Red Hat Advanced Cluster Security for Kubernetes 4.5

Collector のトラブルシューティング

Collector のトラブルシューティング

Last Updated: 2024-09-16

Red Hat Advanced Cluster Security for Kubernetes 4.5 Collector のトラブルシューティング

Collector のトラブルシューティング

法律上の通知

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.

概要

このガイドを使用して、ログを取得し、失敗した Collector の問題をデバッグする方法を学習してください。

目次

第1章 COLLECTOR ログと POD ステータスの取得と分析

トラブルシューティングの最初のステップは、ログと Pod のステータスを取得することです。ログにより、エラーの根本原因を特定できます。さらに、Pod の最新のステータスを調べると、失敗メッセージに関する情報が得られます。

1.1. COLLECTOR ログの取得

まず、失敗した Collector からのログを調べる必要があります。環境とアクセス権限に応じて、次の 2 つの方法でログを取得できます。

- **oc** または **kubectl** コマンドを使用したログの取得
- RHACS 診断バンドルからのログの取得

1.1.1. oc または kubectl コマンドによるログの取得

oc または **kubectl** コマンドを使用して、実行中の Collector Pod からログを取得できます。必要に応じて、現在の Collector Pod が再起動している場合は、以前の Collector Pod のログを確認することもできます。

前提条件

- Pod とログを一覧表示する権限がある。

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

(1) Kubernetes を使用する場合は、**oc** の代わりに **kubectl** を入力します。

手順

1. ラベル **app=collector** が付いたすべての Pod を一覧表示します。

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

(1) Kubernetes を使用する場合は、**oc** の代わりに **kubectl** を入力します。

出力例

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

2. Collector Pod のログを取得します。

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

(1) Kubernetes を使用する場合は、**oc** の代わりに **kubectl** を入力します。**<collector_pod_name>** には、Collector Pod の名前 (**collector-vclg5** など) を指定します。

3. (オプション) 現在の Collector Pod が再起動している場合は、以前の Collector Pod のログを確認できます。

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

(1) Kubernetes を使用する場合は、**oc** の代わりに **kubectl** を入力します。**<collector_pod_name>** には、Collector Pod の名前 (**collector-vclg5** など) を指定します。

1.1.2. RHACS 診断バンドルからのログの取得

Red Hat Advanced Cluster Security for Kubernetes (RHACS) ユーザーインターフェイスから診断バンドルをダウンロードして、Collector ログにアクセスすることもできます。診断バンドルをダウンロードしたら、すべての Collector Pod のログを調べることができます。詳細は、診断バンドルの生成 を参照してください。

1.2. COLLECTOR POD のステータスの分析

Pod の最新のステータスを調べることは、Collector のクラッシュの原因を特定するもう 1 つの簡単な方法です。失敗メッセージは最新の状態に記録され、**kubectl describe pod** または **oc describe pod** コマンドを使用してアクセスできます。

手順

- Collector Pod に関する情報を表示できます。

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

(1) Kubernetes を使用する場合は、**oc** の代わりに **kubectl** を入力します。**<collector_pod_name>** には、Collector Pod の名前 (**collector-vclg5** など) を指定します。

