Red Hat Advanced Cluster Security for Kubernetes 4.4

发行注记

Red Hat Advanced Cluster Security for Kubernetes 发行版本的主要新功能及变化信息

Last Updated: 2024-06-28

Red Hat Advanced Cluster Security for Kubernetes 4.4 发行注记

Red Hat Advanced Cluster Security for Kubernetes 发行版本的主要新功能及变化信息

法律通告

摘要

此发行注记介绍了 Red Hat Advanced Cluster Security for Kubernetes 的新功能、功能增强、重要的技术变化、弃用和删除的功能、程序错误修正以及任何已知问题的信息。

目录

第 1 章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 4.4

Red Hat Advanced Cluster Security for Kubernetes (RHACS)是一个企业级的 Kubernetes 原生容器安全解决方案，可在应用程序生命周期的构建、部署和运行时阶段保护您的关键应用程序。Red Hat Advanced Cluster Security for Kubernetes 部署到基础架构中，并与您的 DevOps 工具和工作流集成。这种集成提供了更高的安全性和合规性，使 DevOps 和 InfoSec 团队能够操作安全性。

表 1.1. 发行日期

RHACS 版本	发布于
4.4.0	2024 年 3 月 28 日
4.4.1	2024 年 4 月 22 日
4.4.2	2024 年 5 月 20 日
4.4.3	2024 年 6 月 11 日

1.1. 关于此版本

RHACS 4.4 包括以下新功能、改进和更新：

Compliance

- 新的合规功能（技术预览）

网络

- 内部实体的网络图增强
- 构建时网络策略工具现已正式发布

平台

- init-bundle 图形用户界面改进
- eBPF CO-RE 集合方法默认启用
- 为 RHACS Central 使用自己的数据库现已正式发布
- 支持 ROSA 托管 control plane 上的 RHACS
- 生命周期更新
- 与 Red Hat OpenShift Cluster Manager 和 Paladin Cloud 集成，以发现未安全的集群
- 使用 roxctl CLI 在手动升级过程中迁移到 Red Hat OpenShift SCC
- 使用云源集成进行集群发现
- Central 的简短 API 令牌

policy

- 增强的 roxctl deployment check 命令
- 使用简短令牌验证 AWS 和 GCP 集成（技术预览）

漏洞管理

- 使用上游 ClairCore 的扫描程序 V4 （技术预览）
- 使用组件和组件源过滤工作负载 CVE

1.2. 新功能

此发行版本改进了与以下组件和概念相关的改进：

1.2.1. 使用上游 ClairCore 的扫描程序 V4 （技术预览）

重要

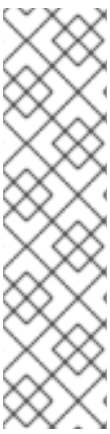
扫描程序 V4 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

在 RHACS 4.4 中，新的 Scanner V4 集成现有 StackRox Scanner 和 Red Hat Quay 附带的 上游 Clair V4 Scanner，提供增强功能。

以下是新 Scanner V4 的主要亮点：

- **一致且准确的扫描** ：在整个红帽产品生态系统、Red Hat RHACS 和 Red Hat Quay 中可靠的漏洞扫描结果。
- **扩展的语言和操作系统支持** ：以语言漏洞扫描并包含 Oracle Linux、SUSE Linux Enterprise 和 Photon OS 在操作系统扫描中扩展对 Golang 的支持。
- **全面的漏洞数据库源** ：使用 **OSV.dev** 作为所有受支持的编程语言软件包的漏洞数据库源。RHACS Scanner V4 使用此许可证的 OSV.dev 上可用的 OSV 数据库。https://github.com/google/osv.dev/blob/master/LICENSE



注意

- 在 RHACS 4.4 中，StackRox Scanner 和新的 Scanner V4 都可用于扫描工作负载，现有的 StackRox Scanner 会报告节点和平台漏洞。
- RHACS 升级和新安装默认使用 StackRox Scanner。
- 现在，除了默认的 StackRox 扫描器外，您还可以启用新的 Scanner V4。扫描程序 V4 专为扫描镜像而设计，而 StackRox Scanner 仍需要扫描节点和平台。这为您提供了额外的好处，以及保护环境的扩展范围。
- 红帽计划在以后的发行版本中将新的 Scanner V4 设为默认的 Scanner。

