Red Hat Advanced Cluster Management for Kubernetes 2.6

リリースノート

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。

Last Updated: 2023-11-14

Red Hat Advanced Cluster Management for Kubernetes 2.6 リリースノート

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。

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

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

現在のリリースについて学びます。

注記: Red Hat Advanced Cluster Management の 2.4 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。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の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、リリースされます。

詳細は、本リリースの新機能を参照してください。

- 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。
- オープンソースの **Open Cluster Management** リポジトリーでは、オープンコミュニティーからの貢献、コミュニケーションやデプロイメントへの準備が整いました。open-cluster-management.io を参照してください。詳細は GitHub リポジトリー でも確認できます。
- 製品の主要なコンポーネントについては、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。
- スタートガイド では、(本製品を使用開始するための) 一般的なタスク、さらに **トラブルシューティングガイド** について言及します。
- 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

1.1.1. Web コンソール

- URL を使用して OpenShift Container Platform ルートを介して Grafana にアクセスできるようになりました。URL の例の詳細は Grafana ダッシュボードの設計 を参照してください。

```
https://grafana-open-cluster-management-observability.{OPENSHIFT_INGRESS_DOMAIN}
```

- クラスターのインポート中およびクラスターの作成後に、**AnsibleJob** テンプレートを指定できます。詳細は コンソールを使用したクラスターでの実行用の **AnsibleJob** テンプレート設定 を参照してください。

コンソールの概要 でコンソールの詳細を確認してください。

1.1.2. クラスター

クラスターライフサイクルのドキュメントは、マルチクラスターエンジン Operator のクラスターライフサイクルの概要 に、Kubernetes Operator Operator 用のマルチクラスターエンジンのドキュメントとして配置されるようになりました。

- **マルチクラスターエンジン Operator** は、クラスターのフリート管理を強化するソフトウェア Operator として一般提供されています。マルチクラスターエンジン 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 クラスターライフサイクル管理をサポートします。Red Hat OpenShift Container Platform は、マルチクラスターエンジン Operator の前提条件です。
- アクセス許可クラスターセット **bind** は、**ManagedClusterSetBinding** を作成することにより、クラスターセットを namespace にバインドするアクセス許可を付与します。詳細は ManagedClusterSet へのユーザーまたはグループのロールベースのアクセス制御許可の割り当て を参照してください。
- マネージドクラスターを作成すると、管理を容易にするために **global** と呼ばれる **ManagedClusterSet** が自動的に作成されます。詳細は、 グローバル ManagedClusterSet を参照してください。
- **By uploading a YAML** オプションを選択すると、インフラストラクチャー環境に複数のホストを同時に追加できます。詳細は Scaling hosts to an infrastructure environment を参照してください。
- インフラストラクチャー環境にアクセスするためのナビゲーションメニューオプションが、**Infrastructure environment** から **Host inventory** に変更されました。
- Central Infrastructure Management サービスで作成された単一ノードの OpenShift クラスターにワーカーを追加できます。詳細は コンソールを使用したクラスターの作成 を参照してください。

1.1.3. アプリケーション

- 必要に応じて、namespace スコープのリソースを監視するように Helm チャネルタイプを設定して、それらのリソースに対する手動の変更を元に戻すことができます。namespace リソースを監視するように Helm を設定する を参照してください。

- **OpenShift**、**Flux**、および **Argo CD** アプリケーションタイプを作成および表示できます。**ApplicationSet** は、このコントローラーから生成される Argo アプリケーションを表します。コンソールの概要 を参照してください。

他のアプリケーションのトピックについては、アプリケーションの管理 を参照してください。

1.1.4. ガバナンス

- ポリシージェネレーター設定で **configurationPolicyAnnotations** パラメーターを使用して、生成された設定ポリシーにキーと値のペアのアノテーションを指定できます。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。

- マネージドクラスターごとに設定ポリシーコントローラーの並行処理性を設定して、同時に評価できる設定ポリシーの数を変更します。詳しくは、設定ポリシーコントローラーの設定 を参照してください。

- **pruneObjectBehavior** パラメーターを使用してリソースをクリーンアップします。ポリシーによって作成されたリソースの消去 を参照してください。

- ポリシー違反イベントごとにガバナンス Ansible Automation を実行するように設定するには、**everyEvent** モードを使用します。ガバナンスのための Ansible Tower の設定 の **コンソールからのポリシー違反の自動化作成** セクションを参照してください。

- **matchLabels** と **matchExpressions** パラメーターを使用して、ポリシーコントローラーのラベルで namespace を選択します。詳しくは、設定ポリシー YAML テーブル を参照してください。

- 名前で namespace を選択するには、**include** パラメーターと **exclude** パラメーターでファイルパス式を定義します。詳細は、設定ポリシー YAML テーブル を参照してください。

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。

1.1.5. アドオン

詳細は、リリースノート を参照してください。

- Red Hat Advanced Cluster Management で永続ボリューム要求をコピーするための VolSync Operator が一般提供されるようになりました。詳細は VolSync 永続ボリューム複製サービス を参照してください。

1.2. 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 クラスターについては、OpenShift Container Platform の既知の問題 を参照してください。

- ドキュメントの既知の問題

- インストールの既知の問題

- Web コンソールの既知の問題

1.2.1. ドキュメントの既知の問題

1.2.1.1. カスタマーポータルのドキュメントリンクは、上位レベルのセクションにリンクしている場合がある

場合によっては、カスタマーポータルの Red Hat Advanced Cluster Management ドキュメントの他のセクションへの内部リンクが指定されたセクションに直接リンクしないことがあります。最上位のセクションにリンクされる場合もあります。

これが発生した場合は、指定されたセクションを手動で見つけるか、次の手順を実行して解決できます。

1. 解決されていないリンクを正しいセクションにコピーして、ブラウザーのアドレスバーに貼り付けます。たとえば、**https://access.redhat.com/documentation/ja-jp/red_hat_advanced_cluster_management_for_kubernetes/2.6/html/clusters/index#volsync** のようになります。

2. リンクの **html** を **html-single** に置き換えます。新しい URL は、**https://access.redhat.com/documentation/ja-jp/red_hat_advanced_cluster_management_for_kubernetes/2.6/html-single/clusters/index#volsync** を読み込む必要があります。

