Red Hat Quay 3.12

在 Red Hat Quay 中使用 Clair 报告漏洞

在 Red Hat Quay 中使用 Clair 报告漏洞

Last Updated: 2024-11-08

Red Hat Quay 3.12 在 Red Hat Quay 中使用 Clair 报告漏洞

在 Red Hat Quay 中使用 Clair 报告漏洞

法律通告

摘要

Clair 入门

目录

前言

本指南中的内容概述了 Red Hat Quay 的 Clair，它在独立的 Red Hat Quay 和 Operator 部署上运行 Clair，以及高级 Clair 配置。

部分 I. 在 RED HAT QUAY 概述中带有 CLAIR 的漏洞报告

本指南中的内容解释了 Red Hat Quay 上 Clair 的关键目的和概念。它还包含有关 Clair 发行版本的信息以及官方 Clair 容器的位置。

第 1 章 CLAIR 安全扫描程序

Clair v4 (Clair)是一个开源应用程序，它利用静态代码分析来解析镜像内容和报告影响内容的漏洞。Clair 与 Red Hat Quay 打包，可用于独立和 Operator 部署。它可以在高度可扩展的配置中运行，根据企业环境，可以单独扩展组件。

1.1. 关于 CLAIR

Clair 使用来自国家漏洞数据库(NVD)的通用漏洞评分系统(CVSS)数据来增强漏洞数据，这是美国政府与安全相关的信息的美国政府存储库，包括各种软件组件和系统中的已知漏洞和安全问题。使用 NVD 中的分数为 Clair 提供以下优点：

- 数据同步.Clair 可以定期将其漏洞数据库与 NVD 同步。这样可确保它具有最新的漏洞数据。
- 匹配和增强.Clair 将容器镜像中发现的漏洞的元数据和标识符与来自 NVD 的数据进行比较。这个过程涉及将唯一标识符（如通用漏洞和暴露(CVE) ID）与 NVD 中的条目匹配。找到匹配项时，Clair 可以使用来自 NVD 的更多详细信息（如严重性分数、描述和引用）增强其漏洞信息。
- 严重性分数.NVD 为漏洞分配严重性分数，如通用漏洞评分系统(CVSS)分数，以指示与每个漏洞相关的潜在影响和风险。通过合并 NVD 的严重性分数，Clair 可以针对它所检测到的漏洞的严重程度提供更多上下文。

如果 Clair 从 NVD 找到漏洞，则向 UI 上的用户报告了对容器镜像中检测到的漏洞的严重性和标准化评估。CVSS 增强数据提供以下优点：

- 漏洞优先级排序.通过利用 CVSS 分数，用户可以根据自己的严重性来优先选择漏洞，帮助他们首先解决最重要的问题。
- 评估风险.CVSS 分数可帮助 Clair 用户了解对容器化应用程序造成漏洞的潜在风险。
- 通信严重性.CVSS 分数为 Clair 用户提供了一种标准化的方式，用于交流不同团队和机构中的漏洞的严重性。
- 通知修复策略.CVSS 丰富数据可以指导 Quay.io 用户开发适当的补救策略。
- 合规性和报告.将 CVSS 数据整合到 Clair 生成的报告中，可帮助组织展示其解决安全漏洞并遵守行业标准和法规的承诺。

1.1.1. Clair 发行版本

Clair 的新版本会定期发布。构建 Clair 所需的源代码打包为存档并附加到每个版本。Clair 版本可在 Clair 版本 中找到。

发行工件还包括 **clairctl** 命令行界面工具，该工具使用开放主机从互联网获取更新器数据。

Clair 4.7.4
Clair 4.7.4 于 2024-05-01 发布。进行了以下更改：

- 默认层下载位置已更改。如需更多信息，请参阅 磁盘使用情况注意事项。

Clair 4.7.3
Clair 4.7.3 在 2024-02-26 中发布。进行了以下更改：

- Clair 的最低 TLS 版本现在是 1.2。在以前的版本中，服务器允许 1.1 连接。

Clair 4.7.2

Clair 4.7.2 在 2023-10-09 上发布。进行了以下更改：

- 已删除 CRDA 支持。

Clair 4.7.1
Clair 4.7.1 作为 Red Hat Quay 3.9.1 的一部分发布。进行了以下更改：

- 在这个版本中，您可以查看 Red Hat Enterprise Linux (RHEL)源中未修补的漏洞。如果要查看未修补的漏洞，您可以将 **ignore_unpatched** 参数设置为 **false**。例如：

```
updaters:
  config:
    rhel:
      ignore_unpatched: false
```

  要禁用此功能，您可以将 **ignore_unpatched** 设置为 **true**。

Clair 4.7
Clair 4.7 作为 Red Hat Quay 3.9 的一部分发布，包括对以下功能的支持：

- 对容器镜像中的 Golang 模块和 RubeGems 进行原生支持。
- 更改为 OSV.dev 作为任何编程语言软件包管理器的漏洞数据库源。
  - 这包括 GitHub 安全公告或 PyPA 等流行源。
  - 这允许离线功能。
- 将 pyup.io 用于 Python，CRDA 用于 Java 已被暂停。
- Clair 现在支持 Java、Golang、Python 和 Ruby 依赖项。

1.1.2. Clair 漏洞数据库

Clair 使用以下漏洞数据库报告镜像中的问题：

- Ubuntu Oval 数据库
- Debian 安全跟踪器
- Red Hat Enterprise Linux (RHEL) Oval 数据库
- SUSE Oval 数据库
- Oracle Oval 数据库
- alpine SecDB 数据库
- VMware Photon OS 数据库
- Amazon Web Services (AWS) UpdateInfo
- 开源漏洞(OSV)数据库

1.1.3. Clair 支持的依赖项

Clair 支持识别和管理以下依赖项：

- Java
- Golang
- Python
- Ruby

这意味着它可以分析和报告这些语言中项目依赖的第三方库和软件包，以便正常工作。

当包含 Clair 不支持的语言中软件包的镜像推送到您的存储库时，无法对这些软件包执行漏洞扫描。用户不会收到不支持的依赖项或软件包的分析或安全报告。因此，应考虑以下后果：

- 安全风险.未扫描的漏洞的依赖项或软件包可能会给您的机构带来安全风险。
- 合规问题.如果您的机构有特定的安全或合规要求、未扫描或部分扫描，容器镜像可能会导致与某些法规不合规。

注意

扫描的镜像被索引，并创建了漏洞报告，但可能会省略某些不支持的语言中的数据。例如，如果您的容器镜像包含 Lua 应用，则不会提供来自 Clair 的反馈，因为 Clair 不会检测到它。它可以检测容器镜像中使用的其他语言，并显示检测到这些语言的 CVE。因此，Clair 镜像 *会根据 Clair 支持的内容进行完全扫描*。

1.1.4. Clair 容器

Red Hat Ecosystem Catalog 可以找到与 Red Hat Quay 捆绑的官方下游 Clair 容器。

官方上游容器在 Quay.io/projectquay/clair 中打包并作为容器发布。latest 标签跟踪 Git 开发分支。版本标签从对应的版本构建。

1.2. CLAIR 严重性映射

Clair 提供了漏洞评估和管理的综合方法。它的一个重要功能是安全数据库严重性字符串的规范化。这个过程通过将漏洞的严重性映射到预定义的值集来简化对漏洞的评估。通过这个映射，客户端可以有效地响应漏洞的严重性，而无需对每个安全数据库的唯一严重性字符串进行解码。这些映射的严重性字符串与对应安全数据库中发现的严重性一致，确保漏洞评估的一致性和准确性。

1.2.1. Clair 严重性字符串

Clair 警报具有以下严重性字符串的用户：

- Unknown
- negligible
- 低
- Medium
- High
- Critical

这些严重性字符串与相关安全数据库中找到的字符串类似。

alpine 映射
alpine SecDB 数据库不提供严重性信息。所有漏洞的严重性都将是 Unknown。

Alpine 严重性	Clair 严重性
*	Unknown

AWS 映射
AWS UpdateInfo 数据库提供严重性信息。

AWS 严重性	Clair 严重性
低	低
中	Medium
重要	High
critical	Critical

Debian 映射
Debian Oval 数据库提供严重性信息。

Debian 严重性	Clair 严重性
*	Unknown
Unimportant	低
低	Medium
Medium	High
High	Critical

Oracle 映射
Oracle Oval 数据库提供严重性信息。

Oracle 严重性	Clair 严重性
N/A	Unknown
低	低
中	Medium

Oracle 严重性	Clair 严重性
重要	High
CRITICAL	Critical

RHEL 映射
RHEL Oval 数据库提供严重性信息。

RHEL 严重性	Clair 严重性
None	Unknown
低	低
Moderate（中度）	Medium
重要的	High
Critical	Critical

SUSE 映射
SUSE Oval 数据库提供严重性信息。

重要性	Clair 严重性
None	Unknown
低	低
Moderate（中度）	Medium
重要的	High
Critical	Critical

Ubuntu 映射
Ubuntu Oval 数据库提供严重性信息。

重要性	Clair 严重性
Untriaged	Unknown
negligible	negligible

重要性	Clair 严重性
低	低
Medium	Medium
High	High
Critical	Critical

OSV 映射

表 1.1. CVSSv3

基本分数	Clair 严重性
0.0	negligible
0.1-3.9	低
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

表 1.2. CVSSv2

基本分数	Clair 严重性
0.0-3.9	低
4.0-6.9	Medium
7.0-10	High

第 2 章 CLAIR 概念

以下小节介绍了 Clair 的工作原理概述。

2.1. 实践中的 CLAIR

Clair 分析分为三个不同的部分：索引、匹配和通知。

2.1.1. 索引

Clair 的 indexer 服务在了解容器镜像的组成方面扮演着重要角色。在 Clair 中，容器镜像表示被称为 "manifests"。清单用于理解镜像层的内容。为简化此过程，Clair 利用了开放容器项目(OCI)清单和层，专为内容寻址而设计，从而减少重复性任务。

在索引过程中，使用代表容器镜像的清单，并划分到其基本组件中。索引器的作业是取消镜像包含的软件包、原始分发及其依赖的软件包存储库。然后，在 Clair 的数据库中记录并存储了这一宝贵的信息。在索引过程中收集的 insights 作为生成全面漏洞报告的基础。此报告可以无缝传输到匹配节点以进一步分析和操作，帮助用户对其容器镜像的安全性做出明智决策。

