



Red Hat Advanced Cluster Management for Kubernetes 2.8

リリースノート

リリースノート

Red Hat Advanced Cluster Management for Kubernetes 2.8 リリースノート

リリースノート

法律上の通知

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.

概要

新機能、エラータの更新、既知の問題、非推奨と削除、および GDPR と FIPS の準備に関する製品の考慮事項に関するリリースノートの詳細をお読みください。

目次

第1章 リリースノート	3
1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES の新機能	3
1.2. エラータの更新	6
1.3. 既知の問題	7
1.4. 非推奨と削除	28
1.5. GDPR に対応するための RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES プラット フォームでの考慮事項	35
1.6. FIPS READINESS	42

第1章 リリースノート

現在のリリースについて学びます。

注記: Red Hat Advanced Cluster Management の 2.6 以前のバージョンはサービスから **削除** され、サポートされなくなりました。バージョン 2.6 以前のドキュメントは更新されていません。ドキュメントはそのまま利用できますが、エラータやその他の更新はなく、非推奨となります。

- [Red Hat Advanced Cluster Management for Kubernetes の新機能](#)
- [エラータの更新](#)
- [既知の問題と制限](#)
- [非推奨と削除](#)
- [GDPR に対応するための Red Hat Advanced Cluster Management for Kubernetes での考慮事項](#)
- [FIPS readiness](#)

現在サポートされているリリースのいずれか、製品ドキュメントで問題が発生した場合は、[Red Hat サポート](#) にアクセスして、トラブルシューティングを行ったり、[ナレッジベース](#) の記事を表示したり、サポートチームに連絡したり、ケースを開いたりすることができます。認証情報でログインする必要があります。[Red Hat Customer PortalFAQ](#) で、カスタマーポータルドキュメントの詳細を確認することもできます。

1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES の新機能

Red Hat Advanced Cluster Management for Kubernetes では、可観測性を提供し、ビルトインされたガバナンス、クラスターおよびアプリケーションライフサイクル管理で、Kubernetes ドメイン全体を可視化します。今回のリリースでは、より多くの環境でのクラスター管理、アプリケーション向けの GitOps 統合などが可能になりました。

重要: 一部の機能およびコンポーネントは [テクノロジープレビュー](#) として指定され、リリースされません。

- [インストール](#)
- [Web コンソール](#)
- [クラスター](#)
- [アプリケーション](#)
- [ガバナンス](#)
- [アドオン](#)
- [バックアップおよび復元](#)

1.1.1. インストール

Operator Lifecycle Manager の **OperatorCondition** リソースを利用して、効率的な Red Hat Advanced Cluster Management for Kubernetes アップグレード手順を強制実行できるようになりました。これにより、リリースが省略されることを回避できます。詳細は、[アップグレード](#) を参照してください。

1.1.2. Web コンソール

- クラスタアドオンに関する情報は、**Overview** ページから取得できます。可用性と正常性に関する情報は、**Cluster add-ons** をクリックすると確認できます。
- Grafana コンポーネントがバージョン 8.1.3 から 8.5.20 にアップグレードされました。[Grafana バージョンの確認](#) を参照してください。
- 認証情報を作成するときに内部認証局を追加すると、その証明書情報を使用して **clouds.yaml** が自動的に更新されるようになりました。
- **search-api** と **search_indexer** がメトリクスを公開するようになりました。[コンソールでの検索の概要](#) を参照してください。
- **envVar** セクションを使用して検索 Pod の環境変数を複数追加し、名前を付ける各変数の値を指定します。[検索のカスタマイズと設定](#) を参照してください。
- **prometheus-alertmanager** が v0.25.0 にアップグレードされました。
- Thanos が v0.31.0 にアップグレードされました。
- 複数のノードを選択して、**Utilization** ダッシュボードから表示できるようになりました。
- Grafana ダッシュボード内を移動しても、フィルターと時間範囲はそのまま保持されます。
- サービスが有効な場合、**Alert Analysis**、**Clusters by Alert**、**Alerts by Cluster** の 3 つのダッシュボードが提供されます。
- 新しい **Remove automation template** オプションがクラスタページで使用できるようになりました。
- 選択に基づき、**Automation** および **Policy Automation** エディターから説明、Ansible テンプレートへのリンク、インベントリを受信できるようになりました。

Web コンソールからの可観測性に関するその他のトピックについては、[可観測性サービスの概要](#) を参照してください。

1.1.3. クラスタ

クラスタのライフサイクルコンポーネントと機能は、クラスタフリートの管理を強化するソフトウェア Operator であるマルチクラスタエンジン Operator 内にあります。マルチクラスタエンジン Operator は、クラウドおよびデータセンター全体の Red Hat OpenShift Container Platform および Kubernetes クラスタライフサイクル管理をサポートします。このテクノロジーでは、OpenShift Container Platform が前提条件です。

[クラスタライフサイクルの概要](#) でリリースノート、タスク、およびサポート情報を表示します。

1.1.4. アプリケーション

- Argo CD プルモデルを使用すると、プッシュモデルに使用されるのと同じ **ApplicationSet** CRD を使用して、ハブクラスタから各マネージドクラスタにリソースをデプロイできます。Pull モデルの実装では、OpenShift Cluster Manager の登録、配置、**manifestWork** API が適用され、ハブクラスタがハブクラスタとマネージドクラスタ間の安全な通信チャンネルを使用してリソースをデプロイできるようになります。詳細は、[プッシュアンドプルモデルを使用した Argo CD のデプロイ](#) を参照してください。

- アプリケーション配置許容を設定して、アプリケーションを Red Hat OpenShift GitOps にデプロイするマネージドクラスターを登録します。詳細は [Red Hat Advanced Cluster Management および OpenShift GitOps のアプリケーション配置許容範囲の設定](#) を参照してください。

他のアプリケーションのトピックは、[アプリケーションの管理](#) を参照してください。

1.1.5. ガバナンス

- ポリシーおよびポリシーセットの配置ラベルセレクターを指定するとともに、ポリシーを複製するときに余分なメタデータを削除するようにポリシージェネレーターを設定できるようになりました。詳細は、[ポリシージェネレーター設定の参照テーブル](#) を参照してください。
- **copyConfigMapData** 関数と **copySecretData** 関数を使用して、特定の ConfigMap またはシークレットのデータコンテンツをコピーします。詳細は、[テンプレート関数](#) を参照してください。
- ポリシーテンプレートに複数の YAML 文字列を追加します。詳細は、[設定ポリシー YAML テーブル](#) を参照してください。
- これで、**policy.open-cluster-management.io/description** アノテーションを使用して、ポリシーの説明を作成、編集、表示できるようになりました。[コンソールからのクラスターセキュリティポリシーの作成](#) を参照してください。
- ポリシーの伝播時に、ハブクラスターテンプレートで **.ManagedClusterLabels** 変数を使用して、マネージドクラスターからラベル値を検索します。比較表は、[ハブクラスターとマネージドクラスターテンプレートの比較](#) セクションで確認できます。
- Red Hat Advanced Cluster Management ポリシーを使用することで、ハブクラスター上でのマルチクラスターディストリビューションと Gatekeeper 監査結果の集約に Gatekeeper の統合を活用できます。[gatekeeper 制約と制約テンプレートの統合](#) を参照してください。
- API サーバーの要求とバーストのレートを設定して、設定ポリシーコントローラーの応答性を変更できます。詳細は、[API サーバーへの要求のレート設定](#) を参照してください。
- Red Hat OpenShift Platform Plus ポリシーセットを適用して Red Hat OpenShift Platform Plus をインストールします。詳細は、[Red Hat OpenShift Platform Plus ポリシーセット](#) を参照してください。

ダッシュボードとポリシーフレームワークに関する詳細は、[ガバナンス](#) を参照してください。

1.1.6. アドオン

- Rsync-TLS レプリケーションを使用して永続ボリュームをレプリケートできるようになりました。Rsync-TLS は、セキュリティを強化するために stunnel が指定する TLS で保護されたトンネルを使用します。詳細は、[Rsync-TLS レプリケーションの設定](#) を参照してください。

1.1.7. バックアップおよび復元

ハブクラスターの災害復旧ソリューションは、[バックアップと復元](#) を参照してください。

1.1.8. このリリースの詳細

- [Red Hat Advanced Cluster Management for Kubernetes へようこそ](#) から Red Hat Advanced Cluster Management for Kubernetes の概要を確認してください。

- Red Hat Advanced Cluster Management [リリースノート](#) の [既知の問題と制限](#) など、その他のリリースノートを参照してください。
- 製品の主要なコンポーネントは、[マルチクラスターアーキテクチャー](#) のトピックを参照してください。
- サポート情報などは、Red Hat Advanced Cluster Management [トラブルシューティングガイド](#) を参照してください。
- オープンコミュニティからの相互作用、成長、および貢献のために、オープンソースの [Open Cluster Management](#) リポジトリにアクセスします。[open-cluster-management.io](#) を参照してください。詳細は、[GitHub](#) [リポジトリ](#) にアクセスしてください。

1.2. エラータの更新

デフォルトでは、エラータの更新はリリース時に自動的に適用されます。リリースが入手可能になれば、詳細がここに公開されます。

重要: 参考までに、[エラータ](#) リンクと Jira 番号がコンテンツに追加され、内部で使用される可能性があります。ユーザーは、アクセス権が必要なリンクを利用できない可能性があります。

FIPS の通知: [spec.ingress.sslCiphers](#) で独自の暗号を指定しない場合、[multiclusterhub-operator](#) は暗号のデフォルトリストを提供します。2.4 の場合には、このリストには、FIPS 承認されていない暗号が2つ含まれます。バージョン 2.4.x 以前からアップグレードし、FIPS コンプライアンスが必要な場合は、[multiclusterhub](#) リソースから、以下の2つの暗号 ([ECDHE-ECDSA-CHACHA20-POLY1305](#) および [ECDHE-RSA-CHACHA20-POLY1305](#)) を削除します。

アップグレードの詳細は、[Operator を使用したアップグレード](#) を参照してください。

1.2.1. Errata 2.8.6

- コンソールでの読み込み時間が長くなる可能性のあるメモリーリークに対処します。(ACM-9886)
- マネージドクラスターデータを復元するときにパーミッションエラーが発生する問題を修正します。このエラーは、[ManagedServiceAccount](#) によって作成されていないトークンを使用して発生し、必要なインポートパーミッションがありません。(ACM-10159)
- 1つ以上の製品コンテナイメージに更新を配信します。

1.2.2. Errata 2.8.5

- リソースが間違った順序で復元された問題を修正します。(ACM-8857)
- [config-policy-controller-uninstall](#) Pod のステータスが正しくないため、アンインストール時に遅延が発生する問題を修正しました。(ACM-8947)
- 1つ以上の製品コンテナイメージに更新を配信します。

1.2.3. Errata 2.8.4

- 1つ以上の製品コンテナイメージに更新を配信します。

1.2.4. Errata 2.8.3

- 1つ以上の製品コンテナイメージとセキュリティー修正プログラムの更新を提供します。

1.2.5. エラータ 2.8.2

- 1つ以上の製品コンテナイメージとセキュリティー修正プログラムの更新を提供します。
- 一部のオブジェクトが準拠していない場合でもポリシーが準拠の状態を表示するという問題が修正されました。(ACM-6171)
- コンソールから **ApplicationSet** アプリケーションをデプロイするときにエラーメッセージが表示される問題を修正しました。(ACM-6003)
- ラベルが空白のポリシーが適用されない問題を修正しました。(ACM-5398)

