Red Hat Advanced Cluster Security for Kubernetes 4.5

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: 2024-09-16

Red Hat Advanced Cluster Security for Kubernetes 4.5 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

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をまとめています。

目次

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 4.5

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す。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。Red Hat Advanced Cluster Security for Kubernetes はインフラストラクチャーにデプロイされ、DevOps ツールおよびワークフローと統合されます。この統合により、セキュリティーとコンプライアンスが向上し、DevOps チームと InfoSec チームがセキュリティーを運用できるようになります。

表1.1 リリース日

RHACS バージョン	リリース日
4.5.0	2024 年 7 月 24 日
4.5.1	2024 年 8 月 14 日

1.1. リリース 4.5.0 について

RHACS 4.5 には、次の新機能、改善点、および更新が含まれています。

コンプライアンス

- コンプライアンスの更新

ネットワーク

- ビルド時のネットワークポリシーツールの更新

プラットフォーム

- RHACS Cloud Service のエクスペリエンスの強化
- **roxctl** をインストールする GitHub アクション
- 署名検証用に独自の PKI を導入する
- RHACS Cloud Service の組み込みのメール通知機能

Vulnerability Management

- Vulnerability Management 2.0 の一般提供
- Scanner V4 の一般提供

1.2. 新機能

今回のリリースでは、以下のコンポーネントおよび概念に関連する拡張機能が追加されました。

1.2.1. Scanner V4 の一般提供

Scanner V4 の一般提供が開始しました。Scanner V4 は、StackRox Scanner とアップストリームの Clair V4 Scanner の機能を統合し、次の改善点を備えています。

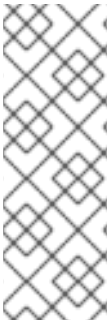
- **一貫性のある正確なスキャン**: Scanner V4 は、エコシステム全体の Red Hat 製品を対象に、信頼性の高い脆弱性スキャン結果を提供します。
- **言語の拡張とオペレーティングシステムのサポート**:
  - RHACS は言語の脆弱性スキャンで Golang をサポートするようになりました。
  - RHACS は、オペレーティングシステムのスキャンで Oracle Linux、SUSE Linux Enterprise、Photon OS をサポートするようになりました。
- **包括的な脆弱性データベースソース**: Scanner V4 は、サポートされているすべてのプログラミング言語パッケージの脆弱性データベースソースとして OSV.dev を使用します。

詳細は、RHACS Scanner V4 について を参照してください。

1.2.2. Vulnerability Management 2.0 の一般提供

このリリースにより、Vulnerability Management 2.0 の一般提供が開始します。Red Hat はすべての更新を単一の統合された **Vulnerability Management** ダッシュボードに統合しました。これにより、直感的なナビゲーションによる強化されたユーザーエクスペリエンスを提供します。

- 各担当者向けの脆弱性管理ビューを備えています。たとえば、**Node CVEs** ビューには、基盤となる CoreOS ホストに影響を与える CVE に関する情報のみが表示されます。ホスト更新を担当するチームは、その情報を使用して、的確なアクションを実行できます。
- 脆弱性を効率的にトリアージして修復するための実用的なデータを提供します。
- 監査機能を備えた強化された **例外管理** ワークフローを備えています。
- デフォルトのフィルタービューがユーザーセッション間で保持されるようになりました。
- コレクションをスコープとする包括的な脆弱性オンデマンドレポートをダウンロードできます。



注記

この更新の一環として、**リスク許容** ワークフローが **例外管理** に置き換えられます。RHACS 4.5 にアップグレードすると、次の変更が行われます。

- 既存の延期要求および誤検知要求が **例外管理** に移行されます。
- グローバルにスヌーズされたイメージ CVE が移行され、**例外管理** で承認された延期が作成されます。

1.2.3. コンプライアンスの更新

このリリースには、**Compliance** ビューに対する次の更新が含まれています。

- メールサーバーと統合して、スケジュールされたレポートを送信できます。
- あらゆるスキャン設定に対してオンデマンドレポートを生成できるようになりました。RHACS はメールで送信できます。

- スキャン結果をプロファイル別にフィルタリングして、特定のコンプライアンス標準に絞り込むことができます。
- プロファイルにベンチマーク名が追加され、コンテキストと明確さがさらに向上しました。
- スキャン結果にベンチマークに関連するコントロールのデータが追加され、コンプライアンス体制を包括的に把握できるようになりました。

