



Red Hat Advanced Cluster Security for Kubernetes 4.4

关于

欢迎使用 Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes 4.4 关于

欢迎使用 Red Hat Advanced Cluster Security for Kubernetes

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

本文档概述了 Red Hat Advanced Cluster Security for Kubernetes 和文档。它包括指向常见安装任务、操作程序和集成指令的链接。

目录

第 1 章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 4.4 文档	3
1.1. 安装操作	3
1.2. 运行 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES	3
1.3. 为 KUBERNETES 配置 RED HAT ADVANCED CLUSTER SECURITY	3
1.4. 与其他产品集成	3

第 1 章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 4.4 文档

欢迎使用官方的 Red Hat Advanced Cluster Security for Kubernetes 文档，您可以在其中了解 Red Hat Advanced Cluster Security for Kubernetes 并开始了解其功能。

进入 Red Hat Advanced Cluster Security for Kubernetes 文档，您可以使用以下方法之一：

- 使用左侧导航栏浏览文档。
- 从此 Welcome 页面上的内容中选择您感兴趣的内容。

1.1. 安装操作

- [了解不同平台的安装方法](#)：确定您的产品和平台的最佳安装方法。

1.2. 运行 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES

探索您可以使用 Red Hat Advanced Cluster Security for Kubernetes 执行的各种活动：

- [查看仪表盘](#)：查找有关 Red Hat Advanced Cluster Security for Kubernetes 实时互动仪表盘的信息。了解如何使用它查看所有主机、容器和服务的关键指标。
- [管理合规性](#)：了解如何根据行业标准运行自动检查和验证合规性，包括 CIS、NIST、PCI 和 HIPAA。
- [管理漏洞](#)：了解如何识别和确定补救漏洞的优先级。
- [响应违反情况](#)：了解如何查看策略违反情况，深入到违反情况的实际原因，并采取纠正措施。

1.3. 为 KUBERNETES 配置 RED HAT ADVANCED CLUSTER SECURITY

探索 Red Hat Advanced Cluster Security for Kubernetes 中的以下典型的配置任务：

- [添加自定义证书](#)：了解如何在 Red Hat Advanced Cluster Security for Kubernetes 中使用自定义 TLS 证书。设置证书后，用户和 API 客户端不必绕过证书安全警告。
- [备份 Red Hat Advanced Cluster Security for Kubernetes](#)：了解如何为 Red Hat Advanced Cluster Security for Kubernetes 执行手动和自动数据备份，并在基础架构灾难或损坏数据时使用这些备份进行数据恢复。
- [为安全集群配置自动升级](#)：通过为每个安全集群自动化升级过程来保持最新状态。

1.4. 与其他产品集成

了解如何将 Red Hat Advanced Cluster Security for Kubernetes 与以下产品集成：

- [与 PagerDuty 集成](#)：了解如何与 PagerDuty 集成，并将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 PagerDuty。
- [与 Slack 集成](#)：了解如何与 Slack 集成，并将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 Slack。

- [与 Sumo Logic 集成](#) : 了解如何与 Sumo Logic 集成, 并将警报从 Red Hat Advanced Cluster Security for Kubernetes 转发到 Sumo Logic。
- [使用 syslog 协议集成](#) : 了解如何与安全信息和事件管理(SIEM)系统或 syslog 收集器集成, 以进行数据保留和安全调查。