# Red Hat Advanced Cluster Management for Kubernetes 2.7

## 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: 2024-03-21

# Red Hat Advanced Cluster Management for Kubernetes 2.7 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



## 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。バージョン 2.4 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。

- 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. Web コンソール

- 検索設定可能なコレクションを使用して、ハブクラスターおよびマネージドクラスターによって収集される Kubernetes リソースを管理します。詳しくは、設定可能な検索コレクションの作成 を参照してください。

- OpenShift Container Platform モニタリングを使用してユーザー定義のメトリックを収集します。詳細については、ユーザーワークロードメトリックの追加 を参照してください。
- **search.search.open-cluster-management.io** という名前の新しいカスタムリソース定義が検索機能に追加されます。検索をさらにカスタマイズするには、詳細について、検索のカスタマイズと設定 を参照してください。
- PostgreSQL データベースのストレージと設定を編集して、検索を最適化します。検索のカスタマイズと設定 を参照してください。
- Grafana でマネージドクラスターラベルを使用できるようになりました。Grafana でマネージドクラスターラベルを使用する を参照してください。

### 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、クラスターフリート管理を強化するソフトウェア Operator であるマルチクラスターエンジン Operator 内で文書化されています。

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 の前提条件ですが、Red Hat Advanced Cluster Management はそうではありません。

クラスター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。

### 1.1.3. アプリケーション

これで、**LeaderElection** を使用して、障害が発生した場合にコントローラーが新しいリーダーを選択するようにリクエストする方法を変更できるようになりました。これにより、一度に 1 つのリーダーインスタンスのみが調整を処理することが保証されます。コントローラーが **LeaderElection** を取得するのにかかる時間を増減できます。リーダー選択の設定 を参照してください。

**AnsibleJob** カスタムリソースを使用して、Ansible Automation Platform ワークフローを起動できるようになりました。**job_template_name** フィールドを **workflow_template_name** に置き換えて、一連のジョブを追跡します。Ansible Automation Platform 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。

### 1.1.4. ガバナンス

- 自動化からポリシー違反の詳細を受け取ることができます。ガバナンスの自動化設定 を参照してください。
- ログは、**ManagedClusterAddOn** リソースを使用してポリシーコントローラー名で区別されるようになりました。デバッグログの設定 を参照してください。
- ポリシーフレームワークは、依存関係を使用したポリシーまたはポリシーテンプレートのアクティブ化をサポートするようになりました。ポリシーの依存関係 を参照してください。
- ポリシージェネレーターは、柔軟性を高めるために、ローカルおよびリモートの Kustomize 設定を参照するようになりました。詳細は、ポリシージェネレーター を参照してください。
- テンプレート処理を自動的に調整するようにハブクラスターテンプレートを設定します。たとえば、シークレットやその他のリソースをハブクラスターからマネージドクラスターに同期します。再処理のための特別なアノテーション を参照してください。

- 処理後にテンプレート文字列を囲む引用符を削除するには、**toLiteral** 関数を使用します。詳細については、**toLiteral** 関数 を参照してください。

- OpenShift GitOps (ArgoCD) を使用してポリシー定義を管理できます。OpenShift GitOps (ArgoCD) を使用したポリシー定義の管理 を参照してください。

- **History** 列のオブジェクトにパッチを適用するポリシーのステータスイベントを受け取るようになりました。詳細については、ガバナンス ページ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

- restic および rclone ムーバーは、デフォルトで非ルートとして実行されるようになり、SE Linux 機能がなくなりました。restic と rclone のムーバー Pod は、namespace 内の Pod が制限された権限で実行されることを Pod Security Standards が必要としない場合、namespace に対する昇格権限を必要としません。

- 新しい Submariner **LoadBalancer** モードを使用すると、Microsoft Azure Red Hat OpenShift クラスターおよび Red Hat OpenShift Service on AWS クラスターのデプロイを簡素化できます。詳細については、コンソールを使用した Submariner 用の Microsoft Azure Red Hat OpenShift の準備 (テクノロジープレビュー) および コンソールを使用して Red Hat OpenShift Service on AWS で Submariner を準備する (テクノロジープレビュー) を参照してください。

- Submariner は、セキュリティー上の懸念を軽減できるように、非接続クラスターをサポートするようになりました。詳細については、非接続クラスターへの Submariner のデプロイ を参照してください。