1.2.4. RHACS Cloud Service の組み込みのメール通知機能

Red Hat Advanced Cluster Security Cloud Service (RHACS Cloud Service) を使用している場合は、新しい組み込みのメール通知機能を使用して、サードパーティーのメールプロバイダーを設定せずにメール通知を送信できます。

1.2.5. roxctl をインストールする GitHub アクション

roxctl-installer-action GitHub アクションが利用可能になりました。これを使用すると、GitHub ワークフローに **roxctl** をインストールし、CI パイプラインで **roxctl image check** コマンドと **roxctl image scan** コマンドを実行できます。

1.2.6. 署名検証用に独自の PKI を導入する

このリリースより前は、イメージ署名は事前に設定されたキーに対してのみ検証できました。RHACS 4.5 では、イメージ署名の検証が拡張され、証明書の検証も含まれるようになりました。この方法は公開鍵の検証に加えて使用できるため、署名を検証するために独自の公開鍵基盤 (PKI) を導入できます。

1.2.7. ビルド時のネットワークポリシーツールの更新

このリリースでは、**roxctl netpol generate** コマンドの更新が導入されています。

- デフォルトでは、コマンドは DNS 接続にポート **53** を使用します。
- **--dnsport** オプションを使用して、デフォルトの DNS ポートをオーバーライドできます。OpenShift Container Platform を使用している場合、OpenShift Container Platform はデフォルトでポート **5353** を使用するため、**roxctl** を使用してネットワークポリシーを生成するときには、常にポートを変更する必要があります。たとえば、**roxctl netpol generate --dnsport 5353 <other-options>** を使用します。

OpenShift Container Platform および名前付きポートを使用するその他のシステムの使用を簡素化するために、Red Hat は今後のリリースで **--dnsport** オプションを拡張し、文字列と数字を使用できるようにする予定です。この変更により、生成されるネットワークポリシーで、特定のポート番号の代わりに、**dns** などの名前付きポートを使用できるようになります。これにより、移植性が向上します。

詳細は、ビルド時のネットワークポリシーの生成 を参照してください。

1.2.8. RHACS Cloud Service のエクスペリエンスの強化

console.redhat.com での RHACS Cloud Service のエクスペリエンスが向上し、トライアルへのサインアップやサポートの利用が容易になりました。

1.3. 主な技術上の変更点

- RHACS Operator で、シークレットと config map の設定をキャッシュするためのラベルセレクターが追加されました。これにより、特に大規模なクラスターでメモリー消費量が大幅に削減

されます。テストでは、新しい OpenShift Container Platform クラスターのメモリー使用量が 28% 減少したことが確認されました。

- RHACS Operator で、Operator によって作成されるすべての Helm チャートリソースとシークレットに **app.stackrox.io/managed-by: operator** ラベルが追加されました。これにより、編成と可視性が向上します。
- RHACS Operator で、次のタイプのシークレットを取得するために API サーバーに送信されるリクエストの数が増加しました。
  - Operator が管理していないシークレット
  - キャッシュラベルセレクターと一致しないシークレット
- Scanner DB が、以前のバージョンである PostgreSQL 12 に代わって、PostgreSQL 15 で実行されるようになりました。データベースは永続化されないため、移行は不要であり、追加の手順なしで Scanner を引き続き使用できます。
- Nexus と Red Hat レジストリーの統合で、**/v2/<name>/manifests/<reference>** への HEAD リクエストを使用してマニフェストダイジェストをプルするようになりました。この変更により、Scanner V4 の使用時に **unsupported digest algorithm error** が発生していた問題が解決されます。環境変数 **ROX_ATTEMPT_MANIFEST_DIGEST** を **false** に設定することで、この新しい動作をオフにすることができます。
- RHACS に新しいポリシーカテゴリーが追加されました。一部のデフォルトポリシーに、これらの新しいポリシーカテゴリーがタグ付けされています。

表1.2 新しいポリシーカテゴリー

ポリシーのカテゴリー	ポリシー
Zero Trust	デプロイメントに 1 つ以上のイングレスネットワークポリシーが必要
	不正なネットワークフロー
Supply Chain Security	スキャンなしのイメージ
	30 日経過したスキャン
	90 日経過したイメージ
	必須のアノテーション: Email
	必要なアノテーション: Owner/Team
	必要なラベル: Owner/Team
	latest タグ