3. 新しい URL にリンクして、ドキュメントで指定されたセクションを見つけます。

1.2.2. インストール関連の既知の問題

1.2.2.1. Errata 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
```

1.2.2.2. 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。

1.2.2.3. 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。

1.2.2.4. 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。

1.2.3. Web コンソールの既知の問題

1.2.3.1. LDAP ユーザー名の大文字と小文字が区別される

LDAP ユーザー名は、大文字と小文字が区別されます。LDAP ディレクトリーで設定したものと全く同じ名前を使用する必要があります。

1.2.3.2. 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ー を参照してください。

1.2.3.3. 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
```

1.2.3.4. 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 multicloud-console haproxy.router.openshift.io/timeout=Xs
```

1.2.3.5. 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。

1.2.4. 可観測性関連の既知の問題

1.2.4.1. 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。

1.2.4.2. 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。

1.2.4.3. ROKS クラスターおよび HyperShift クラスターからのデータはありません

Red Hat Advanced Cluster Management の可観測性は、組み込みダッシュボードで、ROKS クラスターおよび HyperShift 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 および HyperShift が管理するサーバーからの API サーバーメトリック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/Namespace(Workload)** の ROKS クラスターおよび HyperShift クラスターをサポートしないパネルが含まれます。

1.2.4.4. ROKS クラスターおよび HyperShift クラスターからの etcd データはありません

ROKS クラスターおよび HyperShift クラスターの場合、Red Hat Advanced Cluster Management の可観測性は、ダッシュボードの **etcd** パネルにデータを表示しません。

1.2.4.5. search-collector Pod による CPU の使用率が高くなる

1000 のクラスターを管理するハブクラスターで検索を無効にすると、メモリー不足 (OOM) が原因で **search-collector** Pod がクラッシュします。以下の手順を実行します。

1. ハブクラスターで検索が無効にされている場合、**search-redisgraph-pod** はデプロイされないため、**search-collector** デプロイメントを **0** レプリカにスケールダウンしてメモリーの使用量を削減します。
2. ハブクラスターで検索が有効になっている場合 (**search-redisgraph-pod** がデプロイされていることを意味する) は、**search-collector** デプロイメントを編集して割り当てられるメモリーを増やします。

1.2.4.6. 証明書が無効な場合に検索 Pod が TLS ハンドシェイクを完了できない

まれに、検索 Pod は証明書の変更後に自動的に再デプロイされない場合があります。これにより、サービス Pod 全体で証明書が一致しなくなるため、転送レイヤーセキュリティー (TLS) ハンドシェイクが失敗します。この問題を修正するには、検索 Pod を再起動して証明書をリセットします。

1.2.4.7. 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。

1.2.4.8. 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。

1.2.4.9. 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。

1.2.4.10. マネージドクラスターで Grafana のデプロイが失敗する

マニフェストのサイズが 50,000 バイトを超えると、Grafana インスタンスはマネージドクラスターにデプロイされません。可観測性をデプロイした後、**local-cluster** のみが Grafana に表示されます。

1.2.4.11. 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
```

1.2.4.12. 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
```

1.2.5. クラスター管理の既知の問題

クラスター管理に関する次の既知の問題と制限を参照してください。

1.2.5.1. クラスター作成用の切断されたインストール設定は入力できないか、入力しても無視される

ベアメタルプロバイダーと切断されたインストールを使用してクラスターを作成する場合、**切断されたインストールの設定** セクションの認証情報にすべての設定を保存する必要があります。クラスター作成コンソールエディターでそれらを入力することはできません。

VMware vSphere または Red Hat OpenStack Platform プロバイダーを使用してクラスターを作成し、切断されたインストールを行う場合、ミラーレジストリーにアクセスするために証明書が必要な場合は、**切断されたインストールの設定セクション**の認証情報の**追加の信頼バンドル**フィールドに証明書を入力する必要があります。.その証明書をクラスター作成コンソールエディターに入力すると、無視されます。

1.2.5.2. 切断されたインストーラーの認証情報は、証明書を区別しない

ベアメタル、VMware vSphere、または Red Hat OpenStack Platform プロバイダーの認証情報を作成する場合、インストーラーは証明書を区別しないため、**切断されたインストールのプロキシーと設定**の**追加の信頼バンドル**フィールドには同じ値が含まれていることに注意してください。これらの機能を個別に使用することもできます。また、プロキシーインストールと非接続インストールで異なる証明書が必要な場合は、フィールドに複数の証明書を入力できます。

1.2.5.3. アドオンの削除時にマネージドクラスターで必要な VolSync CSV の手動削除

ハブクラスターから VolSync **ManagedClusterAddOn** を削除すると、マネージドクラスターの VolSync Operator サブスクリプションが削除されますが、クラスターサービスバージョン (CSV) は削除されません。マネージドクラスターから CSV を削除するには、VolSync を削除する各マネージドクラスターで以下のコマンドを実行します。

```
oc delete csv -n openshift-operators volsync-product.v0.4.0
```

別のバージョンの VolSync がインストールされている場合は、**v0.4.0** をインストール済みバージョンに置き換えます。

1.2.5.4. マネージドクラスターセットを削除してもそのラベルが自動的に削除されない

ManagedClusterSet を削除した後に、クラスターセットに関連付ける各マネージドクラスターに追加されるラベルは自動的に削除されません。削除したマネージドクラスターセットに含まれる各マネージドクラスターからラベルを手動で削除します。ラベルは **cluster.open-cluster-management.io/clusterset:<ManagedClusterSet Name>** のようになります。

1.2.5.5. ClusterClaim エラー

ClusterPool に対して Hive **ClusterClaim** を作成し、**ClusterClaimspec** の有効期限のフィールドを無効な golang タイム値に手動で設定すると、Red Hat Advanced Cluster Management は不正な要求だけでなく、すべての **ClusterClaims** の実行および調整を停止します。

このエラーが発生すると、**clusterclaim-controller** Pod ログに以下の内容が表示されます。これは、プール名と、無効な有効期限が含まれた特定の例です。

