



Red Hat Advanced Cluster Security for Kubernetes 4.4

Collector 故障排除

Collector 故障排除

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

使用本指南了解如何在 Collector 中检索日志并调试问题。

目录

第 1 章 检索和分析 COLLECTOR 日志和 POD 状态	3
1.1. 检索 COLLECTOR 日志	3
1.2. 分析 COLLECTOR POD 状态	4
第 2 章 经常发生的错误条件	5
2.1. 无法连接到 SENSOR	5
2.2. 内核驱动程序不可用	6
2.3. 无法载入内核驱动程序	7

第 1 章 检索和分析 COLLECTOR 日志和 POD 状态

故障排除中的第一步是检索日志和 pod 状态。日志可以帮助您识别错误的根本原因。另外，检查 pod 的最新状态可以了解有关失败的信息。

1.1. 检索 COLLECTOR 日志

首先，您应该从失败的 Collector 检查日志。根据您的环境和访问权限，您可以以两种方式获取这些日志：

- 使用 `oc` 或 `kubectl` 命令检索日志
- 从 RHACS 诊断捆绑包中检索日志

1.1.1. 使用 `oc` 或 `kubectl` 命令检索日志

您可以使用 `oc` 或 `kubectl` 命令从正在运行的 Collector pod 获取日志。另外，如果当前的 Collector pod 正在重启，您也可以从以前的 Collector pod 检查日志。

先决条件

- 确保具有列出 pod 和日志的颁发机构：

```
$ oc auth can-i get pods && oc auth can-i get pods --subresource=logs 1
```

- 1 如果使用 Kubernetes，请输入 `kubectl` 而不是 `oc`。

流程

1. 列出带有标签 `app=collector` 的所有 pod：

```
$ oc get pods -n stackrox -l app=collector 1
```

- 1 如果使用 Kubernetes，请输入 `kubectl` 而不是 `oc`。

输出示例

```
collector-vclg5 1/2 CrashLoopBackOff 2 (25s ago) 2m41s+
```

2. 获取 Collector pod 的日志：

```
$ oc logs -n stackrox <collector_pod_name> collector 1
```

- 1 如果使用 Kubernetes，请输入 `kubectl` 而不是 `oc`。对于 `<collector_pod_name>`，指定 Collector pod 的名称，如 `collector-vclg5`。

3. （可选）如果当前的 Collector pod 正在重启，您可以检查前面 Collector pod 的日志：

```
$ oc logs -n stackrox <collector_pod_name> collector --previous 1
```

- 1 如果使用 Kubernetes，请输入 **kubectl** 而不是 **oc**。对于 **<collector_pod_name>**，指定 Collector pod 的名称，如 **collector-vclg5**。

1.1.2. 从 RHACS 诊断捆绑包中检索日志

您还可以通过从 Red Hat Advanced Cluster Security for Kubernetes (RHACS) 用户界面下载诊断捆绑包来访问 Collector 日志。下载诊断捆绑包后，您可以检查所有 Collector pod 的日志。如需更多信息，请参阅 [生成诊断捆绑包](#)。

1.2. 分析 COLLECTOR POD 状态

检查 pod 的最新状态是确定 Collector 崩溃原因的另一种简单的方法。失败消息被记录到最新状态，并可使用 **kubectl describe pod** 或 **oc describe pod** 命令访问。

流程

- 描述 Collector pod :

```
$ oc describe pod -n stackrox <collector_pod_name> 1
```

- 1 如果使用 Kubernetes，请输入 **kubectl** 而不是 **oc**。对于 **<collector_pod_name>**，指定 Collector pod 的名称，如 **collector-vclg5**。

输出示例

```
# ...
Last State:   Terminated
Reason:      Error
Message:     No suitable kernel object downloaded 1
Exit Code:   1
Started:    Fri, 21 Oct 2022 11:50:56 +0100
Finished:   Fri, 21 Oct 2022 11:51:25 +0100
# ...
```