- **roxctl** CLI が OpenShift Container Platform のマニフェストを生成するときに、OpenShift Container Platform 3.x ではなく OpenShift Container Platform 4.x がデフォルトで使用されるようになりました。

- スキャン委譲設定に基づいて、イメージウォッチの再処理によってトリガーされたイメージスキャンを委譲できるようになりました。この機能をオフにするには、Central の環境変数 **ROX_DELEGATE_WATCHED_IMAGE_REPROCESSING** を **false** に設定します。

- Scanner V4 Matcher が、イテレーターを使用して脆弱性の同時更新を完了するようになりました。これにより、メモリー消費量が 4 GB から 500 MB に削減されます。

- RHACS 4.5 では、Central の起動パフォーマンスを向上させるために、初期レジストリー統合リポジトリーリスト **/v2/_catalog** がゆっくりと入力されるようになりました。この変更により、自動生成された統合が多数ある環境で起動時間が短縮されます。

- RHACS 4.5 には、デバッグ目的で Scanner V4 への匿名アクセスを有効にする新しい設定オプション **ROX_SCANNER_V4_ALLOW_ANONYMOUS_AUTH** があります。この機能は、開発ビルドではデフォルトでオンになっており、リリースビルドではオフになっています。

- **roxctl** CLI で作成されるデプロイメントバンドルに、デフォルトで PodSecurityPolicies (PSPs) が含まれなくなりました。Kubernetes 1.25 以前にデプロイするデプロイメントバンドルを生成する場合は、**--enable-pod-security-policies** オプションを指定する必要があります。

- RHACS 4.5 では、**ROX_UNQUALIFIED_SEARCH_REGISTRIES** が **true** に設定されている場合の Sensor イメージスキャンのイベント処理が改善されています。この機能拡張により、一意のイメージごとに同時スキャン要求が 1 つだけ許可されるようになり、不要なスキャンが削減されます。さらに、同じイメージに複数の名前が見つかった場合に、スキャンキャッシュヒットの確率が高まります。**ROX_UNQUALIFIED_SEARCH_REGISTRIES** が **true** の場合、この機能はデフォルトでオンになります。これをオフにするには、Sensor で **ROX_SENSOR_SINGLE_SCAN** を **false** に設定します。

- RHACS アドミッションコントローラー Webhook のデフォルトのタイムアウト設定が 20 秒から 10 秒に短縮されました。その結果、ValidatingWebhookConfiguration 内の実質的なタイムアウトが 12 秒になりました。この変更は、OpenShift Container Platform の無条件の上限である 13 秒に合わせたものです。インラインイメージスキャンなどで、より長いタイムアウトを使用している場合は、**SecuredCluster** カスタムリソースの **admissionControl.timeoutSeconds**、Helm の **admissionControl.dynamic.timeout**、または **admission-controller.yaml** ファイル内のセンサーデプロイメントバンドル **ValidatingWebhookConfiguration** マニフェスト内で、より長いタイムアウトを明示的に指定する必要があります。

- RHACS 4.5 では、ノードおよびプラットフォームの CVE をスヌーズする機能がデフォルトで無効になっています。以前の動作に戻すには、Central で **ROX_VULN_MGMT_LEGACY_SNOOZE** を **true** に設定する必要があります。

1.4. ドキュメントの更新

- オフラインモードで Scanner 定義を更新すると、Scanner は 5 分ごとに Central からデータを取得し、Central はオンラインデータを 5 - 20 分ごとに更新し、オフラインデータを 3 時間ごとに更新することがドキュメントに明記されました。詳細は、オフラインモードでの Scanner 定義の更新 を参照してください。

- デフォルトポリシーの表示と設定、ポリシーカテゴリーの管理、独自のカテゴリーの作成に関するドキュメントが更新されました。詳細は、セキュリティーポリシーの管理 を参照してください。

- ドキュメントが更新され、ビルド時のネットワークポリシーの生成 セクションに **--dnsport** オプションとサンプルへのリンクが追加されました。

- サポートされているオペレーティングシステムとバージョンのリストが、サポートされているオペレーティングシステム セクションで更新されました。

- RHACS Cloud Service の組み込みのメール通知機能を使用する方法に関する新しい情報が、ドキュメントに追加されました。詳細は、RHACS Cloud Service でのメールとの統合 を参照してください。
- RHACS のコンプライアンス機能の使用方法に関する詳細な手順が記載されているコンプライアンス管理ガイドが更新されました。詳細は、コンプライアンス機能の概要 を参照してください。