```
E0203 07:10:38.266841       1 reflector.go:138] sigs.k8s.io/controller-runtime/pkg/cache/internal/informers_map.go:224: Failed to watch *v1.ClusterClaim: failed to list *v1.ClusterClaim: v1.ClusterClaimList.Items: []v1.ClusterClaim: v1.ClusterClaim.v1.ClusterClaim.Spec: v1.ClusterClaimSpec.Lifetime: unmarshalerDecoder: time: unknown unit "w" in duration "1w", error found in #10 byte of ...|time":"1w"}},{"apiVe|..., bigger context ...|clusterPoolName":"policy-aas-hubs","lifetime":"1w"}}, {"apiVersion":"hive.openshift.io/v1","kind":"Cl|...
```

無効な要求を削除できます。

不正な要求が削除されると、要求は追加の対話なしに正常に調整を開始します。

1.2.5.6. 製品チャネルが、プロビジョニングされたクラスターと同期されない

clusterimageset は **fast** チャネルに置かれますが、プロビジョニングされたクラスターは **stable** チャネルにあります。現時点で、製品は **channel** をプロビジョニングされた OpenShift Container Platform クラスターと同期しません。

OpenShift Container Platform コンソールで適切なチャネルに切り替えます。**Administration** > **Cluster Settings** > **Details Channel** の順にクリックします。

1.2.5.7. カスタム CA 証明書を使用したマネージドクラスターの、復元されたハブクラスターへの接続の復元は失敗する可能性がある

カスタム CA 証明書を使用してクラスターを管理したハブクラスターのバックアップを復元した後、マネージドクラスターとハブクラスター間の接続が失敗する場合があります。これは、復元されたハブクラスターで CA 証明書がバックアップされなかったためです。接続を復元するには、マネージドクラスターの namespace にあるカスタム CA 証明書情報を、復元されたハブクラスターの **<managed_cluster>-admin-kubeconfig** シークレットにコピーします。

ヒント: バックアップコピーを作成する前にこの CA 証明書をハブクラスターにコピーする場合は、バックアップコピーにシークレット情報が含まれます。将来、バックアップコピーを使用して復元する場合、ハブとマネージドクラスター間の接続は自動的に完了します。

1.2.5.8. ローカルクラスターが自動的に再作成されない場合がある

disableHubSelfManagement が **false** に設定されている場合、local-cluster は **MulticlusterHub** Operator によって再作成されます。ローカルクラスターをデタッチした後、ローカルクラスターが自動的に再作成されない場合があります。

- この問題を解決するには、**MulticlusterHub** によって監視されるリソースを変更します。以下の例を参照してください。

  ```
  oc delete deployment multiclusterhub-repo -n <namespace>
  ```

- local-cluster を適切にデタッチするには、**MultiClusterHub** で **disableHubSelfManagement** を true に設定します。

1.2.5.9. オンプレミスクラスターを作成する場合は、サブネットを選択する必要がある

Red Hat Advanced Cluster Management コンソールを使用してオンプレミスクラスターを作成する場

Red Hat Advanced Cluster Management コンソールを使用してオンプレミスクラスターを作成する場合は、クラスターで使用可能なサブネットを選択する必要があります。必須フィールドとしてマークされていません。

1.2.5.10. Infrastructure Operator を使用したクラスターのプロビジョニングに失敗する

Infrastructure Operator を使用して OpenShift Container Platform クラスターを作成する場合、ISO イメージのファイル名は長すぎる可能性があります。長いイメージ名により、イメージのプロビジョニングとクラスターのプロビジョニングが失敗します。この問題が生じるかどうかを確認するには、以下の手順を実行します。

1. 以下のコマンドを実行して、プロビジョニングするクラスターのベアメタルホスト情報を表示します。

```
oc get bmh -n <cluster_provisioning_namespace>
```

2. **describe** コマンドを実行して、エラー情報を表示します。

```
oc describe bmh -n <cluster_provisioning_namespace> <bmh_name>
```

3. 以下の例と同様のエラーは、ファイル名の長さが問題であることを示します。

```
Status:
  Error Count:    1
  Error Message:  Image provisioning failed: ... [Errno 36] File name too long ...
```

この問題が発生する場合、これは通常 OpenShift Container Platform の以下のバージョンで発生します。インフラストラクチャー Operator がイメージサービスを使用していないためです。

- 4.8.17 以前
- 4.9.6 以前

このエラーを回避するには、OpenShift Container Platform をバージョン 4.8.18 以降、または 4.9.7 以降にアップグレードしてください。

1.2.5.11. 別の名前で再インポートした後に local-cluster のステータスがオフラインになる

local-cluster という名前のクラスターを、誤って別の名前のクラスターとして再インポートしようとすると、**local-cluster** と再インポートしたクラスターのステータスが **offline** と表示されます。

このケースから回復するには、以下の手順を行います。

1. ハブクラスターで以下のコマンドを実行して、ハブクラスターの自己管理の設定を一時的に編集します。

```
oc edit mch -n open-cluster-management multiclusterhub
```

2. **spec.disableSelfManagement=true** の設定を追加します。
3. ハブクラスターで以下のコマンドを実行し、local-cluster を削除し、再デプロイします。

```
oc delete managedcluster local-cluster
```

4. 以下のコマンドを実行して **local-cluster** 管理設定を削除します。