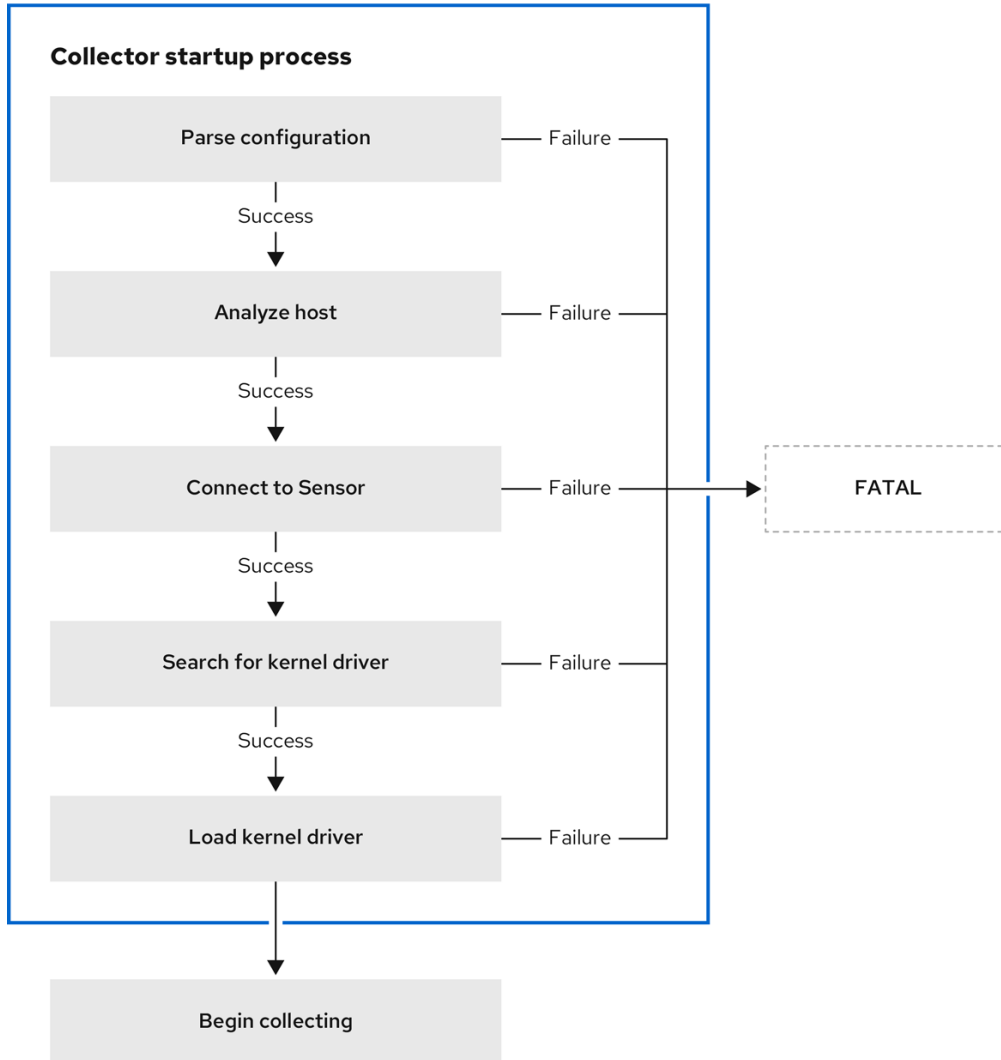
- 1 在这个示例中，您可以看到 Collector 无法下载内核驱动程序。

第 2 章 经常发生的错误条件

当 Collector 配置其自身并为系统查找或下载内核驱动程序时，Collector 启动过程中会出现大多数错误。

下图显示了 Collector 启动过程的主要部分：

图 2.1. 收集器 pod 启动过程



304_RHACS_0123

如果启动过程中的任何部分失败，日志会显示一个诊断概述，详细描述了哪些步骤成功或失败。

以下日志文件示例演示了成功启动：

```

[INFO 2022/11/28 13:21:55] == Collector Startup Diagnostics: ==
[INFO 2022/11/28 13:21:55] Connected to Sensor? true
[INFO 2022/11/28 13:21:55] Kernel driver available? true
[INFO 2022/11/28 13:21:55] Driver loaded into kernel? true
[INFO 2022/11/28 13:21:55] =====
  