1.5. 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、削除されました。

非推奨の機能は引き続き RHACS に含まれ、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。非推奨および削除済みの主な機能の最新リストについては、次の表を参照してください。削除された、または非推奨になった一部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、各機能に次のステータスが表示されます。

- GA: 一般公開された機能
- 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
- NA: 該当なし

表1.3 非推奨および削除機能のトラッカー

機能	RHACS 4.3	RHACS 4.4	RHACS 4.5
definitions.stackrox.io	GA	DEP	DEP
roxctl connectivity-map	DEP	DEP	DEP
roxctl generate netpol	DEP	DEP	DEP
/v1/clustercves/suppress API	DEP	DEP	DEP
/v1/clustercves/unsuppress API	DEP	DEP	DEP
/v1/cve/requests API	DEP	DEP	DEP
/v1/nodecves/suppress API	DEP	DEP	DEP
/v1/nodecves/unsuppress API	DEP	DEP	DEP
Vulnerability Management (1.0) メニュー項目	DEP	DEP	DEP

機能	RHACS 4.3	RHACS 4.4	RHACS 4.5
Vulnerability Report Creator 権限	DEP	DEP	DEP
/v1/availableAuthProviders エンドポイント	GA	DEP	DEP
/v1/tls-challenge エンドポイント	GA	DEP	DEP
/v1/summary/counts エンドポイント	NA	NA	DEP
Istio の脆弱性の報告	GA	DEP	DEP
カスタム Security Context Constraints (SCC): • **stackrox-collector** • **stackrox-admission-control** • **stackrox-sensor**	DEP	REM	NA
CIS Docker v1.2.0 コンプライアンス標準	DEP	REM	NA
PCI DSS 3.2.1 コンプライアンス標準	DEP	REM	NA
NIST SP 800-53 コンプライアンス標準	DEP	REM	NA
NIST SP 800-190 コンプライアンス標準	DEP	REM	NA
HIPAA 164 コンプライアンス標準	DEP	REM	NA
CIS Kubernetes v1.5 コンプライアンス標準	DEP	REM	NA
Central のコンポーネントの参照イメージプルシークレット名: • **stackrox** • **stackrox-scanner**	GA	REM	NA

機能	RHACS 4.3	RHACS 4.4	RHACS 4.5
セキュアクラスターのコンポーネントの参照イメージプルシークレット名: • **stackrox** • **stackrox-scanner** • **secured-cluster-services-main** • **secured-cluster-services-collector** • **collector-stackrox**	GA	REM	NA
rhacs-collector* および **rhacs-collector-slim*** イメージ	NA	NA	DEP
カーネルサポートパッケージとドライバーダウンロード機能	NA	NA	DEP

1.5.1. 非推奨の機能

このセクションでは、上記の表に記載されている非推奨の機能とその他の変更点を説明します。

- ストリーム API リクエストと単項 API リクエストのレスポンスデータを統一するために、次の点が変更されました。
  - 失敗した単項 API リクエストに対して返される **error** フィールドが非推奨になりました。**error** フィールドの代わりに、**message** フィールドを使用してエラー情報を取得してください。**message** フィールドには、**error** フィールドと同じ情報が含まれます。
  - RHACS の次のリリースで、Red Hat は gRPC ストリーム API に対して返されるエラー応答内の **grpcCode**、**httpCode**、および **httpStatus** フィールドを削除します。代わりに、**grpcCode** データを含む新しいフィールド **code** が応答に追加されます。
- **/v1/summary/counts** API が非推奨になりました。
- 脆弱性例外を管理するための **/v1/cve/requests** API が非推奨になりました。新しい **/v2/vulnerability-exceptions/** API を使用してください。
- **rhacs-collector*** および **rhacs-collector-slim*** イメージが非推奨になりました。これらは機能的には同じであり、カーネルドライバーを含んでいません。
- カーネルサポートパッケージとドライバーダウンロード機能が非推奨になりました。
- **Vulnerability Management** の **Dashboard** ビューが非推奨になりました。代わりに、**Workload CVEs**、**Exception Management**、**Platform CVEs**、および **Node CVEs** ビューを使用してください。
- Amazon S3 外部バックアップ統合と Google Cloud Storage の相互運用性が非推奨になりました。バックアップには Google Cloud Storage 統合 を使用する必要があります。