```
oc edit mch -n open-cluster-management multiclusterhub
```

5. 前の手順で追加した **spec.disableSelfManagement=true** を削除します。

1.2.5.12. Ansible 自動化を使用したクラスタープロビジョニングがプロキシー環境で失敗する

マネージドクラスターを自動的にプロビジョニングするように設定された AnsibleJob テンプレートは、以下の条件の両方が満たされると失敗する可能性があります。

- ハブクラスターで、クラスター全体のプロキシーが有効になっている。
- Ansible Tower には、プロキシーを介してのみアクセスできる。

1.2.5.13. klusterlet Operator のバージョンは、ハブクラスターと同じである必要がある

klusterlet Operator をインストールしてマネージドクラスターをインポートする場合には、klusterlet Operator のバージョンは、ハブクラスターのバージョンと同じでなければなりません。そうでないと、klusterlet Operator は動作しません。

1.2.5.14. マネージドクラスター namespace を手動で削除できない

マネージドクラスターの namespace を手動で削除できません。マネージドクラスター namespace は、マネージドクラスターの割り当てを解除した後に自動的に削除されます。マネージドクラスターの割り当てを解除する前に手動でマネージドクラスター namespace を削除する場合は、マネージドクラスターの削除後にマネージドクラスターに継続的な終了ステータスが表示されます。この終了マネージドクラスターを削除するには、割り当てを解除したマネージドクラスターからファイナライザーを手動で削除します。

1.2.5.15. バージョン 2.3 にアップグレードした後にクラスターの認証情報を変更できない

Red Hat Advanced Cluster Management をバージョン 2.3 にアップグレードすると、アップグレード前に Red Hat Advanced Cluster Management で作成して管理されていたマネージドクラスターの認証情報シークレットが変更できなくなります。

1.2.5.16. ハブクラスターとマネージドクラスターのクロックが同期されない

ハブクラスターおよびマネージドクラスターの時間が同期されず、コンソールで **unknown** と表示され、最数的に、数分以内に **available** と表示されます。Red Hat OpenShift Container Platform ハブクラスターの時間が正しく設定されていることを確認します。ノードのカスタマイズ を参照してください。

1.2.5.17. IBM OpenShift Container Platform Kubernetes Service クラスターの特定のバージョンのインポートはサポートされていない

IBM OpenShift Container Platform Kubernetes Service バージョン 3.11 のクラスターをインポートすることはできません。IBM OpenShift Kubernetes Service の 3.11 よりも後のバージョンはサポート対象です。

1.2.5.18. プロビジョニングされたクラスターのシークレットの自動更新はサポートされていない

クラウドプロバイダー側でクラウドプロバイダーのアクセスキーを変更する場合は、Kubernetes

Operator 用のマルチクラスターエンジンのコンソールで、クラウドプロバイダーの対応する認証情報を手動で更新する必要もあります。これは、マネージドクラスターがホストされ、マネージドクラスターの削除を試みるクラウドプロバイダーで認証情報の有効期限が切れる場合に必要です。

1.2.5.19. マネージドクラスターからのノード情報を検索で表示できない

検索で、ハブクラスターのリソース用の RBAC がマッピングされます。Red Hat Advanced Cluster Management のユーザー RBAC 設定によっては、マネージドクラスターからのノードデータが表示されない場合があります。また検索の結果は、クラスターの **Nodes** ページに表示される内容と異なる場合があります。

1.2.5.20. クラスターを破棄するプロセスが完了しない

マネージドクラスターを破棄してから 1 時間経過してもステータスが **Destroying** のままで、クラスターが破棄されません。この問題を解決するには、以下の手順を実行します。

1. クラウドに孤立したリソースがなく、マネージドクラスターに関連付けられたプロバイダーリソースがすべて消去されていることを確認します。
2. 以下のコマンドを入力して、削除するマネージドクラスターの **ClusterDeployment** 情報を開きます。

   ```
   oc edit clusterdeployment/<mycluster> -n <namespace>
   ```

   mycluster は、破棄するマネージドクラスターの名前に置き換えます。

   namespace は、マネージドクラスターの namespace に置き換えます。
3. **hive.openshift.io/deprovision** ファイナライザーを削除し、クラウドのクラスターリソースを消去しようとするプロセスを強制的に停止します。
4. 変更を保存して、**ClusterDeployment** が削除されていることを確認します。
5. 以下のコマンドを実行してマネージドクラスターの namespace を手動で削除します。

   ```
   oc delete ns <namespace>
   ```

   namespace は、マネージドクラスターの namespace に置き換えます。

1.2.5.21. OpenShift Container Platform Dedicated でコンソールを使用して OpenShift Container Platform マネージドクラスターをアップグレードできない

Red Hat Advanced Cluster Management コンソールを使用して、OpenShift Container Platform Dedicated 環境にある OpenShift Container Platform マネージドクラスターをアップグレードすることはできません。

1.2.5.22. ワークマネージャーのアドオン検索の詳細

特定のマネージドクラスターにある特定のリソースの検索詳細ページで問題が発生する可能性があります。マネージドクラスターの work-manager アドオンが **Available** ステータスであることを確認してから検索する必要があります。

1.2.5.23. IBM Power または IBM Z システムハブクラスターとの Ansible Tower 統合は使用できない

Ansible Automation Platform Resource Operator では **ppc64le** イメージまたは **s390x** イメージが提供されないので、IBM Power または IBM Z システムで Red Hat Advanced Cluster Management for Kubernetes ハブクラスターが実行されている場合には、Ansible Tower 統合を使用できません。

1.2.5.24. Red Hat OpenShift Container Platform 以外のマネージドクラスターでは、LoadBalancer が有効にされている必要がある

Red Hat OpenShift Container Platform および OpenShift Container Platform 以外のクラスターの両方は Pod ログ機能をサポートしますが、OpenShift Container Platform 以外のクラスターでは、この機能を使用できるように **LoadBalancer** が有効にされている必要があります。**LoadBalancer** を有効にするには、以下の手順を実行します。

1. クラウドプロバイダーごとに **LoadBalancer** 設定が異なります。詳細は、クラウドプロバイダーのドキュメントを参照してください。
2. **managedClusterInfo** のステータスで **loggingEndpoint** をチェックして、**LoadBalancer** が Red Hat Advanced Cluster Management で有効にされているかどうかを確認します。
3. 以下のコマンドを実行して、**loggingEndpoint.IP** または **loggingEndpoint.Host** に有効な IP アドレスまたはホスト名が設定されていることを確認します。

```
oc get managedclusterinfo <clusterName> -n <clusterNamespace> -o json | jq -r
'.status.loggingEndpoint'
```

LoadBalancer のタイプについての詳細は、Kubernetes のドキュメント のService ページを参照してください。

1.2.5.25. アップグレード後に Cluster-proxy-addon が起動しない

バージョン 2.4.x から 2.5.0 にアップグレードした後、**cluster-proxy-addon** が起動せず、**cluster-proxy-addon-manager** が nil ポインター例外を発生させます。

この問題を回避するには、以下の手順を実行します。

1. **cluster-proxy-addon** を無効にします。詳細は、高度な設定 を参照してください。
2. **open-cluster-management** namespace から **cluster-proxy-signer** シークレットを削除します。
3. **cluster-proxy-addon** を有効にします。

1.2.5.26. OpenShift Container Platform 4.10.z では、プロキシー設定を使用するホストコントロールプレーンクラスターはサポートされません

OpenShift Container Platform 4.10.z でクラスター全体のプロキシー設定を使用してホスティングサービスクラスターを作成すると、**nodeip-configuration.service** サービスがワーカーノードで開始されません。

1.2.5.27. Azure で OpenShift Container Platform 4.11 クラスターをプロビジョニングできない

Azure で OpenShift Container Platform 4.11 クラスターをプロビジョニングすると、認証 Operator のタイムアウトエラーが原因で失敗します。この問題を回避するには、**install-config.yaml** ファイルで別のワーカーノードタイプを使用するか、**vmNetworkingType** パラメーターを **Basic** に設定します。次の **install-config.yaml の** 例を参照してください。