1.2.6. エラータ 2.8.1

- 1つ以上の製品コンテナイメージとセキュリティー修正プログラムの更新を提供します。
- ルートポリシーステータスがなくなる問題を修正しました。(ACM-6291)

1.3. 既知の問題

アプリケーション管理に関する既知の問題を確認します。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#) を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

クラスター管理または [クラスターのライフサイクル](#) は、`{product-title-short}` の有無にかかわらず、マルチクラスターエンジンオペレーターによって提供されます。以下は、`{product-title-short}` にも適用される、クラスター管理に関する既知の問題と制限事項です。クラスター管理の既知の問題のほとんどは、[クラスターライフサイクルの既知の問題](#) にあるクラスターライフサイクルのドキュメントに記載されています。

- [インストール関連の既知の問題](#)
- [ビジネス継続性関連の既知の問題](#)
- [コンソール関連の既知の問題](#)
- [アプリケーション関連の既知の問題](#)
- [可観測性関連の既知の問題](#)
- [ガバナンス関連の既知の問題](#)
- [ネットワーク関連の既知の問題](#)

1.3.1. インストール関連の既知の問題

インストールに関する既知の問題を確認してください。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#)[OpenShift Container Platform known issues] を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

1.3.1.1. エラータリリースへのアップグレード後も非推奨のリソースが残る

2.4.x から 2.5.x にアップグレードしてから 2.6.x にアップグレードした後、マネージドクラスターの namespace に非推奨のリソースが残る場合があります。バージョン 2.6.x が 2.4.x からアップグレードされた場合、これらの非推奨のリソースを手動で削除する必要があります。

注記: バージョン 2.5.x からバージョン 2.6.x にアップグレードする前に、30 分以上待つ必要があります。

コンソールから削除するか、削除するリソースに対して次の例のようなコマンドを実行できます。

```
oc delete -n <managed cluster namespace> managedclusteraddons.addon.open-cluster-management.io <resource-name>
```

残っている可能性のある非推奨のリソースのリストを参照してください。

```
managedclusteraddons.addon.open-cluster-management.io:  
policy-controller  
manifestworks.work.open-cluster-management.io:  
-klusterlet-addon-appmgr  
-klusterlet-addon-certpolicyctrl  
-klusterlet-addon-crds  
-klusterlet-addon-iampolicyctrl  
-klusterlet-addon-operator  
-klusterlet-addon-policyctrl  
-klusterlet-addon-workmgr
```

1.3.1.2. Red Hat Advanced Cluster Management のアップグレード後に Pod が復旧しないことがある

Red Hat Advanced Cluster Management を新しいバージョンにアップグレードした後、**StatefulSet** に属するいくつかの Pod が **failed** 状態のままになることがあります。このまれなイベントは、[Kubernetes の既知の問題](#) が原因です。

この問題の回避策として、失敗した Pod を削除します。Kubernetes は、正しい設定で自動的に再起動します。

1.3.1.3. OpenShift Container Platform クラスターのアップグレード失敗のステータス

Openshift Container Platform クラスターがアップグレードの段階に入ると、クラスター Pod は再起動され、クラスターのステータスが 1-5 分ほど、**upgrade failed** のままになることがあります。この動作は想定されており、数分後に解決されます。

1.3.1.4. MultiClusterEngine の作成ボタンが機能しない

Red Hat OpenShift Container Platform コンソールに Red Hat Advanced Cluster Management for Kubernetes をインストールすると、ポップアップウィンドウに次のメッセージが表示されます。

MultiClusterEngine required

Create a MultiClusterEngine instance to use this Operator.

ポップアップウィンドウメッセージの **Create MultiClusterEngine** ボタンが機能しない場合があります。この問題を回避するには、提供された API セクションの MultiClusterEngine タイルで **インスタンスの作成** を選択します。

1.3.2. ビジネス継続性関連の既知の問題

Red Hat Advanced Cluster Management for Kubernetes の既知の問題を確認してください。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#)[OpenShift Container Platform known issues] を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

1.3.2.1. バックアップおよび復元の既知の問題

1.3.2.1.1. OADP 1.1.2 以降を使用すると、BackupSchedule に FailedValidation ステータスが表示される

Red Hat Advanced Cluster Management のバックアップおよび復元コンポーネントを有効にし、**DataProtectionApplication** リソースを正常に作成すると、**BackupStorageLocation** リソースが **Available** のステータスで作成されます。OADP バージョン 1.1.2 以降を使用している場合、**BackupSchedule** リソースを作成すると、次のメッセージが表示されてステータスが **FailedValidation** になることがあります。

```
oc get backupschedule -n open-cluster-management-backup
NAME PHASE MESSAGE
rosa-backup-schedule FailedValidation Backup storage location is not available. Check
velero.io.BackupStorageLocation and validate storage credentials.
```

このエラーは、**BackupStorageLocation** リソースの **ownerReference** の値がないために発生します。**DataProtectionApplication** リソースの値は、**ownerReference** の値として使用する必要があります。

この問題を回避するには、**ownerReference** を **BackupStorageLocation** に手動で追加します。

1. 次のコマンドを実行して、**oadp-operator.v1.1.2** ファイルを開きます。

```
oc edit csv -n open-cluster-management-backup oadp-operator.v1.1.2
```

2. OADP Operator CSV の **1** を **0** に置き換えて、**spec.deployments.label.spec.replicas** の値を編集します。
3. 次の例のとおり、YAML スクリプトの **ownerReference** アノテーションにパッチを適用します。

```
metadata:
  resourceVersion: '273482'
  name: dpa-sample-1
  uid: 4701599a-cdf5-48ac-9264-695a95b935a0
  namespace: open-cluster-management-backup
  ownerReferences: <<
```

```
apiVersion: oadp.openshift.io/v1alpha1
blockOwnerDeletion: true
controller: true
kind: DataProtectionApplication
name: dpa-sample
uid: 52acd151-52fd-440a-a846-95a0d7368ff7
```

4. **spec.deployments.label.spec.replicas** の値を 1 に戻し、新しい設定でデータ保護アプリケーションプロセスを開始します。

1.3.2.1.2. Velero 復元の制限

データが復元される新しいハブクラスターにユーザーが作成したリソースがある場合、新しいハブクラスターはアクティブなハブクラスターとは異なる設定を持つことができます。たとえば、バックアップデータが新しいハブクラスターで復元される前に、新しいハブクラスターで作成された既存のポリシーを含めることができます。

既存のリソースが復元されたバックアップの一部でない場合、Velero はそれらをスキップするため、新しいハブクラスターのポリシーは変更されず、新しいハブクラスターとアクティブなハブクラスターの間で異なる設定が生じます。

この制限に対処するために、クラスターのバックアップと復元のオペレーターは、**restore.cluster.open-cluster-management.io** リソースが作成されたときに、ユーザーが作成したリソースをクリーンアップする復元後の操作、または別の復元操作を実行します。

詳細は、[バックアップおよび復元 Operator のインストール](#) トピックを参照してください。

1.3.2.1.3. パッシブ設定では管理対象クラスターが表示されない

管理対象クラスターは、アクティブ化データがパッシブハブクラスターで復元された場合にのみ表示されます。

1.3.2.1.4. マネージドクラスターリソースが復元されない

local-cluster マネージドクラスターリソースの設定を復元し、新しいハブクラスターで **local-cluster** データを上書きすると、設定が正しく設定されません。リソースにはクラスター URL の詳細など、**local-cluster** 固有の情報が含まれているため、以前のハブクラスター **local-cluster** のコンテンツはバックアップされません。

復元されたクラスターの **local-cluster** リソースに関連するすべての設定変更を手動で適用する必要があります。[バックアップおよび復元 Operator のインストール](#) トピックの [新しいハブクラスターの準備](#) を参照してください。

1.3.2.1.5. 復元された Hive マネージドクラスターは、新しいハブクラスターに接続できない場合がある

Hive マネージドクラスターの変更またはローテーションされた認証局 (CA) のバックアップを新しいハブクラスターで復元すると、マネージドクラスターは新しいハブクラスターへの接続に失敗します。このマネージドクラスターの **admin kubeconfig** シークレット (バックアップで使用可能) が無効になっているため、接続は失敗します。

新しいハブクラスター上のマネージドクラスターの復元された **admin kubeconfig** シークレットを手動で更新する必要があります。

1.3.2.1.6. インポートされたマネージドクラスターに Pending Import ステータスが表示される

プライマリーハブクラスターに手動でインポートされたマネージドクラスターは、アクティブ化データがパッシブハブクラスターで復元されると、**Pending Import** のステータスを示します。詳細は、[管理されたサービスアカウントを使用したクラスターの接続](#) を参照してください。

1.3.2.1.7. ハブクラスターを復元した後、`appliedmanifestwork` がマネージドクラスターから削除されない

ハブクラスターデータが新しいハブクラスターで復元される時、**appliedmanifestwork** は固定クラスターセットではないアプリケーションサブスクリプションの配置規則を持つマネージドクラスターから削除されません。

固定クラスターセットではないアプリケーションサブスクリプションの配置規則の例を次に示します。

```
spec:
  clusterReplicas: 1
  clusterSelector:
    matchLabels:
      environment: dev
```

その結果、マネージドクラスターが復元されたハブクラスターから切り離されると、アプリケーションは孤立します。

この問題を回避するには、配置ルールで固定クラスターセットを指定します。以下の例を参照してください。

```
spec:
  clusterSelector:
    matchLabels:
      environment: dev
```

次のコマンドを実行して、残りの **appliedmanifestwork** を手動で削除することもできます。

```
oc delete appliedmanifestwork <the-left-appliedmanifestwork-name>
```

1.3.2.1.8. `appliedmanifestwork` は削除されず、ハブクラスター配置ルールには固定クラスターセットがない

ハブクラスターデータが新しいハブクラスターで復元される時、**appliedmanifestwork** は固定クラスターセットではないアプリケーションサブスクリプションの配置規則を持つマネージドクラスターから削除されません。その結果、マネージドクラスターが復元されたハブクラスターから切り離されると、アプリケーションは孤立します。

固定クラスターセットではないアプリケーションサブスクリプションの配置規則の例を次に示します。

```
spec:
  clusterReplicas: 1
  clusterSelector:
    matchLabels:
      environment: dev
```

この問題を回避するには、配置ルールで固定クラスターセットを指定します。以下の例を参照してください。

```
spec:
  clusterSelector:
    matchLabels:
      environment: dev
```

次のコマンドを実行して、残りの **appliedmanifestwork** を手動で削除できます。

```
oc delete appliedmanifestwork <the-left-appliedmanifestwork-name>
```

1.3.2.1.9. appliedmanifestwork が削除されず、agentID が仕様がない

Red Hat Advanced Cluster Management 2.6 をプライマリーハブクラスターとして使用しているが、リストアハブクラスターがバージョン 2.7 以降である場合、このフィールドは 2.7 リリースで導入されたため、**applymanifestworks** の仕様に エージェント ID がありません。これにより、マネージドクラスターのプライマリーハブに追加の **appliedmanifestworks** が生成されます。

この問題を回避するには、プライマリーハブクラスターを Red Hat Advanced Cluster Management 2.7 にアップグレードしてから、新しいハブクラスターにバックアップを復元します。

applymanifestwork ごとに **spec.agentID** を手動で設定して、マネージドクラスターを修正します。

1. 次のコマンドを実行して、**agentID** を取得します。

```
oc get klusterlet klusterlet -o jsonpath='{.metadata.uid}'
```

2. 以下のコマンドを実行して、**appliedmanifestwork** ごとに **spec.agentID** を設定します。

```
oc patch appliedmanifestwork <appliedmanifestwork_name> --type=merge -p '{"spec": {"agentID": "$AGENT_ID"}}'
```

