Red Hat Advanced Cluster Security for Kubernetes 3.73

リリースノート

Red Hat Advanced Cluster Security for Kubernetes リリースの主な新機能と変更点

Last Updated: 2023-07-07

Red Hat Advanced Cluster Security for Kubernetes 3.73 リリースノート

Red Hat Advanced Cluster Security for Kubernetes リリースの主な新機能と変更点

法律上の通知

Copyright © 2023 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

Red Hat Advanced Cluster Security for Kubernetes リリースノートでは、新機能および拡張機能のすべて、主な技術上の変更点、非推奨および削除された機能、バグ修正、および一般公開バージョンの既知の問題についてまとめています。

目次

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.73

Red Hat Advanced Cluster Security for Kubernetes (RHACS) は、エンタープライズ対応の Kubernetes ネイティブのコンテナーセキュリティーソリューションであり、アプリケーションライフサイクルのビルド、デプロイ、ランタイムの各段階で重要なアプリケーションを保護します。インフラストラクチャーにデプロイし、DevOps ツールおよびワークフローと統合して、より優れたセキュリティーとコンプライアンスを提供し、DevOps および InfoSec チームがセキュリティーを運用できるようにします。

表1.1 リリース日

RHACS バージョン	リリース日
3.73.0	2022 年 12 月 6 日
3.73.1	2022 年 12 月 19 日
3.73.2	2023 年 2 月 6 日
3.73.3	2023 年 3 月 6 日
3.73.4	2023 年 4 月 11 日
3.73.5	2023 年 5 月 31 日

1.1. このリリースについて

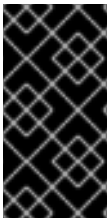
RHACS 3.73 には、以下が含まれます。

- Red Hat Advanced Cluster Security クラウドサービス (フィールドトライアル)
- ACSCS ユーザー向けの脆弱性管理ダッシュボードの改善
- PostgreSQL データベースオプション (テクノロジープレビュー)
- ビルド時の Kubernetes ネットワークポリシージェネレーター (テクノロジープレビュー)
- 機能強化とバグ修正

1.2. 新機能

1.2.1. Red Hat Advanced Cluster Security クラウドサービス

Red Hat Advanced Cluster Security Cloud Service (ACSCS) は、RHACS デプロイメントを簡素化および高速化する Red Hat マネージドサービスです。



重要

ACSCS は、フィールドトライアルリリースとして利用できます。フィールドトライアルでは、承認されたお客様に Red Hat Advanced Cluster Security Cloud Service への試用目的でのアクセスを提供します。詳細については、Red Hat セールス にお問い合わせください。

ACSCS では、Red Hat が RHACS Central インスタンスをホストして維持します。Red Hat は、業界標準のサービスレベルアグリーメント (SLA) により、インスタンスの高可用性を保証します。ACSCS インスタンスを起動したら、セキュアなクラスターとイメージリポジトリーを接続し、統合を設定して、Red Hat OpenShift Container Platform、Amazon Elastic Kubernetes Service (EKS)、Microsoft Azure Kubernetes Service (AKS)、および Kubernetes エンジン (GKE) でハイブリッド Kubernetes インフラストラクチャーをセキュリティー保護できます。

詳細および ACSCS の試用は、Red Hat Advanced Cluster Security Cloud Service への早期アクセスのリクエスト を参照してください。

次の新しいドキュメントトピックが ACSCS のインストールに利用できます。

- RHACS クラウドサービスの概要
- Red Hat OpenShift での RHACS クラウドサービスのセットアップ
- 他のプラットフォームでの RHACS クラウドサービスのセットアップ

注記

次のドキュメントトピックは、ACSCS には適用されません。

- Red Hat OpenShift での RHACS のセントラルサービスのインストール
- オプション - Operator を使用した RHACS の Central 設定オプションの設定
- 他のプラットフォームでの RHACS のセントラルサービスのインストール
- central-services Helm チャートをデプロイした後の設定オプションの変更
- Central クラスターのアップグレード
- オフラインモードの有効化
- HTTP を介した RHACS ポータルの公開
- 外部ネットワークアクセス用のプロキシーの設定
- エンドポイントの設定
- Prometheus による監視
- OpenShift Container Platform OAuth サーバーをアイデンティティープロバイダーとして設定
- Red Hat Advanced Cluster Security for Kubernetes のバックアップ
- バックアップからの復元