有关 Scanner V4 的常规信息，请参阅关于 RHACS Scanner V4。

有关安装 RHACS 时启用扫描器 V4 的更多信息，请参阅：

- 在 Red Hat OpenShift 上安装 RHACS 中的 "stackrox Scanner settings"
- 在其他平台上 安装 RHACS中的 "scanner V4"

除了运行默认 StackRox 扫描器所需的内存和存储外，扫描程序 V4 也具有额外的内存和存储要求。

有关 StackRox Scanner 和 Scanner V4 的资源要求的更多信息，请参阅：

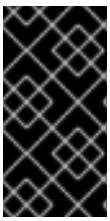
- Red Hat Advanced Cluster Security for Kubernetes 的默认资源要求 中的"常规要求"
- 推荐的 Red Hat Advanced Cluster Security for Kubernetes 资源要求

1.2.2. 新的合规功能（技术预览）

重要

Compliance 2.0 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。



重要

要使用新的 Compliance 功能，您必须安装 Compliance Operator。

如需更多信息，请参阅在 Red Hat Advanced Cluster Security for Kubernetes 中使用 Compliance Operator。

RHACS 4.4 提供结合 Compliance Operator 和 RHACS 的无缝体验。现在，您可以配置、调度并运行基础架构扫描，并从 RHACS 查看结果。

在以后的发行版本中，红帽计划提供以下额外功能：

- 修复问题，并从 RHACS 仪表板导出合规性扫描的结果。
- 创建自定义配置集。
- 支持工作负载合规性。

1.2.3. 构建时网络策略工具现已正式发布

RHACS 4.4 提供以下工具来帮助您在构建时开发 Kubernetes 网络策略：

- **roxctl netpol generate** - 通过分析本地目录中的项目的 YAML 清单来生成满足应用程序的要求的 Kubernetes 网络策略。
- **roxctl netpol connectivity map** - 列出项目中网络策略允许的连接。
- **roxctl netpol connectivity diff** - 列出两个项目版本之间的允许连接差异。

您可以使用 **roxctl** CLI 访问构建时网络策略工具。

如需更多信息，请参阅 构建时网络策略工具。

1.2.4. 内部实体的网络图增强

在 RHACS 4.4 中，选择到集群中的私有 IP 地址的连接（之前被错误地识别为外部实体），现在在网络图中显示为内部实体。

这修复了在以下情况发生时错误地识别为外部的连接，例如：

- 服务的类型已更改为或从集群 IP 地址更改为或从集群 IP 地址。
- 部署会被重启并接收新的 pod IP 地址，从而导致其他通信方尝试访问旧的 IP 地址。
- 容器会尝试与本地链接的 IP 地址通信。

如需更多信息，请参阅 网络图。

1.2.5. init-bundle 图形用户界面改进

RHACS 4.4 现在提供了一种简单的方法来添加安全集群，并在 RHACS 门户的一个位置管理它们。此发行版本还提供了新的指导，以帮助您在创建 init 捆绑包时为您提供帮助。

如需更多信息，请参阅以下更新的文档：

RHACS 云服务

- 在 Red Hat OpenShift 上生成 并应用 init 捆绑包
- 在 Kubernetes 上生成 并应用 init 捆绑包

RHACS

- 为 Red Hat OpenShift 上的 RHACS 生成并应用 init 捆绑包
- 在其他平台上为 RHACS 生成并应用 init 捆绑包

1.2.6. 与 Red Hat OpenShift Cluster Manager 和 Paladin Cloud 集成，以发现未安全的集群

在 RHACS 4.4 中，您现在可以通过与 Red Hat OpenShift Cluster Manager 和 Paladin Cloud 集成来发现不受 RHACS 保护的新集群。此功能在 OpenShift 环境中或云平台中提供了集群列表，如 Amazon Elastic Kubernetes Service (Amazon EKS)、Google Kubernetes Engine (Google GKE)和 Microsoft Azure Kubernetes Service (Microsoft AKS)，并提供发现机制来提高您机构的安全性。