1.5.2. 削除された機能

このセクションでは、上記の表に記載されている削除された機能とその他の変更点を説明します。

- Red Hat は、3.9.0 より古いバージョンの Helm のサポートを終了しました。RHACS では、**stackrox-central-services** および **stackrox-secured-cluster-services** Helm チャートをレンダリングするために、Helm バージョン 3.9.0 以降が必要になりました。
- **ROX_SCANNER_V4_NODE_JS_SUPPORT** 環境変数が、**ROX_SCANNER_V4_PARTIAL_NODE_JS_SUPPORT** 環境変数に置き換えられました。
- **EBPF** コレクションが削除されました。アップグレードすると、設定が自動的に **CORE_BPF** に変換され、**forceCollection** オプションが適用されなくなります。
- RHACS バージョン 3.74 以前からバージョン 4.5 への直接アップグレードがサポートされなくなりました。バージョン 4.5 以降にアップグレードするには、まずバージョン 4.4 にアップグレードする必要があります。

1.6. バージョン 4.5.0 のバグ修正

リリース日: 2024 年 7 月 24 日

- 以前は、バグにより、管理者権限を持たないユーザーが、**read** 権限を持つクラスターおよび namespace のリスニングエンドポイントデータにアクセスできませんでした。この更新により、**read** 権限を持つユーザーが、リスニングエンドポイントサービスからデータを受信できるようになりました。

1.7. リリース 4.5.1 について

このリリースには、注目すべき技術的な変更とバグ修正が含まれています。

1.7.1. バージョン 4.5.1 での変更点

- RHACS ポータルのネットワークグラフとネットワークポリシージェネレーターが更新され、**AdminNetworkPolicy** リソースおよび **BaselineAdminNetworkPolicy** リソースはネットワークグラフ内またはネットワークポリシー生成中に考慮されないことが明確になりました。
- RHACS コンポーネントは、CVE-2024-41110: Docker Engine の認可プラグインの脆弱性 (AuthZ) の修正を含むバージョンに更新されました。

1.7.2. バージョン 4.5.1 のバグ修正

リリース日: 2024 年 8 月 14 日

- RHACS 4.5.0 にアップグレードする場合、状況によっては、**uni_compliance_integrations_clusterid** 制約の **central-db** エラーによりアップグレードが失敗しました。この問題が修正されました。
- RHACS 4.5.0 にアップグレードした後、64 個を超えるコアを持つノードの場合、Collector はリングバッファーサイズが許可されていないというエラーを表示しました。この問題が修正されました。
- Google がデフォルトのネットワークサービスにマネージドパブリック IP アドレス範囲 **34.118.224.0/20** を使用するように変更したため、Google Kubernetes Engine (GKE) バージョン 1.29 以降を実行しているクラスターを持つユーザーのネットワークグラフが壊れていました。ネットワークグラフでは、この IP アドレス範囲が外部としてマークされています。この問題が修正されました。

1.8. イメージのバージョン

Red Hat Advanced Cluster Security for Kubernetes イメージを手動でプル、再タグ付け、およびレジストリーにプッシュできます。最新バージョンには次のイメージが含まれています。

表1.4 Red Hat Advanced Cluster Security for Kubernetes のイメージ

Image	説明	現行バージョン
Main	Central、Sensor、Admission コントローラー、および Compliance コンポーネントが含まれます。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-rhel8:4.5.1**
Central DB	Central にデータベースストレージを提供する PostgreSQL インスタンス。	**registry.redhat.io/advanced-cluster-security/rhacs-central-db-rhel8:4.5.1**
Scanner	イメージおよびノードをスキャンします。	1. **registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:4.5.1** 2. **registry.redhat.io/advanced-cluster-security/rhacs-scanner-slim-rhel8:4.5.1**
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-rhel8:4.5.1**
Scanner V4	イメージをスキャンします。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-v4-rhel8:4.5.1**
Scanner V4 DB	Scanner V4 のイメージスキャン結果と脆弱性定義を保存します。	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-v4-db-rhel8:4.5.1**
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。	1. **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:4.5.1** 2. **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:4.5.1**