IndexReport 存储在 Clair 的数据库中。它可以进入匹配 者 节点，以计算漏洞报告。

2.1.2. 匹配

使用 Clair 时，匹配节点负责与提供的索引报告匹配的漏洞。

匹配者负责保持漏洞数据库最新。匹配者运行一组更新器，它会定期为新内容探测其数据源。当发现新漏洞时，会将其存储在数据库中。

匹配器 API 旨在在查询时始终提供最新的漏洞报告。漏洞报告总结了清单的内容以及影响内容的任何漏洞。

当发现新漏洞时，会将其存储在数据库中。

匹配器 API 设计为经常使用。它旨在在查询时始终提供最新的 **VulnerabilityReport**。**VulnerabilityReport** 总结了清单的内容以及影响内容的任何漏洞。

2.1.3. 通知程序服务

Clair 使用通知程序服务来跟踪新的安全数据库更新，并在新的或移除的漏洞影响了索引清单时通知用户。

当通知程序了解影响之前索引清单的新漏洞时，它使用 **config.yaml** 文件中配置的方法来发出有关新更改的通知。返回的通知会表达因为更改而发现的最重要的漏洞。这可避免为相同的安全数据库更新创建过量通知。

当用户收到通知时，它会根据匹配者发出一个新的请求，以接收最新的漏洞报告。

您可以通过以下机制订阅通知：

- Webhook 交付
- AMQP 交付
- Stomp 传输

配置通知程序是通过 Clair YAML 配置文件完成的。

2.2. CLAIR 身份验证

在当前的迭代中，Clair v4 (Clair)在内部处理身份验证。

注意

以前的 Clair 版本使用 JWT 代理来授权身份验证。

通过在配置的 **auth** 键下指定配置对象来配置身份验证。可能存在多个身份验证配置，但它们按以下顺序优先使用：

1. PSK.使用这个身份验证配置，Clair 使用预共享密钥实施基于 JWT 的身份验证。
2. 配置。例如：

```
auth:
  psk:
    key: >-
      MDQ4ODBlNDAtNDc0ZC00MWUxLThhMzAtOTk0MzEwMGQwYTMxCg==
    iss: 'issuer'
```

在此配置中，**auth** 字段需要两个参数： 是，即验证所有传入请求的签发者，密钥 是验证请求的 base64 代码对称密钥。

2.3. CLAIR 更新器

Clair 使用名为 *updaters* 的 **Go** 软件包，其中包含获取和解析不同漏洞数据库的逻辑。

更新器通常与一个匹配器结合使用，以解释是否有与软件包相关的漏洞。管理员可能希望更频繁地更新漏洞数据库，或者不会从它们知道的数据库导入漏洞。

2.4. 有关 CLAIR 更新器的信息

下表提供了有关每个 Clair 更新器的详细信息，包括配置参数、简短描述、相关 URL 以及它们与之交互的相关组件。此列表不详细，一些服务器可能会发出重定向，而某些请求 URL 会动态构建，以确保漏洞数据检索。

对于 Clair，每个更新器负责获取和解析与特定软件包类型或分发相关的漏洞数据。例如，Debian 更新器侧重于基于 Debian 的 Linux 发行版，而 AWS 更新程序则侧重于特定于 Amazon Web Services Linux 发行版的漏洞。了解软件包类型对于漏洞管理非常重要，因为不同的软件包类型可能具有唯一的安全问题，需要特定的更新和补丁。

注意

如果您在带有 Clair 的更新器 URL 环境中使用代理服务器，您必须识别哪些 URL 需要添加到代理 allowlist 中，以确保 Clair 可以访问它们。使用下表在代理允许列表中添加更新器 URL。

表 2.1. Clair updater 信息

Updater	描述	urls	组件
alpine	Alpine updater 负责获取和解析与 Alpine Linux 发行版中软件包相关的漏洞数据。	• **https://secdb.alpinelinux.org/**	Alpine Linux SecDB 数据库
aws	AWS 更新器侧重于基于 AWS Linux 的软件包，确保特定于 Amazon Web Services 的自定义 Linux 发行版的漏洞信息保持最新状态。	• **http://repo.us-west-2.amazonaws.com/2018.03/updates/x86_64/mirror.list** • **https://cdn.amazonlinux.com/2/core/latest/x86_64/mirror.list** • **https://cdn.amazonlinux.com/al2023/core/mirrors/latest/x86_64/mirror.list**	Amazon Web Services (AWS) UpdateInfo
Debian	Debian 更新器对于跟踪与 Debian 基于 Debian 的 Linux 发行版相关的软件包中的漏洞至关重要。	• **https://deb.debian.org/** • **https://security-tracker.debian.org/tracker/data/json**	Debian 安全跟踪器
clair.cvss	Clair 通用漏洞评分系统(CVSS)更新器侧重于维护有关漏洞及其关联的 CVSS 分数的数据。这不与特定的软件包类型绑定，而是一般的严重性和风险评估。	• **https://nvd.nist.gov/feeds/json/cve/1.1/**	国家漏洞数据库 (NVD)以 JSON 格式用于常见漏洞和暴露 (CVE)数据
oracle	Oracle 更新器专用于 Oracle Linux 软件包，维护影响 Oracle Linux 系统的漏洞的数据。	• **https://linux.oracle.com/security/oval/com.oracle.elsa-*.xml.bz2**	Oracle Oval 数据库
Photon	Photon 更新器处理 VMware Photon OS 中的软件包。	• **https://packages.vmware.com/photon/photon_oval_definitions/**	VMware Photon OS oval 定义
rhel	Red Hat Enterprise Linux (RHEL) 更新器负责维护 Red Hat Enterprise Linux 发行版中软件包的漏洞数据。	• **https://access.redhat.com/security/cve/** • **https://access.redhat.com/security/data/oval/v2/PULP_MANIFEST**	Red Hat Enterprise Linux (RHEL) Oval 数据库

Updater	描述	urls	组件
rhcc	Red Hat Container Catalog (RHCC)更新器已连接到红帽的容器镜像。此更新程序确保与红帽容器化软件相关的漏洞信息保持最新状态。	• **https://access.redhat.com/security/data/metrics/cvemap.xml**	资源处理程序配置控制器(RHCC)数据库
SUSE	SUSE 更新器管理 SUSE Linux 发行版系列中的软件包的漏洞信息，包括 openSUSE、SUSE、SUSE Enterprise Linux 等。	• **https://support.novell.com/security/oval/**	SUSE Oval 数据库
ubuntu	Ubuntu updater 专门用于跟踪与基于 Ubuntu 的 Linux 发行版关联的软件包中的漏洞。Ubuntu 是 Linux 生态系统中的一个常见发行版。	• **https://security-metadata.canonical.com/oval/com.ubuntu.*.cve.oval.xml** • **https://api.launchpad.net/1.0/**	Ubuntu Oval 数据库
osV	开源漏洞(OSV)更新程序专门跟踪开源软件组件中的漏洞。OSV 是一个关键资源，提供有关各种开源项目中安全问题的详细信息。	• **https://osv-vulnerabilities.storage.googleapis.com/**	开源漏洞数据库

2.5. 配置更新器

updaters 可通过 **clair-config.yaml** 文件中的 **updaters.sets** 键配置。

重要

- 如果没有填充 **set** 字段，则默认为使用所有集合。在使用 all sets 中，Clair 会尝试访问每个更新器的 URL 或 URL。如果使用代理环境，则必须在代理允许列表中添加这些 URL。
- 如果在 matcher 进程（默认的设置）中自动运行更新程序，则运行更新器的周期会在 matcher 的配置字段下配置。

2.5.1. 选择特定的更新器集

使用以下引用为您的 Red Hat Quay 部署选择一个或多个更新器。

为多个更新器配置 Clair

多个特定的更新器

```
#...
updaters:
```

```
  sets:
    - alpine
    - aws
    - osv
#...
```

为 Alpine 配置 Clair

alpine config.yaml 示例

```
#...
updaters:
  sets:
    - alpine
#...
```

为 AWS 配置 Clair

AWS config.yaml 示例

```
#...
updaters:
  sets:
    - aws
#...
```

为 Debian 配置 Clair

Debian config.yaml 示例

```
#...
updaters:
  sets:
    - debian
#...
```

为 Clair CVSS 配置 Clair

Clair CVSS config.yaml 示例

```
#...
updaters:
  sets:
    - clair.cvss
#...
```

为 Oracle 配置 Clair

Oracle config.yaml 示例

```
#...
updaters:
  sets:
```

```
    - oracle
#...
```

为 Photon 配置 Clair

Photon config.yaml 示例

```
#...
updaters:
  sets:
    - photon
#...
```

为 SUSE 配置 Clair

SUSE config.yaml 示例

```
#...
updaters:
  sets:
    - suse
#...
```

为 Ubuntu 配置 Clair

Ubuntu config.yaml 示例

```
#...
updaters:
  sets:
    - ubuntu
#...
```

为 OSV 配置 Clair

OSV config.yaml 示例

```
#...
updaters:
  sets:
    - osv
#...
```

2.5.2. 为完整的 Red Hat Enterprise Linux (RHEL)覆盖选择更新程序集

要完全覆盖 Red Hat Enterprise Linux (RHEL)中的漏洞，您必须使用以下更新程序集：

- **RHEL**.在这个版本中，确保您具有影响 RHEL 的漏洞的最新信息。
- **RHCC**.此更新程序会跟踪与红帽容器镜像相关的漏洞。
- **Clair.cvss**.通过提供通用漏洞和暴露(CVE)评分，对漏洞的严重性和风险评估提供了全面的视图。

- **OSV**.此更新程序侧重于跟踪开源软件组件中的漏洞。建议使用这个更新，因为 Java 和 Go 在 RHEL 产品中是通用的。

RHEL 更新程序示例

```
#...
updaters:
  sets:
    - rhel
    - rhcc
    - clair.cvss
    - osv
#...
```

2.5.3. 高级更新器配置

在某些情况下，用户可能希望为特定的行为配置更新程序，例如，如果要列出开源漏洞(OSV)更新器的特定生态系统。

高级更新器配置可能对代理部署或 air gapped 部署很有用。这些场景中的特定更新器的配置可以通过在 **updaters** 对象的 **config** 环境变量下放置一个键来传递。用户应检查其 Clair 日志到双检查名称。

以下 YAML 片段详细介绍了一些 Clair 更新器可用的各种设置

重要

对于更多用户，不需要高级更新器配置。

配置 **alpine** 更新器

```
#...
updaters:
  sets:
    - apline
  config:
    alpine:
      url: https://secdb.alpinelinux.org/
#...
```

配置 **debian** 更新器

```
#...
updaters:
  sets:
    - debian
  config:
    debian:
      mirror_url: https://deb.debian.org/
      json_url: https://security-tracker.debian.org/tracker/data/json
#...
```