Paladin Cloud 当前提供了一个免费试用，可帮助您了解 Paladin 云如何与 RHACS 一起工作，以保护云中的 Red Hat OpenShift 和 Kubernetes 部署。

有关免费试用版本的更多信息，请访问 Paladin Cloud Free Trial。

1.2.7. eBPF CO-RE 集合方法默认启用

RHACS 4.4 引进了基于 eBPF 编译的默认运行时集合方法(CO-RE)。

这个方法成为从这个版本开始的默认设置，除非在安全集群的配置中明确覆盖。

CO-RE 方法是创建可移植 eBPF 应用程序的现代方法，可确保跨内核版本和配置的兼容性，而无需在目标机器上更改或编译运行时源代码。当您升级到新版本时，从 eBPF 到 eBPF CO-RE 的迁移是自动的。

以下是这个新集合方法的一些优点：

- 您可以在目前没有包含在 support 软件包中的大量 Linux 操作系统中运行 RHACS 保护的集群。
- 如果您离线，不再需要更新 Collector 支持软件包。通过避免与 eBPF 探测检索相关的问题，如丢失网络连接的风险，或者探测不存在，您可以平稳更新集群。

1.2.8. CORE BPF 集合方法现在可用于 ppc64le 架构

RHACS 4.2 包括基于 BPF CO-RE (Compile Once-Run Everywhere)的运行时集合方法，该方法可在 **x86_64** 和 **s390x** 构架中可用。从 RHACS 4.4 开始，BPF CO-RE 现在在 **ppc64le** 构架上正式发布。要启用它，请将安全集群的 **collector.collectionMethod** 参数的值设置为 **CORE_BPF**。

1.2.9. 为 RHACS Central 使用自己的数据库现已正式发布

现在，在 RHACS 4.4 中，您可以使用自己的与 Central 兼容的数据库，可让您在集群内部或外部部署。无论是在裸机、虚拟机或云托管服务上，您可以根据具体要求定制部署。为确保最佳性能，您必须运行与 RHACS Central 服务接近的数据库。

如需更多信息，请参阅使用 Operator 方法安装带有外部数据库的 Central。

1.2.10. 支持 ROSA 托管 control plane 上的 RHACS

在 RHACS 4.4 中，您可以使用托管的 control plane (HCP)集群在 AWS (ROSA)上安装并运行 RHACS。HCP 集群中支持 Central 和安全集群服务。

注意

如果使用 HCP 集群，访问限制了 Kubernetes API 服务器审计日志的主要节点。因此，HCP 集群不支持依赖 Kubernetes 审计日志中事件的 RHACS 运行时策略。

这意味着 RHACS 无法检查 API 的使用方式，例如，用于修改 **ConfigMap**、**Secret**、**SecurityContextConstraints** (SCC)、**ClusterRoles** 等敏感资源。

1.2.11. 增强的 roxctl deployment check 命令

RHACS 4.4 提供了一个增强的 **roxctl deployment check** 命令，它包括了 **--cluster** 和 **--namespace** 选项。这些命令可用于新的 **--verbose** 标志。通过启用 **--verbose** 标志，您可以在策略检查过程中收到每个部署的附加信息。扩展信息包括基于角色的访问控制(RBAC)权限级别以及应用的网络策略的完整列表。

现在，您可以使用 **--file** 标志指定一个或多个部署来发送到 Central 的 YAML 文件。您还可以指定多个 YAML 文件来发送到 Central 以进行以空格分开的策略评估，例如 **--file=<yaml_filename** 1>、**--file=<yaml_filename2&** gt; 等等。

如需更多信息，请参阅 检查部署 YAML 文件。

1.2.12. 使用组件和组件源过滤工作负载 CVE

使用 RHACS 4.4，您可以使用漏洞管理 2.0 根据组件及其源重新定义漏洞视图。

您可以使用以下过滤器选项：

- **按组件过滤** ：使用组件名称来缩小漏洞范围。例如，如果 Ruby Action Pack 包含漏洞，则组件是 **actionpack**。
- **按组件源过滤** ： 标识包含漏洞的软件元素类型，如 **NODEJS** 或 **OS**。您可以根据您的特定需求定制您的视图。

