構建思科安全終端Linux聯結器核心模組

目錄

簡介

本文說明如何確定當前運行的系統核心何時無法使用Cisco Secure Endpoint Linux聯結器的檔案系統和網路監控所需的預編譯核心模組，以及如何手動編譯核心模組以使檔案系統和網路監控可正常運行。

就本文而言，「不受支援的核心」是Linux聯結器所支援的核心版本，但是該核心版本所需的特定預編譯核心模組不包含在聯結器安裝程式包中，因此必須手動編譯。對於使用滾動版本更新的作業系統上運行的指定Linux聯結器版本（例如Amazon Linux 2）來說，情況可能如此。

並非所有的Linux發行版和核心版本都支援運行編譯的核心模組。本文將對人工編譯可使用的核心模組進行識別。

必要條件

需求

- 對於基於RHEL的系統，安裝由分銷商提供的gcc;為當前運行的核心安裝了核心級別。
- 對於使用Unbreakable Enterprise Kernel(UEK)的系統，安裝由分發提供的gcc;為當前運行的核心安裝了kernel-uek-devel。

適用性

作業系統

- RHEL/CentOS 7
- Oracle Linux 7 Red Hat相容核心(RHCK)
- Oracle Linux 7 UEK 5及更低版本
- Amazon Linux 2

核心版本

- 網路監控核心模組可以針對核心版本2.6到4.14（含）進行編譯。
- 檔案系統監控核心模組可編譯為核心版本3.10到4.14（包括4.14）。

附註：

- 在核心版本2.6到3.10中，聯結器使用redirfs（樹外核心模組）進行檔案系統監視，該監視不適用於自定義編譯。
- 4.14和4.19之間的核心版本與聯結器不相容，也不適用於自定義編譯。
- 對於核心版本4.19和更新版本，聯結器使用eBPF模組進行檔案系統和網路監控。請參閱Linux核心級故障文章，瞭解有關解決這些核心版本上的此故障的詳細資訊。

聯結器版本

- 1.16.0及更高版本
- 1.18.0及更高版本用於建立自定義UEK核心模組

diag

當聯結器在含有不受支援核心的電腦上運行時，將引發故障8（即時檔案系統監視器無法啟動）和故障9（即時網路監視器無法啟動），並且聯結器將在沒有檔案系統或網路監視的降級狀態下運行。

可以從終端視窗執行以下步驟，以確定聯結器是否正在不受支援的核心上運行：

1. 驗證接頭是否出現故障8和/或故障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. 檢查當前運行的核心是否介於2.6和4.14之間（含這兩個值），並且它是否與任何預編譯的核心模組版本都不匹配。
   以下命令顯示當前運行的核心版本：

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

   使用下列命令列出隨聯結器打包的可用預編譯核心模組版本：

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
```

   在上面的示例中，核心版本4.14.97-90.72.amzn2.x86_64未包含在可用核心模組的清單中。

如果滿足以下所有條件，則Linux聯結器適用於編譯自定義核心模組：

- 聯結器發生故障8和/或9。
- 當前核心版本介於2.6和4.14之間（包括這兩個版本）。
- 預編譯的核心模組/opt/cisco/amp/bin/modules

解析

如果Linux聯結器在不支援的核心上運行，則可以使用以下過程為系統編譯自定義核心模組：

1. 安裝所需的系統依賴項：

   ```
   $ yum install gcc
   ```

   gcc是編譯具有特定選項的核心模組所必需的。在使用基於RHEL的核心的系統上，使用以下命令安裝所需的核心軟體包：

   ```
   $ yum install kernel-devel-$(uname -r)
   ```

   在使用UEK的系統上，使用以下命令安裝所需的核心軟體包：

   ```
   $ yum install kernel-uek-devel-$(uname -r)
   ```

   根據您的系統，需要kernel-devely-$(uname-r)kernel-uek-devely-$(uname-r)才能為當前運行的核心編譯核心模組。
2. 運行具有root許可權的compile_kmods.sh指令碼：

   ```
   $ sudo /opt/cisco/amp/bin/compile_kmods.sh
   ```

   compile_kmods.sh指令碼將嘗試為當前運行的核心版本編譯檔案系統和網路監控核心模組。自定義核心模組將在 /opt/cisco/amp/extras/modules 目錄。執行結束時，指令碼將自動重新啟動聯結器，以便可以將新編譯的核心模組載入到系統上。
3. 確認故障8和9已清除：

   ```
   $ /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
   ```

更多命令

compile_kmods.sh執行檔在Secure Endpoint Linux聯結器1.16.0版和更新版本中可用，並且它自動安裝在相容的作業系統發行版中。compile_kmods.sh執行檔在Secure Endpoint Linux connector 1.18.0版和更新版本中進行了改進，以支援UEK的自定義編譯。

核心版本2.6至4.14支援用於網路監控的自定義編譯核心模組，而核心版本3.10至4.14支援用於檔案系統監控的自定義編譯核心模組。

可用命令

附註：compile_kmods.sh執行檔必須使用root許可權運行。

- -h/-help示可用選項的完整清單：

  ```
  $ /opt/cisco/amp/bin/compile_kmods.sh --help Usage: compile_kmods [OPTIONS] OPTIONS: -f, --
  force force overwriting compiled kmod -h, --help show help
  ```
- -f/—force選項可用於強制覆蓋先前編譯的自定義核心模組，以便覆蓋當前運行的核心。當當前自定義核心模組是使用較舊版本的聯結器構建的，並且需要使用更新版本的聯結器重新編譯時，應使用此引數。聯結器更新過程不會在更新過程中重新編譯客戶核心模組。

疑難排解

如果故障8和/或9在 *解析* 請按照以下步驟操作，然後可以執行以下步驟來進一步調查問題：

- 在系統日誌/var/log/messages內容類似的日誌行： 以下日誌說明電腦上當前運行的核心版本不使用核心模組監視檔案系統和網路。在大於或等於4.18的核心版本上，使用eBPF模組監視檔案系統和網路。

  ```
  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
  ```

  以下日誌說明在預編譯的核心模組目錄中找不到核心版本， /opt/cisco/amp/bin/modules，與當前運行的核心版本相容：

  ```
  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
  ```

  以下日誌說明在自定義編譯的核心模組目錄中找不到核心版本，
  /opt/cisco/amp/extra/modules，與當前運行的核心版本相容：

  ```
  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
  ```

- 檢查是否載入了Secure Endpoint Linux聯結器檔案系統和網路監控核心模組：

  ```
  $ lsmod | grep ampfsm ampfsm 24576 0
  ```

  ```
  $ lsmod | grep ampnetworkflow ampnetworkflow 65536 0
  ```

- 將Secure Endpoint Linux聯結器升級到更新版本（如果可用）。