```

日志输出确认 Collector 连接到 Sensor 并加载内核驱动程序。您可以使用此日志检查 Collector 是否成功启动。

2.1. 无法连接到 SENSOR

在启动时，首先检查您可以连接到 Sensor。Sensor 负责下载处理网络事件的内核驱动程序和 CIDR 块，使其成为启动过程的基本部分。以下日志表示您无法连接到 Sensor：

```
Collector Version: 3.15.0
OS: Ubuntu 20.04.4 LTS
Kernel Version: 5.4.0-126-generic
Starting StackRox Collector...
[INFO 2023/05/13 12:20:43] Hostname: 'hostname'
[...]
[INFO 2023/05/13 12:20:43] Sensor configured at address: sensor.stackrox.svc:9998
[INFO 2023/05/13 12:20:43] Attempting to connect to Sensor
[INFO 2023/05/13 12:21:13]
[INFO 2023/05/13 12:21:13] == Collector Startup Diagnostics: ==
[INFO 2023/05/13 12:21:13] Connected to Sensor? false
[INFO 2023/05/13 12:21:13] Kernel driver candidates:
[INFO 2023/05/13 12:21:13] =====
[INFO 2023/05/13 12:21:13]
[FATAL 2023/05/13 12:21:13] Unable to connect to Sensor.
```

这个错误可能意味着 Sensor 没有正确启动，或者 Collector 配置不正确。要解决这个问题，您必须验证 Collector 配置以确保 Sensor 地址正确，并且 Sensor pod 正常运行。

查看 Collector 日志，以专门检查配置的 Sensor 地址。另外，您可以运行以下命令：

```
$ kubectl -n stackrox get pod <collector_pod_name> -o jsonpath='{.spec.containers[0].env[?(@.name=="GRPC_SERVER")].value}' ❶
```

❶ 对于 **<collector_pod_name>**，指定 Collector pod 的名称，如 **collector-vc1g5**。

2.2. 内核驱动程序不可用

收集器确定它是否有节点内核版本的内核驱动程序。收集器首先搜索带有正确版本和类型的驱动程序的本地存储，然后尝试从 Sensor 下载驱动程序。以下日志表示本地内核驱动程序或 Sensor 中的驱动程序都不存在：

```
Collector Version: 3.15.0
OS: Alpine Linux v3.16
Kernel Version: 5.15.82-0-virt
Starting StackRox Collector...
[INFO 2023/05/30 12:00:33] Hostname: 'alpine'
[INFO 2023/05/30 12:00:33] User configured collection-method=ebpf
[INFO 2023/05/30 12:00:33] Afterglow is enabled
[INFO 2023/05/30 12:00:33] Sensor configured at address: sensor.stackrox.svc:443
[INFO 2023/05/30 12:00:33] Attempting to connect to Sensor
[INFO 2023/05/30 12:00:33] Successfully connected to Sensor.
[INFO 2023/05/30 12:00:33] Module version: 2.5.0-rc1
[INFO 2023/05/30 12:00:33] Config: collection_method:0, useChiselCache:1, scrape_interval:30,
turn_off_scrape:0, hostname:alpine, processesListeningOnPorts:1, logLevel:INFO
[INFO 2023/05/30 12:00:33] Attempting to find eBPF probe - Candidate versions:
[INFO 2023/05/30 12:00:33] collector-ebpf-5.15.82-0-virt.o
[INFO 2023/05/30 12:00:33] Attempting to download collector-ebpf-5.15.82-0-virt.o
[INFO 2023/05/30 12:00:33] Attempting to download kernel object from
https://sensor.stackrox.svc:443/kernel-objects/2.5.0/collector-ebpf-5.15.82-0-virt.o.gz ❶
```

```
[INFO 2023/05/30 12:00:33] HTTP Request failed with error code 404 2
[WARNING 2023/05/30 12:02:03] Attempted to download collector-ebpf-5.15.82-0-virt.o.gz 90 time(s)
[WARNING 2023/05/30 12:02:03] Failed to download from collector-ebpf-5.15.82-0-virt.o.gz
[WARNING 2023/05/30 12:02:03] Unable to download kernel object collector-ebpf-5.15.82-0-virt.o to
/module/collector-ebpf.o.gz
[WARNING 2023/05/30 12:02:03] No suitable kernel object downloaded for collector-ebpf-5.15.82-0-
virt.o
[ERROR 2023/05/30 12:02:03] Failed to initialize collector kernel components.
[INFO 2023/05/30 12:02:03]
[INFO 2023/05/30 12:02:03] == Collector Startup Diagnostics: ==
[INFO 2023/05/30 12:02:03] Connected to Sensor? true
[INFO 2023/05/30 12:02:03] Kernel driver candidates:
[INFO 2023/05/30 12:02:03] collector-ebpf-5.15.82-0-virt.o (unavailable)
[INFO 2023/05/30 12:02:03] =====
[INFO 2023/05/30 12:02:03]
[FATAL 2023/05/30 12:02:03] Failed to initialize collector kernel components. 3
```

