



Red Hat Advanced Cluster Security for Kubernetes 3.70

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

Red Hat Advanced Cluster Security for Kubernetes 3.70 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

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Release_notes.ent file |.

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 3.70	3
1.1. 新機能	3
1.1.1. Cosign 公開鍵に対するイメージ署名の検証	3
1.1.2. 欠落している Kubernetes ネットワークポリシーを特定する	3
1.2. 機能拡張	4
1.2.1. Spring の重大な脆弱性の特定	4
1.2.2. Amazon ECR レジストリーの自動統合	4
1.2.3. Pod セキュリティーコンテキストの検証の改善	4
1.2.4. 許可される包含および除外スコープの数の増加	4
1.2.5. OpenShift Container Platform コンソールで ACS 管理者ユーザーのクレデンシャルを簡単に見つける	4
1.3. 主な技術上の変更点	4
1.3.1. RHCOS ノードの脆弱性スキャンとレポート	5
1.4. 非推奨および削除された機能	5
1.4.1. 非推奨の機能	6
1.4.2. 削除された機能	6
1.5. バグ修正	6
1.5.1. バージョン 3.70.2 で解決	6
1.5.2. バージョン 3.70.1 で解決	7
1.5.3. バージョン 3.70.0 で解決	7
1.6. イメージのバージョン	7

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.70

表1.1 リリース日

RHACS バージョン	リリース日
3.70.0	2022 年 6 月 2 日
3.70.1	2022 年 6 月 22 日
3.70.2	2022 年 10 月 5 日

Red Hat Advanced Cluster Security for Kubernetes は、ビルド、デプロイ、ランタイム全体で重要なアプリケーションを保護する、エンタープライズ対応の Kubernetes ネイティブコンテナセキュリティソリューションです。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を運用できるようにします。



重要

2022 年 10 月 20 日に出されたアップストリームの脆弱性フィードで予期しないスキーマが変更され、Red Hat は破損した CVE データファイルを <https://definitions.stackrox.io> に公開し、多くの Central インスタンスが破損したファイルをダウンロードしました。その結果、Central が破損したフィードデータを処理すると失敗し、**CrashLoopBackOff** の状態になります。Red Hat は、破損した CVE データファイルを修正する手順をすでに完了していますが、すでに影響を受けている Central インスタンスでは、**CrashLoopBackOff** の状態から自動で抜け出すことはできません。Central を機能する状態に戻すには、[CrashLoopBackOff - 2022-10-20 Incident の Central](#) の手順に従います。

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.70 には、機能強化、バグ修正、スケール改善などの変更が含まれています。

1.1. 新機能

1.1.1. Cosign 公開鍵に対するイメージ署名の検証

RHACS を使用して、事前設定されたキーに対してイメージシグネチャーを検証することにより、クラスター内のコンテナイメージの整合性を確保できます。ポリシーを作成して、署名されていないイメージや署名が確認されていないイメージをブロックし、アドミSSIONコントローラーを使用して不正な展開の作成を停止することでポリシーを適用することもできます。Cosign 鍵署名検証をサポートします。詳細は、[イメージの署名の確認](#) を参照してください。

1.1.2. 欠落している Kubernetes ネットワークポリシーを特定する

Kubernetes ネットワークポリシーは、クラスター内でゼロトラストネットワークを有効にするために不可欠です。横方向の動きの機会を制限することにより、ネットワーク攻撃の影響を軽減します。デフォルトでは、Kubernetes リソースは分離されていません。ネットワークポリシーを適用することは、ユーザーに任せることをお勧めするベストプラクティスです。

RHACS 3.70 には、入力ネットワークポリシーによって制限されていない展開を簡単に識別し、それに応じて違反アラートをトリガーできる新しいデフォルトポリシーが付属しています。

- デフォルトのポリシーは、**Deployments** という名前で、少なくとも1つの入力ネットワークポリシーが必要です。これはデフォルトでは無効にされます。
- このデフォルトのポリシーは、**入力ネットワークポリシーが欠落している場合にアラート** と呼ばれる新しいポリシー基準を使用します。
- Pod 分離ギャップを特定するには、このデフォルトポリシーのクローンを作成するか、ポリシー基準を使用して選択したリソースで有効にすることにより、新しいポリシーを作成します。