```
compute:
- hyperthreading: Enabled
  name: 'worker'
  replicas: 3
  platform:
    azure:
      type:  Standard_D2s_v3
      osDisk:
        diskSizeGB: 128
      vmNetworkingType: 'Basic'
```

1.2.5.28. クライアントが iPXE スクリプトにアクセスできない

iPXE は、オープンソースのネットワークブートファームウェアです。詳細は、iPXE を参照してください。

ノードの起動時に、一部の DHCP サーバーの URL の長さ制限により、**InfraEnv** カスタムリソース定義の **ipxeScript** URL が切り取られ、コンソールに次のエラーメッセージが表示されます。

起動可能なデバイスがありません

この問題を回避するには、以下の手順を実行します。

1. 自動インストールを使用して **bootArtifacts** を公開する場合は、**InfraEnv** カスタムリソース定義を適用します。これは次のファイルのようになります。

```
status:
  agentLabelSelector:
    matchLabels:
      infraenvs.agent-install.openshift.io: qe2
  bootArtifacts:
    initrd: https://assisted-image-service-multicluster-engine.redhat.com/images/0000/pxe-initrd?api_key=0000000&arch=x86_64&version=4.11
    ipxeScript: https://assisted-service-multicluster-engine.redhat.com/api/assisted-install/v2/infra-envs/00000/downloads/files?api_key=000000000&file_name=ipxe-script
    kernel: https://mirror.openshift.com/pub/openshift-v4/x86_64/dependencies/rhcos/4.11/latest/rhcos-live-kernel-x86_64
    rootfs: https://mirror.openshift.com/pub/openshift-v4/x86_64/dependencies/rhcos/4.11/latest/rhcos-live-rootfs.x86_64.img
```

2. 短い URL で **bootArtifacts** を公開するプロキシーサーバーを作成します。
3. 次のコマンドを実行して、**bootArtifacts** をコピーし、プロキシーに追加します。

```
for artifact in oc get infraenv qe2 -ojsonpath="{.status.bootArtifacts}" | jq ". | keys[]" | sed "s/\"//g"
do curl -k oc get infraenv qe2 -ojsonpath="{.status.bootArtifacts.${artifact}}"` -o $artifact
```

4. **ipxeScript** アーティファクトプロキシー URL を **libvirt.xml** の **bootp** パラメーターに追加します。

1.2.5.29. カスタム Ingress ドメインが正しく適用されない

マネージドクラスターのインストール中に **ClusterDeployment** リソースを使用してカスタム Ingress

ドメインを指定できますが、変更はインストール後に **SyncSet** リソースを使用してのみ適用されます。その結果、**clusterdeployment.yaml** ファイルの **spec** フィールドには、指定したカスタム Ingress ドメインが表示されますが、**status** には引き続きデフォルトのドメインが表示されます。

1.2.6. アプリケーション管理の既知の問題

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。

1.2.6.1. アプリケーション ObjectBucket チャネルタイプは、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。

1.2.6.2. 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。

1.2.6.3. 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。

1.2.6.4. 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、ソースリポジトリーに合わせて調整されません。

1.2.6.5. 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。以下のサンプルを参照してください。

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

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。

1.2.6.6. Editor ロールのアプリケーションエラー

Editor ロールで実行するユーザーは、アプリケーションで **read** または **update** の権限のみが割り当てられているはずにもかかわらず、誤ってアプリケーションの **create** および **delete** の操作ができてしまいます。OpenShift Container Platform Operator Lifecycle Manager のデフォルト設定により、当製品の設定が変更されてしまいます。この問題を回避するには、以下の手順を参照してください。

1. **oc edit clusterrole applications.app.k8s.io-v1beta2-edit -o yaml** を実行して、アプリケーションのクラスターロールの編集を開きます。
2. verbs リストから **create** および **delete** を削除します。
3. 変更を保存します。

1.2.6.7. 配置ルールの編集ロールエラー

Editor ロールで実行するユーザーは、配置ルールで **read** または **update** の権限のみが割り当てられているはずにもかかわらず、誤って **create** および **delete** の操作もできてしまいます。OpenShift Container Platform Operator Lifecycle Manager のデフォルト設定により、当製品の設定が変更されてしまいます。この問題を回避するには、以下の手順を参照してください。

1. **oc edit clusterrole placementrules.apps.open-cluster-management.io-v1-edit** を実行して、アプリケーションの編集クラスターロールを開きます。
2. verbs リストから **create** および **delete** を削除します。
3. 変更を保存します。

1.2.6.8. 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ーです。

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。

1.2.6.9. 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で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 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
```

1.2.6.10. アプリケーションチャネルには一意の namespace が必要

同じ namespace に複数のチャネルを作成すると、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** に追加のチャネルを作成します。一意の namespace でチャネルを作成するようにしてください。すべてのチャネルには個別の namespace が必要ですが、GitHub チャネルは例外で、別 GitHub のチャネルと namespace を共有できます。

1.2.6.11. 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。

1.2.6.12. Ansible Automation Platform Operator によるプロキシー外の Ansible Tower へのアクセス

Ansible Automation Platform(AAP)Operator は、プロキシー対応の OpenShift Container Platform クラスター外の Ansible Tower にアクセスできません。解決するには、Ansible tower をプロキシー内にインストールします。Ansible Tower が提供するインストール手順を参照してください。

1.2.6.13. バージョン 2.4 で Helm Argo アプリケーションを編集する場合、テンプレート情報は表示されません

Helm Argo アプリケーションを作成して編集すると、YAML ファイルが正しい間、テンプレート情報は空で表示されます。エラーを修正するには、エラータ 2.4.1 にアップグレードしてください。