1.2.13. 生命周期更新

RHACS 4.4 提供 RHACS 发行生命周期的扩展，并添加了完整和维护支持阶段。

如需更多信息，请参阅 Red Hat Advanced Cluster Security for Kubernetes 支持政策 。

如需有关 OpenShift Operator 维护生命周期的更多信息，请参阅红帽知识库解决方案 OpenShift Operator 生命周期。

有关与 Red Hat OpenShift 发行版本的兼容性和支持性的更多信息，请参阅红帽知识库解决方案 Red Hat Advanced Cluster Security for Kubernetes 支持列表。

1.2.14. 使用简短令牌验证 AWS 和 GCP 集成（技术预览）

重要

使用简短的令牌对 AWS 和 GCP 集成的身份验证只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

RHACS 4.4 引进了对使用短令牌验证 Amazon Web Service (AWS)和 Google Cloud Platform (GCP)集成的支持。

对于 Amazon ECR、AWS Security Hub 和 AWS S3 集成，支持使用安全令牌服务(STS)通过 AssumeRole 进行身份验证。

在 RHACS 门户中，进入 **Platform Configuration → Integrations**，然后选择集成类型，例如 **Amazon ECR**。您可以选择现有集成，或者点击 **New integration** 来创建新集成。

在集成表单中，选择 **Use container IAM role** 来启用适用于 Amazon EKS 和 Red Hat OpenShift 集群的 STS AssumeRole。

对于 Google Artifact Registry、Google Container Registry、Google Security Command Center 和 Google Cloud Storage 集成，支持通过工作负载身份联邦进行身份验证。

在 RHACS 门户中，进入 **Platform Configuration → Integrations**，然后选择集成类型，如 **Google Artifact Registry**。您可以选择现有集成，或者点击 **New integration** 来创建新集成。

在集成表单中，选择 **Use workload identity** 为 Google GKE 和 Red Hat OpenShift 集群启用令牌联邦。

如需更多信息，请参阅使用简短令牌集成 RHACS。

1.2.15. 使用云源集成进行集群发现

RHACS 4.4 引入了一个新的云源集成类型，其中包括 Paladin Cloud 和 Red Hat OpenShift Cluster Manager 的集成类型。集成的云源可让 RHACS 从连接的帐户发现集群资产。RHACS 与已由 Central 保护的集群匹配。

在 RHACS 门户中，进入 **Platform Configuration → Clusters → Discovered**cluster 来查看发现的集群的当前状态。

如需更多信息，请参阅 与云管理平台集成。

1.2.16. Central 的简短 API 令牌

RHACS 4.4 引入了提供短期 API 令牌选项，以便与 Central API 交互。

您可以为 OpenID Connect (OIDC)身份令牌交换简短的 API 令牌。这可用于在 CI 环境中进行身份验证和授权机器，例如：

在 RHACS 门户中，进入 **Platform Configuration → Integrations → Machine access 配置**来创建配置，以便为短期的 RHACS-issued 令牌启用交换 OIDC 身份令牌。

1.2.17. 使用 roxctl CLI 在手动升级过程中迁移到 Red Hat OpenShift SCC

使用 RHACS 4.4 时，平台脱离使用自定义安全性上下文约束(SCC)。相反，RHACS 服务使用 Red Hat OpenShift SCC，可确保将来的操作以及 RHACS 的一致安全状态。