配置 **clair.cvs** 更新器

```
#...
```

```
updaters:
  config:
    clair.cvss:
      url: https://nvd.nist.gov/feeds/json/cve/1.1/
#...
```

配置 **oracle updater**

```
#...
updaters:
  sets:
    - oracle
  config:
    oracle-2023-updater:
      url:
        - https://linux.oracle.com/security/oval/com.oracle.elsa-2023.xml.bz2
    oracle-2022-updater:
      url:
        - https://linux.oracle.com/security/oval/com.oracle.elsa-2022.xml.bz2
#...
```

配置照片更新器

```
#...
updaters:
  sets:
    - photon
  config:
    photon:
      url: https://packages.vmware.com/photon/photon_oval_definitions/
#...
```

配置 **rhel updater**

```
#...
updaters:
  sets:
    - rhel
  config:
    rhel:
      url: https://access.redhat.com/security/data/oval/v2/PULP_MANIFEST
      ignore_unpatched: true (1)
#...
```

1 布尔值.是否包含有关没有相应补丁或更新的漏洞的信息。

配置 **rhcc** 更新器

```
#...
updaters:
  sets:
    - rhcc
  config:
```

```
    rhcc:
      url: https://access.redhat.com/security/data/metrics/cvemap.xml
#...
```

配置使用更新器

```
#...
updaters:
  sets:
    - suse
  config:
    suse:
      url: https://support.novell.com/security/oval/
#...
```

配置 **ubuntu** 更新器

```
#...
updaters:
  config:
    ubuntu:
      url: https://api.launchpad.net/1.0/
      name: ubuntu
      force: 1
        - name: focal 2
          version: 20.04 3
#...
```

1 用于强制在生成的 UpdaterSet 中包含特定发行版和版本详情，而不考虑它们的状态。如果要确保更新器配置中一致包含特定的发行版和版本，则很有用。

2 指定您要强制包含在 UpdaterSet 中的发布名称。

3 指定您要强制进入 UpdaterSet 的发行版本。

配置 **osv updater**

```
#...
updaters:
  sets:
    - osv
  config:
    osv:
      url: https://osv-vulnerabilities.storage.googleapis.com/
      allowlist: 1
        - npm
        - pypi
#...
```

1 允许的生态系统列表。如果未设置，则允许所有生态系统。必须为小写。有关支持的生态系统列表，请查看有关 定义的生态系统 的文档。

2.5.4. 禁用 Clair Updater 组件

在某些情况下，用户可能希望禁用 Clair 更新器组件。在断开连接的环境中运行 Red Hat Quay 时，需要禁用更新程序。

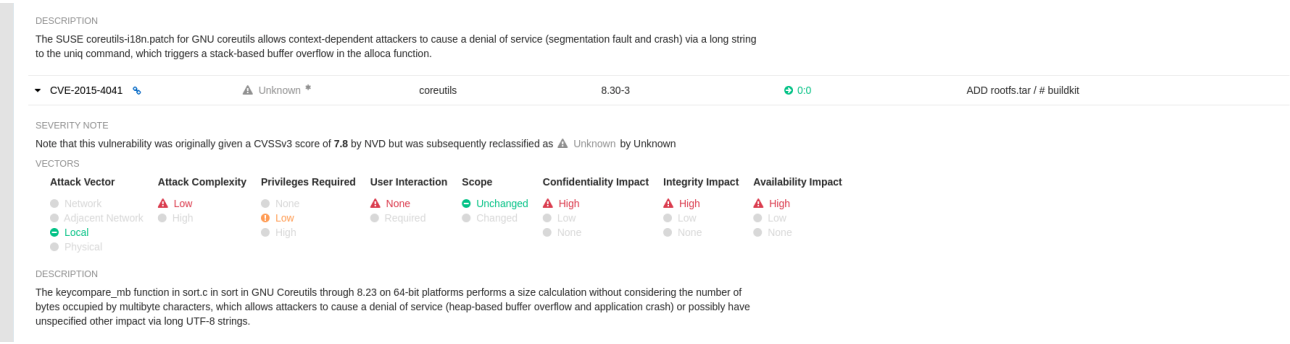
在以下示例中，Clair updaters 被禁用：

```
#...
matcher:
  disable_updaters: true
#...
```

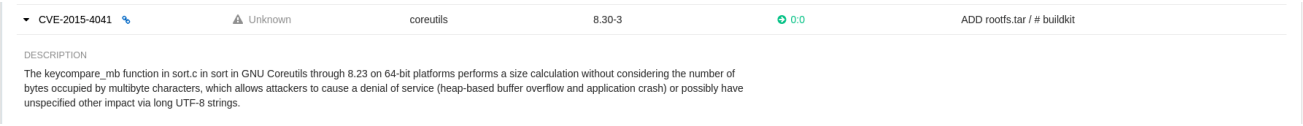
2.6. 国家漏洞数据库中的 CVE 评级

从 Clair v4.2 开始，在 Red Hat Quay UI 中可以查看通用漏洞评分系统(CVSS)数据。另外，Clair v4.2 从国家漏洞数据库中为检测到的漏洞添加了 CVSS 分数。

在这个版本中，如果漏洞的 CVSS 分数在分布分数的 2 级内，则 Red Hat Quay UI 默认存在分发的分数。例如：



这与前面的接口不同，它只显示以下信息：



2.7. FEDERAL INFORMATION PROCESSING STANDARD (FIPS)就绪与合规性

美国国家标准与技术研究院(NIST)开发的联邦信息处理标准(FIPS)被认为是保护和加密敏感数据的高度认可，特别是在银行、医疗保健和公共区等高度监管领域。Red Hat Enterprise Linux (RHEL)和 OpenShift Container Platform 通过提供 *FIPS 模式* 来支持 FIPS，该系统只允许使用特定的 FIPS 验证的加密模块，如 **openssl**。这样可确保 FIPS 合规性。

2.7.1. 启用 FIPS 合规性

使用以下步骤在 Red Hat Quay 部署中启用 FIPS 合规性。

前提条件

- 如果您运行 Red Hat Quay 的独立部署，则您的 Red Hat Enterprise Linux (RHEL)部署是版本 8 或更高版本，并启用 FIPS。
- 如果要在 OpenShift Container Platform 上部署 Red Hat Quay，OpenShift Container Platform 是版本 4.10 或更高版本。

- 您的 Red Hat Quay 版本为 3.5.0 或更高版本。
- 如果您在 IBM Power 或 IBM Z 集群中使用 OpenShift Container Platform 上的 Red Hat Quay：
  - OpenShift Container Platform 版本 4.14 或更高版本是必需的
  - 需要 Red Hat Quay 版本 3.10 或更高版本
- 您有 Red Hat Quay 部署的管理特权。

流程

- 在 Red Hat Quay **config.yaml** 文件中，将 **FEATURE_FIPS** 配置字段设置为 **true**。例如：

```
---
FEATURE_FIPS = true
---
```

  将 **FEATURE_FIPS** 设置为 **true** 时，Red Hat Quay 会使用 FIPS 兼容哈希功能运行。

部分 II. RED HAT QUAY 中的 CLAIR

本指南包含在独立和 OpenShift Container Platform Operator 部署中在 Red Hat Quay 上运行 Clair 的步骤。

第 3 章 在独立 RED HAT QUAY 部署中设置 CLAIR

对于独立的 Red Hat Quay 部署，您可以手动设置 Clair。

流程

1. 在 Red Hat Quay 安装目录中，为 Clair 数据库数据创建一个新目录：

```
$ mkdir /home/<user-name>/quay-poc/postgres-clairv4
```

2. 输入以下命令为 **postgres-clairv4** 文件设置适当的权限：

```
$ setfacl -m u:26:-wx /home/<user-name>/quay-poc/postgres-clairv4
```

3. 输入以下命令部署 Clair PostgreSQL 数据库：

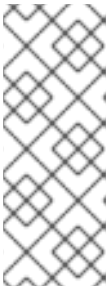
```
$ sudo podman run -d --name postgresql-clairv4 \
  -e POSTGRESQL_USER=clairuser \
  -e POSTGRESQL_PASSWORD=clairpass \
  -e POSTGRESQL_DATABASE=clair \
  -e POSTGRESQL_ADMIN_PASSWORD=adminpass \
  -p 5433:5432 \
  -v /home/<user-name>/quay-poc/postgres-clairv4:/var/lib/pgsql/data:Z \
  registry.redhat.io/rhel8/postgresql-13:1-109
```

4. 为您的 Clair 部署安装 PostgreSQL **uuid-ossp** 模块：

```
$ sudo podman exec -it postgresql-clairv4 /bin/bash -c 'echo "CREATE EXTENSION IF NOT
EXISTS \"uuid-ossp\"" | psql -d clair -U postgres'
```

输出示例

```
CREATE EXTENSION
```



注意

Clair 需要 **uuid-ossp** 扩展添加到其 PostgreSQL 数据库中。对于具有适当特权的用户，Clair 会自动添加创建扩展。如果用户没有正确的特权，则必须在启动 Clair 前添加扩展。

如果扩展不存在，则 Clair 尝试启动时会显示以下错误： **ERROR: Please load the "uuid-ossp"** 扩展。**(SQLSTATE 42501)**。

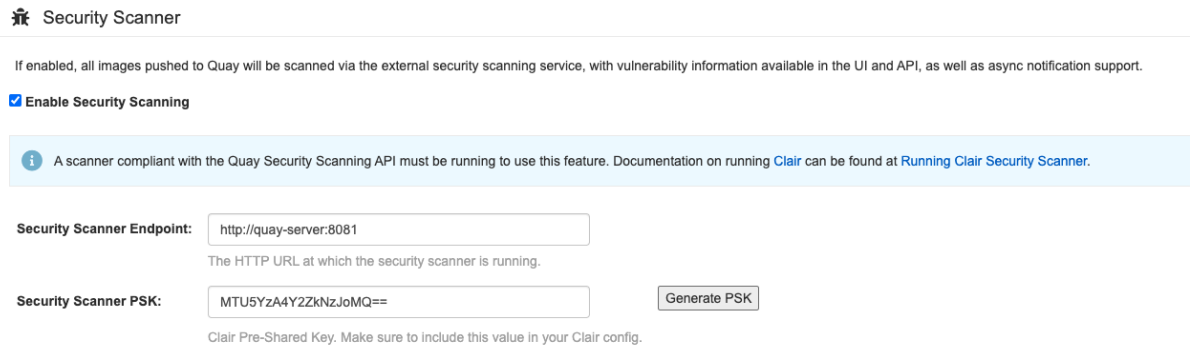
5. 如果 **Quay** 容器正在运行并在配置模式中重启它，请将现有配置作为卷载入：

```
$ sudo podman run --rm -it --name quay_config \
  -p 80:8080 -p 443:8443 \
  -v $QUAY/config:/conf/stack:Z \
  registry.redhat.io/quay/quay-rhel8:v3.12.3 config secret
```

