# Red Hat Advanced Cluster Management for Kubernetes 2.3

## 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: 2023-03-19

# Red Hat Advanced Cluster Management for Kubernetes 2.3 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。

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

## 法律上の通知



## 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

Red Hat Advanced Cluster Management の 2.1 バージョンが **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がなくても非推奨になります。以前のバージョンのドキュメントもサポートされていません。

- 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

## 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展開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
  - 可観測性
- クラスター
- アプリケーション
- ガバナンス

### 1.1.1. Web コンソール

- サイドバーナビゲーションに変更が加えられ、他の製品と合わせることでユーザーエクスペリエンスが向上されました。ナビゲーションから、さまざまな製品機能にアクセスできます。

ヘッダーを使用すると、Red Hat OpenShift Container Platform、検索、**Configure client** ページに簡単にアクセスし、**About modal** などを表示できるようになります。

- **テクノロジープレビュー:** ナビゲーションから Visual Web ターミナルにアクセスできます。

#### 1.1.1.1. 可観測性

- Red Hat Advanced Cluster Management の可観測性サービスは、Grafana の 7.4.2 をサポートします。詳細は、「可観測性サービス」のセクションを参照してください。
- コンポーネントごとに、可観測性ストレージのサイズを設定できるようになりました。詳細は、MultiClusterObservability CR の作成 を参照してください
- 可観測性の API ストレージバージョンは **v1beta2** になりました。**v1beta2** バージョンは、**v1beta1** と **v1beta2** カスタムリソース定義の両方を取得します。
- 可観測性サービスに記録ルールを追加して、集約クエリー式から取得する、新しいメトリクスを指定できるようになりました。詳細は、「カスタムメトリクスの追加」を参照してください。
- **MultiClusterObservability** カスタムリソースで **詳細** 設定をカスタマイズできるようになりました。詳細は、 **詳細** 設定の追加 を参照してください。
- デフォルトのメトリクスを削除できるようになりました。詳細は、「デフォルトメトリクスの削除」を参照してください。
- Red Hat Insights で、接続クラスターで発生する可能性のある問題についての情報を受信できるようになりました。詳細は、「Red Hat Insights での可観測性 」を参照してください。
- Grafana コンソールから **etcd** ダッシュボードを表示できるようになりました。「etcd テーブルの表示」を参照してください。
- Single Node OpenShift (SNO) クラスターから送信されるメトリクスを SNO ラベルで識別できるようになりました。詳細は、「データの表示および展開」を参照してください。
- 独自 (BYO: Bring Your Own) の可観測性認証局 (CA) 証明書を使用できるようになりました。詳細は、「独自 (BYO: Bring Your Own) の可観測性認証局 (CA) 証明書 」を参照してください。
- 可観測性 Pod のレプリカ数を更新できるようになりました。詳細は、「コンソールからの **multiclusterobservability** CR レプリカの更新」を参照してください。
- Red Hat Advanced Cluster Management ハブクラスターで、マネージドクラスターから **Alertmanager** にアラートを転送できるようになりました。詳細は、「送信アラート」を参照してください。
- 外部 API で OpenShift Container Platform ルート (**rbac-query-proxy**) を使用してメトリクスをクエリーできます。詳細は、「外部メトリクスクエリーの使用」を参照してください。

### 1.1.2. クラスター

- Red Hat Advanced Cluster Management コンソールでのクラスターのアップグレードに、OpenShift Container Platform バージョン 4.6 以降のチャネルを選択できるようになりました。チャネルを選択すると、お使いのクラスターに利用可能なアップグレードが通知されます。詳細は、「チャネルの選択」を参照してください。

- コンソールでクラスターの作成プロセスが更新され、より直感的に操作をすすめることができます。詳細は、「クラスターの作成」を参照してください。
- HiveConfig リソースを直接編集できるようになり、**MultiClusterHub Operator** では変更を元に戻せません。HiveConfig リソースが削除されると、**MultiClusterHub** Operator は **MultiClusterHub** リソースの初回作成時に以前の設定通りに再作成します。
- ハブクラスターで認証情報を更新すると、マネージドクラスターで自動的に更新されるようになりました。
- Red Hat Advanced Cluster Management コンソールからマネージドクラスターを使用して Red Hat OpenStack Platform で OpenShift Container Platform のマネージドクラスターを作成できるようになりました。詳細は、「Red Hat OpenStack Platform でのクラスターの作成」を参照してください。
- OpenShift Container Platform クラスターを管理対象としてインポートして、IBM Power システムでホストできるようになりました。
- **BareMetalAsset** CR および Red Hat Advanced Cluster Management Web コンソールを使用してベアメタルアセットを管理する情報を追加しました。詳細は、ベアメタルアセットの作成および変更 を参照してください。