1.3.2.1.10. managed-serviceaccount アドオンステータスは Unknown と表示されます。

マネージドクラスター **appliedmanifestwork addon-managed-serviceaccount-deploy** は、新しいハブクラスターの Kubernetes Operator リソースのマルチクラスターエンジンで有効にせずに Managed Service Account を使用している場合は、インポートされたマネージドクラスターから削除されます。

マネージドクラスターは引き続き新しいハブクラスターにインポートされますが、**managed-serviceaccount** アドオンのステータスは **Unknown** と表示されます。

マルチクラスターエンジン Operator リソースで Managed Service Account を有効にした後、**managed-serviceaccount** アドオンを回復できます。Managed Service Account を有効にする方法は、[自動インポートの有効化](#) を参照してください。

1.3.3. コンソール関連の既知の問題

コンソールの既知の問題を確認してください。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#) を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

1.3.3.1. PostgreSQL Pod の CrashLoopBackoff 状態を検索する

search-postgres Pod は **CrashLoopBackoff** 状態です。Red Hat Advanced Cluster Management が **hugepages** パラメーターが有効になっているノードを含むクラスターにデプロイされており、これらのノードで **search-postgres** Pod がスケジュールされている場合、Pod は起動しません。

search-postgres Pod のメモリーを増やすには、次の手順を実行します。

1. 以下のコマンドを使用して **search-operator** Pod を一時停止します。

```
oc annotate search search-v2-operator search-pause=true
```

2. **hugepages** パラメーターの制限を使用して、**search-postgres** デプロイメントを更新します。次のコマンドを実行して、**hugepages** パラメーターを **512Mi** に設定します。

```
oc patch deployment search-postgres --type json -p [{"op": "add", "path": "/spec/template/spec/containers/0/resources/limits/hugepages-2Mi", "value": "512Mi"}]
```

3. Pod のメモリー使用量を確認する前に、**search-postgres** Pod が **Running** 状態にあることを確認します。以下のコマンドを実行します。

```
oc get pod <your-postgres-pod-name> -o jsonpath="Status: {.status.phase}"
```

4. 次のコマンドを実行して、**search-postgres** Pod のメモリー使用量を確認します。

```
oc get pod <your-postgres-pod-name> -o jsonpath='{.spec.containers[0].resources.limits.hugepages-2Mi}'
```

512Mi の値が表示されます。

1.3.3.2. コンソール機能は Firefox の以前のバージョンで表示されない場合がある

以前のバージョンの Firefox のダークテーマスタイルには、既知の問題があります。コンソールの互換性を最適化するため、最新版にアップグレードしてください。

詳しくは、[サポートされているブラウザ](#) を参照してください。

1.3.3.3. searchcustomization におけるストレージサイズの制限

searchcustomization CR でストレージサイズを更新する場合、PVC 設定は変更されません。ストレージサイズを更新する必要がある場合は、以下のコマンドで PVC (**<storageclassname>-search-redisgraph-0**) を更新します。

```
oc edit pvc <storageclassname>-search-redisgraph-0
```

1.3.3.4. 検索クエリーの解析エラー

環境が大規模になり、スケーリングのためにさらに多くのテストが必要になると、検索クエリーがタイムアウトになり、解析エラーメッセージが表示されることがあります。このエラーは、検索クエリーを 30 秒間待機した後に表示されます。

次のコマンドでタイムアウト時間を延長します。

```
kubectl annotate route multcloud-console haproxy.router.openshift.io/timeout=Xs
```

1.3.3.5. クラスターセットのネームスペースバインディングを編集できない

admin または **bind** ロールを使用してクラスターセットの namespace バインディングを編集すると、次のメッセージのようなエラーが発生する場合があります。

ResourceError: managedclustersetbindings.cluster.open-cluster-management.io "<cluster-set>" is forbidden: User "<user>" cannot create/delete resource "managedclustersetbindings" in API group "cluster.open-cluster-management.io" in the namespace "<namespace>".

この問題を解決するには、バインドする namespace で **ManagedClusterSetBinding** リソースを作成または削除する権限も持っていることを確認してください。ロールバインディングでは、クラスターセットを namespace にバインドすることしかできません。

1.3.3.6. Hosted control plane クラスターをプロビジョニングした後、水平スクロールが機能しない

Hosted control plane クラスターをプロビジョニングした後、**ClusterVersionUpgradeable** パラメーターが長すぎると、Red Hat Advanced Cluster Management コンソールのクラスター概要を水平方向にスクロールできない場合があります。結果として、非表示のデータを表示することはできません。

この問題を回避するには、ブラウザのズームコントロールを使用してズームアウトするか、Red Hat Advanced Cluster Management コンソールウィンドウのサイズを大きくするか、テキストをコピーして別の場所に貼り付けます。

1.3.3.7. EditApplicationSet 拡張機能の繰り返しを設定する

複数のラベル式を追加するか、**ApplicationSet** のクラスターセクターに入ろうとすると、式を入力するにはデプロイメントしてくださいというメッセージが繰り返し表示されることがあります。この問題にもかかわらず、クラスターの選択を入力することはできます。

1.3.3.8. アプリケーションコンソールは Argo CD プルモデルをサポートしません。

Argo CD プルモデルを使用して **ApplicationSet** リソースをデプロイすると、アプリケーションが **Topology** ページから正しく表示されません。Argo CD プルモデルを使用した **ApplicationSet** アプリケーションのデプロイはサポートされていません。

1.3.4. アプリケーションの既知の問題と制限事項

アプリケーション管理に関する既知の問題を確認します。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#) を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

アプリケーションライフサイクルコンポーネントについては、次の既知の問題を参照してください。

1.3.4.1. ローカルクラスターは pull モデルのマネージドクラスターとして除外されます

ハブクラスターアプリケーションセットはターゲットマネージドクラスターにデプロイされますが、マネージドハブクラスターであるローカルクラスターはターゲットマネージドクラスターとして除外されます。

1.3.4.2. Argo CD コントローラーと伝播コントローラーは同時に調整する可能性があります

Argo CD コントローラーと伝播コントローラーの両方が同じアプリケーションリソース上で調整し、マネージドクラスター上で異なるデプロイメントモデルからのアプリケーションデプロイメントの重複インスタンスが発生する可能性があります。

Pull モデルを使用してアプリケーションをデプロイする場合、Argo CD **argocd.argoproj.io/skip-reconcile** アノテーションが **ApplicationSet** のテンプレートセクションに追加されると、Argo CD コントローラーはこれらのアプリケーションリソースを無視します。

argocd.argoproj.io/skip-reconcile アノテーションは、GitOps operator バージョン 1.9.0 以降でのみ使用できます。競合を防ぐには、プルモデルを実装する前に、ハブクラスターとすべてのマネージドクラスターが GitOps operator バージョン 1.9.0 にアップグレードされるまで待ってください。

1.3.4.3. リソースのデプロイに失敗する

MulticlusterApplicationSetReport にリストされているすべてのリソースは、実際にはマネージドクラスターにデプロイされます。リソースのデプロイに失敗した場合、そのリソースはリソースリストには含まれませんが、原因はエラーメッセージにリストされます。

1.3.4.4. リソースの割り当てには数分かかる場合があります

1,000 を超えるマネージドクラスターと、数百のマネージドクラスターにデプロイされた Argo CD アプリケーションセットがある大規模環境の場合、ハブクラスターでの Argo CD アプリケーションの作成には数分かかる場合があります。次のファイル例に示されているように、アプリケーションセットの **clusterDecisionResource** ジェネレーターで **requeueAfterSeconds** を **zero** に設定できます。

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: cm-allclusters-app-set
  namespace: openshift-gitops
spec:
  generators:
  - clusterDecisionResource:
      configMapRef: ocm-placement-generator
      labelSelector:
        matchLabels:
          cluster.open-cluster-management.io/placement: app-placement
      requeueAfterSeconds: 0
```

1.3.4.5. アプリケーション **ObjectBucket** チャンネルタイプは、許可リストと拒否リストを使用できない

subscription-admin ロールの **ObjectBucket** チャンネルタイプで許可リストと拒否リストを指定することはできません。他の種類のチャンネルでは、サブスクリプションの許可リストと拒否リストによって、デプロイできる Kubernetes リソースとデプロイできない Kubernetes リソースが示されます。

1.3.4.5.1. Argo アプリケーションを 3.x OpenShift Container Platform マネージドクラスターにデプロイできない

Infrastructure.config.openshift.io API は 3.x では使用できないため、コンソールから Argo **ApplicationSet** を 3.x OpenShift Container Platform マネージドクラスターにデプロイすることはできません。

1.3.4.6. multicluster_operators_subscription イメージへの変更は自動的に有効にならない

マネージドクラスターで実行している **application-manager** アドオンは、以前は **klusterlet Operator** により処理されていましたが、サブスクリプション Operator により処理されるようになりました。サブスクリプション Operator は **multicluster-hub** で管理されていないため、**multicluster-hub** イメージ マニフェスト ConfigMap の **multicluster_operators_subscription** イメージへの変更は自動的に有効 になりません。

サブスクリプション Operator が使用するイメージが、**multicluster-hub** イメージマニフェスト ConfigMap の **multicluster_operators_subscription** イメージを変更することによってオーバーライド された場合、マネージドクラスターの **application-manager** アドオンは、サブスクリプション Operator Pod が再起動するまで新しいイメージを使用しません。。Pod を再起動する必要があります。

1.3.4.7. サブスクリプション管理者以外はポリシーリソースをデプロイできない

Red Hat Advanced Cluster Management バージョン 2.4 では、デフォルトで **policy.open-cluster-management.io/v1** リソースがアプリケーションサブスクリプションによってデプロイされなくなりました。

サブスクリプション管理者は、このデフォルトの動作を変更するためにアプリケーションサブスクリプションをデプロイする必要があります。

詳細は、[サブスクリプション管理者としての許可リストおよび拒否リストの作成](#) を参照してください。以前の Red Hat Advanced Cluster Management バージョンの既存のアプリケーションサブスクリプションによってデプロイされた **policy.open-cluster-management.io/v1** リソースは、サブスクリプション管理者がアプリケーションサブスクリプションをデプロイしていない限り、ソースリポジトリに合わせて調整されません。

1.3.4.8. アプリケーション Ansible フックのスタンドアロンモード

Ansible フックのスタンドアロンモードはサポートされていません。サブスクリプションを使用してハブクラスターに Ansible フックをデプロイするには、次のサブスクリプション YAML を使用できます。

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
    name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    local: true
```

ただし、**spec.placement.local:true** ではサブスクリプションが **standalone** モードで実行されているため、この設定では Ansible インストールが作成されない可能性があります。ハブモードでサブスクリプションを作成する必要があります。

1. **local-cluster** にデプロイする配置ルールを作成します。次のサンプルを参照してください。ここでの **local-cluster: "true"** はハブクラスターを指します。

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: <towhichcluster>
  namespace: hello-openshift
spec:
  clusterSelector:
    matchLabels:
      local-cluster: "true"
```

2. 使用しているサブスクリプションで、作成した配置ルールを参照します。以下のサンプルを参照してください。

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
    name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    placementRef:
      name: <towhichcluster>
      kind: PlacementRule
```

両方を適用すると、ハブクラスターに作成された Ansible インスタンスが表示されます。

1.3.4.9. 配置ルールの更新後にアプリケーションがデプロイされない

配置ルールの更新後にアプリケーションがデプロイされない場合は、**application-manager** Pod が実行されていることを確認します。**application-manager** は、マネージドクラスターで実行する必要があるサブスクリプションコンテナです。

oc get pods -n open-cluster-management-agent-addon |grep application-manager を実行して確認できます。