- 1 日志显示尝试首先定位模块，然后是从 Sensor 下载驱动程序的任何努力。
- 2 404 错误表示节点内核没有内核驱动程序。
- 3 由于缺少驱动程序，Collector 进入 **CrashLoopBackOff** 状态。

内核版本 文件包含所有支持的内核版本的列表。

2.3. 无法载入内核驱动程序

在 Collector 启动前，它会载入内核驱动程序。然而，在个别情况下，您可能会遇到 Collector 无法加载内核驱动程序的问题，从而导致各种错误消息或异常。在这种情况下，您必须检查日志来识别载入内核驱动程序时失败的问题。

考虑以下 Collector 日志：

```
[INFO 2023/05/13 14:25:13] Hostname: 'hostname'
[...]
[INFO 2023/05/13 14:25:13] Successfully downloaded and decompressed /module/collector.o
[INFO 2023/05/13 14:25:13]
[INFO 2023/05/13 14:25:13] This product uses ebpf subcomponents licensed under the GNU
[INFO 2023/05/13 14:25:13] GENERAL PURPOSE LICENSE Version 2 outlined in the /kernel-
modules/LICENSE file.
[INFO 2023/05/13 14:25:13] Source code for the ebpf subcomponents is available at
[INFO 2023/05/13 14:25:13] https://github.com/stackrox/falcosecurity-libs/
[INFO 2023/05/13 14:25:13]
-- BEGIN PROG LOAD LOG --
[...]
-- END PROG LOAD LOG --
[WARNING 2023/05/13 14:25:13] libscap: bpf_load_program()
event=tracepoint/syscalls/sys_enter_chdir: Operation not permitted
[ERROR 2023/05/13 14:25:13] Failed to setup collector-ebpf-6.2.0-20-generic.o
[ERROR 2023/05/13 14:25:13] Failed to initialize collector kernel components.
[INFO 2023/05/13 14:25:13]
[INFO 2023/05/13 14:25:13] == Collector Startup Diagnostics: ==
[INFO 2023/05/13 14:25:13] Connected to Sensor? true
[INFO 2023/05/13 14:25:13] Kernel driver candidates:
```

```
[INFO 2023/05/13 14:25:13] collector-ebpf-6.2.0-20-generic.o (available)
[INFO 2023/05/13 14:25:13] =====
[INFO 2023/05/13 14:25:13]
[FATAL 2023/05/13 14:25:13] Failed to initialize collector kernel components.
```

如果您遇到此类错误，您不太可能自己修复它。因此，将其报告给 Red Hat Advanced Cluster Security for Kubernetes (RHACS)支持团队，或创建 [GitHub 问题](#)。