel الخاصة بمراقبة نظام الملفات لإصدارات kernel من 3.10 إلى 4.14 الشاملة.

ملاحظات:

- في إصدارات kernel 2.6 حتى 3.10، يستخدم الموصل تقاربر (وحدة kernel خارج الشجرة) لمراقبة نظام الملفات التي لا تنطبق على التحويل البرمجي المخصص.
- إصدارات Kernel التي تتراوح بين 4.19 و 4.14 غير متوافقة مع الموصل كما أنها غير قابلة للتطبيق على التحويل البرمجي المخصص.
- بالنسبة للإصدارات الأحدث من 4.19 Kernel، يستخدم الموصل وحدات eBPF المضمنة لنظام الملفات ومراقبة الشبكة. ارجع إلى مقالة أطلب kernel-devel من Linux للحصول على تفاصيل حول حل هذا الخطأ في إصدارات kernel هذه.

إصدارات الموصل

- الإصدار 1.16.0 والإصدارات الأحدث
- الإصدار 1.18.0 والإصدارات الأحدث لإنشاء وحدات مخصصة لنواة UEK

ديناميكيات Kernel غير معتمدة

عندما يتم تشغيل الموصل على جهاز كمبيوتر مزود بنواة غير مدعومة، سوف يتم رفع (فشلت الخطأ 8 والخطأ 9 (فشلت شاشة نظام الملفات في الوقت الحقيقي في البدء) الخطأ 8 (فشلت شاشة الشبكة في الوقت الحقيقي في البدء) وسيتم تشغيل الموصل في حالة متدهورة دون مراقبة نظام الملفات أو الشبكة.

يمكن تنفيذ الخطوات التالية من نافذة وحدة طرفية لتحديد ما إذا كان الموصل قيد التشغيل على عنصر kernel غير معتمد:

1. تحقق من وجود خطأ في الموصل 8 و/أو ظهور خطأ 9:

```
$ /opt/cisco/amp/bin/ampcli status [logger] Set minimum reported log level to notice Trying to connect... Connected. Status: Connected Mode: Degraded Scan: Ready for scan Last Scan: none Policy: unsupported kernel example (#7607) Command-line: Enabled Faults: 2 Critical Fault IDs: 8, 9 ID 8 - Critical: Realtime filesystem monitor failed to start. ID 9 - Critical: Realtime network monitor failed to start.
```

2. تحقق من أن نواة kernel الجاري تشغيلها حاليا تتراوح بين 2.6 و 4.14، بما في ذلك، وأنها لا تطابق أي من إصدارات وحدة kernel المحولة مسبقا.
   يعرض الأمر التالي إصدار kernel الجاري تشغيله الحالي:

```
$ uname -r 4.14.97-90.72.amzn2.x86_64
```

   يتم سرد إصدارات وحدة kernel المحولة مسبقا المتوفرة المحزمة مع الموصل باستخدام

الأمر التالي:

3.
```
$ ls /opt/cisco/amp/bin/modules/ 4.14.186-146.268.amzn2.x86_64 4.14.198-152.320.amzn2.x86_64 4.14.209-160.335.amzn2.x86_64 4.14.219-161.340.amzn2.x86_64 4.14.225-169.362.amzn2.x86_64 4.14.192-147.314.amzn2.x86_64 4.14.200-155.322.amzn2.x86_64 4.14.209-160.339.amzn2.x86_64 4.14.219-164.354.amzn2.x86_64 4.14.231-173.360.amzn2.x86_64 4.14.193-149.317.amzn2.x86_64 4.14.203-156.332.amzn2.x86_64 4.14.214-160.339.amzn2.x86_64 4.14.225-168.357.amzn2.x86_64 4.14.231-173.361.amzn2.x86_64
```
في المثال أعلاه، الإصدار 4.14.97-90.72.amzn2.x86_64 غير مدرج في قائمة وحدات kernel المتوفرة.

يعد موصل Linux مناسبا لتجميع وحدات kernel المخصصة إذا كان لك ما يلي صحيحا:

- الموصل به خطأ (أخطاء) 8 و/أو 9 مفعم.
- يتوافق إصدار kernel الحالي بين 2.6 و 4.14، بما في ذلك.
- الـ تم تضمين إصدار kernel الحالي في قائمة وحدات kernel النمطية المحملة مسبقا /opt/cisco/amp/bin/modules

رارق

إذا كان موصل Linux يعمل على نواة غير مدعومة، يمكن إستخدام الإجراء التالي لتجميع وحدات kernel المخصصة للنظام:

1. تثبيت تبعيات النظام المطلوبة:

```
$ yum install gcc
```
يلزم توفر لتجميع وحدات kernel بخيارات محددة.في المنظمة التي تستخدم نواة kernel المطلوبة: إلى RHEL، أستخدم الأمر التالي لتركيب حزمة kernel المستندة

```
$ yum install kernel-devel-$(uname -r)
```
في المنظمة التي تستخدم UEK، أستخدم الأمر التالي لتثبيت حزمة kernel المطلوبة:
```
$ yum install kernel-uek-devel-$(uname -r)
```
حسب النظام الخاص بك، يلزم Kernel-devel-$(uname -r) orkernel-uek-devel-$(uname -r) لتجميع وحدات kernel الخاصة بنواة التشغيل الحالية.