コンソールで **kind:pod cluster:yourcluster** を検索して、**application-manager** が実行されているかどうかを確認することもできます。

検証できない場合は、もう一度、クラスターのインポートを試行して検証を行います。

1.3.4.10. サブスクリプション Operator が SCC を作成しない

Red Hat OpenShift Container Platform SCC の詳細は、[Security Context Constraints \(SCC\) の管理](#) を参照してください。これは、マネージドクラスターに必要な追加設定です。

デプロイメントごとにセキュリティーコンテキストとサービスアカウントが異なります。サブスクリプション Operator は SCC CR を自動的に作成できず、管理者が Pod のパーミッションを制御します。Security Context Constraints (SCC) CR は、関連のあるサービスアカウントに適切なパーミッションを有効化して、デフォルトではない namespace で Pod を作成する必要があります。使用している namespace で SCC CR を手動で作成するには、以下の手順を実行します。

1. デプロイメントで定義したサービスアカウントを検索します。たとえば、以下の **nginx** デプロイメントを参照してください。

```
nginx-ingress-52edb
nginx-ingress-52edb-backend
```

2. 使用している namespace に SCC CR を作成して、サービスアカウントに必要なパーミッションを割り当てます。以下の例を参照してください。 **kind: SecurityContextConstraints** が追加されています。

```
apiVersion: security.openshift.io/v1
defaultAddCapabilities:
kind: SecurityContextConstraints
metadata:
  name: ingress-nginx
  namespace: ns-sub-1
priority: null
readOnlyRootFilesystem: false
requiredDropCapabilities:
fsGroup:
  type: RunAsAny
runAsUser:
  type: RunAsAny
seLinuxContext:
  type: RunAsAny
users:
- system:serviceaccount:my-operator:nginx-ingress-52edb
- system:serviceaccount:my-operator:nginx-ingress-52edb-backend
```

1.3.4.11. アプリケーションチャンネルには一意の namespace が必要

同じ namespace に複数のチャンネルを作成すると、ハブクラスターでエラーが発生する可能性があります。

たとえば、namespace **charts-v1** は、Helm タイプのチャンネルとしてインストーラーで使用するの で、**charts-v1** に追加のチャンネルを作成します。一意の namespace でチャンネルを作成するようにしてください。すべてのチャンネルには個別の namespace が必要ですが、GitHub チャンネルは例外で、別 GitHub のチャンネルと namespace を共有できます。

1.3.4.12. Ansible Automation Platform ジョブが失敗する

互換性のないオプションを選択すると、Ansible ジョブの実行に失敗します。Ansible Automation Platform は、**-cluster-scoped** のチャンネルオプションが選択されている場合にのみ機能します。これは、Ansible ジョブを実行する必要があるすべてのコンポーネントに影響します。

1.3.4.13. Ansible Automation Platform Operator は、プロキシ外の Ansible Automation Platform にアクセスする

Red Hat Ansible Automation Platform Operator は、プロキシ対応の OpenShift Container Platform クラスターの外部にある Ansible Automation Platform にアクセスできません。解決するには、プロキシ内に Ansible Automation Platform をインストールできます。Ansible Automation Platform によって提供されるインストール手順を参照してください。

1.3.4.14. アプリケーション名の要件

アプリケーション名は 37 文字を超えることができません。この数を超えた場合、アプリケーションのデプロイメント時に以下のエラーが表示されます。

```
status:  
  phase: PropagationFailed  
  reason: 'Deployable.apps.open-cluster-management.io "_long_lengthy_name_" is invalid:  
  metadata.labels: Invalid value: "_long_lengthy_name_": must be no more than 63 characters/n'
```

1.3.4.15. アプリケーションコンソールテーブルの制限事項

コンソールのさまざまな **アプリケーション** の表に対する以下の制限を確認してください。

- **Overview** ページの **Applications** の表と、**Advanced configuration** ページの **Subscriptions** の表にある **Clusters** の列では、アプリケーションリソースのデプロイ先のクラスター数が表示されます。アプリケーションは、ローカルクラスターのリソースで定義されているため、実際のアプリケーションリソースがローカルクラスターにデプロイされているかどうかにかかわらず、ローカルのクラスターは検索結果に含まれます。
- **Subscriptions** の **Advanced configuration** 表にある **Applications** の列には、サブスクリプションを使用するアプリケーションの合計数が表示されますが、サブスクリプションが子アプリケーションをデプロイする場合には、これらも検索結果に含まれます。
- **Channels** の **Advanced configuration** 表にある **Subscriptions** の列には、対象のチャンネルを使用するローカルクラスター上のサブスクリプション合計数が表示されます。ただし、他のサブスクリプションがデプロイするサブスクリプションは検索結果には含まれますが、ここには含まれません。

1.3.4.16. アプリケーションコンソールトポロジーのフィルタリング機能がない

2.8 では **Application** の **Console** と **Topology** が変更されています。コンソールの **Topology** ページにフィルタリング機能はありません。

1.3.4.17. 許可リストと拒否リストがオブジェクトストレージアプリケーションで機能しない

allow リストおよび **deny** リストの機能は、オブジェクトストレージアプリケーションのサブスクリプションでは機能しません。

1.3.5. 可観測性関連の既知の問題

Red Hat Advanced Cluster Management for Kubernetes の既知の問題を確認してください。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#)[OpenShift Container Platform known issues] を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

1.3.5.1. サービスレベルの概要ダッシュボードでローカルクラスターが重複する

さまざまなハブクラスターが同じ S3 ストレージを使用して Red Hat Advanced Cluster Management の可観測性をデプロイする場合、**重複する local-clusters** は **Kubernetes/Service-Level Overview/API Server** ダッシュボード内で検出および表示できます。重複クラスターは、**Top Clusters**、**Number of clusters that has exceeded the SLO**、および **Number of clusters that are meeting the SLO** のパネル内の結果に影響を及ぼします。**local-clusters** は、共有 S3 ストレージに関連付けられた一意のクラスターです。複数の **local-clusters** がダッシュボード内で表示しないようにするには、一意のハブクラスターごとに、ハブクラスター専用の S3 バケットを使用して可観測性をデプロイすることが推奨されます。

1.3.5.2. 可観測性エンドポイント Operator がイメージのプルに失敗する

可観測性エンドポイント Operator は、MultiClusterObservability CustomResource (CR) へのデプロイにプルシークレットを作成したにもかかわらず、**open-cluster-management-observability** namespace にプルシークレットがない場合に問題が発生します。新しいクラスターをインポートする場合、または Red Hat Advanced Cluster Management で作成された Hive クラスターをインポートする場合は、マネージドクラスターにプルイメージシークレットを手動で作成する必要があります。

詳細は、[可観測性の有効化](#) を参照してください。

1.3.5.3. ROKS クラスターにデータがない

Red Hat Advanced Cluster Management の可観測性は、組み込みダッシュボードで、ROKS クラスターのデータが表示されないパネルがあります。これは、ROKS が、管理対象サーバーからの API サーバーメトリクスを公開しないためです。以下の Grafana ダッシュボードには、**Kubernetes/API server**、**Kubernetes/Compute Resources/Workload**、**Kubernetes/Compute Resources/Namespaces(Workload)** の ROKS クラスターをサポートしないパネルが含まれます。

1.3.5.4. ROKS クラスターに etcd データがない

ROKS クラスターの場合に、Red Hat Advanced Cluster Management の可観測性のダッシュボードの **etcd** パネルでデータが表示されません。

1.3.5.5. Grafana コンソールでメトリクスが利用できない

- Grafana コンソールでアノテーションのクエリーに失敗する:
Grafana コンソールで特定のアノテーションを検索すると、トークンの有効期限が切れているために、以下のエラーメッセージが表示されることがあります。

"annotation Query Failed"

ブラウザーを更新し、ハブクラスターにログインしていることを確認します。

- **rbac-query-proxy** Pod のエラー:
managedcluster リソースにアクセス権がないために、プロジェクトでクラスターのクエリーを実行すると以下のエラーが表示される場合があります。

no project or cluster found

ロールのパーミッションを確認し、適切に更新します。詳細は、[ロールベースのアクセス制御](#)を参照してください。

1.3.5.6. マネージドクラスターでの Prometheus データ喪失

デフォルトでは、OpenShift の Prometheus は一時ストレージを使用します。Prometheus は、再起動されるたびにすべてのメトリックデータを失います。

Red Hat Advanced Cluster Management が管理する OpenShift Container Platform マネージドクラスターで可観測性を有効または無効にすると、可観測性エンドポイント Operator は、ローカルの Prometheus を自動的に再起動する alertmanager 設定を追加して **cluster-monitoring-config ConfigMap** を更新します。

1.3.5.7. Out-of-order サンプルの取り込みエラー

Observability **receive** Pod では、以下のエラーをレポートします。

```
Error on ingesting out-of-order samples
```

このエラーメッセージは、マネージドクラスターがメトリクス収集間隔中に送信した時系列データが、以前の収集間隔中に送信した時系列データよりも古いことを意味します。この問題が発生した場合には、データは Thanos レシーバーによって破棄され、Grafana ダッシュボードに表示されるデータにギャップが生じる場合があります。エラーが頻繁に発生する場合は、メトリックコレクションの間隔をより大きい値に増やすことが推奨されます。たとえば、間隔を 60 秒に増やすことができます。

この問題は、時系列の間隔が 30 秒などの低い値に設定されている場合にのみ見られます。メトリクス収集の間隔がデフォルト値の 300 秒に設定されている場合には、この問題は発生しません。

1.3.5.8. アップグレード後に Grafana のデプロイが失敗する

2.6 より前の以前のバージョンでデプロイされた **grafana-dev** インスタンスがあり、環境を 2.6 にアップグレードすると、**grafana-dev** は機能しません。次のコマンドを実行して、既存の **grafana-dev** インスタンスを削除する必要があります。

```
./setup-grafana-dev.sh --clean
```

次のコマンドでインスタンスを再作成します。

```
./setup-grafana-dev.sh --deploy
```

1.3.5.9. klusterlet-addon-search Pod が失敗する

メモリー制限に達したため、**klusterlet-addon-search** Pod が失敗します。マネージドクラスターで **klusterlet-addon-search** デプロイメントをカスタマイズして、メモリーの失われると制限を更新する必要があります。ハブクラスターで、**search-collector** という名前の **ManagedclusterAddon** カスタムリソースを編集します。**search-collector** に以下のアノテーションを追加し、メモリー **addon.open-cluster-management.io/search_memory_request=512Mi** および **addon.open-cluster-management.io/search_memory_limit=1024Mi** を更新します。

たとえば、**foobar** という名前のマネージドクラスターがある場合、次のコマンドを実行して、メモリーリクエストを **512Mi** に変更し、メモリー制限を **1024Mi** に変更します。

```
oc annotate managedclusteraddon search-collector -n foobar \
addon.open-cluster-management.io/search_memory_request=512Mi \
addon.open-cluster-management.io/search_memory_limit=1024Mi
```

1.3.5.10. **disableHubSelfManagement** を有効にすると、Grafana ダッシュボードのリストが空になる

multiclusterengine カスタムリソースで **disableHubSelfManagement** パラメーターが **true** に設定されている場合、Grafana ダッシュボードには空のラベルリストが表示されます。ラベルリストを表示するには、パラメーターを **false** に設定するか、パラメーターを削除する必要があります。詳細は、[disableHubSelfManagement](#) を参照してください。

1.3.5.10.1. エンドポイント URL に完全修飾ドメイン名 (FQDN) を含めることはできません

endpoint パラメーターに FQDN またはプロトコルを使用すると、可観測性 Pod は有効になりません。次のエラーメッセージが表示されます。

```
Endpoint url cannot have fully qualified paths
```