#### 1.1.2.1. クラスター (テクノロジープレビュー)

本リリースでは、以下の機能は **テクノロジープレビュー機能** です。

- IBM Power システムでハブクラスターをホストする機能をテストできます。
- **ManagedClusterSet** でリソースをグループ化して、マネージドクラスター、クラスタープール、クラスターデプロイメント、およびクラスター要求の RBAC アクセスパーミッションを制御できます。詳細は、ManagedClusterSets (テクノロジープレビュー) のドキュメントを参照してください。
- マネージドクラスターのインストールまたはアップグレードを開始するように、**AnsibleJob** テンプレートを設定できるようになりました。詳細は、「マネージドクラスターで実行する Ansible Tower タスクの設定」を参照してください。
- クラスタープールを作成して、リソースの管理を向上し、必要に応じて OpenShift Container Platform クラスターを要求できるようになりました。詳細は、「クラスタープールの管理」を参照してください。
- Red Hat Advanced Cluster Management で作成された特定の OpenShift Container Platform マネージドクラスターを休止して、より柔軟にリソースを管理できます。詳細は、「作成したクラスターの休止」を参照してください。
- VMware vSphere および Google Cloud Platform マネージドクラスターで Submariner ネットワークサービスを設定できるようになりました。サービスの詳細は、Submariner を参照してください。
- Red Hat Advanced Cluster Management コンソールを使用して、クラスターに Submariner をデプロイできるようになりました。詳細は、「コンソールを使用した Submariner のデプロイ」を参照してください。
- **MachinePools** リソースを使用して、Red Hat Advanced Cluster Management またはコマンドラインからクラスターをスケーリングできます。詳細は、「Resizing a cluster」を参照してください。

- OpenShift Cluster Manager で利用可能な OpenShift Container Platform 4 クラスターを検出できます。クラスターの検出後に、クラスターをインポートして管理できます。詳細は、Discovery サービスの概要 (テクノロジープレビュー) を参照してください。

### 1.1.3. アプリケーション

- **Search** ページから表示するアプリケーションを選択したら、**Applications** ページに移動します。詳細は、「ArgoCD アプリケーションのクエリー」を参照してください。
- Red Hat Advanced Cluster Management がインストールされている OpenShift Container Platform クラスターに Argo アプリケーションをデプロイする場合には、Argo アプリケーションを **アプリケーション** テーブルおよび **Topology** ビューで可視化できるようになりました。
- **Overview** または **Topology** の概要から、Argo エディターを起動し、Argo アプリケーションを管理できます。
- アプリケーションコンソールの強化機能として他に、Git リポジトリーのチャネルタイプに固有の **Commit hash** と **Tag** が含まれます。さらに、新規の調整入力が Git と Helm リポジトリータイプの両方に追加されます。
- チャネル設定で、不要なリソースの調整を回避するために調整頻度オプション (high、medium、low、off) を選択できるようになり、サブスクリプション Operator のオーバーロードを防ぐことができます。詳細は、「Git リソースのサブスクライブ」の **調整オプション** を参照してください。
- **リポジトリーの調整レート** は、デフォルト値が **medium** に設定された状態でコンソールに追加されます。自動調整が無効になっている場合は、リソースによるマージや、現在調整された設定の置き換えがないため、調整オプションは表示されません。
- サブスクリプションを設定して、Amazon Simple Storage Service (Amazon S3) オブジェクトストレージサービスで定義したリソースをサブスクライブできます。詳細は、Object Storage リポジトリーを使用したアプリケーションの管理 を参照してください。
- コンソールから、**ApplicationSet** 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す **ApplicationSet** を表示できます。アプリケーションコンソールの詳細は、「アプリケーションコンソールの概要 」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

- 設定ポリシーにテンプレートを追加したり、含めることが可能になりました。詳細は、「設定ポリシーでのテンプレートのサポート」を参照してください。
- Red Hat Advanced Cluster Management は、Red Hat OpenShift Container Platform Service Serving 証明書を使用するようになりました。詳細は、「証明書」を参照してください。
- Ansible Tower でポリシー違反の自動化を作成できるようになりました。詳細は、「Ansible Tower でのガバナンスの設定」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。

詳細は、『リリースノート』を参照してください。

## 1.2. エラータの更新

デフォルトでは、エラータの更新はリリース時に自動的に適用されます。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。2.3 の場合には、この一覧には、FIPS 承認**されていない**暗号が 2 つ含まれます。バージョン 2.3.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。

### 1.2.1. Errata 2.3.12

- 1 つ以上の製品コンテナーイメージおよびセキュリティー修正に更新を配信します。

### 1.2.2. Errata 2.3.11

- バージョン 2.2 からのアップグレード後に正しくない Pod 名が原因で可観測性が失敗することがありました。(Bugzilla #2087277)
- 1 つ以上の製品コンテナーイメージおよびセキュリティー修正に更新を配信します。