### 1.1.6. バックアップおよび復元

- 管理されたサービスアカウントコンポーネントを使用して、インポートされたクラスターを新しいハブクラスターに自動的に接続できます。詳細については、マネージドサービスアカウントを使用してクラスターを自動的に接続する を参照してください。

### 1.1.7. 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ーからの相互作用、成長、および貢献のために、オープンソースの **Open Cluster Management** リポジトリーにアクセスします。open-cluster-management.io を参照してください。詳細については、GitHub リポジトリー にアクセスしてください。

## 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。

非推奨と削除の詳細は、リリースノートの 非推奨と削除 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
  - 可観測性の既知の問題
- クラスター管理の既知の問題
- アプリケーション管理の既知の問題
- ガバナンスの既知の問題
- バックアップおよび復元の既知の問題
- Submariner 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/2.7/html/add-ons/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/2.7/html-single/add-ons/index#volsync** のようになります。
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. デプロイされたリソースをアップグレード後に表示するには、RBAC ユーザーに追加のロールとロールバインディングが必要である

Red Hat Advanced Cluster Management バージョン 2.7 にアップグレードすると、**apps.open-cluster-management.io** グループ内のリソースに対するユーザー権限が利用できなくなります。Red Hat Advanced Cluster Management バージョン 2.7 以降、これらのカスタムリソース定義が OLM によってデプロイされなくなり、以下の変更が行われました。

1. リソース作成に選択できるカードとして、Red Hat Advanced Cluster Management サブスクリプションコンソールビューでリソースタイプが使用できなくなりました。

2. デフォルトロールに割り当てられた集計ルールを持つ **clusterroles** は、API リソースの種類には適用されません。

RBAC ユーザーがこれらのリソースにアクセスする必要がある場合は、適切な権限を付与する必要があります。

#### 1.2.2.2. 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
```

#### 1.2.2.3. 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。

#### 1.2.2.4. 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。

#### 1.2.2.5. 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。

#### 1.2.3.6. 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、ブラウザー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。

#### 1.2.3.7. Red Hat Ansible Automation Platform Operator との統合使用時のエラー

Ansible Automation Platform Operator に依存する統合を使用していて、Red Hat OpenShift Container Platform クラスターにインストールされている Operator を表示する権限がない場合は、次のようなエラーメッセージが表示される場合があります。

**The Ansible Automation Platform Operator is required to use automation templates.Version 2.2.1 or greater is required to use workflow job templates in automation templates.**

Operator がインストールされていることをシステム管理者に確認した場合は、エラーメッセージを無視しても問題ありません。

### 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/Namespace(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。

#### 1.2.4.4. 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。

#### 1.2.4.5. 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。

#### 1.2.4.6. 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。

#### 1.2.4.7. 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。

#### 1.2.4.8. 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。

#### 1.2.4.9. 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
```

#### 1.2.4.10. 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
```

#### 1.2.4.11. 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。

#### 1.2.4.12. 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
```

#### 1.2.4.13. 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。

### 1.2.5. クラスター管理の既知の問題

クラスター管理または **クラスターライフサイクル** は、Red Hat Advanced Cluster Management の有無にかかわらず、マルチクラスターエンジン Operator によって提供されます。Red Hat Advanced Cluster Management のみに適用されるクラスター管理に関する以下の既知の問題と制限事項を参照してください。ほとんどのクラスター管理の既知の問題は 、クラスターライフサイクルに関する既知の問題 のクラスターライフサイクルドキュメントにあります。

#### 1.2.5.1. IBM Power または IBM Z システムハブクラスターとの Ansible Automation Platform 統合を使用できない

Red Hat Advanced Cluster Management for Kubernetes ハブクラスターが IBM Power または IBM Z システムで実行されている場合、Ansible Automation Platform Resource Operator は **ppc64le** および **s390x** イメージを提供しないため、Ansible Automation Platform 統合を使用することはできません。

### 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. ブロック状態のアプリケーション

アプリケーションが **blocked** 状態にある場合、サブスクリプションにはクラスターがオフラインであると表示されますが、クラスターは **healthy** および **ready** 状態にあります。