プロトコルなしで URL を入力します。**endpoint** 値は、シークレットの次の URL に似ている必要があります。

```
endpoint: example.com:443
```

1.3.5.10.2. Grafana のダウンサンプリングデータの不一致

履歴データをクエリーしようとしたときに、計算されたステップ値とダウンサンプリングされたデータの間に不一致がある場合、結果は空になります。たとえば、計算されたステップ値が **5m** で、ダウンサンプリングされたデータが1時間間隔の場合、データは Grafana から表示されません。

この不一致は、URL クエリーパラメーターが Thanos Query フロントエンドデータソースを介して渡される必要があるために発生します。その後、データが欠落している場合、URL クエリーは他のダウンサンプリングレベルに対して追加のクエリーを実行できます。

Thanos Query フロントエンドデータソース設定を手動で更新する必要があります。以下の手順を実行します。

1. Query フロントエンドデータソースに移動します。
2. クエリーパラメーターを更新するには、Misc セクションをクリックします。
3. Custom query parameters フィールドから、**max_source_resolution=auto** を選択します。
4. データが表示されていることを確認するには、Grafana ページを更新します。

Grafana ダッシュボードからクエリーデータが表示されます。

1.3.5.11. メトリックコレクターがプロキシ設定を検出しない

addonDeploymentConfig を使用して設定したマネージドクラスター内のプロキシ設定は、メトリックコレクターによって検出されません。回避策として、マネージドクラスター **ManifestWork** を削除してプロキシを有効化できます。**ManifestWork** を削除すると、**addonDeploymentConfig** の変更が強制的に適用されます。

1.3.5.12. カスタム CA バンドルを使用した HTTPS プロキシはサポートされていない

カスタム CA バンドルが必要な場合、マネージドクラスターのプロキシ設定は機能しません。

1.3.6. ガバナンス関連の既知の問題

ガバナンスに関する既知の問題を確認してください。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#)[OpenShift Container Platform known issues] を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

1.3.6.1. Red Hat Advanced Cluster Management からログアウトできない

外部アイデンティティプロバイダーを使用して Red Hat Advanced Cluster Management にログインする場合は、Red Hat Advanced Cluster Management からログアウトできない可能性があります。これは、Red Hat Advanced Cluster Management に IBM Cloud および Keycloak をアイデンティティプロバイダーとしてインストールして使用する場合に発生します。

Red Hat Advanced Cluster Management からログアウトするには、外部アイデンティティプロバイダーからログアウトしておく必要があります。

1.3.6.2. Gatekeeper Operator のインストールに失敗する

Red Hat OpenShift Container Platform バージョン 4.9 に gatekeeper Operator をインストールする場合、インストールに失敗します。OpenShift Container Platform をバージョン 4.9.0. にアップグレードする前に、gatekeeper Operator をバージョン 0.2.0 にアップグレードする必要があります。詳細は、[gatekeeper および gatekeeper Operator のアップグレード](#) を参照してください。

1.3.6.3. namespace が Terminating 状態で停止している場合に、設定ポリシーが準拠と表示される

設定ポリシーで **complianceType** のパラメーターに **mustnothave**、**remediationAction** のパラメーターに **enforce** が設定されている場合に、ポリシーは Kubernetes API に削除要求が送信されてから、準拠と表示されます。そのため、ポリシーが準拠と表示されているにもかかわらず、Kubernetes オブジェクトは、**Terminating** の状態のままになってしまう可能性があります。

1.3.6.4. ポリシーでデプロイされた Operator が ARM をサポートしない

ARM 環境へのインストールはサポートされますが、ポリシーを使用してデプロイされる Operator は ARM 環境をサポートしない可能性があります。Operator をインストールする以下のポリシーは ARM 環境をサポートしません。

- [Quay Container Security Operator の Red Hat Advanced Cluster Management ポリシー](#)
- [コンプライアンス Operator 向けの Red Hat Advanced Cluster Management ポリシー](#)

1.3.6.5. ConfigurationPolicy CRD が終了中にスタックする

KlusterletAddonConfig でポリシーコントローラーを無効にするか、クラスターをデタッチして、管理対象クラスターから **config-policy-controller** アドオンを削除すると、**ConfigurationPolicy** CRD が中断状態でスタックする場合があります。**ConfigurationPolicy** CRD が中断状態でスタックしている場合

に、アドオンを後で再インストールしても、新しいポリシーがクラスターに追加されない可能性があります。次のエラーが表示されることもあります。

```
template-error; Failed to create policy template: create not allowed while custom resource definition is terminating
```

次のコマンドを使用して、CRD がスタックしているかどうかを確認します。

```
oc get crd configurationpolicies.policy.open-cluster-management.io -o=jsonpath='{.metadata.deletionTimestamp}'
```

削除のタイムスタンプがリソースにある場合に、CRD はスタックします。この問題を解決するには、クラスターに残っている設定ポリシーからすべてのファイナライザーを削除します。マネージドクラスターで次のコマンドを使用し、**<cluster-namespace>** をマネージドクラスターの namespace に置き換えます。

```
oc get configurationpolicy -n <cluster-namespace> -o name | xargs oc patch -n <cluster-namespace> --type=merge -p '{"metadata":{"finalizers": []}]'
```

設定ポリシーリソースはクラスターから自動的に削除され、CRD は中断状態を終了します。アドオンがすでに再インストールされている場合には、CRD は削除タイムスタンプなしで自動的に再作成されます。

1.3.6.6. 既存の設定ポリシーを変更するときに PruneObjectBehavior が機能しない

既存の設定ポリシーを変更するときに **PruneObjectBehavior** が機能しない **pruneObjectBehavior** が機能しない可能性がある以下の理由を確認してください。

- 設定ポリシーで **pruneObjectBehavior** を **DeleteAll** または **DeletelfCreated** に設定すると、変更前に作成された古いリソースは正しく消去されません。設定ポリシーを削除すると、ポリシーの作成およびポリシーの更新による新しいリソースのみが追跡および削除されます。
- **pruneObjectBehavior** を **None** に設定するか、パラメーター値を設定しない場合、マネージドクラスター上で古いオブジェクトが意図せずに削除される可能性があります。具体的には、これはユーザーがテンプレート内の **name**、**namespace**、**kind**、または **apiversion** を変更したときに発生します。パラメーターフィールドは、**object-templates-raw** または **namespaceSelector** のパラメーターが変更されると動的に変更できます。

1.3.6.7. ポリシーステータスは、適用時に更新が繰り返されることを示している

ポリシーが **remediationAction: enforce** に設定されていて、繰り返し更新されている場合、Red Hat Advanced Cluster Management コンソールには、更新が成功しても繰り返し違反が表示されます。このエラーについては、次の2つの考えられる原因と解決策を参照してください。

- 別のコントローラーまたはプロセスも、異なる値でオブジェクトを更新しています。この問題を解決するには、ポリシーを無効にして、ポリシーの **objectDefinition** とマネージドクラスターのオブジェクトの違いを比較します。値が異なる場合は、別のコントローラーまたはプロセスが値を更新している可能性があります。オブジェクトの **metadata** を確認して、値が異なる理由を特定してください。
- ポリシーの適用時に Kubernetes がオブジェクトを処理するため、**ConfigurationPolicy** の **objectDefinition** が一致しません。この問題を解決するには、ポリシーを無効にして、ポリシーの **objectDefinition** とマネージドクラスターのオブジェクトの違いを比較します。キーが異なるか欠落している場合、

Kubernetes は、デフォルト値または空の値を含むキーを削除するなど、キーをオブジェクトに適用する前に処理した可能性があります。

注記: `pruneObjectBehavior` が **None** 以外に設定されている場合、ポリシーを無効にするとオブジェクトがクリーンアップされます。この場合、`pruneObjectBehavior` を **None** に設定して、ポリシーが無効になった後もオブジェクトが存在するようにします。

たとえば、**Secret** リソース内の `stringData` マップは、Kubernetes によって、**base64** でエンコードされた値を持つ `data` に変換されます。`stringData` を使用する代わりに、文字列の代わりに **base64** でエンコードされた値を含む `data` を直接使用します。

1.3.6.8. Pod セキュリティポリシーは OpenShift Container Platform 4.12 以降ではサポートされません

Pod セキュリティポリシーのサポートは、OpenShift Container Platform 4.12 以降、および Kubernetes v1.25 以降から削除されました。**PodSecurityPolicy** リソースを適用すると、次の非準拠メッセージを受け取る場合があります。

```
violation - couldn't find mapping resource with kind PodSecurityPolicy, please check if you have CRD
deployed
```

1.3.6.9. ポリシーテンプレート名が重複すると、一貫性のない結果が生じる

同じポリシーテンプレート名でポリシーを作成すると、検出されない一貫性のない結果が返されますが、原因がわからない場合があります。たとえば、**create-pod** という名前の複数の設定ポリシーを含むポリシーを定義すると、一貫性のない結果が発生します。**Best practice:** ポリシーテンプレートに重複した名前を使用しないようにします。

1.3.6.10. ガバナンスデプロイメントが無効になっている場合、エラーが発生せずにシャットダウンしない

MultiClusterHub オブジェクトでガバナンスデプロイメントを無効にすると、デプロイメントはエラーなしでクリーンアップされません。次の手順を実行してガバナンスを無効にし、デプロイメントもクリーンアップされるようにします。

1. マネージドクラスターの **KlusterletAddonConfig** で **policyController** を無効にします。すべてのマネージドクラスターに対してこれを行う場合は、次のコマンドを実行します。

```
for CLUSTER in $(oc get managedclusters -o jsonpath='{.items[].metadata.name}'); do
  oc patch -n ${CLUSTER} klusterletaddonconfig ${CLUSTER} --type=merge --
  patch='{"spec":{"policyController":{"enabled":false}}}'
done
```

2. ローカルクラスターの場合のみ: ローカルクラスターの **governance-policy-framework-uninstall** Pod が **CrashLoopBackOff** にある場合は、ローカルクラスターの **ManifestWork** を削除し、**ManagedClusterAddon** のファイナライザーを削除します。以下のコマンドを実行します。

```
oc delete manifestwork -n local-cluster -l open-cluster-management.io/addon-
name=governance-policy-framework
oc patch managedclusteraddon -n local-cluster governance-policy-framework --type=merge -
-patch='{"metadata":{"finalizers":[]}]'
```

- 必要に応じて、**MultiClusterHub** オブジェクトの **spec.overrides** セクションの **grc** 要素を **false** に設定して、ガバナンスをグローバルに無効にします。以下のコマンドを実行します。

```
oc edit multiclusterhub <name> -n <namespace>
```

- ローカルクラスターの場合のみ: ローカルクラスターポリシーがある場合は、次のコマンドを実行してポリシーを削除できます。

```
oc delete policies -n local-cluster --all
```

- KlusterletAddonConfig** でガバナンスを再度有効にするには、**MultiClusterHub** の **spec.overrides** セクションの **grc** 要素を再度有効にします。以下のコマンドを実行します。

```
for CLUSTER in $(oc get managedclusters -o jsonpath={.items[].metadata.name}); do
  oc patch -n ${CLUSTER} klusterletaddonconfig ${CLUSTER} --type=merge --
  patch='{"spec":{"policyController":{"enabled":true}}}'
done
```

- デプロイが失敗した場合、**governance-policy-addon-controller** のリースが失効している可能性があります。次のコマンドを使用してリースを削除します。

```
oc delete lease governance-policy-addon-controller-lock -n <namespace>
```