### 1.2.3. Errata 2.3.10

- 1 つ以上の製品コンテナーイメージおよびセキュリティー修正に更新を配信します。

### 1.2.4. Errata 2.3.9

- 1 つ以上の製品コンテナーイメージおよびセキュリティー修正に更新を配信します。

### 1.2.5. Errata 2.3.8

- 1 つ以上の製品コンテナーイメージおよびセキュリティー修正に更新を配信します。

### 1.2.6. Errata 2.3.7

- 1 つ以上の製品コンテナーイメージおよびセキュリティー修正に更新を配信します。

### 1.2.7. Errata 2.3.6

- 直前のバージョンの CRD の情報が更新されていないことを提案するアップグレード時のエラーを修正します。(Bugzilla #2015663)
- 最近アップグレードしたマネージドクラスターで、限られた帯域幅の発生する問題を解決します。(Bugzilla #2021128)
- Red Hat Advanced Cluster Management をバージョン 2.3.5 から 2.3.6 にアップグレードした後、マネージドクラスターのアドオンが Red Hat Advanced Cluster Management コンソールに表示されませんでした。(Bugzilla #2050847)
- 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。

### 1.2.8. Errata 2.3.5

- 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。

### 1.2.9. Errata 2.3.4

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.3.4 の更新について以下に一覧としてまとめています。

- Red Hat OpenShift Container Platform バージョン 4.9 で Red Hat Advanced Cluster Management バージョン 2.3 が正しく動作しない問題を修正します。バージョン 2.3.4 以降、OpenShift Container Platform バージョン 4.9 での実行時に Red Hat Advanced Cluster Management がサポートされるようになりました。(Bugzilla #1984470)

- Resource Optimization ダッシュボードが OpenShift Container Platform バージョン 4.9 クラスターの CPU 使用パネルにデータを表示できない問題が修正されました。(Bugzilla #2021766)

- 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。

### 1.2.10. エラータ 2.3.3

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.3.3 の更新について以下に一覧としてまとめています。

- ソース Git リポジトリーを含む **NO_PROXY** 設定が適用されないため、プロキシーが有効な場合にアプリケーションのサブスクリプションが失敗する原因となっていた問題が修正されました。(Bugzilla #2000951)

- VMware マネージドクラスターが、**VMware** セクションではなく、コンソールの **Overview** ページで**Other**というセクションに表示されていた問題を修正します。(Bugzilla #2004188)

- Grafana Pod のメモリ要件が、安定するのではなく、アクティブなクライアントで継続的に増加する原因となっていた問題を修正します。(GitHub #13382)

- Red Hat OpenShift Kubernetes Service (ROKS)にデプロイされる際に、OpenShift Container Platform ヘッダーバーからの Red Hat Advanced Cluster Management コンソールリンクを修正します。(GitHub #14353)

- **ppc64le** 環境で **management-ingress** Pod が複数回再起動することになる問題が修正されました。(GitHub #15729)

- **cluster-manager-admin** ロールを持つユーザーによるポリシー自動化の作成、編集、または削除を妨げていた問題が修正されました。(GitHub #15750)

- Red Hat Advanced Cluster Management バージョン 2.1 にデプロイしたアプリケーションが、Red Hat Advanced Cluster Management バージョン 2.3 にアップグレードした後にトポロジーを正しく表示しない問題が修正されました。(GitHub #15765)

- アップグレード後に一部のマネージドクラスターのパフォーマンスが低下したマルチクラスター可観測性 Operator の問題が修正されました。(GitHub #15996、#16123)

- 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。

### 1.2.11. エラータ 2.3.2

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.3.2 の更新について以下に一覧としてまとめています。

- コンソールから認証情報のドキュメントへのリンクが修正されました。(GitHub #14993)
- マルチクラスター可観測性オペランドが正常にアップグレードできない問題が修正されました。(Bugzilla #1993188)
- 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。

### 1.2.12. エラータ 2.3.1

いくつかの製品イメージの 2.3 バージョンの問題を修正します。

## 1.3. 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。以下の一覧には、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。

- 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

### 1.3.1. インストールの既知の問題

#### 1.3.1.1. OpenShift Container Platform バージョン 4.9 との互換性の問題

OpenShift Container Platform バージョン 4.9 と Red Hat Advanced Cluster Management バージョン 2.3 との互換性を判断するための機能テストが進行中です。互換性を確認するまでは、OpenShift Container Platform バージョン 4.9 で Red Hat Advanced Cluster Management バージョン 2.3 を使用する場合に互換性の問題が発生する可能性があります。

#### 1.3.1.2. バージョン 2.2.x から 2.3.1 へのアップグレードが進行しない

Red Hat Advanced Cluster Management をバージョン 2.2.x から 2.3.1 にアップグレードすると、アップグレードに失敗します。**Multiclusterhub** ステータスは、コンポーネントエラーメッセージに **failed to download chart from helm repo** を表示します。**no endpoints available for service "ocm-webhook"** 問題を参照するエラーも表示される場合があります。

ハブクラスターで、Red Hat Advanced Cluster Management がインストールされている namespace で以下のコマンドを実行し、デプロイメントを再起動してバージョン 2.3.1 にアップグレードします。

```
oc delete deploy ocm-proxyserver ocm-controller ocm-webhook multiclusterhub-repo
```

**注記:** エラーは解決しますが、調整プロセスはすぐに開始されない可能性があります。これは、製品がインストールされているのと同じ namespace で **multicluster-operators-standalone-subscription** を再起動して高速化できます。