#### 1.2.6.2. 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。

#### 1.2.6.3. 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。

#### 1.2.6.4. 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。

#### 1.2.6.5. 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。

#### 1.2.6.6. 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。

#### 1.2.6.7. 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。

#### 1.2.6.8. 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。

#### 1.2.6.9. 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。

#### 1.2.6.10. 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 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
```

#### 1.2.6.11. 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。

#### 1.2.6.12. 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。

#### 1.2.6.13. Ansible Automation Platform Operator は、プロキシー外の Ansible Automation Platform にアクセスする

Red Hat Ansible Automation Platform Operator は、プロキシー対応の 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、プロキシー内に 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。

#### 1.2.6.14. 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

2.7 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. 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。

### 1.2.7. ガバナンス関連の既知の問題

### 1.2.8. ポリシージェネレーターによって ignorePending フラグが無視される

ポリシージェネレーターで **consolidateManifests: true** を 設定した場合、**ignorePending** フラグは無視されます。

**ignorePending** 関数を実装する必要がある場合は、**consolidateManifests: false** を設定できます。

#### 1.2.8.1. 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。

#### 1.2.8.2. 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。

#### 1.2.8.3. 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。

#### 1.2.8.4. 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

#### 1.2.8.5. 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。

### 1.2.9. 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 **DeleteIfCreated** 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。

#### 1.2.9.1. 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。これは、次の 2 つの場合に発生する可能性があります。

- 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。

  既知の例:

| Kind | 問題の説明 |
| --- | --- |
| **PodSecurityPolicy** | Kubernetes は、値が **false** に設定されたキーを削除します。これは、マネージドクラスター上の結果のオブジェクトで確認できます。この場合、ポリシーの **objectDefinition** からキーを削除します。 |
| **Secret** | **stringData** マップは Kubernetes によって処理され、**base64** でエンコードされた値を持つ **data** になります。**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。 |

#### 1.2.9.2. 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。

#### 1.2.9.3. 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
```

### 1.2.10. 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。

1. 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}
```

2. 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}
```

### 1.2.11. バックアップおよび復元の既知の問題

#### 1.2.11.1. 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。

#### 1.2.11.2. 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。

詳細については、バックアップおよび復元 Operator の管理 トピックの **復元前のハブクラスターのクリーニング** を参照してください。

#### 1.2.11.3. 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。

#### 1.2.11.4. 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 2.6 から 2.7 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。

#### 1.2.11.5. 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 の管理 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。

#### 1.2.11.6. 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。

#### 1.2.11.7. 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。詳細については、マネージドサービスアカウントを使用してクラスターを自動的に接続する を参照してください。

#### 1.2.11.8. 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とき、**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ルール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>
```

#### 1.2.11.9. 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とき、**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ルール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>
```

#### 1.2.11.10. appliedmanifestwork が削除されず、agentID が仕様にない

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'"}}'
   ```

#### 1.2.11.11. 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。

### 1.2.12. Submariner の既知の問題

#### 1.2.12.1. 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。

#### 1.2.12.2. 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。

#### 1.2.12.3. 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。

#### 1.2.12.4. 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。

#### 1.2.12.5. 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。

#### 1.2.12.6. 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。

#### 1.2.12.7. 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
```

#### 1.2.12.8. 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。

#### 1.2.12.9. 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。

### 1.2.13. 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** のクラスターセレ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。

#### 1.2.13.1. 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するには、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 **stable-0.14** に設定する必要があります。

## 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. エラータ 2.9.1

- 外部エンドポイントの Kubernetes シークレットを作成するときに **tlsSecretMountPath** が機能しなくなる問題を修正しました。(ACM-7717)
- 1 つ以上の製品コンテナーイメージに更新を配信します。

### 1.3.2. Errata 2.7.11

- 1 つ以上の製品コンテナーイメージに更新を配信します。

### 1.3.3. Errata 2.7.10

- 1 つ以上の製品コンテナーイメージに更新を配信します。

- Pod が誤ったレジストリーからイメージをプルする原因となっていた問題を修正します。(ACM-6615)
- 空の **ラベル** パラメーターが原因でポリシーが認識されない原因となっていた問題を修正します。(ACM-7055)
- ポリシーテンプレートの変更により、マージ不整合が生じたり、コントローラーが応答しなくなる問題を修正しました。(ACM-7799)