1.2.1.1. ACSCS ユーザー向けの脆弱性管理ダッシュボードの改善

ACSCS では、RHACS ポータルの脆弱性管理ダッシュボードにいくつかの更新が含まれています。オンプレミスの RHACS インストールには、将来のバージョンで最終的にこれらの更新プログラムが含まれます。ACSCS には次の変更が含まれています。

- 脆弱性管理ダッシュボードでは、Common Vulnerabilities and Exposures (CVE) を **Image CVE**、**Node CVE**、および **Platform CVE** カテゴリーにグループ化するようになりました。**Vulnerability Management** ビューのヘッダーで **CVE** をクリックすると、これらのカテゴリーにアクセスできます。または、エンティティーのリストを表示すると、これらのカテゴリーは **All entities** の下に表示されます。

- **Node CVEs** および **Image CVEs** リストビューで:

  - 新しい **Operating System** 列には、CVE を含むイメージのベースオペレーティングシステムが表示されます。

  - 新しい **Severity** 列には、オペレーティングシステムのコンテキストにおけるパッケージの脆弱性の重大度が表示されます。オペレーティングシステムによっては、1 つの CVE の重大度レベルが異なる場合があります。

- 一部の CVE は、複数のカテゴリーで発生する場合があります。特定のカテゴリーの CVE に対して 延期して承認 オプションを選択すると、その CVE は選択したカテゴリーに対してのみ延期されます。たとえば、ある CVE が **Node CVE** と **Image CVE** の両方に適用される場合、その CVE を **Node CVE** カテゴリーから除外すると、引き続き **Image CVE** カテゴリーに表示されます。

1.2.2. PostgreSQL データベースオプション (テクノロジープレビュー)

重要

PostgreSQL のサポートはテクノロジープレビュー機能のみです。テクノロジープレビュー機能は、Red Hat 製品のサービスレベルアグリーメント (SLA) の対象外であり、機能的に完全ではないことがあります。Red Hat は実稼働環境でこれらを使用することを推奨していません。テクノロジープレビューの機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行いフィードバックを提供していただくことを目的としています。

Red Hat のテクノロジープレビュー機能のサポート範囲に関する詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

RHACS は将来、バックエンドデータベースとして PostgreSQL を使用し、現在使用されているインメモリー RocksDB データベースを置き換えます。この移行は、現在のアーキテクチャーから PostgreSQL ベースのアーキテクチャーへの完全に自動化された移行を伴う、将来のリリースアップグレードの一部になります。

PostgreSQL を使用すると、お客様は、パフォーマンスの向上、データベースをスケーリングするための標準的なデータベース手順、バックアップと復元、および PostgreSQL データベースバックアップを使用した障害からの復旧というメリットを享受できます。さらに、既存の PostgreSQL インフラストラクチャーを使用して、RHACS 用の PostgreSQL データベースをプロビジョニングできます。

RHACS バージョン 3.73 では、PostgreSQL オプションがテクノロジープレビュー機能として利用できます。テクノロジープレビュープログラムへの参加に関心がある場合は、Red Hat が協力して手動で PostgreSQL に移行し、この機能をリリースする前にテスト環境でこれらの利点を確認できるようにします。参加するには、Red Hat アカウント担当者にお問い合わせください。

注記

Red Hat がこの機能をリリースすると、PostgreSQL が RHACS の要件となり、PostgreSQL を使用せずに RHACS をアップグレードすることはできなくなります。

1.2.3. ビルド時の Kubernetes ネットワークポリシージェネレーター (テクノロジープレビュー)

重要

ビルド時の Kubernetes ネットワークポリシージェネレーターは、テクノロジープレビュー機能のみです。テクノロジープレビュー機能は、Red Hat 製品のサービスレベルアグリーメント (SLA) の対象外であり、機能的に完全ではないことがあります。Red Hat は実稼働環境でこれらを使用することを推奨していません。テクノロジープレビューの機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行いフィードバックを提供していただくことを目的としています。

Red Hat のテクノロジープレビュー機能のサポート範囲に関する詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