#### 1.3.1.3. バージョン 2.3.0 から 2.3.1 へのアップグレードが ImagePullBackOff エラーで失敗する

Red Hat Advanced Cluster Management をバージョン 2.3.0 から 2.3.1 にアップグレードする場合、マネージドクラスターの **open-cluster-management-agent-addon** namespace の **klusterlet-addon-operator** Pod は **ImagePullBackOff** エラーを返します。

この問題を解決するには、ハブクラスターで以下の手順を実行し、バージョン 2.3.1 にアップグレードします。

1. 以下のコマンドを実行して **MultiClusterHub** マニフェストの **ConfigMap** を削除します。

```
oc delete cm -n open-cluster-management mch-image-manifest-2.3.0
```

2. 以下のコマンドを実行して、コントローラーの Pod を再起動します。

```
oc delete po -n open-cluster-management -lapp=klusterlet-addon-controller-v2
```

3. ハブの **open-cluster-management-observability** namespace の Grafana Pod を 2.3.0 から 2.3.1 にアップグレードすると **ImagePullBackOff** エラーを返す場合は、以下のコマンドを実行して Pod を再起動して正しいイメージを使用します。

```
oc delete po -n open-cluster-management -lname=multicluster-observability-operator
```

Red Hat Advanced Cluster Management バージョン 2.3.1 を実行しています。

#### 1.3.1.4. 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。

### 1.3.2. Web コンソールの既知の問題

#### 1.3.2.1. クラスターページと検索結果間のノードの不一致

**Cluster** ページに表示されているノード数と **Search** の結果で差異が生じる場合があります。

#### 1.3.2.2. 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。

#### 1.3.2.3. 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

この製品は、Linux、macOS、および Windows で利用可能な Mozilla Firefox 74.0 または最新バージョンをサポートします。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。

#### 1.3.2.4. 空白スペースを含めた値を使用して検索できない

コンソールおよび Visual Web ターミナルから、値に空白が含まれている場合には検索できません。

#### 1.3.2.5. kubeadmin がログアウトすると、空白ページのブラウザータブが開く

**kubeadmin** でログインしており、ドロップダウンメニューから **Log out** オプションをクリックすると、コンソールはログイン画面に戻りますが、**/logout** URL のブラウザータブが開きます。このページは空白であるため、コンソールに影響を与えずにタブを閉じることができます。

#### 1.3.2.6. シークレットの内容が表示されない

セキュリティー上の理由で、検索時にマネージドクラスターにあるシークレットの内容は表示されません。コンソールからシークレットを検索すると、以下のエラーメッセージが表示される場合があります。

```
Unable to load resource data - Check to make sure the cluster hosting this resource is online
```

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

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

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

### 1.3.3. 可観測性の既知の問題

#### 1.3.3.1. 可観測性エンドポイントオペレーターがイメージのプルに失敗する

可観測性エンドポイントオペレーターは、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拘らず、**open-cluster-management-observability** namespace にプルシークレットがない場合に問題が発生します。新しいクラスターをインポートする場合、または Red Hat Advanced Cluster Management で作成された Hive クラスターをインポートする場合は、マネージドクラスターにプルイメージシークレットを手動で作成する必要があります。

詳細は、「可観測性の有効化」を参照してください。

#### 1.3.3.2. ROKS クラスターにはデータがありません

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。

#### 1.3.3.3. ROKS クラスターに etcd データがない

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

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

クラスターを 1000 台管理するハブクラスターで検索が無効になっている場合に、**search-collector** Pod の CPU 使用率のレベルが通常よりも高くなります。4 日間の CPU 使用率は約 2.148Mi です。**search-collector** のレプリカ数を **0** に減して、メモリー使用量を減らすことができます。

#### 1.3.3.5. 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。

#### 1.3.3.6. Grafana コンソールでメトリクスが利用できない

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

  **"annotation Query Failed"**

  ブラウザーを更新し、ハブクラスターにログインしていることを確認します。

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

  **no project or cluster found**

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

#### 1.3.3.7. クラスターは 2.3.2 へのアップグレード後の低下です。

可観測性が有効化されている 2.3.2 にアップグレードする場合は、可観測性アドオンが準備状態にないため、一部のクラスターのパフォーマンスが低下します。**multicluster-observability-operator** Pod を再起動するには、以下のコマンドを実行します。

```
oc delete po multicluster-observability-operator -n open-cluster-management
```

可観測性 Pod が再作成されます。

#### 1.3.3.8. 可観測性のステートフルセットが、非接続環境で誤ったイメージを使用する

まれに、非接続環境では、Pod がイメージをプルできないため、可観測性 **StatefulSet** の一部の Pod が次のステータス **ErrPullImage** でスタックします。これらの Pod で定義されたイメージは、関連する **StatefulSets** で定義されるイメージとは異なります。この問題を修正するには、誤ったイメージを使用する Pod を削除する必要があります。Pod は自動的に再起動し、正しいイメージを使用する必要があります。