1.2.6.14. 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'
```

1.2.6.15. 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。

1.2.6.16. 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

2.6 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。

1.2.6.17. ApplicationSet リソースがトポロジーにステータスを表示しない

ApplicationSet YAML で定義された namespace とは異なる namespace にリソースをデプロイする **ApplicationSet** アプリケーションを作成すると、リソースのステータスがトポロジーに表示されません。

1.2.6.18. 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。

1.2.6.19. ApplicationSet トポロジーステータスアイコンが回転し続ける

ApplicationSet アプリケーションがデプロイされているが、Argo アプリケーションが関連付けられていない場合に、**ApplicationSet** トポロジーステータスアイコンが継続的に回転します。

1.2.6.20. ハブクラスターのアップグレード後にリストされた、サポートされていない OpenShift Container Platform バージョン

ハブクラスターを 2.5 より前のバージョンから 2.6 にアップグレードした後、サポートされていない OpenShift Container Platform バージョンの一部がコンソールの **クラスター** ページに一覧表示されます。

2.5 サブスクリプションコントローラーより前のバージョンでデプロイされた古い **clusterImageSet** リソースは、アップグレード後に削除されません。これを解決するには、OpenShift Container Platform のバージョンがサポートされていない **clusterImageSet** リソースを手動で削除します。たとえば、次のコマンドを実行して **img4.7.0-x86-64-appsub clusterImageSet** を削除します。

```
oc delete clusterimageset img4.7.0-x86-64-appsub
```

1.2.6.21. ハブクラスターを新しいハブクラスターに復元した後、アプリケーションサブスクリプションを削除できない

ハブクラスターデータを新しいハブクラスターに復元する場合、マネージドクラスターが配置クラスター決定リストから削除された後でも、マネージドクラスター上の既存のアプリケーションサブスクリプションは削除されません。

次の手順を実行することで、この問題を回避できます。

1. マネージドクラスターに移動します。
2. 次のコマンドを実行して、孤立した **AppliedManifestWork** を取得します。

   ```
   oc get appsub -n <appsub NS> <appsub Name> -o yaml
   ```

   出力は次の例のような内容になります。

   ```
   ownerReferences:
   - apiVersion: work.open-cluster-management.io/v1
     kind: AppliedManifestWork
     name: 6e01d06846c6ca2ac4ed6c9b0841e720af2de12a171108768f42285d7f873585-test-appsub-1-ns-git-app-1
     uid: f69fe90b-7f5f-483a-86b2-dcd5e041321a
   ```

3. 次のコマンドを実行して、孤立した **AppliedManifestWork** を削除します。これにより、アプリケーションサブスクリプションも削除されます。

   ```
   oc delete AppliedManifestWork 6e01d06846c6ca2ac4ed6c9b0841e720af2de12a171108768f42285d7f873585-test-appsub-1-ns-git-app-1
   ```

1.2.6.22. ApplicationSet ウィザードがパスを自動的にフェッチしない

以前に作成した **ApplicationSet** と同じ URL とブランチで新しい **ApplicationSet** を作成すると、ApplicationSet ウィザードはパスを自動的にフェッチしません。

この問題を回避するには、**Path** フィールドにパスを手動で入力します。

1.2.7. ガバナンス関連の既知の問題

1.2.7.1. 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ー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ー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ープロバイダーからログアウトしておく必要があります。

1.2.7.2. 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。

1.2.7.3. 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関わらず、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。

1.2.7.4. 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

1.2.7.5. 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。

1.2.7.6. 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場合には、**pruneObjectBehavior** 機能の **DeleteAll** または **DeleteIfCreated** では、変更前に作成された古いリソースは消去されません。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。

1.2.7.7. ポリシーテンプレートの問題

設定ポリシーのポリシーテンプレートを編集すると、次の問題が発生する場合があります。

- 設定ポリシーの名前を新しい名前に変更すると、古い名前の設定ポリシーのコピーが残ります。
- ハブクラスターのポリシーから設定ポリシーを削除すると、設定ポリシーはマネージドクラスターに残りますが、その状態は提供されません。これを解決するには、ポリシーを無効にしてから再度有効にします。ポリシー全体を削除することもできます。

1.2.7.8. Pod セキュリティーポリシーが OpenShift 4.12 以降でサポートされない

Pod セキュリティー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
```

1.2.8. バックアップおよび復元の既知の問題

1.2.8.1. バックアップおよび復元機能が IBM Power および IBM Z で動作しない

ハブクラスターのバックアップおよび復元機能には、Data Protection (OADP) Operator の OpenShift API が必要です。OADP Operator は、IBM Power または IBM Z アーキテクチャーでは使用できません。

1.2.8.2. バックアップの競合の回避

ハブクラスターは passive から primary クラスターに戻されると、異なるクラスターが同じストレージの場所にあるデータをバックアップできます。これにより、バックアップの競合が発生します。つまり、最新のバックアップが passive ハブクラスターによって生成されたことを意味します。

BackupSchedule.cluster.open-cluster-management.io リソースがハブクラスターで有効になっているため、passive ハブクラスターはバックアップを生成しますが、このハブクラスターは primary ハブクラスターでなくなったため、バックアップデータは書き込みできるべきではありません。以下のコマンドを実行して、バックアップの競合があるかどうかを確認します。

```
oc get backupschedule -A
```

以下のステータスが返される場合があります。

```
NAMESPACE       NAME              PHASE           MESSAGE
openshift-adp   schedule-hub-1    BackupCollision   Backup acm-resources-schedule-20220301234625, from cluster with id [be97a9eb-60b8-4511-805c-298e7c0898b3] is using the same storage location. This is a backup collision with current cluster [1f30bfe5-0588-441c-889e-eaf0ae55f941] backup. Review and resolve the collision then create a new BackupSchedule resource to  resume backups from this cluster.
```

BackupSchedule.cluster.open-cluster-management.io リソースの **status** を **BackupCollision** に設定して、バックアップの競合を回避します。**BackupSchedule** リソースによって作成される **Schedule.velero.io** リソースは自動的に削除されます。