6. 登录到配置工具，点 UI 的 **Security Scanner** 部分中的 **Enable Security Scanning**。

7. 使用尚未在 **quay-server** 系统上使用端口设置 Clair 的 HTTP 端点，如 **8081**。
8. 使用 **Generate PSK** 按钮创建预共享密钥(PSK)。

安全扫描器 UI



9. 验证并下载 Red Hat Quay 的 **config.yaml** 文件，然后停止运行配置编辑器的 **Quay** 容器。
10. 将新配置捆绑包提取到 Red Hat Quay 安装目录中，例如：

```
$ tar xvf quay-config.tar.gz -d /home/<user-name>/quay-poc/
```

11. 为您的 Clair 配置文件创建一个文件夹，例如：

```
$ mkdir /etc/opt/clairv4/config/
```

12. 进入 Clair 配置文件夹：

```
$ cd /etc/opt/clairv4/config/
```

13. 创建 Clair 配置文件，例如：

```
http_listen_addr: :8081
introspection_addr: :8088
log_level: debug
indexer:
  connstring: host=quay-server.example.com port=5433 dbname=clair user=clairuser
password=clairpass sslmode=disable
  scanlock_retry: 10
  layer_scan_concurrency: 5
  migrations: true
matcher:
  connstring: host=quay-server.example.com port=5433 dbname=clair user=clairuser
password=clairpass sslmode=disable
  max_conn_pool: 100
  migrations: true
  indexer_addr: clair-indexer
notifier:
  connstring: host=quay-server.example.com port=5433 dbname=clair user=clairuser
password=clairpass sslmode=disable
  delivery_interval: 1m
  poll_interval: 5m
  migrations: true
auth:
```

```
  psk:
    key: "MTU5YzA4Y2ZkNzJoMQ=="
    iss: ["quay"]
# tracing and metrics
trace:
  name: "jaeger"
  probability: 1
  jaeger:
    agent:
      endpoint: "localhost:6831"
    service_name: "clair"
metrics:
  name: "prometheus"
```

有关 Clair 配置格式的更多信息，请参阅 Clair 配置参考。

14. 使用容器镜像启动 Clair，挂载在来自您创建的文件中的配置中：

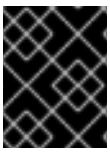
```
$ sudo podman run -d --name clairv4 \
-p 8081:8081 -p 8088:8088 \
-e CLAIR_CONF=/clair/config.yaml \
-e CLAIR_MODE=combo \
-v /etc/opt/clairv4/config:/clair:Z \
registry.redhat.io/quay/clair-rhel8:v3.12.3
```

注意

也可以运行多个 Clair 容器，但在单一容器之外，强烈建议使用 Kubernetes 或 OpenShift Container Platform 等容器编配器的部署场景。

3.1. 将 CLAIR 与上游镜像用于 RED HAT QUAY

对于大多数用户，不需要从当前版本(4.7.4)中独立升级 Clair。然而，在某些情况下，客户可能希望出于各种原因从上游 存储库拉取 Clair 镜像，如出于特定程序错误修复或尝试尚未发布下游的新功能。您可以使用以下步骤在 Red Hat Quay 中运行 Clair 的上游版本。



重要

Clair 的上游版本尚未经过充分测试，以便与 Red Hat Quay 兼容。因此，这种组合可能会导致部署出现问题。

流程

1. 如果 Clair 正在运行，输入以下命令停止 Clair：

```
$ podman stop <clairv4_container_name>
```

2. 导航到 上游存储库，找到要使用的 Clair 版本，并将它拉取到您的本地计算机。例如：

```
$ podman pull quay.io/projectquay/clair:nightly-2024-02-03
```

3. 使用容器镜像启动 Clair，挂载在来自您创建的文件中的配置中：

```
$ podman run -d --name clairv4 \
-p 8081:8081 -p 8088:8088 \
-e CLAIR_CONF=/clair/config.yaml \
-e CLAIR_MODE=combo \
-v /etc/opt/clairv4/config:/clair:Z \
quay.io/projectquay/clair:nightly-2024-02-03
```

第 4 章 OPENSHIFT CONTAINER PLATFORM 中的 CLAIR

要在 OpenShift Container Platform 上的 Red Hat Quay 部署中设置 Clair v4 (Clair)，建议使用 Red Hat Quay Operator。默认情况下，Red Hat Quay Operator 安装或升级 Clair 部署以及 Red Hat Quay 部署自动配置 Clair。

第 5 章 测试 CLAIR

使用以下步骤测试独立 Red Hat Quay 部署或基于 OpenShift Container Platform Operator 的部署中的 Clair。

先决条件

- 您已部署了 Clair 容器镜像。

流程

1. 输入以下命令拉取示例镜像：

```
$ podman pull ubuntu:20.04
```

2. 输入以下命令将镜像标记到 registry 中：

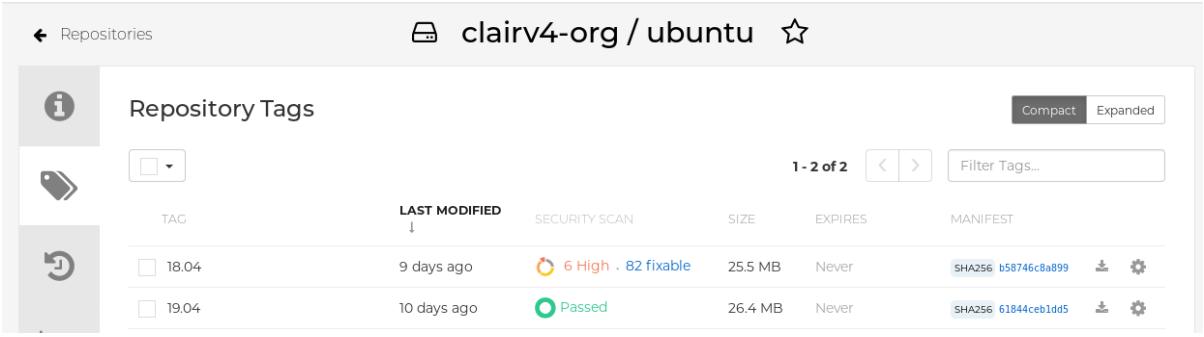
```
$ sudo podman tag docker.io/library/ubuntu:20.04 <quay-server.example.com>/<user-name>/ubuntu:20.04
```

3. 输入以下命令将镜像推送到 Red Hat Quay registry：

```
$ sudo podman push --tls-verify=false quay-server.example.com/quayadmin/ubuntu:20.04
```

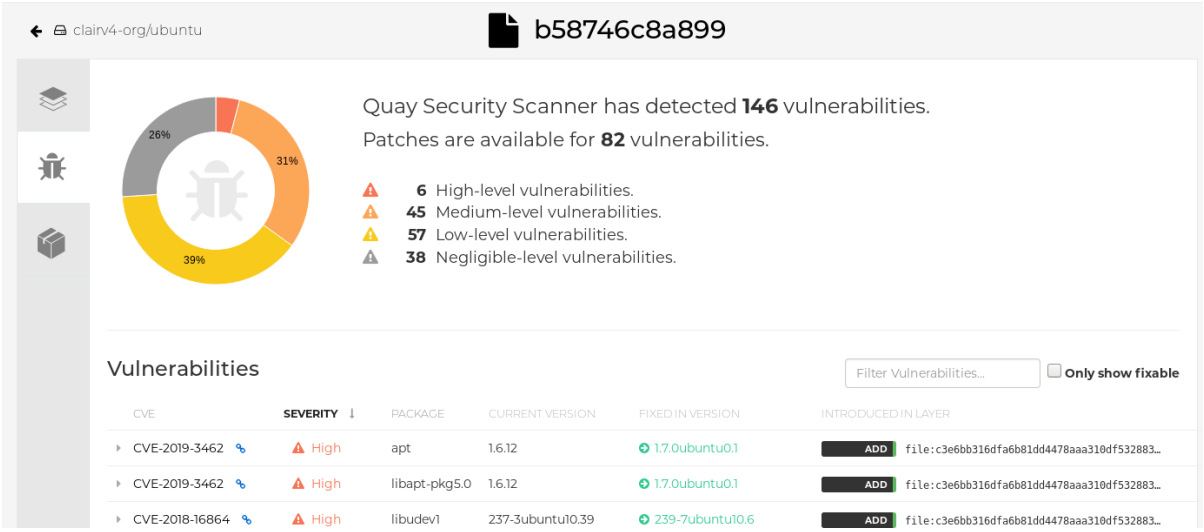
4. 通过 UI 登录您的 Red Hat Quay 部署。
5. 单击存储库名称，如 **quayadmin/ubuntu**。
6. 在导航窗格中，单击 **Tags**。

报告概述



7. 点镜像报告（如 45 个介质）显示更详细的报告：

报告详情



注意

在某些情况下，Clair 显示有关镜像的重复报告，如 **ubi8/nodejs-12** 或 **ubi8/nodejs-16**。这是因为同名的漏洞适用于不同的软件包。这个行为预期是 Clair 漏洞报告，且不会作为程序错误解决。

部分 III. 高级 CLAIR 配置

使用本节配置高级 Clair 功能。

第 6 章 UNMANAGED CLAIR 配置

Red Hat Quay 用户可以使用 Red Hat Quay OpenShift Container Platform Operator 运行非受管 Clair 配置。此功能允许用户创建非受管 Clair 数据库，或者在没有非受管数据库的情况下运行其自定义 Clair 配置。

非受管 Clair 数据库允许 Red Hat Quay Operator 在地理复制环境中工作，Operator 的多个实例必须与同一数据库通信。当用户需要在集群外存在的高可用性(HA) Clair 数据库时，也可以使用非受管 Clair 数据库。

6.1. 使用非受管 CLAIR 数据库运行自定义 CLAIR 配置

使用以下步骤将 Clair 数据库设置为 unmanaged。

重要

您不能为 Red Hat Quay 和 Clair 部署使用相同的外部管理的 PostgreSQL 数据库。您的 PostgreSQL 数据库还必须与其他工作负载共享，因为在连接密集型工作负载（如 Red Hat Quay 或 Clair）时，它可能会耗尽 PostgreSQL 端的自然连接限制。另外，Red Hat Quay 或 Clair 不支持 pgBouncer，因此这不是解决这个问题的选项。