#### 1.3.3.9. 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ック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、メトリクスコレクションの間隔をより大きい値に増やすことが推奨されます。たとえば、間隔を 60 秒に増やすことができます。

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

### 1.3.4. クラスター管理の既知の問題

#### 1.3.4.1. マネージドクラスターの削除時にマネージドクラスターの namespace が終了しなくなる

マネージドクラスターを削除すると、その **マニフェスト** 作業リソースが削除されないため、マネージドクラスターの namespace が終了状態のままになる可能性があります。以下のコマンドを実行して残りの **manifestworks** リソースを削除し、namespace を削除します。

```
kubectl -n <managed-cluster-namespace> get manifestworks | grep -v NAME | awk '{print $1}' | xargs
kubectl -n <managed-cluster-namespace> patch manifestworks -p '{"metadata":{"finalizers": []}}' --
type=merge
```

#### 1.3.4.2. 無効なクラスターデプロイメントが作成されている。

クラスターのデプロイ時に無効な情報が提供されると、起動できなくても **作成** ステータスが uncreatable クラスターステータスに表示されます。**install-config** ファイルで指定されたリージョンに一致しないデプロイメントに指定されたリージョンなどの無効な情報により、以下のエラーが Hive プロビジョニング Pod に追加されます。

```
provision failed, requirements not met
```

Red Hat Advanced Cluster Management バージョン 2.3 では、クラスター **作成** のステータスを引き続き報告しますが、無効な情報によりクラスターの作成が妨げられます。

#### 1.3.4.3. 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

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

#### 1.3.4.4. Google Cloud Platform でのクラスタープロビジョニングに失敗する

Google Cloud Platform(GCP)でのクラスターのプロビジョニングを試みると、以下のエラーを出して失敗する可能性があります。

```
Cluster initialization failed because one or more operators are not functioning properly.
The cluster should be accessible for troubleshooting as detailed in the documentation linked below,
https://docs.openshift.com/container-platform/latest/support/troubleshooting/troubleshooting-installations.html
The 'wait-for install-complete' subcommand can then be used to continue the installation
```

GCP プロジェクトで ネットワークセキュリティー API を有効にして、このエラーを回避することができます。これにより、クラスターのインストールを継続できます。

#### 1.3.4.5. 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別の名前でクラスターとして再インポートしようとすると、**local-cluster** のステータスが「offline」を表示します。

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。

#### 1.3.4.6. クラスターのステータスは、Ansible クラスターの作成の失敗後にコンソールのさまざまなビューで異なります。

クラスターの作成の試行中に無効な Ansible ジョブテンプレート名を指定しても、クラスターはコンソールの複数の異なる画面に異なるステータスを表示します。**Infrastructure** > **Clusters** > **Managed clusters** を選択してステータスを表示すると、**Failed** ステータスが表示されます。**Infrastructure** > **Clusters** > **Cluster sets** > **<your_cluster_set_name>** > **Managed clusters** を選択すると、ステータスは **Creating** で停止します。今回の場合は、正しいステータスが **Failed** となっています。クラスターを再度作成して、正しい Ansible テンプレート名を入力できます。

#### 1.3.4.7. local-cluster が自動的に再インポートされない可能性がある

local-cluster をデタッチした後に、local-cluster が自動的に再インポートされないことがあります。これが発生すると、ローカルクラスターは Red Hat Advanced Cluster Management コンソールに **Pending Import** の一定のステータスを表示します。

local-cluster を再インポートするには、以下の手順を実行します。

1. 以下のコマンドを実行して klusterlet デプロイメントを削除します。

```
oc -n open-cluster-management-agent delete deployment klusterlet
```

2. 以下のコマンドを実行して **managedcluster-import-controller** を再起動します。

```
oc -n open-cluster-management get pods -l app=managedcluster-import-controller-v2 | awk 'NR>1{print $1}' | xargs oc -n open-cluster-management delete pods
```

#### 1.3.4.8. マネージドクラスターの clusterdeployment が終了状態のままになる

Red Hat Advanced Cluster Management コンソールで作成したマネージドクラスターを削除すると、マネージドクラスターの **clusterdeployment** は終了状態のままになる可能性があります。この問題を回避するには、この **clusterdeployment** を削除するには、クラスターの **agentclusterinstall** リソースを編集して **agentclusterinstall.agent-install.openshift.io/ai-deprovision** ファイナライザーを手動で削除します。

#### 1.3.4.9. 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。

#### 1.3.4.10. アーキテクチャー全体のクラスターを作成できない

ハブクラスターのアーキテクチャーとは異なるアーキテクチャーでマネージドクラスターを作成するには、両方のアーキテクチャーのファイルが含まれるリリースイメージ (**ClusterImageSet**) を作成する必要があります。たとえば、**ppc64le** ハブクラスターから **x86_64** クラスターを作成することはできません。OpenShift Container Platform リリースレジストリーは、マルチアーキテクチャーイメージマニフェストを提供しないため、クラスターの作成に失敗します。