如需更多信息，请参阅 手动升级过程中迁移 SCC。

1.3. 主要的技术变化

- **scanner-db** 的默认内存要求已从 200MiB 增加到 512MiB，以防止在内存压力达到节点时数据库初始化期间出现内存不足(OOM)错误。
- scanner-slim 可以从 **additional-ca-sensor** secret 正确读取额外的证书颁发机构(CA)。
- 旧的 RHACS 版本报告了 **v** 的 Alpine Linux 版本，例如 **alpine:v3.14**。RHACS 现在报告没有 **v** 的情况，例如 **alpine:3.14**。如果您有依赖于 **v** 前缀的策略，请更新它们以删除 **v**。
- 管理员访问权限不需要将临时扫描请求委派给安全集群。
- 现在，如果 **ROX_DISABLE_AUTOGENERATED_REGISTRIES** 设置为 **true**，则自动生成的集成会在 Central 启动时删除。
- **/v1/administration/usage** API 端点现在被视为稳定。
- 通过在启动时请求 **central-monitoring-tls** \ **sensor-monitoring-tls** secret，您可以确保存在 Red Hat OpenShift 监控 **/metrics** 服务器证书。只有在启用了 Red Hat OpenShift Monitoring 时才适用此要求。
- 使用 **ROX_MEMLIMIT** 环境变量，它替换配置文件中的 **GOMEMLIMIT** 变量。虽然您仍然可以使用标准 Go 环境变量 **GOMEMLIMIT**，但您应该使用 **ROX_MEMLIMIT** 来更有效地捕获部署的内存限值。**ROX_MEMLIMIT** 将 Go 进程的软内存限值设置为配置的数量的 95%。将 **ROX_MEMLIMIT** 定义为一个整数，但没有代表字节数的单位。
  如果使用 roxctl CLI 升级 RHACS，则需要手动编辑部署以使用新变量。

  如需更多信息，请参阅使用 roxctl CLI 手动升级。
- 发布开源而不是 **stackrox.io** helm chart。

- Sensor 即使没有连接到 Central，Sensor 会捕获运行时事件。
- 现在，您可以在没有任何问题的情况下从未经身份验证的电子邮件通知程序编辑端点。但是，如果端点不是未经身份验证的，则仍需要凭证才能进行更改。
- 当删除由其他对象引用的集合（如报告配置）时，错误消息现在包含要删除的集合的名称和引用对象。
- Central 中的 **ROX_SCAN_TIMEOUT** 环境变量现在默认设置为 10 分钟，而不是 6 分钟。
- 如 RHACS 4.2 中声明，**/v1/resources** 端点需要经过身份验证的用户。
- 使用 **--version** 进程参数时，默认策略 **systemctl Execution** 不会触发。这个变化不会造成安全问题，因为打印的信息会在创建时与 **systemd** 支持的功能相关，而不是主机操作系统的功能。
- **指定的默认策略 No resource requests 或 limits** 已重命名为 **No CPU 请求或内存限值**。它不再检查 CPU 限值或内存请求，而是特别识别是否指定了 CPU 请求和内存限值。
- 从 UI 配置身份验证提供程序和所需属性的声明映射。
- 配置 API 令牌过期日期。如果没有指定，API 令牌将在 1 年后过期。
- **Network → Listening Endpoints** 页面中提供的信息有所改进和更新，包括有关端点的新信息，如 pod UID 和命名空间，以及从已删除的 pod 中删除端点。

1.4. 文档添加

- 新的 **roxctl** CLI 命令参考指南，提供使用 **roxctl** CLI 命令的综合参考信息。
  如需更多信息，请参阅 roxctl CLI 命令参考中的"roxctl "。

1.5. 弃用和删除的功能

早期版本中提供的一些功能已弃用或删除。

弃用的功能仍然包含在 RHACS 中，并且仍然被支持。但是，这个功能会在以后的发行版本中被删除，且不建议在新的部署中使用。有关已弃用和删除的主要功能的最新列表，请查看下表。表后提供了有关某些删除或已弃用功能的附加信息。