流程

- 在 Quay Operator 中，将 **QuayRegistry** 自定义资源的 **clairpostgres** 组件设置为 **managed: false** ：

```
apiVersion: quay.redhat.com/v1
kind: QuayRegistry
metadata:
  name: quay370
spec:
  configBundleSecret: config-bundle-secret
  components:
    - kind: objectstorage
      managed: false
    - kind: route
      managed: true
    - kind: tls
      managed: false
    - kind: clairpostgres
      managed: false
```

6.2. 使用非受管 CLAIR 数据库配置自定义 CLAIR 数据库

Red Hat Quay on OpenShift Container Platform 允许用户提供自己的 Clair 数据库。

使用以下步骤创建自定义 Clair 数据库。

注意

以下流程使用 SSL/TLS 认证设置 Clair。要查看不使用 SSL/TLS 认证设置 Clair 的类似流程，请参阅"使用受管 Clair 配置自定义 Clair 数据库"。

流程

1. 输入以下命令来创建包含 **clair-config.yaml** 的 Quay 配置捆绑包 secret：

```
$ oc create secret generic --from-file config.yaml=./config.yaml --from-file extra_ca_cert_rds-ca-2019-root.pem=./rds-ca-2019-root.pem --from-file clair-config.yaml=./clair-config.yaml --from-file ssl.cert=./ssl.cert --from-file ssl.key=./ssl.key config-bundle-secret
```

Clair config.yaml 文件示例

```
indexer:
    connstring: host=quay-server.example.com port=5432 dbname=quay user=quayrdsdb password=quayrdsdb sslrootcert=/run/certs/rds-ca-2019-root.pem sslmode=verify-ca
    layer_scan_concurrency: 6
    migrations: true
    scanlock_retry: 11
log_level: debug
matcher:
    connstring: host=quay-server.example.com port=5432 dbname=quay user=quayrdsdb password=quayrdsdb sslrootcert=/run/certs/rds-ca-2019-root.pem sslmode=verify-ca
    migrations: true
metrics:
    name: prometheus
notifier:
    connstring: host=quay-server.example.com port=5432 dbname=quay user=quayrdsdb password=quayrdsdb sslrootcert=/run/certs/rds-ca-2019-root.pem sslmode=verify-ca
    migrations: true
```

注意

- 数据库证书挂载到 **clair-config.yaml** 中的 Clair 应用程序 pod 上的 **/run/certs/rds-ca-2019-root.pem** 下。在配置 **clair-config.yaml** 时，必须指定它。
- Clair on OpenShift config 中包括了一个 **clair-config.yaml** 示例。

2. 将 **clair-config.yaml** 文件添加到捆绑包 secret 中，例如：

```
apiVersion: v1
kind: Secret
metadata:
  name: config-bundle-secret
  namespace: quay-enterprise
data:
  config.yaml: <base64 encoded Quay config>
  clair-config.yaml: <base64 encoded Clair config>
  extra_ca_cert_<name>: <base64 encoded ca cert>
  ssl.crt: <base64 encoded SSL certificate>
  ssl.key: <base64 encoded SSL private key>
```

注意

更新后，提供的 **clair-config.yaml** 文件会被挂载到 Clair pod 中。任何未提供的字段都使用 Clair 配置模块自动填充默认值。

3. 您可以点击 **Build History** 页面中的提交或运行 **oc get pods -n <namespace** > 来检查 Clair pod 的状态。例如：

```
$ oc get pods -n <namespace>
```

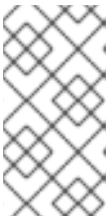
输出示例

```
NAME                                    READY   STATUS    RESTARTS   AGE
f192fe4a-c802-4275-bcce-d2031e635126-9l2b5-25lg2   1/1     Running   0          7s
```

第 7 章 使用受管 CLAIR 数据库运行自定义 CLAIR 配置

在某些情况下，用户可能希望使用受管 Clair 数据库运行自定义 Clair 配置。这在以下情况中很有用：

- 当用户想要禁用特定的更新器资源时。
- 当用户在断开连接的环境中运行 Red Hat Quay 时。有关在断开连接的环境中运行 Clair 的更多信息，请参阅 在断开连接的环境中的 Clair。



注意

- 如果您在断开连接的环境中运行 Red Hat Quay，则 **clair-config.yaml** 的 **airgap** 参数必须设置为 **true**。
- 如果您在断开连接的环境中运行 Red Hat Quay，则应禁用所有更新器组件。

7.1. 将 CLAIR 数据库设置为 MANAGED

使用以下步骤将 Clair 数据库设置为 managed。

流程

- 在 Quay Operator 中，将 **QuayRegistry** 自定义资源的 **clairpostgres** 组件设置为 **managed: true** ：

```
apiVersion: quay.redhat.com/v1
kind: QuayRegistry
metadata:
  name: quay370
spec:
  configBundleSecret: config-bundle-secret
  components:
    - kind: objectstorage
      managed: false
    - kind: route
      managed: true
    - kind: tls
      managed: false
    - kind: clairpostgres
      managed: true
```

7.2. 使用受管 CLAIR 配置自定义 CLAIR 数据库

Red Hat Quay on OpenShift Container Platform 允许用户提供自己的 Clair 数据库。

使用以下步骤创建自定义 Clair 数据库。

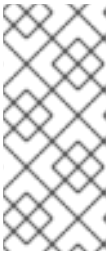
流程

1. 输入以下命令来创建包含 **clair-config.yaml** 的 Quay 配置捆绑包 secret：

```
$ oc create secret generic --from-file config.yaml=./config.yaml --from-file extra_ca_cert_rds-ca-2019-root.pem=./rds-ca-2019-root.pem --from-file clair-config.yaml=./clair-config.yaml config-bundle-secret
```

Clair config.yaml 文件示例

```
indexer:
    connstring: host=quay-server.example.com port=5432 dbname=quay user=quayrdsdb password=quayrdsdb sslmode=disable
    layer_scan_concurrency: 6
    migrations: true
    scanlock_retry: 11
log_level: debug
matcher:
    connstring: host=quay-server.example.com port=5432 dbname=quay user=quayrdsdb password=quayrdsdb sslmode=disable
    migrations: true
metrics:
    name: prometheus
notifier:
    connstring: host=quay-server.example.com port=5432 dbname=quay user=quayrdsdb password=quayrdsdb sslmode=disable
    migrations: true
```



注意

- 数据库证书挂载到 **clair-config.yaml** 中的 Clair 应用程序 pod 上的 **/run/certs/rds-ca-2019-root.pem** 下。在配置 **clair-config.yaml** 时，必须指定它。
- Clair on OpenShift config 中包括了一个 **clair-config.yaml** 示例。

2. 将 **clair-config.yaml** 文件添加到捆绑包 secret 中，例如：

```
apiVersion: v1
kind: Secret
metadata:
  name: config-bundle-secret
  namespace: quay-enterprise
data:
  config.yaml: <base64 encoded Quay config>
  clair-config.yaml: <base64 encoded Clair config>
```

注意

- 更新后，提供的 **clair-config.yaml** 文件会被挂载到 Clair pod 中。任何未提供的字段都使用 Clair 配置模块自动填充默认值。

3. 您可以点击 **Build History** 页面中的提交或运行 **oc get pods -n <namespace>** > 来检查 Clair pod 的状态。例如：

```
$ oc get pods -n <namespace>
```

输出示例

```
NAME                                                READY   STATUS    RESTARTS   AGE
f192fe4a-c802-4275-bcce-d2031e635126-9l2b5-25lg2    1/1     Running   0          7s
```

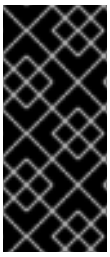
第 8 章 在断开连接的环境中的 CLAIR

注意

目前，IBM Power 和 IBM Z 不支持在断开连接的环境中部署 Clair。

Clair 使用一组称为 *updaters* 的组件来处理从各种漏洞数据库获取和解析数据。默认情况下，更新程序会被设置，以直接从互联网拉取漏洞数据，并立即使用。但是，有些用户可能要求 Red Hat Quay 在断开连接的环境中运行，或者不需要直接访问互联网的环境。Clair 支持断开连接的环境，方法是使用不同类型的更新工作流来考虑网络隔离。这通过使用 **clairctl** 命令行界面工具来工作，该工具通过使用开放主机从互联网获取更新器数据，从而安全地将数据传送到隔离的主机，然后将隔离主机上的 updater 数据非常重要到 Clair。

使用本指南在断开连接的环境中部署 Clair。



重要

由于已知的 PROJQUAY-6577，Red Hat Quay Operator 无法正确呈现自定义的 Clair **config.yaml** 文件。因此，以下流程目前无法正常工作。

用户必须从开始创建整个 Clair 配置本身，而不依赖于 Operator 来填充字段。要做到这一点，按照流程中的说明，在断开连接的环境中启用 Clair 扫描镜像。

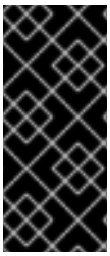
注意

目前，Clairrichment 数据是 CVSS 数据。目前在断开连接的环境中不支持增强数据。

有关 Clair 更新器的更多信息，请参阅 "Clair updaters"。

8.1. 在断开连接的 OPENSHIFT CONTAINER PLATFORM 集群中设置 CLAIR

使用以下步骤在断开连接的 OpenShift Container Platform 集群中设置 OpenShift Container Platform 置备的 Clair pod。



重要

由于已知的 PROJQUAY-6577，Red Hat Quay Operator 无法正确呈现自定义的 Clair **config.yaml** 文件。因此，以下流程目前无法正常工作。

用户必须从开始创建整个 Clair 配置本身，而不依赖于 Operator 来填充字段。要做到这一点，按照流程中的说明，在断开连接的环境中启用 Clair 扫描镜像。

8.1.1. 为 OpenShift Container Platform 部署安装 clairctl 命令行工具工具

使用以下步骤为 OpenShift Container Platform 部署安装 **clairctl** CLI 工具。

流程

1. 输入以下命令为 OpenShift Container Platform 集群中的 Clair 部署安装 **clairctl** 程序：

```
$ oc -n quay-enterprise exec example-registry-clair-app-64dd48f866-6ptgw -- cat
/usr/bin/clairctl > clairctl
```

注意

不正式，可以下载 **clairctl** 工具

2. 设置 **clairctl** 文件的权限，以便可由用户执行并运行，例如：

```
$ chmod u+x ./clairctl
```

8.1.2. 为 OpenShift Container Platform 上的 Clair 部署检索并解码 Clair 配置 secret

使用以下步骤为 OpenShift Container Platform 上置备的 Clair 实例检索和解码配置 secret。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。