### 1.3.4. Errata 2.7.9

- 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。

### 1.3.5. Errata 2.7.8

- 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。

### 1.3.6. Errata 2.7.7

- 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。
- マネージドクラスターを Red Hat Advanced Cluster Management for Kubernetes に追加する際に **enableUserWorkload: true** 設定が削除される原因となっていた問題が修正されました。(ACM-3938)
- 管理 Pod が予約コアに固定されず、正しいアノテーションを見逃す問題を修正します。(ACM-5110)
- 検索インデクサーがエラーを報告する原因となっていた問題を修正します。(ACM-5168)
- **enableUserWorkload: true** 設定を削除するときに **uwl-metrics-controller** デプロイメントが自動的に削除されない問題を修正します。(ACM-5268)
- コンソールの **Create cluster** ボタンおよび **Import cluster** ボタンを無効にした **APIService** の問題を修正します。(ACM-5460)
- アラート転送を無効にするときに **hub-alertmanager-router-ca** シークレットおよび **observability-alertmanager-accessor** シークレットを削除する問題を修正します。(ACM-5623)
- ハブクラスターのリカバリー中に、サブスクリプションベースのワークロードに関連付けられた管理対象リソースが削除される原因となっていた問題を修正します。(ACM-5795)

### 1.3.7. Errata 2.7.6

- マネージドクラスターカスタムリソースでハブクラスターテンプレート関数を使用するポリシーのルートポリシーのステータスを修正します。(ACM-5547)
- ハブクラスターのポリシーと、マネージドクラスターのポリシー間でステータスが一致しなくなる問題を修正します。(ACM-6042)

### 1.3.8. Errata 2.7.5

- 1 つ以上の製品コンテナーイメージに更新を配信します。

### 1.3.9. Errata 2.7.4

- 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。

### 1.3.10. Errata 2.7.3

- アプリケーションの数が多い場合でも、**Applications** サイドバーの読み込みが速くなりました。(ACM-2503)
- Red Hat OpenShift Container Platform クラスター全体のプロキシーが有効になっている場合に、**cluster-proxy-addon** を使用できなくなる問題を修正しました。(ACM-3208)
- ガバナンスリソースが空のフィールドなしで、一貫性のないコンプライアンスステータスで作成される原因となった問題を修正します。(ACM-3424)
- **ClusterIP** サービスは、準備ができた場合にのみ解決されるようになりました。(ACM-3751)
- **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-4685)

### 1.3.11. Errata 2.7.2

- Microsoft Azure での Red Hat OpenShift Container Platform 4.12 の使用のサポートを追加します。(ACM-3223)
- ポリシーテンプレートで 1 行を超える YAML コンテンツのサポートを追加します。(ACM-3517)

### 1.3.12. エラータ 2.7.1

- マネージドクラスターがオンラインであってもトポロジーでオフラインと表示される原因となっていたコンソールの問題を修正します。(ACM-3466)

## 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 2.3 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 2.3 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。

**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 |
|---|---|---|---|---|
| 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 | **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 |
| 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。 | 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 |
|---|---|---|---|---|
| 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。 | |

| 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 |
|---|---|---|---|---|
| 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 |
| 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 |
| 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 |
|---|---|---|---|---|
| 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 |
|---|---|---|---|---|
| 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 **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。 |

| 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 |
|---|---|---|---|---|
| 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。 |
| 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 |
| インストーラー | **operator.open-cluster-management.io_multiclusterhubs_crd.yaml** の別の cert-manager の設定 | 2.3 | なし | なし |

### 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 |
|---|---|---|---|---|

| 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 |
|---|---|---|---|---|
| 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 |
| 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 | コミュニティー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 |

| 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 | 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。 |
| 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。 |
| 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。 |
| 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 |
| アプリケーション | 単一の ArgoCD インポートモード。ハブクラスターの Argo CD サーバーにインポートされるシークレット。 | 2.3 | クラスターシークレットは、複数の ArgoCD サーバーにインポートできます。 | 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 | ArgoCD クラスター統合: **spec.applicationManager.argocdCluster** | 2.3 | マネージドクラスターを登録する GitOps クラスターおよび配置カスタムリソースを作成します。 | マネージドクラスターでの GitOps の設定 |
| ガバナンス | **cert-manager** の内部証明書管理 | 2.3 | アクションは不要です。 | 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 | 整合性シールド (テクノロジープレビュー) | 2.7 | なし | コミュニティー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。 |

## 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



### 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 は FIPS 用に設計されています。FIPS モードの Red Hat OpenShift Container Platform で実行している場合、OpenShift Container Platform は、OpenShift Container Platform でサポートされるアーキテクチャーのみで FIPS Validation 用に NIST に送信される Red Hat Enterprise Linux 暗号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がある場合は、FIPS モードで動作するように設定された 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され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** を設定します。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.

### 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。