RHACS 3.73 では、アプリケーション YAML マニフェストに基づいて Kubernetes ネットワークポリシーを生成するために、**roxctl** コマンドラインインターフェイス (CLI) に新しいビルド時の機能が導入されています。これを使用して、クラスターにアプリケーションをデプロイする前に、CI/CD パイプラインの一部としてネットワークポリシーを開発できます。

Red Hat は、NP-Guard プロジェクト の開発者と協力してこの機能を開発しました。ビルド時のネットワークポリシージェネレーターは、ローカルフォルダー内の Kubernetes マニフェストを分析します。これには、サービスマニフェスト、設定マップ、および Pod、Deployment、ReplicaSet、Job、DaemonSet、StatefulSet などのワークロードマニフェストが含まれます。必要な接続を検出し、Pod の分離を実現するための Kubernetes ネットワークポリシーを作成します。これらのポリシーは、必要なイングレストラフィックとエグレストラフィックよりも多くも少なくも許可しません。ビルド時のネットワークポリシー生成機能の場合、**roxctl** CLI は RHACS Central と通信する必要はありません。したがって、あらゆる開発環境で使用できます。

詳細は、ビルド時のネットワークポリシージェネレーターの使用 を参照してください。

1.3. 主な技術上の変更点

- RHACS は GraphQL を内部的に使用して、RHACS ポータルにデータを表示します。ただし、Red Hat は、GraphQL を使用した RHACS のクエリーをサポートしていません。代わりに、REST API クエリーを使用してデータにアクセスします。RHACS 3.73 リリースでは、既存の GraphQL クエリーに重大な変更がいくつか導入されています。GraphQL を使用している場合は、https://access.redhat.com/articles/6986289 を参照し、Red Hat コンサルティングにお問い合わせください。

- Sensor は、**anyuid** Security Context Constraint (SCC) を使用しなくなりました。代わりに、Sensor のデフォルトの SCC は、設定に応じて、**restricted[-v2]** または **stackrox-sensor** になりました。さらに、**restricted** および **restricted-v2** SCC を使用できるようにするために、アドミッションコントロールおよび Sensor デプロイメントの **runAsUser** および **fsGroup** は、OpenShift クラスターで **4000** にハードコーディングされなくなりました。(ROX-9342)

- Central デプロイメントで使用されるサービスアカウント **central** には、Central をデプロイメントする namespace 内の次のリソースへの **get** および **list** アクセスが含まれるようになりました。

    - pods
    - events
    - Namespaces

- CSV エクスポート API **/api/vm/export/csv** では、入力クエリーパラメーターの一部として **CVE Type** フィルターが必要になりました。フィルターを持たないリクエストはエラーを返します。**CVE Type** でサポートされている値は、**IMAGE_CVE**、**K8S_CVE**、**ISTIO_CVE**、**NODE_CVE**、および **OPENSHIFT_CVE** です。

1.4. 非推奨および削除された機能

以前のリリースで利用可能であった一部の機能が非推奨になるか、または削除されました。

非推奨の機能は依然として RHACS に含まれており、引き続きサポートされますが、本製品の今後のリリースで削除されるため、新規デプロイメントでの使用は推奨されません。非推奨および削除された主な機能の最新リストについては、以下の表を参照してください。一部の削除または非推奨の機能に関する追加情報は、表の後にあります。

以下の表では、機能は以下のステータスでマークされています。

- GA: 一般公開機能
- TP: テクノロジープレビュー機能
- DEP: 非推奨機能
- REM: 削除された機能
- 該当なし: 該当なし

表1.2 非推奨および削除機能のトラッカー

機能	RHACS 3.71	RHACS 3.72	RHACS 3.73
RenamePolicyCategory および DeletePolicyCategory アプリケーションプログラミングインターフェイス (API) エンドポイント	DEP	DEP	REM
違反タグとプロセスタグのサポート	DEP	REM	NA
パーミッション: **AuthPlugin**、**AuthProvider**、**Group**、**Licenses**、**Role**、**User**、**Indicator**、**NetworkBaseline**、**ProcessWhitelist**、**Risk**、**APIToken**、**BackupPlugins**、**ImageIntegration**、**Notifier**、**SignatureIntegration**、**ImageComponent**	DEP	DEP	REM
プロパティーによるグループの取得	DEP	DEP	REM
v1/nodes のレスポンスペイロードにおける **storage.Node** オブジェクトの **vulns** フィールド	DEP	DEP	REM