2. قم بتشغيل البرنامج النصي compile_kmods.sh مع امتيازات الجذر:
```
$ sudo /opt/cisco/amp/bin/compile_kmods.sh
```
سيحاول البرنامج النصي compile_kmods.sh إجراء تحويل برمجي لوحدات kernel الخاصة بنظام الملفات ومراقبة الشبكة إلى إصدار kernel الجاري تشغيله حاليا. سيتم إنشاء /opt/cisco/amp/extras/modules دليل. في نهاية التنفيذ، تضمن وحدات kernel المخصصة إلى البرنامج النصي إعادة تشغيل الموصل تلقائيا حتى يمكن تحميل وحدات kernel المحولة حديثا على النظام.

3. تأكد من مسح السلكيين 8 و 9:

```
$ /opt/cisco/amp/bin/ampcli status [logger] Set minimum reported log level to notice Trying to connect... Connected. Status: Connected Mode: Normal Scan: Ready for scan Last Scan: 2021-06-14 05:53 PM Policy: unsupported kernel example (#7607) Command-line: Enabled Faults: None
```

المزيد من الأوامر

يوفر الملف التنفيذي compile_kmods.sh في إصدارات موصل Linux الآمنة من نقطة

النهاية الإصدار 1.16.0 والإصدارات الأحدث، ويتم تثبيت هتيبثت تلقائيا على برامج أنظمة التشغيل المتوافقة. تم تحسين الملف التنفيذي COMPILE_kmods.sh في الإصدار 1.18.0 لموصل نقطة النهاية الآمنة Linux والإصدارات الأحدث لدعم التجميع المخصص من UEKs.

تم دعم وحدات kernel المخصصة المخصصة المخصصة لمراقبة الشبكة على إصدارات kernel من 2.6 إلى 4.14، بينما يتم دعم وحدات kernel المخصصة المخصصة المخصصة لمراقبة نظام الملفات على الإصدارات 3.10 حتى 4.14.

الأوامر المتوفرة

ملاحظة: يجب تشغيل الملف التنفيذي compile_kmods.sh مع امتيازات الجذر.

- يعرض خيار -h/– القائمة الكاملة للخيارات المتوفرة:

```
$ /opt/cisco/amp/bin/compile_kmods.sh --help Usage: compile_kmods [OPTIONS] OPTIONS: -f, --force force overwriting compiled kmod -h, --help show help
```

- يمكن استخدام خيار -f/-force لفرض إضافة وحدة kernel المخصصة التي تم تجميعها مسبقا إلى kernel الجاري تشغيله حاليا بحيث يتم الكتابة فوقه. يجب استخدام هذا الخيار إذا تم استخدام إصدار أقدم من الموصل ويلزم إعادة إنشاء وحدة kernel المخصصة الحالية باستخدام إصدار محدث من الموصل. لا يتم تحديث الموصل عملية مؤقتة لتحويلها برمجيا باستخدام إصدار محدث من الموصل. ال تتطلب إعادة تحويل وحدات نواة العميل برمجيا كجزء من التحديث.

استكشاف الأخطاء وإصلاحها

إذا كان هناك خطأ (أخطاء) 8 و/أو 9 ال يزال مرفوعا بعد *قرار* يتم اتباع الخطوات، ثم يمكن تنفيذ الخطوات التالية لمزيد من التحقيق في المسألة:

- ابحث عن سطور السجل في سجل النظام /var/log/ المماثلة لما يلي: يحتوي السجل التالي أن إصدار kernel الجاري تشغيله الحالي على الكمبيوتر ال يستخدم وحدات Kernel النمطية لنظام الملفات ومراقبة الشبكة. في إصدارات kernel الأكبر من أو تساوي 4.18، يتم مراقبة نظام الملفات والشبكة باستخدام وحدات eBPF.

```
init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.4.117-58.216.amzn2.x86_64'; skipping reinstalling kernel modules
```

  يشير السجل التالي إلى عدم العثور على إصدارات kernel في دليل وحدات kernel المحولة مسبقا، /opt/cisco/amp/bin/modules، المتوافقة مع إصدار kernel الجاري تشغيله الحالي:

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/bin/modules to install init: cisco-amp pre-start: failed to find kernel versions init: cisco-amp pre-start: failed to install and load all required kernel modules in /opt/cisco/amp/bin/modules, continuing without some modules loaded
```

  يشير السجل التالي إلى عدم العثور على إصدارات kernel في دليل وحدات kernel المحولة برمجيا المخصصة، /opt/cisco/amp/extra/modules، المتوافقة مع إصدار kernel الجاري تشغيله الحالي:

```
init: cisco-amp pre-start: finding compatible kernel modules in /opt/cisco/amp/extra/modules to install init: cisco-amp pre-start: failed to find kernel versions init: cisco-amp pre-start: failed to install and load all required kernel modules in /opt/cisco/amp/extra/modules, continuing without some modules loaded
```

- تحقق من تحميل نظام الملفات الآمن لموصل نقطة النهاية Linux والوحدات النمطية لنواة مراقبة الشبكة:

```
$ lsmod | grep ampfsm ampfsm 24576 0

$ lsmod | grep ampnetworkflow ampnetworkflow 65536 0
```

- قم بترقية موصل Secure Endpoint Linux إلى إصدار أحدث، إذا كان متوفرا.

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).