この問題を回避するには、以下の手順を実行します。

1. OpenShift Container Platform リリースレジストリー から、**x86_64** および **ppc64le** リリースイメージの両方を含む マニフェスト一覧 を作成します。

    a. Quay リポジトリーから両方のアーキテクチャーのマニフェストの一覧をプルします。

```
$ podman pull quay.io/openshift-release-dev/ocp-release:4.8.1-x86_64
$ podman pull quay.io/openshift-release-dev/ocp-release:4.8.1-ppc64le
```

b. イメージを管理するプライベートリポジトリーにログインします。

```
$ podman login <private-repo>
```

**private-repo** は、リポジトリーへのパスに置き換えます。

c. 以下のコマンドを実行して、リリースイメージマニフェストをプライベートリポジトリーに追加します。

```
$ podman push quay.io/openshift-release-dev/ocp-release:4.8.1-x86_64 <private-repo>/ocp-release:4.8.1-x86_64
$ podman push quay.io/openshift-release-dev/ocp-release:4.8.1-ppc64le <private-repo>/ocp-release:4.8.1-ppc64le
```

**private-repo** は、リポジトリーへのパスに置き換えます。

d. 新規情報のマニフェストを作成します。

```
$ podman manifest create mymanifest
```

e. 両方のリリースイメージへの参照をマニフェスト一覧に追加します。

```
$ podman manifest add mymanifest <private-repo>/ocp-release:4.8.1-x86_64
$ podman manifest add mymanifest <private-repo>/ocp-release:4.8.1-ppc64le
```

**private-repo** は、リポジトリーへのパスに置き換えます。

f. マニフェストリストの一覧を既存のマニフェストにマージします。

```
$ podman manifest push mymanifest docker://<private-repo>/ocp-release:4.8.1
```

**private-repo** は、リポジトリーへのパスに置き換えます。

2. ハブクラスターで、リポジトリーのマニフェストを参照するリリースイメージを作成します。

a. 以下の例のような情報を含む **YAML** ファイルを作成します。

```
apiVersion: hive.openshift.io/v1
kind: ClusterImageSet
metadata:
  labels:
    channel: fast
    visible: "true"
  name: img4.8.1-appsub
spec:
  releaseImage: <private-repo>/ocp-release:4.8.1
```

**private-repo** は、リポジトリーへのパスに置き換えます。

b. ハブクラスターで以下のコマンドを実行し、変更を適用します。

```
oc apply -f <file-name>.yaml
```

**file-name** を、先の手順で作成した **YAML** ファイルの名前に置き換えます。

3. OpenShift Container Platform クラスターの作成時に新規リリースイメージを選択します。

作成プロセスでは、マージされたリリースイメージを使用してクラスターを作成します。

#### 1.3.4.11. ラベルを変更してクラスターをクラスターセットに再割り当てできない

クラスターのラベルを更新して新規クラスターセットに適用し、クラスターまたはクラスターセットを別のクラスターセットに再割当てできません。クラスターまたはクラスターセットを移動するには、Red Hat Advanced Cluster Management コンソールを使用して、クラスターセットからクラスター/クラスターセットを削除します。クラスターセットから削除した後に、コンソールを使用して新規クラスターセットに追加します。

#### 1.3.4.12. IBM Power ハブクラスターと Ansible Tower 統合を使用できない

Ansible Automation Platform Resource Operator では **ppc64le** イメージが提供されないので、IBM Power 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。

#### 1.3.4.13. 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。

#### 1.3.4.14. OpenShift Container Platform バージョン 4.8 でベアメタルマネージドクラスターを作成できない

ハブクラスターが OpenShift Container Platform バージョン 4.8 でホストされる場合は、Red Hat Advanced Cluster Management ハブクラスターを使用してベアメタルマネージドクラスターを作成することはできません。

#### 1.3.4.15. リソースドロップダウンエラーの作成

マネージドクラスターをデタッチすると、**Create resources** ページが一時的に破損し、以下のエラーが表示される可能性があります。

```
Error occurred while retrieving clusters info. Not found.
```

namespace が自動的に削除されるまで待ちます。待機時間は、クラスターのデタッチ後、5-10 分ほどです。または、namespace が終了状態のままの場合、namespace を手動で削除する必要があります。ページに戻り、エラーが解決されたかどうかを確認します。

#### 1.3.4.16. 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。

#### 1.3.4.17. 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。

#### 1.3.4.18. OpenShift Container Platform 3.11 の割り当てを解除しても open-cluster-management-agent は削除されません。

OpenShift Container Platform 3.11 でマネージドクラスターをデタッチしても、**open-cluster-management-agent** namespace は自動的に削除されません。以下のコマンドを実行して namespace を手動で削除します。

```
oc delete ns open-cluster-management-agent
```

#### 1.3.4.19. 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対象外

クラウドプロバイダーのアクセスキーを変更しても、プロビジョニングされたクラスターのアクセスキーは、namespace で更新されません。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。このような場合は、以下のコマンドを実行して、クラウドプロバイダーでアクセスキーを更新します。