機能	RHACS 3.71	RHACS 3.72	RHACS 3.73
/v1/cves/suppress および **/v1/cves/unsuppress**	DEP	DEP	• RHACS 3.73 の DEP • ACCS の REM
/v1/cves/suppress と **/v1/cves/unsuppress** API ペイロードの **ids** フィールド	DEP	DEP	• RHACS 3.73 の DEP • ACCS の REM
VulnerabilityRequestService エンドポイントの応答に含まれる **storage.VulnerabilityRequest** オブジェクトの **cves.ids** フィールド	DEP	DEP	REM
Ubuntu 21.10 のスキャンサポート	GA	REM	NA
権限 **ClusterCVE**	GA	DEP	DEP
Label と **Annotation** の検索オプション	GA	DEP	DEP
環境変数 **ROX_WHITELIST_GENERATION_DURATION**	NA	NA	REM

1.4.1. 削除された機能

このセクションでは、前の表にリストされている削除された機能の一部に関する追加情報を提供します。

- **ROX_WHITELIST_GENERATION_DURATION** 環境変数は、RHACS 3.73 リリースで削除されました。代わりに **ROX_BASELINE_GENERATION_DURATION** を使用できます。
- Red Hat は **/v1/deploymentswithprocessinfo** エンドポイントのレスポンスから **whitelist_statuses** を削除しました。
- **/v1/cves/suppress** と **/v1/cves/unsuppress** API ペイロードの **ids** フィールドは、RHACS 3.73 リリースで **cves** に名前が変更されます。
- **VulnerabilityRequestService** エンドポイントの応答に含まれる **storage.VulnerabilityRequest** オブジェクトの **cves.ids** フィールドは、RHACS 3.73 リリースで **cves.cves** に名前が変更されます。

- **/v1/groups** エンドポイントでは、**props** フィールドを使用するときに **props.id** フィールドの値を指定しないと、**Get**、**Update**、**Mutate**、および **Remove** 関数を使用できなくなりました。(ROX-11592)
- Red Hat は、RHACS が使用しなかった **ComplianceRunSchedule** リソースを削除しました。
- Red Hat は、RHACS アクセス権限を簡素化しました。次のリストでは、新しい権限について説明し、RHACS 3.73.0 リリースで削除された権限を示します。
  - **Access** 権限は、**AuthPlugin**、**AuthProvider**、**Group**、**Licenses**、**Role**、および **User** 権限を置き換えます。
  - **DeploymentExtension** 権限は、**Indicator**、**NetworkBaseline**、**ProcessWhitelist**、および **Risk** 権限を置き換えます。
  - **Integration** 権限は、**APIToken**、**BackupPlugins**、**ImageIntegration**、**Notifier**、および **SignatureIntegration** 権限を廃止します。
  - **Image** 権限は、**ImageComponent** 権限を置き換えます。
- Central は、**scanner.<namespace>** ではなく、**scanner.<namespace>.svc** エンドポイントで Scanner に接続し、OpenShift Container Platform の **NO_PROXY** 設定を考慮します。**NO_PROXY** を使用していて、イメージスキャンで接続の問題が発生した場合は、***.svc** または **scanner.<namespace>.svc** を **NO_PROXY** 設定に追加します。(ROX-13034)
- RHACS 3.73 リリースでは、**Label** と **Annotation** の検索オプションが削除されています。これらは、次の表に示す検索オプションに置き換えられます。

表1.3 検索オプション

リソース	非推奨の検索オプション	新しい検索オプション
ノード	Label	Node Label
ノード	アノテーション	Node Annotation
Namespace	Label	namespace ラベル
デプロイメント	Label	Deployment Label
ServiceAccount	Label	Service Account Label
ServiceAccount	アノテーション	Service Account Annotation
K8sRole	Label	Role Binding Label
K8sRoleAnnotation	アノテーション	Role Binding Annotation

1.4.2. 非推奨の機能

以下の一覧では、新規パーミッションについて説明し、今後のリリースで削除される非推奨のパーミッションを示しています。

- 新しい権限 **Administration** は、権限 **AllComments**、**Config**、**DebugLogs**、**NetworkGraphConfig**、**ProbeUpload**、**ScannerBundle**、**ScannerDefinitions**、**SensorUpgradeConfig**、および **ServiceIdentity** を非推奨にします。