流程

1. 输入以下命令来检索和解码配置 secret，然后将其保存到 Clair 配置 YAML 中：

```
$ oc get secret -n quay-enterprise example-registry-clair-config-secret  -o "jsonpath=
{$.data['config\.yaml']}" | base64 -d > clair-config.yaml
```

2. 更新 **clair-config.yaml** 文件，使 **disable_updaters** 和 **airgap** 参数设置为 **true**，例如：

```
---
indexer:
  airgap: true
---
matcher:
  disable_updaters: true
---
```

8.1.3. 从连接的 Clair 实例导出更新程序捆绑包

使用以下步骤从可访问互联网的 Clair 实例导出更新程序捆绑包。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。
- 您已检索并解码 Clair 配置 secret，并将其保存到 Clair **config.yaml** 文件中。
- 在 Clair **config.yaml** 文件中，**disable_updaters** 和 **airgap** 参数设置为 **true**。

流程

- 从可访问互联网的 Clair 实例中，将 **clairctl** CLI 工具与您的配置文件一起使用，以导出更新程序捆绑包。例如：

```
$ ./clairctl --config ./config.yaml export-updaters updates.gz
```

8.1.4. 配置对断开连接的 OpenShift Container Platform 集群中的 Clair 数据库的访问

使用以下步骤配置对断开连接的 OpenShift Container Platform 集群中的 Clair 数据库的访问。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。
- 您已检索并解码 Clair 配置 secret，并将其保存到 Clair **config.yaml** 文件中。
- 在 Clair **config.yaml** 文件中，**disable_updaters** 和 **airgap** 参数设置为 **true**。
- 您已从可访问互联网的 Clair 实例导出了更新程序捆绑包。

流程

1. 使用 **oc** CLI 工具确定您的 Clair 数据库服务，例如：

```
$ oc get svc -n quay-enterprise
```

输出示例

```
NAME                              TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)
AGE
example-registry-clair-app        ClusterIP   172.30.224.93    <none>
80/TCP,8089/TCP               4d21h
example-registry-clair-postgres   ClusterIP   172.30.246.88    <none>        5432/TCP
4d21h
...
```

2. 转发 Clair 数据库端口，使其可以从本地机器访问。例如：

```
$ oc port-forward -n quay-enterprise service/example-registry-clair-postgres 5432:5432
```

3. 更新 Clair **config.yaml** 文件，例如：

```
indexer:
  connstring: host=localhost port=5432 dbname=postgres user=postgres
password=postgres sslmode=disable (1)
  scanlock_retry: 10
  layer_scan_concurrency: 5
  migrations: true
  scanner:
    repo:
      rhel-repository-scanner: (2)
        repo2cpe_mapping_file: /data/cpe-map.json
    package:
      rhel_containerscanner: (3)
        name2repos_mapping_file: /data/repo-map.json
```

1. 在多 **connstring** 字段中使用 **localhost** 替换 **host** 的值。
2. 有关 **rhel-repository-scanner** 参数的更多信息，请参阅"Mapping repository to Common Product Enumeration information"。
3. 有关 **rhel_containerscanner** 参数的更多信息，请参阅"Mapping repository to Common Product Enumeration information"。

8.1.5. 将更新程序捆绑包导入到断开连接的 OpenShift Container Platform 集群中

使用以下步骤将更新程序捆绑包导入到断开连接的 OpenShift Container Platform 集群中。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。
- 您已检索并解码 Clair 配置 secret，并将其保存到 Clair **config.yaml** 文件中。
- 在 Clair **config.yaml** 文件中，**disable_updaters** 和 **airgap** 参数设置为 **true**。
- 您已从可访问互联网的 Clair 实例导出了更新程序捆绑包。
- 您已将更新程序捆绑包传送到断开连接的环境中。

流程

- 使用 **clairctl** CLI 工具将更新程序捆绑包导入到 OpenShift Container Platform 部署的 Clair 数据库中。例如：

```
$ ./clairctl --config ./clair-config.yaml import-updaters updates.gz
```

8.2. 为断开连接的 OPENSHIFT CONTAINER PLATFORM 集群设置自助管理的 CLAIR 部署

使用以下步骤为断开连接的 OpenShift Container Platform 集群设置 Clair 的自我管理部署。

重要

由于已知的 PROJQUAY-6577，Red Hat Quay Operator 无法正确呈现自定义的 Clair **config.yaml** 文件。因此，以下流程目前无法正常工作。

用户必须从开始创建整个 Clair 配置本身，而不依赖于 Operator 来填充字段。要做到这一点，按照流程中的说明，在断开连接的环境中启用 Clair 扫描镜像。

8.2.1. 为 OpenShift Container Platform 上的自助管理的 Clair 部署安装 clairctl 命令行工具工具

使用以下步骤在 OpenShift Container Platform 上安装用于自我管理的 Clair 部署的 **clairctl** CLI 工具。

流程

1. 使用 **podman cp** 命令为自我管理的 Clair 部署安装 **clairctl** 程序，例如：

```
$ sudo podman cp clairv4:/usr/bin/clairctl ./clairctl
```

2. 设置 **clairctl** 文件的权限，以便可由用户执行并运行，例如：

```
$ chmod u+x ./clairctl
```

8.2.2. 为断开连接的 OpenShift Container Platform 集群部署自我管理的 Clair 容器

使用以下步骤为断开连接的 OpenShift Container Platform 集群部署自我管理的 Clair 容器。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。

流程

1. 为您的 Clair 配置文件创建一个文件夹，例如：

```
$ mkdir /etc/clairv4/config/
```

2. 创建一个 Clair 配置文件，并将 **disable_updaters** 参数设置为 **true**，例如：

```
---
indexer:
  airgap: true
---
matcher:
  disable_updaters: true
---
```

3. 使用容器镜像启动 Clair，挂载在来自您创建的文件中的配置中：

```
$ sudo podman run -it --rm --name clairv4 \
-p 8081:8081 -p 8088:8088 \
-e CLAIR_CONF=/clair/config.yaml \
-e CLAIR_MODE=combo \
-v /etc/clairv4/config:/clair:Z \
registry.redhat.io/quay/clair-rhel8:v3.12.3
```

8.2.3. 从连接的 Clair 实例导出更新程序捆绑包

使用以下步骤从可访问互联网的 Clair 实例导出更新程序捆绑包。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。
- 您已部署了 Clair。
- 在 Clair **config.yaml** 文件中，**disable_updaters** 和 **airgap** 参数设置为 **true**。

流程

- 从可访问互联网的 Clair 实例中，将 **clairctl** CLI 工具与您的配置文件一起使用，以导出更新程序捆绑包。例如：

```
$ ./clairctl --config ./config.yaml export-updaters updates.gz
```

8.2.4. 配置对断开连接的 OpenShift Container Platform 集群中的 Clair 数据库的访问

使用以下步骤配置对断开连接的 OpenShift Container Platform 集群中的 Clair 数据库的访问。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。
- 您已部署了 Clair。
- 在 Clair **config.yaml** 文件中，**disable_updaters** 和 **airgap** 参数设置为 **true**。
- 您已从可访问互联网的 Clair 实例导出了更新程序捆绑包。

流程

1. 使用 **oc** CLI 工具确定您的 Clair 数据库服务，例如：

```
$ oc get svc -n quay-enterprise
```

输出示例

```
NAME                          TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)
AGE
example-registry-clair-app          ClusterIP      172.30.224.93    <none>
80/TCP,8089/TCP                4d21h
example-registry-clair-postgres     ClusterIP      172.30.246.88    <none>        5432/TCP
4d21h
...
```

2. 转发 Clair 数据库端口，使其可以从本地机器访问。例如：

```
$ oc port-forward -n quay-enterprise service/example-registry-clair-postgres 5432:5432
```

3. 更新 Clair **config.yaml** 文件，例如：

```
indexer:
  connstring: host=localhost port=5432 dbname=postgres user=postgres
password=postgres sslmode=disable (1)
  scanlock_retry: 10
  layer_scan_concurrency: 5
  migrations: true
  scanner:
    repo:
      rhel-repository-scanner: (2)
        repo2cpe_mapping_file: /data/cpe-map.json
```

```
  package:
    rhel_containerscanner: 3
      name2repos_mapping_file: /data/repo-map.json
```

1. 在多 **connstring** 字段中使用 **localhost** 替换 **host** 的值。
2. 有关 **rhel-repository-scanner** 参数的更多信息，请参阅"Mapping repository to Common Product Enumeration information"。
3. 有关 **rhel_containerscanner** 参数的更多信息，请参阅"Mapping repository to Common Product Enumeration information"。

8.2.5. 将更新程序捆绑包导入到断开连接的 OpenShift Container Platform 集群中

使用以下步骤将更新程序捆绑包导入到断开连接的 OpenShift Container Platform 集群中。

先决条件

- 您已安装了 **clairctl** 命令行工具工具。
- 您已部署了 Clair。
- 在 Clair **config.yaml** 文件中，**disable_updaters** 和 **airgap** 参数设置为 **true**。
- 您已从可访问互联网的 Clair 实例导出了更新程序捆绑包。
- 您已将更新程序捆绑包传送到断开连接的环境中。

流程

- 使用 **clairctl** CLI 工具将更新程序捆绑包导入到 OpenShift Container Platform 部署的 Clair 数据库中：

```
$ ./clairctl --config ./clair-config.yaml import-updaters updates.gz
```

8.3. 将存储库映射到通用产品枚举信息

注意

目前，IBM Power 和 IBM Z 不支持将软件仓库映射到通用产品枚举信息。

Clair 的 Red Hat Enterprise Linux (RHEL)扫描程序依赖于通用产品枚举(CPE)文件将 RPM 软件包映射到对应的安全数据，以生成匹配的结果。这些文件由产品安全及每天更新所有。

必须存在 cp 文件，或必须允许访问该文件，以便扫描程序可以正确地处理 RPM 软件包。如果文件不存在，则容器镜像中安装的 RPM 软件包不会被扫描。

表 8.1. Clair cp 映射文件

CPE	到 JSON 映射文件的链接
repos2cpe	Red Hat Repository-to-CPE JSON

CPE	到 JSON 映射文件的链接
names2repos	Red Hat Name-to-Repos JSON.