在下表中，被标记为以下状态的功能：

- GA: 正式发行 (GA)
- TP: 技术预览
- DEP：弃用
- REM: 删除
- NA: 不适用

表 1.2. 弃用和删除的功能

功能	RHACS 4.2	RHACS 4.3	RHACS 4.4
definitions.stackrox.io	GA	GA	DEP
roxctl connectivity-map	DEP	DEP	DEP
roxctl generate netpol	DEP	DEP	DEP
/v1/clustercves/suppress API	GA	DEP	DEP
/v1/clustercves/unsuppress API	GA	DEP	DEP
/v1/cve/requests APIs	GA	DEP	DEP
/v1/nodecves/suppress API	GA	DEP	DEP
/v1/nodecves/unsuppress API	GA	DEP	DEP
漏洞管理(1.0)菜单项	GA	DEP	DEP
漏洞报告 Creator 权限	DEP	DEP	DEP
/v1/availableAuthProviders endpoint	GA	GA	DEP
/v1/tls-challenge endpoint	GA	GA	DEP
Istio 漏洞报告	GA	GA	DEP
自定义安全性上下文约束(SCC)： • **stackrox-collector** • **stackrox-admission-control** • **stackrox-sensor**	DEP	DEP	REM
CIS Docker v1.2.0 合规标准	DEP	DEP	REM
PCI DSS 3.2.1 合规性标准	DEP	DEP	REM
NIST SP 800-53 Compliance standard	DEP	DEP	REM
NIST SP 800-190 合规标准	DEP	DEP	REM
HIPAA 164 合规性标准	DEP	DEP	REM
CIS Kubernetes v1.5 Compliance 标准	DEP	DEP	REM

功能	RHACS 4.2	RHACS 4.3	RHACS 4.4
为 Central 组件引用镜像 pull secret 名称： • **stackrox** • **stackrox-scanner**	GA	DEP	REM
为安全集群组件引用镜像 pull secret 名称： • **stackrox** • **stackrox-scanner** • **secured-cluster-services-main** • **secured-cluster-services-collector** • **collector-stackrox**	GA	DEP	REM

1.5.1. 已弃用的功能

以下部分提供有关上表中列出的已弃用的功能和其他额外更改的信息：

- **/v1/availableAuthProviders** 端点已弃用，并在以后的发行版本中，请确保在与 **/v1/availableAuthProviders** 端点交互时对 **Access** 资源具有至少 **READ** 权限。
- **/v1/tls-challenge** 端点已弃用，并在以后的发行版本中，确保您已在与 **/v1/tls-challenge** 端点的所有交互中包含正确的身份验证。
- Istio 漏洞的报告已弃用，计划在以后的发行版本中删除。

1.5.2. 删除的功能

于 2024 年 4 月 22 日更新

以下部分提供有关上表中列出的删除功能和其他额外更改的信息：

- 删除了对旧的 Helm 版本的支持。渲染 Helm chart **stackrox-central-services** 和 **stackrox-secured-cluster-services** 现在需要 Helm 版本 3.9.0 或更高版本。
- *Compliance* 部分中的 sunburst 小部件已被删除。
- Docker CIS 基准已被删除。
- 自定义 **stackrox** 114 安全性上下文约束(SCC)已被默认 SCC 替代。
- 在 Helm 和 Operator 安装模式中，对带有特定名称的镜像 pull secret 的引用不再自动添加到服务帐户中。如果安装或升级过程中存在 secret，则会出于兼容性的原因添加引用。
  这些特殊 secret 的名称适用于 **stackrox** 和 **stackrox** -scanner 等中央组件，以及 stackrox、**stackrox-scanner**、secured-cluster**- services-main**、**secured- cluster-services-collector** 和 **collector-stackrox** 等安全集群组件。

您必须使用 **imagePullSecrets.useExisting** Helm 值或基于 operator 的安装来明确列出所需的镜像 pull secret，方法是使用 StackRox 自定义资源(CR)中的 **spec.imagePullSecrets** 字段来显式列出基于 Helm 的安装。这在没有集群查找可用性的环境中非常重要，如 ArgoCD 等 CD 管道。