1.2. 機能拡張

1.2.1. Spring の重大な脆弱性の特定

RHACS 3.70 では、Spring Cloud Function RCE 脆弱性 ([CVE-2022-22963](#)) および Spring Framework Spring4Shell RCE 脆弱性 ([CVE-2022-22965](#)) を検出するポリシーが追加されました。このポリシーの重大度はクリティカルで、デフォルトで有効になっています。

1.2.2. Amazon ECR レジストリーの自動統合

Amazon Elastic Container Registry (ECR) のレジストリー統合が、Amazon Web Services (AWS) クラスターに対して自動的に生成されるようになりました。この機能を使用するには、ノードのインスタンス ID および Access Management (IAM) ロールに ECR へのアクセスが許可されている必要があります。ノードで EC2 インスタンスメタデータサービスを無効にすることで、この機能をオフにできます。詳細については、[Amazon EC の統合](#) を参照してください。

1.2.3. Pod セキュリティーコンテキストの検証の改善

Kubernetes セキュリティーコンテキスト内の **allowPrivilegeEscalation** の値を検証するために、新しいポリシー基準が追加されました。このポリシー基準を使用して、コンテナプロセスがその親プロセスよりも多くの特権を取得できるようにデプロイメントが設定されている場合にアラートを提供できます。

1.2.4. 許可される包含および除外スコープの数の増加

以前は、RHACS は、スコープ内で許可される包含スコープと除外スコープの数をそれぞれ 10 に制限していました。この制限は削除されました。

1.2.5. OpenShift Container Platform コンソールで ACS 管理者ユーザーのクレデンシャルを簡単に見つける

推奨される Operator メソッドを使用して RHACS を OpenShift Container Platform にデプロイするお客様は、OpenShift Container Platform コンソールで **admin** ユーザーのクレデンシャルを表示できるようになりました。Central オブジェクトを表示すると、**Details** タブに、**Admin Password Secret Reference** の下の資格情報へのクリック可能なリンクが表示されます。表示されるクレデンシャルは、デフォルトで生成されたパスワード、または以前に設定および保存されたカスタムシークレットです。詳細については、[Central インストールの確認](#) を参照してください。

1.3. 主な技術上の変更点

1.3.1. RHCOS ノードの脆弱性スキャンとレポート

Red Hat Enterprise Linux CoreOS (RHCOS) ノードの脆弱性スキャンとレポートは、スキャンが改善されて精度が向上し、Kubernetes コンポーネントだけでなく完全なホストレベルのスキャンがサポートされるまで無効になっています。現在、RHCOS は、RHCOS から Kubernetes コンポーネントの脆弱性を報告するために、National Vulnerability Database (NVD) の脆弱性データを使用しています。拡張バージョンでは、脆弱性レポートは Red Hat が公開したセキュリティーデータに基づいています。(ROX-10662)

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: テクノジープレビュー機能
- DEP: 非推奨機能
- REM: 削除された機能

表1.2 非推奨および削除機能のトラッカー

機能	RHACS 3.68	RHACS 3.69	RHACS 3.70
デフォルトのポリシーを削除する機能	DEP	DEP	REM
アラートとプロセスにコメントを追加する機能	GA	DEP	DEP
Anchore、Tenable、および Docker 信頼されたレジストリー 統合。	GA	DEP	DEP
スコープアクセス制御用の外部承認プラグイン。	GA	DEP	DEP
Disallowed Dockerfile 行ポリシーフィールドの FROM オプション	GA	GA	DEP
PodSecurityPolicy (PSP) Kubernetes オブジェクト	GA	GA	DEP
RenamePolicyCategory および DeletePolicyCategory エンドポイント	GA	GA	DEP
roxctl helm 出力コマンドの --rhacs オプション	GA	DEP	DEP
policyVersion のないセキュリティーポリシー	DEP	DEP	REM

機能	RHACS 3.68	RHACS 3.69	RHACS 3.70
/v1/policies API エンドポイントレスポンス: field レスポンスボディーパラメーター	DEP	DEP	REM
/v1/policies API エンドポイントレスポンス: whitelists レスポンスボディーパラメーター	DEP	DEP	REM
/v1/nodes および /v1/images API エンドポイントのレスポンス: firstNodeOccurrence レスポンス本文パラメーター	GA	DEP	DEP