除了将 CVE 信息上传到数据库以进行断开连接的 Clair 安装外，还必须使映射文件在本地可用：

- 对于独立的 Red Hat Quay 和 Clair 部署，映射文件必须加载到 Clair pod 中。
- 对于 OpenShift Container Platform 部署的 Red Hat Quay，您必须将 Clair 组件设置为 非受管。然后，必须手动部署 Clair，将配置设置为加载映射文件的本地副本。

8.3.1. 将存储库映射到通用产品枚举示例配置

使用 Clair 配置中的 **repo2cpe_mapping_file** 和 **name2repos_mapping_file** 字段，使其包含 cp JSON 映射文件。例如：

```
indexer:
 scanner:
   repo:
     rhel-repository-scanner:
       repo2cpe_mapping_file: /data/cpe-map.json
   package:
     rhel_containerscanner:
       name2repos_mapping_file: /data/repo-map.json
```

如需更多信息，请参阅 如何将 OVAL 安全数据与已安装的 RPM 完全匹配。

第 9 章 CLAIR 配置概述

Clair 由一个结构化的 YAML 文件配置。每个 Clair 节点都需要指定在其中运行的模式，以及通过 CLI 标记或环境变量配置文件的路径。例如：

```
$ clair -conf ./path/to/config.yaml -mode indexer
```

或者

```
$ clair -conf ./path/to/config.yaml -mode matcher
```

上述命令各自使用相同的配置文件启动两个 Clair 节点。一个运行索引设施，另一个则运行匹配的设施。

如果您以 **combo** 模式运行 Clair，则必须在配置中提供索引器、匹配器和通知程序配置块。

9.1. 有关在代理环境中使用 CLAIR 的信息

如果需要，可以指定 Go 标准库所遵守的环境变量，例如：

- **HTTP_PROXY**

  ```
  $ export HTTP_PROXY=http://<user_name>:<password>@<proxy_host>:<proxy_port>
  ```

- **HTTPS_PROXY**。

  ```
  $ export HTTPS_PROXY=https://<user_name>:<password>@<proxy_host>:<proxy_port>
  ```

- **SSL_CERT_DIR**

  ```
  $ export SSL_CERT_DIR=/<path>/<to>/<ssl>/<certificates>
  ```

- **NO_PROXY**

  ```
  $ export NO_PROXY=<comma_separated_list_of_hosts_and_domains>
  ```

如果您在带有 Clair 的更新器 URL 环境中使用代理服务器，您必须识别哪些 URL 需要添加到代理 allowlist 中，以确保 Clair 可以访问它们。例如，**osv** 更新器需要访问 **https://osv-vulnerabilities.storage.googleapis.com** 来获取生态系统数据转储。在这种情况下，URL 必须添加到代理允许列表中。有关更新器 URL 的完整列表，请参阅 "Clair updater URL"。

您还必须确保将标准 Clair URL 添加到代理 allowlist 中：

- **https://search.maven.org/solrsearch/select**
- **https://catalog.redhat.com/api/containers/**
- **https://access.redhat.com/security/data/metrics/repository-to-cpe.json**
- **https://access.redhat.com/security/data/metrics/container-name-repos-map.json**

在配置代理服务器时，请考虑在 Clair 和这些 URL 之间启用无缝通信所需的任何身份验证要求或特定的代理设置。通过全面记录和解决这些注意事项，您可以在通过代理路由其更新器流量时，确保 Clair 功能有效地路由。

9.2. CLAIR 配置参考

以下 YAML 显示了一个 Clair 配置示例：

```
http_listen_addr: ""
introspection_addr: ""
log_level: ""
tls: {}
indexer:
    connstring: ""
    scanlock_retry: 0
    layer_scan_concurrency: 5
    migrations: false
    scanner: {}
    airgap: false
matcher:
    connstring: ""
    indexer_addr: ""
    migrations: false
    period: ""
    disable_updaters: false
    update_retention: 2
matchers:
    names: nil
    config: nil
updaters:
    sets: nil
    config: nil
notifier:
    connstring: ""
    migrations: false
    indexer_addr: ""
    matcher_addr: ""
    poll_interval: ""
    delivery_interval: ""
    disable_summary: false
    webhook: null
    amqp: null
    stomp: null
auth:
  psk: nil
trace:
    name: ""
    probability: null
    jaeger:
        agent:
            endpoint: ""
        collector:
            endpoint: ""
            username: null
            password: null
        service_name: ""
        tags: nil
        buffer_max: 0
metrics:
    name: ""
```

```
prometheus:
  endpoint: null
dogstatsd:
  url: ""
```

注意

为了完整，以上 YAML 文件列出了每个键。如原样使用此配置文件将导致某些选项未正常设置它们的默认值。

9.3. CLAIR 常规字段

下表描述了 Clair 部署可用的通用配置字段。

字段	Typhttp_listen_ae	描述
http_listen_addr	字符串	配置公开 HTTP API 的位置。 默认： **:6060**
introspection_addr	字符串	配置 Clair 的指标和健康端点在哪里。
log_level	字符串	设置日志记录级别。需要以下字符串之一： **debug-color,debug,info,warn,error,fatal,panic**
tls	字符串	包含提供 TLS/SSL 和 HTTP/2 的 HTTP API 配置的映射。
.cert	字符串	要使用的 TLS 证书。必须是 full-chain 证书。

常规 Clair 字段配置示例

以下示例显示了 Clair 配置。

常规 Clair 字段配置示例

```
# ...
http_listen_addr: 0.0.0.0:6060
introspection_addr: 0.0.0.0:8089
log_level: info
# ...
```

9.4. CLAIR 索引器配置字段

下表描述了 Clair 的 **indexer** 组件的配置字段。

字段	类型	描述
indexer	对象	提供 Clair 索引器节点配置。
.airgap	布尔值	为索引和获取者禁用对互联网的 HTTP 访问。允许私有 IPv4 和 IPv6 地址。数据库连接不受影响。
.connstring	字符串	Postgres 连接字符串。接受格式为 URL 或 libpq 连接字符串。
.index_report_request_concurrency	整数	速率限制索引报告创建请求的数量。把它设置为 **0** 时，以自动调整这个值的大小。设置负值表示无限。自动大小是可用内核数的倍数。 如果超过并发，API 会返回 **429** 状态代码。
.scanlock_retry	整数	一个代表 秒的正整数。在清单扫描时并发索引器锁定，以避免冲突。这个值调整等待索引器轮询锁定的频率。
.layer_scan_concurrency	整数	正整数限制并发层扫描的数量。Indexers 将同时匹配清单的层。这个值调整索引程序并行扫描的层数。
.migrations	布尔值	索引节点处理迁移到其数据库。
.scanner	字符串	索引器配置。 扫描程序允许将配置选项传递给层扫描程序。如果设计于这样做，扫描程序会将此配置传递给它。
.scanner.dist	字符串	具有特定扫描程序的名称和任意 YAML 作为值的映射。
.scanner.package	字符串	具有特定扫描程序的名称和任意 YAML 作为值的映射。
.scanner.repo	字符串	具有特定扫描程序的名称和任意 YAML 作为值的映射。

索引器配置示例

以下示例显示了 Clair 的假设索引器配置。

索引器配置示例

```
# ...
indexer:
  connstring: host=quay-server.example.com port=5433 dbname=clair user=clairuser
password=clairpass sslmode=disable
  scanlock_retry: 10
  layer_scan_concurrency: 5
  migrations: true
# ...
```

9.5. CLAIR 匹配器配置字段

下表描述了 Clair 的 **matcher** 组件的配置字段。

注意

与 **matchers** 配置字段不同。

字段	类型	描述
matcher	对象	提供 Clair 匹配器节点配置。
.cache_age	字符串	控制要提示用户缓存响应的时长。
.connstring	字符串	Postgres 连接字符串。接受格式为 URL 或 libpq 连接字符串。
.max_conn_pool	整数	限制数据库连接池大小。 Clair 允许自定义连接池大小。这个数字直接设定同时允许的活跃数据库连接的数量。 以后的版本将忽略此参数。用户应该通过连接字符串进行配置。
.indexer_addr	字符串	匹配者联系一个索引程序来创建漏洞报告。此索引器的位置是必需的。 默认值为 **30m**。
.migrations	布尔值	匹配者节点处理迁移到其数据库。
.period	字符串	决定新安全公告的更新频率。 默认值为 **30m**。

字段	类型	描述
.disable_updaters	布尔值	是否运行后台更新。 Default: **False**
.update_retention	整数	设置在垃圾回收周期之间保留的更新操作数量。这应该设置为基于数据库大小限制的安全 MAX 值。 默认值为 **10m**。 如果提供的值小于 **0**，则禁用垃圾回收。**2** 是确保将更新与通知进行比较的最小值。

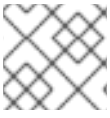
matcher 配置示例

matcher 配置示例

```
# ...
matcher:
  connstring: >-
    host=<DB_HOST> port=5432 dbname=<matcher> user=<DB_USER> password=D<B_PASS>
    sslmode=verify-ca sslcert=/etc/clair/ssl/cert.pem sslkey=/etc/clair/ssl/key.pem
    sslrootcert=/etc/clair/ssl/ca.pem
  indexer_addr: http://clair-v4/
  disable_updaters: false
  migrations: true
  period: 6h
  update_retention: 2
# ...
```

9.6. CLAIR 匹配器配置字段

下表描述了 Clair 的 **matchers** 组件的配置字段。



注意

与 **matcher** 配置字段不同。

表 9.1. matchers 配置字段

字段	类型	描述
matchers	字符串数组	为树内 **matchers** 提供配置。

字段	类型	描述
.names	字符串	一个字符串值列表，用于告知匹配者工厂关于启用的匹配者信息。如果值设为 **null**，则运行匹配者的默认列表。以下字符串被接受：**alpine-matcher**,**aws-matcher**,**debian-matcher**,**gobin**,**java-maven**,**oracle**,**photon**,**python**,**rhel**,**rhel-container-matcher**,**ruby**,**suse**,**ubuntu-matcher**
.config	字符串	提供特定匹配器的配置。 由包含子对象的 matcher 名称键的映射，它将提供给 matchers 工厂构造器。例如：

matchers 配置示例
以下示例显示了一个假设 Clair 部署，它只需要 **alpine**,**aws**,**debian**,**oracle** matchers。

matchers 配置示例

```
# ...
matchers:
  names:
  - "alpine-matcher"
  - "aws"
  - "debian"
  - "oracle"
# ...
```

9.7. CLAIR 更新器配置字段

下表描述了 Clair 更新器组件的配置字段。

表 9.2. 更新器配置字段

字段	类型	描述
Updaters	对象	为匹配者的更新管理器提供配置。

字段	类型	描述
.sets	字符串	一个值列表，告知更新管理器要运行的更新程序。 如果值设为 **null**，则默认的更新程序集合运行如下：**alpine,aws,clair.cvss,debian,oracle,photon,osv,rhel,rhcc suse,ubuntu** 如果留空，则运行零更新器。
.config	字符串	提供特定更新器集的配置。 由 updater 集合的名称键，包含将提供给更新器集的子对象。有关每个更新器的子对象列表，请参阅"高级更新器配置"。