1.6. 请注意即将推出的更改

- 以下搜索术语将被弃用，并计划在以后的发行版本中从部署上下文中删除：
  - 环境密钥、环境值和环境变量源
    - 通过将 **ROX_DEPLOYMENT_ENVVAR_SEARCH** 设置为 **false**，您可以删除这些环境变量术语。
  - 卷目的地、卷名称、卷 ReadOnly、卷来源和卷类型
    - 通过将 **ROX_DEPLOYMENT_VOLUME_SEARCH** 设置为 **false**，您可以删除这些卷术语。
  - Secret 和 Secret 路径
    - 通过将 **ROX_DEPLOYMENT_SECRET_SEARCH** 设置为 **false**，您可以删除这些 secret 术语。
- 以下搜索术语将被弃用，计划在以后的发行版本中从 secret 上下文中删除：
  - Secret Type、Cert Expiration 和 Image Pull Secret Registry
    - 通过将 **ROX_SECRET_FILE_SEARCH** 设置为 **false**，您可以删除这些搜索术语。
- 在 RHACS 4.4 中，当前的 init 捆绑包过程已更改。因此，计划在以后的发行版本中删除 **Integrations → Init Bundle** 页面。
- 在 RHACS 4.4 中，**definitions.stackrox.io** 已被弃用，计划在以后的发行版本中删除。
- 如果您当前使用 RHACS 3.74.x 或更早的版本，则必须在 RHACS 4.4.x 上停止，然后才能继续升级到 RHACS 4.5 或更高版本，因为 RHACS 将其底层数据存储切换到 PostgreSQL。在升级过程中，数据会自动迁移到 PostgreSQL。
  但是，在即将推出的 RHACS 4.5.0 发行版本中，预计以前的数据存储将不再可用。从 RHACS 4.0.0 跳过到 4.4.x 可能会导致数据没有正确迁移。
- stackrox Scanner 不会接收任何新功能，并将进入维护模式。现在，所有持续开发工作都侧重于新的 Scanner V4。

1.7. 程序错误修复

1.7.1. 在 4.4.0 版本中解决

发布日期 ： 2024 年 3 月 28 日

- 修复了 Sensor 在评估进程指示器时减少了分配数量的问题，从而提高了同时接收的大量运行时事件的情况。另外，默认的 gRPC 有效负载大小从 12 MB 增加到 24 MB。
- 修复了 RHACS 与 JIRA Cloud 集成可能会导致创建过程中出现问题的问题。在这个版本中，RHACS 创建的 JIRA 问题被正确优先排序，RHACS 门户集成创建页面中的默认优先级映射已更新，以匹配 JIRA 的默认优先级。

在集成创建过程中添加了检查，以减少保存后问题创建失败的风险。还引入了一个复选框，为您提供禁用优先级设置的选项。

- 修复了在扩展部署时带有 inform 和 enforce 的 RHACS 策略无法正常工作的问题。RHACS 在准入控制器中验证 Webhook 控制器的资源和操作部分中添加了 **deployments/scale**。
  在这个版本中，如果您使用 **oc scale** 命令将部署从 0 扩展到数字，如果部署违反了策略，准入控制器会阻断它。

- 在以前的版本中，当运行测试场景打开用户配置集时，挂起网络会导致一个随机的 flake 问题。在这个版本中，这个问题已被解决，以提高测试执行的可靠性。

- 在以前的版本中，由于后端同步执行，合规触发器扫描调用的问题会在 60 秒后中止。如果您保留并返回，则当前扫描进度可能会丢失。如果您有大量集群和大型数据，则此问题可能会影响您。原因是同步加载数据，以及对待处理 ID 的依赖，它们仅在触发器扫描期间确定。
  在这个版本中，后端调用成为异步，并引入了 API 参数来检索最新的运行，使用户界面(UI)能够识别正在进行中的扫描。改进包括加载在页面负载上运行扫描、显示进度以及在运行扫描期间触发其他扫描的功能。

- 在以前的版本中，编辑与 RHACS 4.1 中特定报告范围关联的自定义漏洞报告会导致报告范围引用丢失，并会触发 **A report 范围** 的信息。
  当创建超过 10 个集合且漏洞报告编辑与 RHACS 4.2 和 4.3 中的 10 个或更多集合相关联时，会出现此问题。UI 从 API 中检索前 10 个集合，可能会导致报告区域缺少引用。这个行为可能会在 RHACS 4.1 和 4.2 中保留。