- Amazon Web Services (AWS)

  ```
  oc patch secret {CLUSTER-NAME}-aws-creds -n {CLUSTER-NAME} --type json -p='[{"op": "add", "path": "/stringData", "value":{"aws_access_key_id": "{YOUR-NEW-ACCESS-KEY-ID}","aws_secret_access_key":"{YOUR-NEW-aws_secret_access_key}"} }]'
  ```

- Google Cloud Platform (GCP)
  この問題は、クラスターを破棄する際に **Invalid JWT Signature** と繰り返し表示されるログのエラーメッセージで特定することができます。ログにこのメッセージが含まれる場合は、新しい Google Cloud Provider サービスアカウント JSON キーを取得し、以下のコマンドを入力します。

  ```
  oc set data secret/<CLUSTER-NAME>-gcp-creds -n <CLUSTER-NAME> --from-file=osServiceAccount.json=$HOME/.gcp/osServiceAccount.json
  ```

  **CLUSTER-NAME** は、お使いのクラスター名に置き換えます。

  **$HOME/.gcp/osServiceAccount.json** ファイルへのパスを、新しい Google Cloud Provider サービスアカウント JSON キーが含まれるファイルへのパスに置き換えます。

- Microsoft Azure

  ```
  oc set data secret/{CLUSTER-NAME}-azure-creds -n {CLUSTER-NAME} --from-file=osServiceAccount.json=$HOME/.azure/osServiceAccount.json
  ```

- VMware vSphere

  ```
  oc patch secret {CLUSTER-NAME}-vsphere-creds -n {CLUSTER-NAME} --type json -p='[{"op": "add", "path": "/stringData", "value":{"username": "{YOUR-NEW-VMware-username}","password":"{YOUR-NEW-VMware-password}"} }]'
  ```

#### 1.3.4.20. root 以外のユーザーで management ingress を実行できない

**management-ingress** サービスを実行するには、**root** でログインする必要があります。

#### 1.3.4.21. 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。

#### 1.3.4.22. 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。

#### 1.3.4.23. 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。

#### 1.3.4.24. 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。

#### 1.3.4.25. IBM Power ハブクラスターでは Argo CD はサポート対象外である

Red Hat Advanced Cluster Management との Argo CD の統合は、利用可能な **ppc64le** イメージがないため、IBM Power で実行されている Red Hat Advanced Cluster Management ハブクラスターでは機能しません。

#### 1.3.4.26. 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。

### 1.3.5. アプリケーション管理の既知の問題

#### 1.3.5.1. Application search undefined error Application table

アプリケーション **テーブル** の **Search application by row** アクションボタンをクリックすると、Search ページに移動します。これは、**Application details** ページから **Search** リソースから受け取ることができるものと同じ事前設定フィルターとは異なる結果になります。

#### 1.3.5.2. Application search undefined error Argo CD

リンクをクリックすると、Argo CD アプリケーションの **アプリケーションの詳細ページからすべての関連アプリケーションを検索** すると、検索ページは無効な事前設定フィルターを返します。

検索コンソールでディレクトリーフィルターを削除して、この問題を解決することができます。

#### 1.3.5.3. プロキシーのアプリケーション作成中にブランチ情報がない

**Create application** エディターを使用して Red Hat Advanced Cluster Management アプリケーションを作成すると、ハブクラスターがプロキシーの背後にあるときに、Git リポジトリーに以下のエラーが発生する可能性があります。

**The connection to the Git repository failed.Cannot get branches.**

代わりに Git リポジトリーの URL に移動して、ブランチ情報を取得できます。ブランチの入力時に、アプリケーションは正しくデプロイされます。

#### 1.3.5.4. アプリケーション Argo 検索の未定義エラー

Argo アプリケーションのクラスターノード検索リンクは **name:undefined** を返す可能性があります。

Argo アプリケーションのクラスターノードの詳細から、検索リンクの **Launch resource in search** をクリックすると、検索フィルターに **name:undefined** が含まれる場合があります。

このエラーを解決するには、**undefined** 値をクラスターノードの詳細のクラスター名に置き換えます。

#### 1.3.5.5. 複数のサブスクリプションが正しくグループ化されていないアプリケーショントポロジークラスター

クラスターが複数のサブスクリプションを使用している場合は、クラスターが **アプリケーショントポロジー** で適切にグループされない可能性があります。

複数のサブスクリプションでアプリケーションをデプロイする場合、**すべてのサブスクリプションビュー** がクラスターノードを適切にグループ化していない可能性があります。

たとえば、**Helm** リポジトリーと **Git** リポジトリーの組み合わせを含む複数のサブスクリプションでアプリケーションをデプロイする場合、**すべてのサブスクリプション** ビューは Helm サブスクリプション内のリソースに対するステータスを適切に表示しません。