バックアップの競合は、**hub-backup-pod** ポリシーにより報告されます。管理者は、どのハブクラスターが対象のストレージの場所にデータを書き込んでいるかを確認する必要があります。次に、passive ハブクラスターから **BackupSchedule.cluster.open-cluster-management.io** リソースを削除し、primary ハブクラスターに新しい **BackupSchedule.cluster.open-cluster-management.io** リソースを再作成して、バックアップを再開します。

詳細は、バックアップおよびリストア Operator の有効化 を参照してください。

1.2.8.3. Velero 復元の制限

以下の復元の制限を確認してください。

- 初期ハブクラスターにバックアップデータを復元する前に、新しいハブクラスターに既存のポリシーが存在する場合、データの復元先の初期ハブクラスターと新規ハブクラスターは同じにはなりません。このポリシーは、バックアップリソースで利用できないポリシーであるため、新しいハブクラスターで実行しないでください。
- Velero は既存のリソースを省略するため、新しいハブクラスターのポリシーは変更されません。したがって、ポリシーは、最初のハブクラスターでバックアップしたポリシーと同じではありません。
- ユーザーが新しいハブクラスターのバックアップを再適用する場合には、新しいハブクラスターには、アクティブなハブクラスターとは異なる設定があります。ハブクラスターに以前の復元からの既存のポリシーがあるため、復元されません。バックアップに想定された更新が含まれている場合でも、ポリシーのコンテンツは、新しいハブクラスターの Velero によって更新されません。

前述の制限に対応するために、**restore.cluster.open-cluster-management.io** リソースが作成されると、クラスターのバックアップおよび復元 Operator は、Velero 復元の開始前にハブクラスターを削除して復元の準備を行う一連の手順を実行します。

詳細は、バックアップおよびリストア Operator の有効化 トピックの **リストア前のハブクラスターの消去** を参照してください。

1.2.8.4. インポートされたマネージドクラスターが表示されない

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、パッシブハブクラスターでアクティベーションデータが復元された場合にのみ表示されます。

1.2.8.5. クラスターのバックアップおよび復元のアップグレードの制限

enableClusterBackup パラメーターを **true** に設定してクラスターを 2.5 から 2.6 にアップグレードすると、次のメッセージが表示されます。

```
When upgrading from version 2.4 to 2.5, cluster backup must be disabled
```

クラスターをアップグレードする前に、**enableClusterBackup** パラメーターを **false** に設定して、クラスターのバックアップおよび復元を無効にします。**MultiClusterHub** リソースの **components** セクションは、次の YAML ファイルのようになります。

アップグレードが完了したら、バックアップおよび復元のコンポーネントを再度有効にすることができます。以下のサンプルを参照してください。

```
overrides:
    components:
      - enabled: true
        name: multiclusterhub-repo
      - enabled: true
        name: search
      - enabled: true
        name: management-ingress
      - enabled: true
        name: console
      - enabled: true
        name: insights
      - enabled: true
        name: grc
      - enabled: true
        name: cluster-lifecycle
      - enabled: true
        name: volsync
      - enabled: true
        name: multicluster-engine
      - enabled: false
        name: cluster-proxy-addon
      - enabled: true
        name: cluster-backup
  separateCertificateManagement: false
```

OADP を手動でインストールした場合は、アップグレードする前に OADP を手動でアンインストールする必要があります。アップグレードが成功し、バックアップおよび復元が再度有効になると、OADP が自動的にインストールされます。

1.2.8.6. 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リストア Operator の有効化 トピックの **新規ハブクラスターの準備** を参照してください。

1.2.8.7. 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。

1.2.8.8. DataProtectionApplication リソースを作成するとエラーが発生する

OADP 1.0 で **DataProtectionApplication** リソースを作成すると、リソースのステータスによって次のようなエラーメッセージが作成される場合があります。

```
Route.route.openshift.io "oadp-dpa-sample-1-aws-registry-route" is invalid: spec.host: Invalid value: "oadp-dpa-sample-1-aws-registry-route-open-cluster-management-backup.dns.name.here": must be no more than 63 characters
```

この問題を解決するには、**backupImages** パラメーターを **false** に設定します。以下の例を参照してください。

```
apiVersion: oadp.openshift.io/v1alpha1
kind: DataProtectionApplication
metadata:
  name: oadp-dpa-sample-1
  namespace: open-cluster-management-backup
spec:
  backupImages: false
  backupLocations:
```

1.2.9. Submariner の既知の問題

1.2.9.1. Globalnet を使用する場合には、OpenShift SDN のみが CNI ネットワークプロバイダーとしてサポートされる

Globalnet を使用していない限り、OpenShift SDN と OVN Kubernetes CNI ネットワークの両方を Submariner で使用できます。Globalnet を使用する場合には、OpenShift SDN のみがサポートされます。

1.2.9.2. 一部の Red Hat Enterprise Linux ノードはワーカーノードとしてサポートされていない

カーネルバージョンが 4.18.0-359.el8.x86_64 から 4.18.0-372.11.1.el8_6.x86_64 の Red Hat Enterprise Linux ワーカー ノードを含むクラスターに Submariner をデプロイすると、アプリケーションワークロードがリモートクラスターとの通信に失敗します。

1.2.9.3. 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ー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ー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。

1.2.9.4. Red Hat Advanced Cluster Management コンソールからの Red Hat OpenStack Platform インフラストラクチャーの作成はサポートされていない

Red Hat OpenStack クラスターの自動クラウド準備は、product-title-short} コンソールの Submariner ではサポートされていません。Red Hat Advanced Cluster Management API を使用して、クラウドを手動で準備できます。

1.2.9.5. Globalnet を使用したヘッドレスサービスはサポートされない場合がある

clusterset.local ドメイン名を使用して、同じクラスターに存在するクライアントからエクスポートされたヘッドレスサービスにアクセスする場合を除き、Globalnet でヘッドレスサービスを使用できます。**clusterset.local** ドメイン名を使用してヘッドレスサービスにアクセスすると、ヘッドレスサービスに関連付けられている **globalIP** はクラスター内でルーティングできず、クライアントに返されます。

cluster.local ドメイン名を使用して、ローカルのヘッドレスサービスにアクセスできます。

1.2.9.6. エアギャップクラスターはサポートされていない

Submariner は、エアギャップ環境でプロビジョニングされたクラスターに対して検証されていません。

1.2.9.7. 多数のゲートウェイをデプロイできない

複数のゲートウェイをデプロイできません。

1.2.9.8. 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。

1.2.9.9. OVN Kubernetes サポートの制限

OVN Kubernetes CNI ネットワークプロバイダーを使用するには、Red Hat OpenShift 4.11 以降が必要です。OVN Kubernetes は Globalnet をサポートしていません。