  在这个版本中，确保保留了链接的集合，避免了错误消息。

1.7.2. 在版本 4.4.1 中解决

发布日期 ：2024 年 4 月 22 日

- 修复了使用 **roxctl** CLI 根据类别过滤新添加或更新策略的问题。

1.7.3. 在 4.4.2 版本中解决

发布日期 ：2024 年 5 月 20 日

此发行版本提供以下程序错误修复：

- 在此次更新之前，带有 128 个或更多内核节点上的 Collector pod 可能会因为 CO-RE BPF 分配内核内存的问题而失败，并带有 **CrashLoopBackOff** 状态。补丁版本解决了这个问题。

- 此发行版本更新了 Scanner 基准漏洞数据，以解决对红帽安全数据源所做的更改，这些数据源与 Scanner 调度的源处理中的早期数据不兼容。这解决了对包含受漏洞影响的软件包的镜像检测到各种漏洞的问题。

- 此发行版本解决了在 Central 运行 RHACS 版本 4.3.6 或更早版本且 Sensor 运行 RHACS 版本 4.4.0 或更高版本时发生的网络图形中的崩溃和呈现错误。

- 此发行版本包括一个新的环境变量 **ROX_API_TOKEN_FILE**，您可以使用它来将 API 的令牌文件路径传递给 **roxctl** CLI。

- 在早期的 RHACS 版本中，当违反情况改变时，RHACS 不会更新警报。此发行版本解决了这个问题，RHACS 会在违反更改时正确更新警报。

此发行版本提供以下更改：

- 现在，默认的 telemetry 端点被设置为一个红帽代理。

此发行版本更新了以下项目来修补漏洞：

- Go 已更新至版本 1.20.12。
- **golang.org/x/net** 模块已从 v0.22.0 更新至 v0.23.0。

1.7.4. 在 4.4.3 版本中解决

发布日期 ：2024 年 6 月 11 日

此发行版本提供以下程序错误修复：

- 修复了 Scanner V4 无法从带有不受信任的 TLS 证书的 registry 中扫描镜像的问题，即使将 TLS 验证设置为 **跳过**。

此发行版本包含以下更新：

- 更新了 Collector 版本，以支持使用 v6.7-rc5 之后的 Linux 内核的 Red Hat Enterprise Linux (RHEL) 9.4 和发行版。
- 向诊断捆绑包中添加了额外的数据库统计信息，以帮助进行故障排除。
- 以下 Scanner 软件包已更新：
  - **GitHub.com/containers/image/v5** 从 v5.29.2 到 v5.29.3
  - **GitHub.com/docker/docker** from v24.0.7 到 v24.0.9

1.8. 已知问题

于 2024 年 4 月 22 日更新

- 目前，IBM Power 架构上的 OpenShift Container Platform 4.12 存在一个问题，其中 CORE_BPF 集合方法无法正常工作。从 RHACS 4.4.1 及之后的版本中，当选择了 CORE_BPF 时，Collector 会自动使用 EBPF 集合方法。

如果您在 IBM Power 架构和离线模式中使用 OpenShift Container Platform 4.12，则必须使用 support 软件包。

1.9. 镜像版本

镜像	描述	当前版本
Main	包括 Central、Sensor、Admission 控制器和 Compliance。还包括在持续集成(CI)系统中使用的 **roxctl**。	**registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8:4.4.3**
扫描程序	扫描镜像和节点。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:4.4.3**

镜像	描述	当前版本
扫描程序数据库（Scanner DB）	存储镜像扫描结果和安全漏洞定义。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:4.4.3**
scanner V4	扫描镜像。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-v4-rhel8:4.4.3**
扫描程序 V4 DB	为 Scanner V4 存储镜像扫描结果和漏洞定义。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-v4-db-rhel8:4.4.3**
Collector	收集 Kubernetes 或 OpenShift Container Platform 集群中的运行时活动。	• **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:4.4.3** • **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:4.4.3**
Central DB	为 Central 提供数据库存储的 PostgreSQL 实例。	**registry.redhat.io/advanced-cluster-security/rhacs-central-db-rhel8:4.4.3**