更新器配置示例
在以下配置中，仅配置 **rhel** set。也会定义特定于 **rhel** updater 的 **ignore_unpatched** 变量。

更新器配置示例

```
# ...
updaters:
  sets:
    - rhel
  config:
    rhel:
      ignore_unpatched: false
# ...
```

9.8. CLAIR 通知程序配置字段

Clair 的一般通知配置字段如下所示。

字段	类型	描述
通知程序	对象	提供 Clair 通知程序节点配置。
.connstring	字符串	Postgres 连接字符串。接受格式为 URL 或 libpq 连接字符串。
.migrations	布尔值	通知程序节点处理迁移到其数据库。

字段	类型	描述
.indexer_addr	字符串	通知程序会联系一个索引程序来创建或获取受漏洞影响的清单。此索引器的位置是必需的。
.matcher_addr	字符串	通知程序联系一个匹配器来列出更新操作并获取 diffs。此匹配器的位置是必需的。
.poll_interval	字符串	通知程序将查询与更新操作的匹配者的频率。
.delivery_interval	字符串	通知程序尝试发送创建或之前失败通知的频率。
.disable_summary	布尔值	控制每个清单是否应当向其中一个通知进行汇总。

通知程序配置示例
以下 通知程序 片断用于最小配置。

通知程序配置示例

```
# ...
notifier:
  connstring: >-
    host=DB_HOST port=5432 dbname=notifier user=DB_USER password=DB_PASS
    sslmode=verify-ca sslcert=/etc/clair/ssl/cert.pem sslkey=/etc/clair/ssl/key.pem
    sslrootcert=/etc/clair/ssl/ca.pem
  indexer_addr: http://clair-v4/
  matcher_addr: http://clair-v4/
  delivery_interval: 5s
  migrations: true
  poll_interval: 15s
  webhook:
    target: "http://webhook/"
    callback: "http://clair-notifier/notifier/api/v1/notifications"
    headers: ""
  amqp: null
  stomp: null
# ...
```

9.8.1. Clair Webhook 配置字段

以下 webhook 字段可用于 Clair notifier 环境。

表 9.3. Clair Webhook 字段

.webhook	对象	为 webhook 发送配置通知程序。

.webhook.target	字符串	提供 webhook 的 URL。
.webhook.callback	字符串	可以检索通知的回调 URL。通知 ID 将附加到此 URL。 这通常是托管 Clair notifier 的位置。
.webhook.headers	字符串	将标头名称与值列表关联的映射。

Webhook 配置示例

Webhook 配置示例

```
# ...
notifier:
# ...
  webhook:
    target: "http://webhook/"
    callback: "http://clair-notifier/notifier/api/v1/notifications"
# ...
```

9.8.2. Clair amqp 配置字段

以下高级消息队列协议(AMQP)字段可用于 Clair 通知程序环境。

.amqp	对象	为 AMQP 交付配置通知程序。 [注意] ==== Clair 不自行声明任何 AMQP 组件。所有尝试使用交换或队列的尝试都只是被动，并且会失败。代理管理员应提前设置交换和队列。====
.amqp.direct	布尔值	如果为 **true**，则通知程序会向配置的 AMQP 代理提供单独的通知（而不是回调）。
.amqp.rollup	整数	当 **amqp.direct** 设为 **true** 时，这个值会通知通知程序在直接发送中发送了多少通知。例如，如果 **direct** 设为 **true**，并且 **amqp.rollup** 设为 **5**，则通知程序在单个 JSON 有效负载中不再提供 5 通知到代理。将值设为 **0** 实际的效果是将其设置为 **1**。
.amqp.exchange	对象	要连接的 AMQP 交换。
.amqp.exchange.name	字符串	要连接的交换的名称。

.amqp.exchange.type	字符串	交换的类型。通常，以下之一：**direct**,**fanout**,**topic**,**标头**.
.amqp.exchange.durability	布尔值	配置的队列是否持久。
.amqp.exchange.auto_delete	布尔值	配置的队列是否使用 **auto_delete_policy**。
.amqp.routing_key	字符串	每个通知发送的路由密钥的名称。
.amqp.callback	字符串	如果 **amqp.direct** 设为 **false**，则会在发送到代理的通知回调中提供此 URL。此 URL 应指向 Clair 的通知 API 端点。
.amqp.uris	字符串	按优先级顺序连接的一个或多个 AMQP 代理的列表。
.amqp.tls	对象	配置到 AMQP 代理的 TLS/SSL 连接。
.amqp.tls.root_ca	字符串	可以读取 root CA 的文件系统路径。
.amqp.tls.cert	字符串	可以读取 TLS/SSL 证书的文件系统路径。 [注意] ==== Clair 还允许 **SSL_CERT_DIR**，如 Go **crypto/x509** 软件包所记录。 ====
.amqp.tls.key	字符串	可以读取 TLS/SSL 私钥的文件系统路径。

AMQP 配置示例

以下示例显示了 Clair 的假设 AMQP 配置。

AMQP 配置示例

```
# ...
notifier:
# ...
  amqp:
    exchange:
        name: ""
        type: "direct"
        durable: true
        auto_delete: false
    uris: ["amqp://user:pass@host:10000/vhost"]
    direct: false
```

```
    routing_key: "notifications"
    callback: "http://clair-notifier/notifier/api/v1/notifications"
    tls:
     root_ca: "optional/path/to/rootca"
     cert: "madatory/path/to/cert"
     key: "madatory/path/to/key"
# ...
```

9.8.3. Clair STOMP 配置字段

以下简单文本介绍的消息协议(STOMP)字段可用于 Clair 通知程序环境。

.stomp	对象	为 STOMP 交付配置通知程序。
.stomp.direct	布尔值	如果为 **true**，则通知程序会向配置的 STOMP 代理提供单独的通知（而非回调）。
.stomp.rollup	整数	如果 **stomp.direct** 设为 **true**，则这个值会限制在单个直接发送中发送的通知数量。例如，如果 **direct** 设置为 **true**，并且 **rollup** 设为 **5**，则通知程序在单个 JSON 有效负载中不会提供 5 通知到代理。将值设为 **0** 实际的效果是将其设置为 **1**。
.stomp.callback	字符串	如果 **stomp.callback** 设为 **false**，则通知回调中提供的 URL 将发送到代理。此 URL 应指向 Clair 的通知 API 端点。
.stomp.destination	字符串	向其发送通知的 STOMP 目的地。
.stomp.uris	字符串	以优先级顺序连接到的一个或多个 STOMP 代理的列表。
.stomp.tls	对象	配置了到 STOMP 代理的 TLS/SSL 连接。
.stomp.tls.root_ca	字符串	可以读取 root CA 的文件系统路径。 [注意] ==== Clair 还尊重 **SSL_CERT_DIR**，如 Go **crypto/x509** 软件包所述。====
.stomp.tls.cert	字符串	可以读取 TLS/SSL 证书的文件系统路径。

.stomp	对象	为 STOMP 交付配置通知程序。
.stomp.tls.key	字符串	可以读取 TLS/SSL 私钥的文件系统路径。
.stomp.user	字符串	配置 STOMP 代理的登录详情。
.stomp.user.login	字符串	要连接的 STOMP 登录。
.stomp.user.passcode	字符串	要连接的 STOMP 传递码。

STOMP 配置示例

以下示例显示了 Clair 的假设 STOMP 配置。

STOMP 配置示例

```
# ...
notifier:
# ...
  stomp:
    desitnation: "notifications"
    direct: false
    callback: "http://clair-notifier/notifier/api/v1/notifications"
    login:
      login: "username"
      passcode: "passcode"
    tls:
     root_ca: "optional/path/to/rootca"
     cert: "madatory/path/to/cert"
     key: "madatory/path/to/key"
# ...
```

9.9. CLAIR 授权配置字段

以下授权配置字段可用于 Clair。

字段	类型	描述
auth	对象	定义 Clair 的外部和基于服务 JWT 的身份验证。如果定义了多个 **auth** 机制，Clair 会选择一个。目前，不支持多个机制。
.psk	字符串	定义预共享密钥身份验证。
.psk.key	字符串	在所有方签名和验证 JWT 之间分发的 base64 编码密钥。

字段	类型	描述
.psk.iss	字符串	要进行验证的 JWT 签发者列表。空列表接受 JWT 声明中的任何签发者。

授权配置示例
以下 授权 片段用于最小配置。

授权配置示例

```
# ...
auth:
  psk:
    key: MTU5YzA4Y2ZkNzJoMQ== 1
    iss: ["quay"]
# ...
```

9.10. CLAIR TRACE 配置字段

以下 trace 配置字段可用于 Clair。

字段	类型	描述
trace	对象	根据 OpenTelemetry 定义分布式追踪配置。
.name	字符串	应用程序 trace 的名称将属于。
.probability	整数	将发生 trace 的可能性。
.jaeger	对象	定义 Jaeger tracing 的值。
.jaeger.agent	对象	定义用于配置发送到 Jaeger 代理的值。
.jaeger.agent.endpoint	字符串	可以在 < **host>:<post** > 语法中提交 trace 的地址。
.jaeger.collector	对象	为配置发送到 Jaeger 收集器定义值。
.jaeger.collector.endpoint	字符串	可以在 < **host>:<post** > 语法中提交 trace 的地址。
.jaeger.collector.username	字符串	Jaeger 用户名。

字段	类型	描述
.jaeger.collector.password	字符串	Jaeger 密码。
.jaeger.service_name	字符串	在 Jaeger 中注册的服务名称。
.jaeger.tags	字符串	用于提供额外的元数据的键值对。
.jaeger.buffer_max	整数	在将内存发送到 Jaeger 后端以进行存储和分析前，可以缓冲的最大 span 数量。

trace 配置示例

以下示例显示了 Clair 的假设跟踪配置。

trace 配置示例

```
# ...
trace:
  name: "jaeger"
  probability: 1
  jaeger:
    agent:
      endpoint: "localhost:6831"
    service_name: "clair"
# ...
```

9.11. CLAIR 指标配置字段

以下指标配置字段可用于 Clair。

字段	类型	描述
metrics	对象	根据 OpenTelemetry 定义分布式追踪配置。
.name	字符串	使用的指标的名称。
.prometheus	字符串	配置 Prometheus 指标导出器。
.prometheus.endpoint	字符串	定义提供指标的路径。

指标配置示例

以下示例显示了 Clair 的假设指标配置。

指标配置示例

```
# ...
metrics:
  name: "prometheus"
  prometheus:
    endpoint: "/metricsz"
# ...
```