1.2.9.10. グローバルネットの制限

Globalnet は、Red Hat OpenShift Data Foundation ディザスターリカバリーソリューションではサポートされていません。局地的なディザスターリカバリーシナリオでは、各クラスター内のクラスターとサービスネットワークに重複しない範囲のプライベート IP アドレスを使用するようにしてください。

1.2.9.11. Microsoft Azure クラスターセット名の長さの制限

Microsoft Azure マネージドクラスターセット名の長さは 20 文字以下にする必要があります。

1.2.9.12. Red Hat OpenShift Container Platform 4.12 は Microsoft Azure ではサポートされない

Microsoft Azure 上の OpenShift Container Platform 4.12 は、ゲートウェイノードの問題によりサポートされていません。

1.3. 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。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。

重要: 参照できるように、エラータ リンクと GitHub 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。

1.3.1. Errata 2.6.8

- 1 つ以上の製品コンテナー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。

1.3.2. Errata 2.6.7

- 1 つ以上の製品コンテナー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。

1.3.3. Errata 2.6.6

- 1 つ以上の製品コンテナー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。

1.3.4. Errata 2.6.5

- パフォーマンスを向上させるために、検索ドロップダウンに表示されるデフォルトのイメージ数を 2500 に減らします。(ACM-2800)
- **must-gather** コマンドは Red Hat OpenShift Container Platform のバージョン番号を収集するようになりました。(ACM-2857)
- **MEMCACHED** インデックスの **max_item_size** 設定がすべての **MEMCACHED** クライアントに変更を反映しない原因となった問題を修正します。(ACM-4684)

1.3.5. エラータ 2.6.4

- **spec.upgrade.monitorTimeout** 設定を **ClusterCurator** API に追加することで、**ClusterCurator** のアップグレードがタイムアウトする問題が修正されます。(ACM-2024)
- 操作の完了後に **ClusterCurator** カスタムリソースの **spec** 変更を回避することで、**ClusterCurator** を ArgoCD などの GitOps ツールで使用できるようにします。(ACM-2197)

1.3.6. エラータ 2.6.3

- 特定のキーと値を持つカスタムラベルをポリシーに追加すると、すべてのポリシーでサービス拒否が発生する問題を修正します。
- ArgoCD のインストールおよび部分的な設定後にアプリケーションが使用できなくなる問題を修正します。

- **open-cluster-management-agent** の **ClusterRoleBindings** が連続して作成される原因となっていたバグを修正します。(Bugzilla #2134796)

1.3.7. エラータ 2.6.2

- マネージドクラスターで **klusterlet-work-agent** が nil ポインターパニックをログに記録する原因となった問題を修正します。(Bugzilla #2041540)
- 特定の **Role** または **ClusterRole** オブジェクトが準拠していないと誤って表示する **inform musthave ConfigurationPolicy** の原因となったバグを修正し、**enforce** 動作を改善します。(Bugzilla #2041540)
- ポリシーで指定されたオブジェクトの検証手順を更新して、無限ループを回避します。(Bugzilla #2041540)

1.3.8. エラータ 2.6.1

- 1 つ以上の製品コンテナー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。

1.4. 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、代わ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 2.4 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。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。

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ー	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
BareMetalAsset	BareMetalAsset **v1alpha1** API は廃止されました。	2.6	この API は使用しないでください。	なし
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ー	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.apps.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	**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。	2.4	**V1beta1** を使用してください。	なし
ManagedClusterSetBindings	**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。	2.4	**V1beta1** を使用してください。	なし

1.4.1.2. API の削除

製品またはカテゴリー	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
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

製品またはカテゴリー	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
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
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ー	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
コンソール	スタンドアロン Web コンソール	2.6	統合 Web コンソールを使用します。	パースペクティブスイッチャーから起動します。詳しくは コンソールへのアクセス を参照してください。
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。
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	インストールの設定については、高度な設定 を参照してください。

製品またはカテゴリー	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	シークレットの管理	2.4	代わりに、シークレットにポリシーハブテンプレートを使用してください。	セキュリティーポリシーの管理 を参照してください。
ガバナンスコンソール	**pod-security-policy**	2.4	なし	なし
ガバナンス	Gatekeeper operator	2.6	代わりにサブスクリプションでインストールしてください。	gatekeeper Operator ポリシーの管理 ポリシー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、代わり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ー	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	ManifestWork	2.6	なし	なし
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。	詳細は コンソールを使用したクラスターでの実行用の AnsibleJob テンプレート設定 を参照してください。
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
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。

製品またはカテゴリー	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
Red Hat Advanced Cluster Management コンソール	Visual Web ターミナル (テクノロジープレビュー)	2.4	代わりにターミナルを使用してください。	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。

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

- 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ー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、コンテナー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、コンテナー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 チャネルがある場合は、Slack の公開コミュニティー
- 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
- 技術コミュニティーでの公開会話

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。

コンテナー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ー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ーを使用して設定 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。このプロパティーには、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ー確保について、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 をバッキングストアとして使用します。

- **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ーを確保できます。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のある 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のある 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 の FIPS readiness が完了しました。Red Hat Advanced Cluster Management は、同じツールを使用して、Red Hat OpenShift Container Platform で使用される Red Hat Enterprise Linux (RHEL) 認定暗号化モジュールに暗号化呼び出しが渡されるようにします。OpenShift の FIPS サポートの詳細は、FIPS 暗号のサポート 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場合は、ハブクラスターで作成された暗号化がマネージドクラスターに保存されるため、FIPS 対応のハブクラスターが必要です。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** 設定で FIPS を有効にします。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。

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** アーキテクチャーでのみ FIPS をサポートします。
- Integrity Shield は、FIPS に対応していないテクノロジープレビューコンポーネントです。
- 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 はストレージの暗号化を提供しません。OpenShift Container Platform ドキュメント Support for FIPS cryptography 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.