1.3.6.11. テンプレートエラーによりオブジェクトが削除されました

設定ポリシー内の構文が正しくないなど、テンプレートエラーがある場合、オブジェクトは削除されません。削除されたオブジェクトを正しい構文で再作成します。

1.3.6.12. ポリシーの自動化用に重複した Ansible ジョブが作成される

Run once モードおよび無効に設定された **PolicyAutomation** がある場合は、追加の Ansible ジョブが作成されます。追加の Ansible ジョブを削除できます。以下の手順を実行します。

- 次のコマンドを実行して、Ansible ジョブリストを表示します。

```
oc get ansiblejob -n {namespace}
```

- 以下のコマンドを使用して、重複した Ansible ジョブを削除します。

```
oc delete ansiblejob {ansiblejob name} -n {namespace}
```

1.3.7. ネットワーク関連の既知の問題

Submariner の既知の問題を確認してください。以下のリストには、本リリースの既知の問題、または以前のリリースから持ち越された既知の問題が記載されています。

Red Hat OpenShift Container Platform クラスターは、[OpenShift Container Platform の既知の問題](#) を参照してください。

非推奨と削除の詳細は、[非推奨と削除](#) を参照してください。

1.3.7.1. Submariner の既知の問題

ネットワーク機能の使用中に発生する可能性がある次の既知の問題と制限事項を参照してください。

1.3.7.1.1. ClusterManagementAddon submariner アドオンを使用しないと失敗する

バージョン 2.8 以前の場合、Red Hat Advanced Cluster Management をインストールするときに、Operator Lifecycle Manager を使用して **submariner-addon** コンポーネントもデプロイします。**MultiClusterHub** カスタムリソースを作成しなかった場合、**submariner-addon** Pod はエラーを送信し、Operator はインストールできません。

ClusterManagementAddon カスタムリソース定義がないため、次の通知が発生します。

```
graceful termination failed, controllers failed with error: the server could not find the requested resource (post clustermanagementaddons.addon.open-cluster-management.io)
```

ClusterManagementAddon リソースは **cluster-manager** デプロイメントによって作成されますが、このデプロイメントが使用可能になるのは **MultiClusterEngine** コンポーネントがクラスターにインストールされてからです。

MultiClusterHub カスタムリソースの作成時にクラスター上ですでに使用可能な **MultiClusterEngine** リソースが存在しない場合、**MultiClusterHub** Operator は **MultiClusterEngine** インスタンスと必要な Operator をデプロイし、前のエラーを解決します。

1.3.7.1.2. Red Hat Advanced Cluster Management が管理できるすべてのインフラストラクチャプロバイダーがサポートされているわけではない

Submariner は、Red Hat Advanced Cluster Management が管理できるすべてのインフラストラクチャプロバイダーでサポートされているわけではありません。サポートされているプロバイダーの一覧は、[Red Hat Advanced Cluster Management のサポートマトリックス](#) を参照してください。

1.3.7.1.3. 限定的なヘッドレスサービスのサポート

Globalnet を使用する場合、セレクターを使用しないヘッドレスサービスのサービスディスカバリーはサポートされません。

1.3.7.1.4. NAT が有効な場合に VXLAN を使用したデプロイはサポートされていない

NAT 以外のデプロイメントのみが VXLAN ケーブルドライバーを使用した Submariner デプロイメントをサポートします。

1.3.7.1.5. OVN Kubernetes には OCP 4.11 以降が必要

OVN Kubernetes CNI ネットワークを使用している場合は、Red Hat OpenShift 4.11 以降が必要です。

1.3.7.1.6. 自己署名証明書により、ブローカーに接続できない場合がある

ブローカーの自己署名証明書により、結合されたクラスターがブローカーに接続できない場合があります。接続は証明書の検証エラーで失敗します。関連する **SubmarinerConfig** オブジェクトで **InsecureBrokerConnection** を **true** に設定すると、ブローカー証明書の検証を無効にできます。以下の例を参照してください。

```
apiVersion: submarineraddon.open-cluster-management.io/v1alpha1
kind: SubmarinerConfig
metadata:
  name: submariner
```

```
namespace: <managed-cluster-namespace>
spec:
  insecureBrokerConnection: true
```

1.3.7.1.7. Submariner は OpenShift SDN または OVN Kubernetes のみサポート

Submariner は、OpenShift SDN または OVN-Kubernetes Container Network Interface (CNI) ネットワークプロバイダーを使用する Red Hat OpenShift Container Platform クラスターのみをサポートします。

1.3.7.1.8. Microsoft Azure クラスターでのコマンド制限

subctl detect firewall inter-cluster コマンドは、Microsoft Azure クラスターでは機能しません。

1.3.7.1.9. カスタム CatalogSource または Subscription で自動アップグレードが機能しない

Red Hat Advanced Cluster Management for Kubernetes がアップグレードされると、Submariner は自動的にアップグレードされます。カスタムの **CatalogSource** または **Subscription** を使用している場合、自動アップグレードは失敗する可能性があります。

マネージドクラスターに Submariner をインストールするときに自動アップグレードが確実に機能するようになるには、各マネージドクラスターの **SubmarinerConfig** カスタムリソースで **spec.subscriptionConfig.channel** フィールドを **steady-0.15** に設定する必要があります。

1.3.7.1.10. OpenShift Container Platform バージョン 4.14 で Red Hat Advanced Cluster Management バージョン 2.8 を使用する場合、Submariner バージョン 0.15 はサポートされません

Red Hat Advanced Cluster Management バージョン 2.8 でリリースされた Submariner バージョン 0.15 は、OpenShift Container Platform バージョン 4.14 以降ではサポートされません。OpenShift Container Platform バージョン 4.14 以降を使用する場合は、Submariner バージョンを 0.16 にアップグレードするか、Submariner バージョン 0.15 および Red Hat Advanced Cluster Management バージョン 2.8 で OpenShift Container Platform バージョン 4.13 を引き続き使用する必要があります。

1.4. 非推奨と削除

Red Hat Advanced Cluster Management for Kubernetes から削除されるか、非推奨となった製品の一部について説明します。**推奨アクション** および詳細にある、代替りのアクションを検討してください。これについては、現在のリリースおよび、1つ前のリリースと2つ前のリリースの表に記載されています。

重要: Red Hat Advanced Cluster Management の 2.6 以前のバージョンは **削除** され、サポートされなくなりました。バージョン 2.6 以前のドキュメントは更新されていません。ドキュメントはそのまま利用できますが、エラーやその他の更新はなく、非推奨となります。

ベストプラクティス: Red Hat Advanced Cluster Management の最新バージョンにアップグレードします。

1.4.1. API の非推奨と削除

Red Hat Advanced Cluster Management は、Kubernetes の API 非推奨ガイドラインに準拠します。このポリシーの詳細は、[Kubernetes の非推奨ポリシー](#) を参照してください。Red Hat Advanced Cluster Management API は、以下のタイムライン以外でのみ非推奨または削除されます。

- **V1** API はすべて、12 ヶ月間または リリース 3 回分 (いずれか長い方) の期間は一般公開され、サポート対象となります。V1 API は削除されませんが、この期間を過ぎると非推奨になる可能性があります。
- **Beta** 版 API はすべて、9 ヶ月間またはリリース 3 回分 (いずれか長い方) の期間は一般公開されます。Beta 版 API は、この期間を過ぎても削除されません。
- **Alpha** 版 API はサポートの必要はありませんが、ユーザーにとってメリットがある場合には、非推奨または削除予定として記載される場合があります。

1.4.1.1. API の非推奨化

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
検出	DiscoveredCluster および DiscoveryConfig v1alpha1 API が非推奨になりました。Discovery API が V1 にアップグレードされました。	2.5	V1 を使用してください。	なし
Placements	v1alpha1 は非推奨となったため、 v1alpha1 API は v1beta1 にアップグレードされます。	2.5	V1beta1 を使用してください。	Placement API v1alpha1 の spec.prioritizerPolicy.configurations.name フィールドが削除されました。 v1beta1 の spec.prioritizerPolicy.configurations.scoreCoordinate.builtIn を使用します。
PlacementDecisions	v1alpha1 は非推奨となったため、 v1alpha1 API は v1beta1 にアップグレードされます。	2.5	V1beta1 を使用してください。	なし
アプリケーション	v1alpha1 API は完全に廃止されます。GitOps クラスター API が V1beta1 にアップグレードされます。	2.5	V1beta1 の使用	なし

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
アプリケーション	deployables.ap ps.open- cluster- management.io	2.5	なし	deployable API は、アップグレードパスにのみ残ります。deployable CR の作成、更新、または削除は調整されません。
ManagedClusterSets	v1beta1 が非推奨となっているため、 v1beta1 API は v1beta2 にアップグレードされます。	2.7	v1beta2 を使用します。	なし
ManagedClusterSetBindings	v1beta1 が非推奨となっているため、 v1beta1 API は v1beta2 にアップグレードされます。	2.7	v1beta2 を使用します。	なし

1.4.1.2. API の削除

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
HypershiftDeployment	HypershiftDeployment API が削除されました。	2.7	この API は使用しないでください。	
BareMetalAssets	v1alpha1 API は削除されました。	2.7	この API は使用しないでください。	Baremetalassets.inventory.open-cluster-management.io
Placements	v1alpha1 API は削除されました。	2.7	代わりに v1beta1 を使用してください。	Placements.cluster.open-cluster-management.io
PlacementDecisions	v1alpha1 API は削除されました。	2.7	代わりに v1beta1 を使用してください。	PlacementDecisions.cluster.open-cluster-management.io

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
ManagedClusterSets	v1alpha1 API は削除されました。	2.7	代わりに v1beta1 を使用してください。	ManagedClusterSets.cluster.open-cluster-management.io
ManagedClusterSetBindings	v1alpha1 API は削除されました。	2.7	代わりに v1beta1 を使用してください。	ManagedClusterSetBindings.cluster.open-cluster-management.io
ClusterManagementAddOn	addOnConfiguration フィールドは ClusterManagementAddOn 仕様で非推奨になりました。	2.7	supportedConfigs フィールドを使用します。	None
ManagedClusterAddOn	addOnConfiguration フィールドは ManagedClusterAddOn 仕様で非推奨になりました。	2.7	supportedConfigs フィールドを使用します。	None
CertPolicyController	v1 API は非推奨になりました。	2.6	この API は使用しないでください。	CertPolicyController.agent.open-cluster-management.io
ApplicationManager	v1 API は非推奨になりました。	2.6	この API は使用しないでください。	ApplicationManager.agent.open-cluster-management.io
IAMPolicyController	v1 API は非推奨になりました。	2.6	この API は使用しないでください。	IAMPolicyController.agent.open-cluster-management.io
PolicyController	v1 API は非推奨になりました。	2.6	この API は使用しないでください。	PolicyController.agent.open-cluster-management.io

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
SearchCollector	v1 API は非推奨になりました。	2.6	この API は使用しないでください。	SearchCollector.agent.open-cluster-management.io
WorkManager	v1 API は非推奨になりました。	2.6	この API は使用しないでください。	WorkManager.agent.open-cluster-management.io

1.4.2. Red Hat Advanced Cluster Management の非推奨機能

非推奨 のコンポーネント、機能またはサービスはサポートされますが、使用は推奨されておらず、今後のリリースで廃止される可能性があります。以下の表に記載されている **推奨アクション** と詳細の代替アクションについて検討してください。