- 権限 **Compliance** は、権限 **ComplianceRuns** を非推奨にします。

1.4.3. 今後の製品内ドキュメント削除のお知らせ

RHACS 3.74 リリース以降、Red Hat はヘルプメニューからアクセスできる製品内ドキュメントを削除します。製品内のドキュメントを使用している場合は、代わりに必要なドキュメントを Red Hat Customer Portal から PDF 形式でダウンロードできます。(リンク: ROX-12839)

1.5. 既知の問題

ACSCS: ユーザー証明書の PKI 認証は、このリリースではサポートされていません。

1.6. バグ修正

1.6.1. バージョン 3.73.0 で解決

- 以前は、StackRox Kubernetes Security Platform - Splunk Technology Add-on を使用していた場合に、**ocp4-cis-node** コンプライアンス標準の結果が Splunk から欠落していました。Splunk 統合には、**ocp4-cis-node** コンプライアンス標準の結果が含まれるようになりました。(ROX-11937)

- 以前、Central は **v1 CronJob** デプロイメント YAML チェックで失敗しました。この問題は修正されています。(ROX-13500)

- 以前は、OpenShift Container Platform クラスターを再起動すると、**scanner-db** Pod が **init** 状態でスタックしていました。この問題は修正されています。(ROX-12556)

1.6.2. バージョン 3.73.1 で解決

- 以前は、RHACS 3.73.0 にアップグレードした後、readiness プローブの失敗により、Central Pod が **CrashLoopBackOff** 状態になりました。パッチリリース 3.73.1 により、この問題が修正されています。

- パッチリリース 3.73.1 は、RHACS ポータルのコンプライアンスダッシュボードがコンプライアンス結果の読み込みに失敗する問題を修正します。

1.6.3. バージョン 3.73.2 で解決

- パッチリリース 3.73.2 は、rocksDB から PostgreSQL への移行中に Central がクラッシュする問題を修正します。(ROX-14469)

- RHACS Operator バージョン 3.73.0 および 3.73.1 の問題により、更新しようとすると、Operator が中央の PersistentVolumeClaim (PVC) の **metadata.ownerReferences** フィールドを誤って削除し、Central および Scanner を更新できませんでした。パッチリリース 3.73.2 により、この問題が修正されています。(ROX-14335)

1.6.4. バージョン 3.73.3 で解決済み

リリース日: 2023 年 3 月 6 日

- RHACS のこのリリースでは、Docker ベースイメージの CVE-2022-47629 が修正されています。
- 今回の更新前は、セキュアなクラスターが OpenShift Container Platform 4.12 を実行している場合、RHACS はランタイムデータを表示しませんでした。詳細については、Red Hat ナレッジベースの記事 RHACS is not shown runtime data を参照してください。この問題は修正されています。
- 以前は、アラート調整ワークフローの問題により、保存された新しいランタイムポリシー違反を調整する場合、Central がクラッシュすることがありました。RHACS は、予期しないランタイムプロセスアラートが発生した場合、エラーをログに記録するようになりました。(ROX-15198)

1.6.5. バージョン 3.73.4 で解決

発売日: 2023 年 4 月 11 日

- この RHACS リリースには、Red Hat Enterprise Linux (RHEL) 8 用の RHSA-2023:1405 OpenSSL セキュリティー更新の修正が含まれています。

1.6.6. バージョン 3.73.5 で解決

リリース日: 2023 年 5 月 31 日

- RHACS のこのリリースには、更新された Golang を使用して RHACS を構築することによる CVE-2023-24540 の修正が含まれています。

1.7. イメージのバージョン

Image	説明	現在のバージョン
Main	Central、Sensor、Admission コントローラー、および Compliance が含まれます。継続的インテグレーション (CI) システムで使用する **roxctl** も含まれます。	**registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8:3.73**
Scanner	イメージおよびノードをスキャンします。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.73**
Scanner DB	イメージのスキャン結果および脆弱性の定義を格納します。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:3.73**

Image	説明	現在のバージョン
Collector	Kubernetes または OpenShift Container Platform クラスターでランタイムアクティビティーを収集します。	• **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.73** • **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.73**