1.4.1. 非推奨の機能

- **Anchore**、**Tenable**、および **Docker Trusted Registry** の統合: RHACS スキャナーはこれらの統合に取って代わります。
- **スコープ付きアクセス制御用の外部認証プラグイン**: 既存の製品内スコープ付きアクセス制御を使用します。
- **Disallowed Dockerfile line policy** フィールドの **FROM** オプション: **FROM** オプションを含む Disallowed Dockerfile line policy フィールドを含むポリシーは、これらのポリシーセクションを削除するように更新する必要があります。

1.4.2. 削除された機能

- RHACS 3.70 は、ポリシーのインポートを含む (ただしこれに限定されない) **policyVersion 1.1** を持たないセキュリティーポリシーをサポートしなくなりました。
- Red Hat Advanced Cluster Security for Kubernetes では、デフォルトポリシーの削除は許可されません。ポリシーを削除するのではなく、不要なデフォルトのポリシーを無効にすることができます。
- **/v1/policies** API エンドポイントの応答は、**field** レスポンスのボディーパラメーターを返しません。

1.5. バグ修正

1.5.1. バージョン 3.70.2 で解決

リリース日: 2022 年 10 月 5 日

本リリースには、ベースイメージの以下の CVE (Common Vulnerabilities and exposures) に対応するセキュリティー更新が含まれています。

- [CVE-2022-2526](#): **systemd-resolved:resolved-dns-stream.c** で **DnsStream** を処理するときの **use-after-free**
- [CVE-2022-29154](#): **rsync**: リモートの任意のファイルが、接続しているピアのディレクトリー内に書き込まれます

1.5.2. バージョン 3.70.1 で解決

リリース日: 2022 年 6 月 22 日

- [CVE-2022-1902](#): 以前は、不適切なサニタイズにより、認証されたユーザーが GraphQL API から Notifier シークレットを取得できました。この問題は修正されています。(ROX-11490)

1.5.3. バージョン 3.70.0 で解決

リリース日: 2022 年 6 月 2 日

- JFrog Artifactory 統合を設定する場合、匿名のプルを許可するために、ユーザー名とパスワードのフィールドがオプションになりました。(ROX-10090)
- 一般的な Webhook 統合でエンドポイント URL の Web ユーザーインターフェイスを検証すると、エラーが発生しました。この問題は修正されました。(ROX-9902)
- ポリシー **OpenShift: Kubeadmin Secret Accessed**は、リクエストがデフォルトの OpenShift **oauth-apiserver-sa** サービスアカウントからのものである場合にトリガーされなくなりました。これは、OpenShift API サーバーで想定されるアクセスパターンであるためです。(ROX-10018)
- **Policies** リストで選択された複数のポリシーの通知を有効または無効にする機能が復活しました。通知ステータスを変更するには、1つ以上のポリシーを選択し、**Bulk Actions** メニューから **Enable notification** または **Disable notification** を選択します。(ROX-9985)
- 読み取り/書き込みパーミッションを持つユーザーがレポートを作成または編集できない脆弱性レポートのパーミッションの問題を修正しました。(ROX-9880)
- RHACS に接続した後に OpenShift Container Platform コンソールへの接続の問題が発生した問題、または OpenShift Container Platform コンソールへの接続が存在する場合に RHACS に接続できない問題を修正しました。Central は、TLS SNI を介して送信された **ServerName** が **:authority** (Host) ヘッダーと一致しないリクエストに対して、**421 Misdirected Request** ステータスコードで応答するようになりました。この機能は、環境変数 **ROX_ALLOW_MISDIRECTED_REQUESTS=true** を設定することでオフにできます。(ROX-9625)
- ポリシーを編集するとき、無効になっているポリシーの **Violations Preview** ウィンドウは使用できませんでした。この問題は修正されています。(ROX-9435)
- ロールベースアクセス制御 (RBAC) 関連のリスク計算を無効にする機能を追加しました。ユーザーは、Central デプロイメント仕様で環境変数 **ROX_INCLUDE_RBAC_IN_RISK=false** を設定して、リスク計算から RBAC を除外できます。(ROX-10627)

1.6. イメージのバージョン

Image	説明	現在のバージョン
-------	----	----------

Image	説明	現在のバージョン
Main	Central、Sensor、Admission Controller、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-rhel8:3.70.2
スキャナー	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-rhel8:3.70.2
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-rhel8:3.70.2
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を収集します。	<ul style="list-style-type: none">● registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.70.2● registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.70.2