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
アプリケーションとガバナンス	PlacementRule	2.8	PlacementRule を使用する可能性のある場所で Placement を使用します	PlacementRule は引き続き使用できますが、サポート対象外であるため、コンソールにはデフォルトで Placement が表示されます。
インストーラー	operator.open-cluster-management.io_multiclusterhubs_crd.yaml の ingress.sslCiphers フィールド	2.7	なし	インストールの設定については、 高度な設定 を参照してください。
インストーラー	operator.open-cluster-management.io_multiclusterhubs_crd.yaml の customCAConfigmap フィールド	2.7	なし	インストールの設定については、 高度な設定 を参照してください。
可観測性	data.custom_rules.yaml.groups.rules が非推奨になりました。	2.5	data.custom_rules.yaml.groups.recording_rules を使用してください。	可観測性のカスタマイズ を参照してください。

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
インストーラー	operator.open-cluster-management.io_multiclusterhubs_crd.yaml の enableClusterProxyAddon および enableClusterBackup フィールド	2.5	なし	インストーラーの設定については、 高度な設定 を参照してください。

1.4.3. 削除

通常、**削除** された項目は、以前のリリースで非推奨となった機能で、製品では利用できなくなっています。削除された機能には、代替の方法を使用する必要があります。以下の表に記載されている **推奨アクション** と詳細の代替アクションについて検討してください。

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
ガバナンス	以前のリリースで使用されていた管理 ingress は削除されました。	2.7	管理 ingress 証明書をカスタマイズできなくなりました。管理イングレスで使用する独自の証明書を持ってきた場合は、コマンド oc -n open-cluster-management delete secret byo-ca-cert byo-ingress-tls-secret を使用して証明書を削除する必要があります。	なし
検索	SearchCustomizations.open-cluster-management.io カスタムリソース定義が削除されました。	2.7	search.open-cluster-management.io/v1alpha1 を使用して検索をカスタマイズします。	なし

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
検索	RedisGraph は、内部データベースとして PostgreSQL に置き換えられました。	2.7	変更は必要ありません。	検索コンポーネントは、内部データベースとして PostgreSQL を使用して再実装されています。
コンソール	スタンドアロン Web コンソール	2.7	統合 Web コンソールを使用します。	詳しくは コンソールへのアクセス を参照してください。
ガバナンス	整合性シールド (テクノロジープレビュー)	2.7	コミュニティが提供する署名ソリューションとして整合性シールドを引き続き使用できます。詳細については、整合性シールドのドキュメント、 入門ドキュメント を参照してください。	なし
ガバナンス	整合性シールド (テクノロジープレビュー)	2.7	なし	コミュニティが提供する署名ソリューションとして整合性シールドを引き続き使用できます。詳細については、整合性シールドのドキュメント、 入門ドキュメント を参照してください。
クラスター	ラベルを使用した Red Hat Ansible ジョブの設定	2.6	コンソールを使用して Red Hat Ansible ジョブを設定します。	詳細については、 コンソールを使用して、クラスターで実行するように、自動化テンプレートを設定する を参照してください。

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
クラスター	ベアメタルアセットを使用したクラスターの作成。	2.6	コンソールでインフラ環境を作る	手順は、 オンプレミス環境でのクラスターの作成 を参照してください。
アドオン Operator	ビルトインのマネージドクラスターアドオンのインストール	2.6	なし	なし
ガバナンス	カスタムポリシーコントローラー	2.6	アクションは不要です。	なし
ガバナンス	未使用の LabelSelector パラメーターは設定ポリシーから削除されます。	2.6	なし	Kubernetes 設定ポリシーコントローラー のドキュメントを参照してください。
ガバナンス	カスタムポリシーコントローラー	2.6	アクションは不要です。	なし
ガバナンス	未使用の LabelSelector パラメーターは設定ポリシーから削除されます。	2.6	なし	Kubernetes 設定ポリシーコントローラー のドキュメントを参照してください。
アプリケーション	deployable コントローラー	2.5	なし	Deployable コントローラーが削除されました。

1.5. GDPR に対応するための RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES プラットフォームでの考慮事項

1.5.1. 注意

本書は、EU 一般データ保護規則 (GDPR: General Data Protection Regulation) への対応準備を容易化するために作成されました。本書では、GDPR に組織が対応する準備を整える際に考慮する必要のある Red Hat Advanced Cluster Management for Kubernetes プラットフォームの設定可能な機能や、製品のあらゆる用途について説明します。機能の選択、設定方法が多数ある上に、本製品は、幅広い方法で製品内だけでなく、サードパーティーのクラスターやシステムで使用できるので、本書で提示している情報は完全なリストではありません。

顧客は EU 一般データ保護規則など、さまざまな法律や規制を確実に遵守する責任を負います。顧客は、顧客の事業に影響を及ぼす可能性のある、関係する法律や規制の特定や解釈、およびこれらの法律や規制を遵守するために必要となる対応について、資格を持った弁護士の助言を受ける責任を単独で負

います。

本書に記載されている製品、サービス、およびその他の機能は、すべての顧客の状況には適しておらず、利用が制限される可能性があります。Red Hat は、法律、会計または監査上の助言を提供するわけではなく、当社のサービスまたは製品が、お客様においていかなる法律または規制を順守していることを表明し、保証するものでもありません。

1.5.2. 目次

- [GDPR](#)
- [GDPR に準拠する製品の設定](#)
- [データのライフサイクル](#)
- [データの収集](#)
- [データストレージ](#)
- [データアクセス](#)
- [データ処理](#)
- [データの削除](#)
- [個人データの使用を制限する機能](#)
- [付録](#)

1.5.3. GDPR

一般データ保護規則 (GDPR) は欧州連合 ("EU") により採用され、2018 年 5 月 25 日から適用されています。

1.5.3.1. GDPR が重要な理由

GDPR は、各自の個人データを処理するにあたり、強力なデータ保護規制フレームワークを確立します。GDPR は以下を提供します。

- 個人の権利の追加および強化
- 個人データの定義の広義化
- データ処理者の義務の追加
- 遵守しない場合に多額の罰金が課される可能性
- 情報流出の通知の義務付け

1.5.3.2. GDPR の詳細情報

- [EU GDPR の情報ポータル](#)
- [Red Hat GDPR の Web サイト](#)

1.5.4. GDPR に準拠する製品の設定

以下のセクションでは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームでのデータ管理のさまざまな点について説明し、GDPR 要件に準拠するための機能に関する情報を提供します。

1.5.5. データのライフサイクル

Red Hat Advanced Cluster Management for Kubernetes は、オンプレミスのコンテナ化アプリケーションの開発および管理のアプリケーションプラットフォームです。この製品は、コンテナオーケストレーターの Kubernetes、クラスターライフサイクル、アプリケーションライフサイクル、セキュリティーフレームワーク (ガバナンス、リスク、コンプライアンス) など、コンテナを管理するための統合環境です。

そのため、Red Hat Advanced Cluster Management for Kubernetes プラットフォームは主に、プラットフォームの設定や管理に関連する技術データ (一部、GDPR の対象となるデータも含む) を処理します。また、Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、プラットフォームの管理ユーザーに関する情報も扱います。このデータについては、GDPR 要件を満たす必要のあるお客様が対応できるように、本書全体で説明します。

このデータは、設定ファイルまたはデータベースとしてローカルまたはリモートのファイルシステム上のプラットフォームで永続化されます。Red Hat Advanced Cluster Management for Kubernetes プラットフォームで実行するように開発されたアプリケーションは、GDPR の影響を受ける他の形式の個人データを扱う可能性があります。プラットフォームデータの保護および管理に使用されるメカニズムは、プラットフォームで実行されるアプリケーションでも利用できます。Red Hat Advanced Cluster Management for Kubernetes プラットフォームで実行されるアプリケーションが収集する個人データを管理して保護するために、追加のメカニズムが必要な場合があります。

Red Hat Advanced Cluster Management for Kubernetes プラットフォームとそのデータフローを最もよく理解するには、Kubernetes、Docker および Operator がどのように機能するか理解する必要があります。このようなオープンソースコンポーネントは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームに不可欠です。Kubernetes デプロイメントは、アプリケーションのインスタンスを配置するのに使用します。これらのアプリケーションのインスタンスは、Docker イメージを参照する Operator に組み込まれます。Operator にはアプリケーションの詳細が含まれ、Docker イメージにはアプリケーションの実行に必要な全ソフトウェアパッケージが含まれます。

1.5.5.1. Red Hat Advanced Cluster Management for Kubernetes プラットフォームを使用したデータフローの種類

Red Hat Advanced Cluster Management for Kubernetes は、プラットフォームとして複数のカテゴリーの技術データを扱いますが、その中には管理者ユーザー ID とパスワード、サービスユーザー ID とパスワード、Kubernetes ノード名など、個人データとみなされる可能性があるものも含まれます。また、Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、プラットフォームの管理ユーザーに関する情報も扱います。プラットフォームで実行されるアプリケーションにより、プラットフォームではまだ知られていない、他のカテゴリーの個人データが取り込まれる可能性があります。

このような技術データの収集/作成、保存、アクセス、セキュリティー設定、ロギング、削除の方法に関する情報は、本書で後述します。

1.5.5.2. オンラインの連絡先として使用される個人データ

お客様は、以下のような情報をさまざまな方法でオンラインからコメント/フィードバック/依頼を送信できます。

- Slack チャンネルがある場合は、Slack の公開コミュニティ

- 製品ドキュメントに関する公開コメントまたはチケット
- 技術コミュニティでの公開会話

通常は、連絡先フォームの件名への個人返信を有効にすると、お客様名とメールアドレスのみが使用され、個人データを使用する場合は [Red Hat オンラインプライバシーステートメント](#) に準拠します。

1.5.6. データの収集

Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、機密性のある個人情報を収集しません。当製品は、管理者ユーザー ID とパスワード、サービスユーザー ID とパスワード、IP アドレス、Kubernetes ノード名など、個人データとみなされる可能性のある技術データを作成し、管理します。また、Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、プラットフォームの管理ユーザーに関する情報も扱います。このような情報には、システム管理者がロールベースのアクセス制御を使用した管理コンソールからアクセスするか、シ Red Hat Advanced Cluster Management for Kubernetes プラットフォームノードにログインしてアクセスした場合にのみアクセス可能です。

Red Hat Advanced Cluster Management for Kubernetes プラットフォームで実行されるアプリケーションでは、個人データが収集される可能性があります。

コンテナ化されたアプリケーションを実行する Red Hat Advanced Cluster Management for Kubernetes プラットフォームの使用を評価し、GDPR 要件を満たす必要がある場合には、以下のよう
に、アプリケーションが収集する個人データの種類と、データの管理方法について考慮する必要があります。

- アプリケーションとの間で行き来するデータはどのように保護されるのか？移動中のデータは暗号化されているか？
- アプリケーションでデータはどのように保存されるのか？使用していないデータは暗号化されるのか？
- アプリケーションのアクセスに使用する認証情報はどのように収集され、保存されるのか？
- アプリケーションがデータソースへのアクセス時に使用する認証情報はどのように収集され、保存されるのか？
- アプリケーションが収集したデータを必要に応じて削除するにはどうすればよいか？

これは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームが収集するデータタイプの完全なリストではありません。上記は検討時に使用できるように例として提供しています。データの種類についてご質問がある場合は、Red Hat にお問い合わせください。

1.5.7. データストレージ

Red Hat Advanced Cluster Management for Kubernetes プラットフォームでは、設定ファイルまたはデータベースとしてローカルまたはリモートファイルシステムのステートフルストアで、プラットフォームの設定や管理に関する技術データは永続化されます。使用されていない全データのセキュリティが確保されるように考慮する必要があります。The Red Hat Advanced Cluster Management for Kubernetes プラットフォームには、**dm-crypt** を使用するステートフルストアで、使用していないデータを暗号化するサポートがあります。