出力例

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

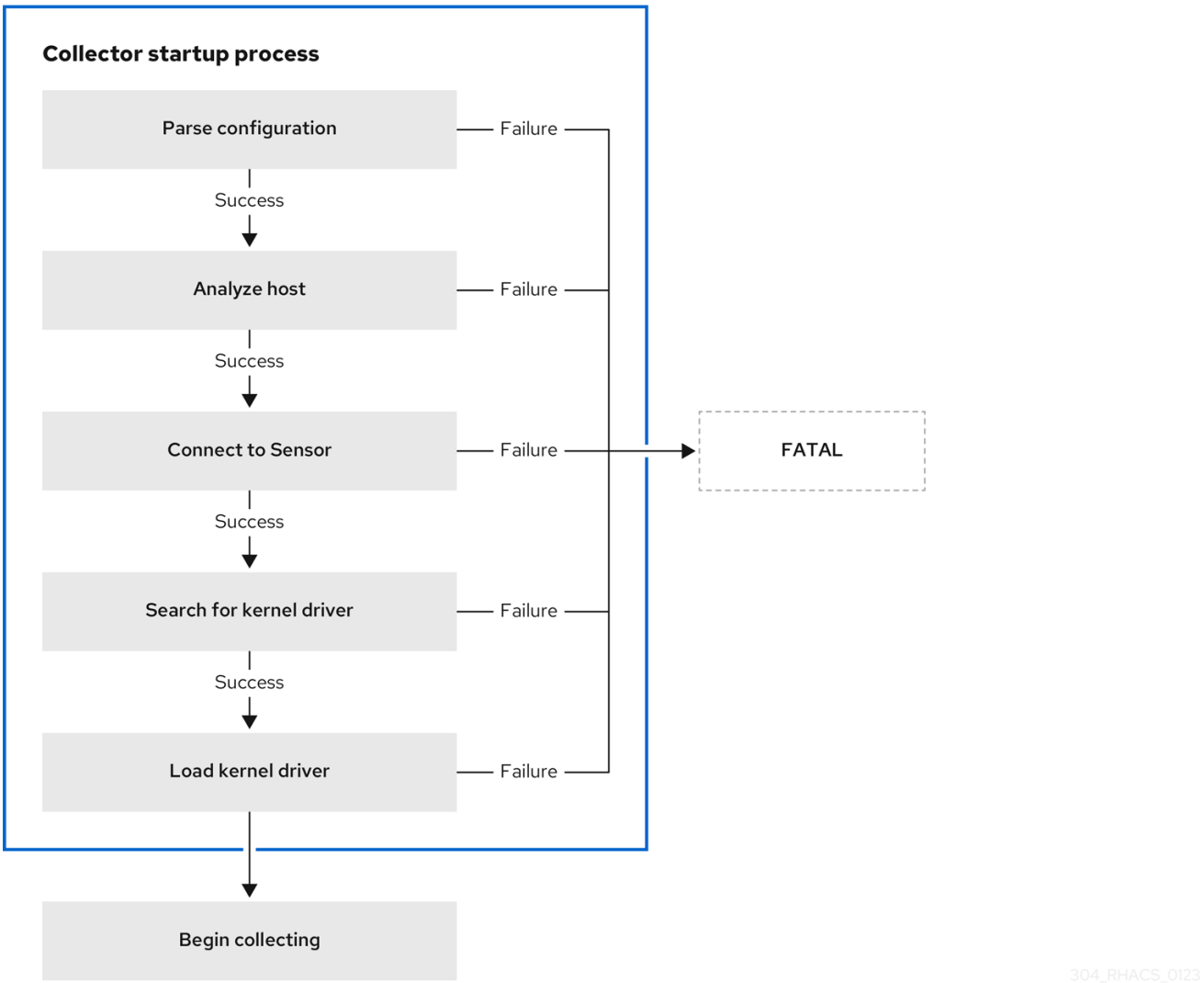
(1) この例では、Collector がカーネルドライバーのダウンロードに失敗したことがわかります。

第2章 よくあるエラー状態

Collector が、自身を設定し、システムのカーネルドライバーを検索またはダウンロードする場合、エラーの大部分は Collector の起動時に発生します。

次の図は、Collector の起動プロセスの主要部分を示しています。

図2.1 Collector Pod の起動プロセス



起動手順の一部が失敗した場合、ログには、成功または失敗した手順の詳細を示す診断概要が表示されます。

次のログファイルの例は、正常な起動を示しています。

```
[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] =====================================
```

ログ出力は、Collector が Sensor に接続し、カーネルドライバーを見つけてロードしたことを確認します。このログを使用して、Collector が正常に起動したかどうかを確認できます。

2.1. SENSOR に接続できない

起動したら、まず Sensor に接続できるかを確認します。Sensor は、ネットワークイベントを処理するためのカーネルドライバーと CIDR ブロックのダウンロードを実行し、起動プロセスの重要な部分となっています。次のログは、Sensor に接続できないことを示しています。

```
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.
```

このエラーは、Sensor が正しく起動していないか、Collector の設定が正しくないことを意味している可能性があります。この問題を解決するには、Collector の設定を確認して、Sensor アドレスが正しく、Sensor Pod が正しく実行されていることを確認する必要があります。

Collector ログを表示して、設定された Sensor アドレスを具体的に確認します。または、次のコマンドを実行できます。

```
$ kubectl -n stackrox get pod <collector_pod_name> -o jsonpath='{.spec.containers[0].env[?(@.name=="GRPC_SERVER")].value}' 1
```

1 **<collector_pod_name>** には、Collector Pod の名前 (**collector-vclg5** など) を指定します。

2.2. カーネルドライバーが利用できない

Collector は、ノードのカーネルバージョン用のカーネルドライバーがあるかどうかを判断します。Collector は、まずローカルストレージで正しいバージョンとタイプのドライバーを検索し、次に Sensor からドライバーをダウンロードしようとします。次のログは、ローカルカーネルドライバーも Sensor のドライバーも存在しないことを示しています。

```
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 (1)
[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) ログ表示では、まずモジュールの検索が試行され、次に Sensor からドライバーをダウンロードしようとします。

(2) 404 エラーは、ノードのカーネルにカーネルドライバーがないことを示します。

(3) ドライバーがないため、Collector は **CrashLoopBackOff** 状態になります。

カーネルバージョン ファイルには、サポートされているすべてのカーネルバージョンのリストが含まれています。

2.3. カーネルドライバーのロードに失敗する

Collector が起動する前に、カーネルドライバーがロードされます。ただし、まれに、Collector がカーネルドライバーをロードできず、さまざまなエラーメッセージや例外が出力されるという問題が発生する場合があります。このような場合は、ログを確認して、カーネルドライバーのロードに失敗した問題を特定する必要があります。

次の Collector ログを検討してください。

```
[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.
```

このようなエラーが発生した場合、自分で修正できる可能性はほとんどありません。このような場合は、Red Hat Advanced Cluster Security for Kubernetes (RHACS) サポートチームに報告するか、GitHub の問題 を作成してください。