以下の項目は、GDPR について考慮する必要がある、データの保存エリアを強調表示しています。

- **プラットフォームの設定データ:** Red Hat Advanced Cluster Management for Kubernetes プラットフォームの設定は、一般的な設定、Kubernetes、ログ、ネットワーク、Docker などの設

定のプロパティを使用して設定 YAML ファイルを更新し、カスタマイズできます。このデータは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームインストーラーへの入力情報として使用し、1つまたは複数のノードをデプロイします。このプロパティには、ブートストラップに使用される管理者ユーザー ID とパスワードも含まれます。

- **Kubernetes 設定データ:** Kubernetes クラスターの状態データは分散 Key-Value Store (KVS) (**etcd**) に保存されます。
- **ユーザー ID、パスワードなどのユーザー認証データ:** ユーザー ID およびパスワードの管理は、クライアントエンタープライズの LDAP ディレクトリーで対応します。LDAP で定義されたユーザーおよびグループは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームのチームに追加して、アクセスロールを割り当てることができます。Red Hat Advanced Cluster Management for Kubernetes プラットフォームでは、LDAP からメールアドレスとユーザー ID は保存されますが、パスワードは保存されません。Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、グループ名を保存し、ログイン時にユーザーが所属する利用可能なグループをキャッシュします。グループメンバーシップは、長期的に永続化されません。エンタープライズ LDAP で未使用時にユーザーおよびグループデータのセキュリティ確保について、考慮する必要があります。Red Hat Advanced Cluster Management for Kubernetes プラットフォームには、認証サービスと、エンタープライズディレクトリーと対応して、アクセストークンを管理する Open ID Connect (OIDC) が含まれます。このサービスは ETCD をバックエンドとして使用します。
- **ユーザー ID とパスワードなどのサービス認証データ:** コンポーネント間のアクセスに Red Hat Advanced Cluster Management for Kubernetes プラットフォームのコンポーネントが使用する認証情報は、Kubernetes Secret として定義します。Kubernetes リソース定義はすべて **etcd** の Key-Value データストアで永続化されます。初期の認証情報の値は、Kubernetes Secret の設定 YAML ファイルとして、プラットフォームの設定データで定義されます。詳細は、Kubernetes ドキュメントの [Secrets](#) を参照してください。

1.5.8. データアクセス

Red Hat Advanced Cluster Management for Kubernetes プラットフォームデータには、以下の定義済みの製品インターフェイスを使用してアクセスできます。

- Web ユーザーインターフェイス (コンソール)
- Kubernetes の **kubectl** CLI
- Red Hat Advanced Cluster Management for Kubernetes CLI
- oc CLI

これらのインターフェイスは、Red Hat Advanced Cluster Management for Kubernetes クラスターに管理権限での変更を加えることができます。Red Hat Advanced Cluster Management for Kubernetes に管理権限でアクセスする場合にセキュリティを確保できます。これには、要求時に認証、ロールマッピング、認可の3つの論理的な段階を順番に使用します。

1.5.8.1. 認証

Red Hat Advanced Cluster Management for Kubernetes プラットフォームの認証マネージャーは、コンソールからのユーザーの認証情報を受け入れ、バックエンドの OIDC プロバイダーに認証情報を転送し、OIDC プロバイダーはエンタープライズディレクトリーに対してユーザーの認証情報を検証します。次に OIDC プロバイダーは認証クッキー (**auth-cookie**) を、JSON Web Token (**JWT**) のコンテンツと合わせて、認証マネージャーに返します。JWT トークンは、認証要求時にグループのメンバーシッ

プに加え、ユーザー ID やメールアドレスなどの情報を永続化します。この認証クッキーはその後コンソールに返されます。クッキーはセッション時に更新されます。クッキーは、コンソールをサインアウトしてから、または Web ブラウザーを閉じてから 12 時間有効です。

コンソールから次回認証要求を送信すると、フロントエンドの NGIX サーバーが、要求で利用可能な認証クッキーをデコードし、認証マネージャーを呼び出して要求を検証します。

Red Hat Advanced Cluster Management for Kubernetes プラットフォーム CLI では、ユーザーはログインに認証情報が必要です。

kubectl と **oc** CLI でも、クラスターへのアクセスに認証情報が必要です。このような認証情報は、管理コンソールから取得でき、12 時間後に有効期限が切れます。サービスアカウント経由のアクセスは、サポートされています。

1.5.8.2. ロールマッピング

Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、ロールベースのアクセス制御 (RBAC) をサポートします。ロールマッピングのステージでは、認証ステージで提示されたユーザー名がユーザーまたはグループロールにマッピングされます。認可時にロールを使用して、認証ユーザーがどのような管理者アクティビティーを実行できるか判断します。

1.5.8.3. 認可

Red Hat Advanced Cluster Management for Kubernetes プラットフォームのロールを使用して、クラスター設定アクション、カタログや Helm リソース、Kubernetes リソースへのアクセスを制御します。クラスター管理者、管理者、Operator、エディター、ビューワーなど、IAM (Identity and Access Management) ロールが複数含まれています。ロールは、チームへの追加時に、ユーザーまたはユーザーグループに割り当てられます。リソースへのチームアクセスは、namespace で制御できます。

1.5.8.4. Pod のセキュリティー

Pod のセキュリティーポリシーを使用して、Pod での操作またはアクセス権をクラスターレベルで制御できるように設定します。

1.5.9. データ処理

Red Hat Advanced Cluster Management for Kubernetes のユーザーは、システム設定を使用して、設定および管理に関する技術データをどのように処理して、データのセキュリティーを確保するかを制御できます。

ロールベースのアクセス制御 (RBAC) では、ユーザーがアクセスできるデータや機能を制御します。

転送中のデータ は **TLS** を使用して保護します。**HTTPS (TLS の下層)** は、ユーザークライアントとバックエンドのサービス間でのセキュアなデータ転送を確保するために使用されます。インストール時に、使用するルート証明書を指定できます。

保管時のデータ の保護は、**dm-crypt** を使用してデータを暗号化することでサポートされます。

Red Hat Advanced Cluster Management for Kubernetes プラットフォームの技術データの管理、セキュリティー確保と同じプラットフォームのメカニズムを使用して、ユーザーが開発したアプリケーションまたはユーザーがプロビジョニングしたアプリケーションの個人データを管理し、セキュリティーを確保することができます。クライアントは、独自の機能を開発して、追加の制御を実装できます。

1.5.10. データの削除

Red Hat Advanced Cluster Management for Kubernetes プラットフォームには、コマンド、アプリケーションプログラミングインターフェイス (API)、およびユーザーインターフェイスのアクションが含まれており、製品が作成または収集したデータを削除します。これらの機能により、サービスユーザー ID およびパスワード、IP アドレス、Kubernetes ノード名、または他のプラットフォームの設定データ、プラットフォームを管理するユーザーの情報などの、技術データを削除できます。

データ削除のサポートに関して考慮する必要がある Red Hat Advanced Cluster Management for Kubernetes プラットフォームのエリア:

- プラットフォーム設定に関連する技術データはすべて、管理コンソールまたは Kubernetes **kubectl** API を使用して削除できます。

アカウントデータ削除のサポートに関して考慮する必要がある Red Hat Advanced Cluster Management for Kubernetes プラットフォームのエリア:

- プラットフォーム設定に関連する技術データはすべて、Red Hat Advanced Cluster Management for Kubernetes または Kubernetes または **kubectl** API を使用して削除できます。

エンタープライズ LDAP ディレクトリーで管理されているユーザー ID およびパスワードを削除する機能は、Red Hat Advanced Cluster Management for Kubernetes プラットフォームが使用する LDAP 製品で提供されます。

1.5.11. 個人データの使用を制限する機能

Red Hat Advanced Cluster Management for Kubernetes プラットフォームでは、エンドユーザーは本書でまとめられている機能を使用し、個人データとみなされるプラットフォーム内の技術データの使用を制限することができます。

GDPR では、ユーザーはデータへのアクセス、変更、取り扱いの制限をする権利があります。本ガイドの他の項を参照して、以下を制御します。

- アクセス権限
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、データへの個別アクセスを設定できます。
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人に対し、このプラットフォームが保持する個人データの情報を提供できます。
- 変更する権限
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人がデータを変更または修正できるようにします。
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人のデータを修正できます。
- 処理を制限する権限
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人データの取り扱いを停止できます。

1.5.12. 付録

Red Hat Advanced Cluster Management for Kubernetes は、プラットフォームとして複数のカテゴリーの技術データを扱いますが、その中には管理者ユーザー ID とパスワード、サービスユーザー ID とパスワード、Kubernetes ノード名など、個人データとみなされる可能性があるものも含まれます。また、Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、プラットフォームの管理ユーザーに関する情報も扱います。プラットフォームで実行されるアプリケーションにより、プラットフォームではまだ知られていない、他のカテゴリーの個人データが取り込まれる可能性があります。

この付録には、プラットフォームサービスでロギングされるデータの情報が含まれます。

1.6. FIPS READINESS

Red Hat Advanced Cluster Management for Kubernetes は FIPS 向けに設計されています。FIPS モードの Red Hat OpenShift Container Platform で実行する場合、OpenShift Container Platform は、OpenShift Container Platform でサポートされているアーキテクチャーでのみ、FIPS 検証のために NIST に提出された Red Hat Enterprise Linux 暗号化ライブラリーを使用します。NIST 検証プログラムの詳細は、[暗号化モジュール検証プログラム](#) を参照してください。RHEL 暗号化ライブラリーの個別バージョンに関して検証用に提出された最新の NIST ステータスについては、[Compliance Activities and Government Standards](#) を参照してください。

FIPS を有効にしてクラスターを管理する予定の場合は、FIPS モードで動作するように設定した OpenShift Container Platform クラスターに Red Hat Advanced Cluster Management をインストールする必要があります。ハブクラスターで作成した暗号化はマネージドクラスターで使用されるため、ハブクラスターは FIPS モードである必要があります。

マネージドクラスターで FIPS モードを有効にするには、OpenShift Container Platform マネージドクラスターをプロビジョニングするときに **fips: true** と設定します。クラスターのプロビジョニング後は、FIPS を有効にすることはできません。詳細は、OpenShift Container Platform ドキュメント [Do you need additional security for your cluster?](#) を参照してください。

1.6.1. 制限事項

Red Hat Advanced Cluster Management および FIPS には以下の制限を確認してください。

- Red Hat OpenShift Container Platform は、x86_64 アーキテクチャーの FIPS のみをサポートします。
- 検索および可観測性コンポーネントによって使用される Persistent Volume Claims (PVC) および S3 ストレージは、指定のストレージを設定する際に暗号化する必要があります。Red Hat Advanced Cluster Management はストレージ暗号化を提供しません。OpenShift Container Platform ドキュメントの [永続ストレージの設定](#) を参照してください。
- Red Hat Advanced Cluster Management コンソールを使用してマネージドクラスターをプロビジョニングする場合は、マネージドクラスター作成の **Cluster details** セクションで以下のチェックボックスを選択して、FIPS 標準を有効にします。

FIPS with information text: Use the Federal Information Processing Standards (FIPS) modules provided with Red Hat Enterprise Linux CoreOS instead of the default Kubernetes cryptography suite file before you deploy the new managed cluster.

1.6.2. 関連情報

- NIST 検証プログラムの詳細は、[暗号化モジュール検証プログラム](#) を参照してください。

- RHEL 暗号化ライブラリーの個別バージョンに関して検証用に提出された最新の NIST ステータスについては、 [Compliance Activities and Government Standards](#) を参照してください。
- OpenShift Container Platform でサポートされるアーキテクチャーの詳細は、 [{cop-short} 4.13 release notes](#) を参照してください。