代わりに、個別のサブスクリプションビューからトポロジーを表示して、正しいクラスターノードをグループ化する情報を表示します。

#### 1.3.5.6. アプリケーショントポロジーのサブスクリプションスイッチ

サブスクリプションドロップダウンメニューを使用してアプリケーションサブスクリプションを切り替えると、アプリケーショントポロジーが失敗する可能性があります。

この問題を解決するか、別のサブスクリプションへの切り替えを試みます。もしくは、ブラウザーを更新してトポロジー表示の更新を確認します。

#### 1.3.5.7. 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、この設定では **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ので、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. お使いの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、Ansible インスタンスがハブクラスターに作成されているのが表示されるはずです。

#### 1.3.5.8. ローカルクラスターへのアプリケーションのデプロイ時の制限

アプリケーションの作成または編集時に **Deploy on local cluster**を選択すると、アプリケーショントポロジーが正しく表示されません。**Deploy on local cluster**は、ハブクラスターにリソースをデプロイして **local cluster** として管理できるようにするオプションですが、今回のリリースではベストプラクティスではありません。

この問題を解決するには、以下の手順を参照してください。

1. コンソールで **Deploy on local cluster**オプションの選択を解除します。
2. **Deploy application resources only on clusters matching specified labels**オプションを選択します。
3. **local-cluster : 'true'** というラベルを作成します。

#### 1.3.5.9. namespace チャネルサブスクリプションのステータスが Failed のままになる

namespace チャネルにサブスクライブして、チャネル、シークレット、ConfigMap、または配置ルールなどの他の関連リソースを修正した後にサブスクリプションの状態が **FAILED** のままになると、namespace サブスクリプションの調整が継続的に行われなくなります。

サブスクリプションの調整を強制的に行い、**FAILED** の状態から抜けるには、以下の手順を完了してください。

1. ハブクラスターにログインします。
2. 以下のコマンドを使用して、サブスクリプションにラベルを手動で追加します。

```
oc label subscriptions.apps.open-cluster-management.io the_subscription_name reconcile=true
```

#### 1.3.5.10. 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拘らず、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。

#### 1.3.5.11. 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拘らず、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。

#### 1.3.5.12. 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には、**klusterlet-addon-appmgr** Pod が実行されていることを確認します。サブスクリプションコンテナーである **klusterlet-addon-appmgr** は、エンドポイントクラスターで実行する必要があります。

**oc get pods -n open-cluster-management-agent-addon** を実行して確認します。

また、コンソールで **kind:pod cluster:yourcluster** を検索し、**klusterlet-addon-appmgr** が実行中であることを確認できます。

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

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

Red Hat OpenShift Container Platform SCC に関する説明は、「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の設定です。

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。

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

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

#### 1.3.5.14. 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。

#### 1.3.5.15. Ansible Automation Platform（早期アクセス）2.0.0 ジョブが失敗する

Ansible Automation Platform（早期アクセス）2.0.0 をインストールすると、**AnsibleJobs** の実行に失敗します。Red Hat Advanced Cluster Management で prehook および posthook **AnsibleJobs** を送信するには、Ansible Automation Platform Resource Operator 0.1.1 を使用します。

#### 1.3.5.16. アプリケーション名の要件

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

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

#### 1.3.5.17. アプリケーションコンソールの表

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ので、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拘らず、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。

### 1.3.6. ガバナンスの既知の問題

#### 1.3.6.1. 自動化を開始する新しいポリシー違反がない場合でも、Ansible Automation ジョブは 1 時間ごとに実行します。

OpenShift Container Platform 4.8 では、終了したリソースの TTL コントローラーはデフォルトで有効になります。つまり、ジョブが毎時削除されます。このジョブクリーンアップにより、Ansible Automation Platform Resource Operator は関連付けられた自動化を再実行します。この自動化は、ポリシーフレームワークで作成された **AnsibleJob** リソースの既存の詳細を使用して再度実行されます。提供された詳細には、以前特定した違反が含まれる可能性があります。これは、繰り返している違反として誤って表示される可能性があります。ジョブをクリーンアップするコントローラーを無効にして、重複した違反を防ぐことができます。ジョブをクリーンアップするコントローラーを無効にするには、以下の手順を行います。

1. 以下のコマンドを実行して **kubeapiservers.operator.openshift.io** リソースを編集します。

   ```
   oc edit kubeapiservers.operator.openshift.io cluster
   ```

2. **unsupportedConfigOverrides** セクションを見つけます。

3. 以下の例のように、**unsupportedConfigOverrides** セクションを更新して、ジョブのクリーンアップ機能を無効にします。

   ```
   unsupportedConfigOverrides:
     apiServerArguments:
   ```

```
    feature-gates:
    - TTLAfterFinished=false
```

4. 以下のコマンドを実行して **kubecontrollermanager** リソースを編集します。

```
oc edit kubecontrollermanager cluster
```

5. **kubecontrollermanager** リソースの同じセクションを更新するには、ステップ 2 と 3 を実行します。

#### 1.3.6.2. PlacementRule matchExpression が新しい matchLabel で削除されない

ポリシー **PlacementRule** を **matchExpressions** から **matchLabels** に更新する場合、古い **matchExpression** は削除されません。

以下の例は、最初のサンプルの **matchExpressions** が 2 つ目のサンプルで **matchLabels** に変更されていますが、**matchExpressions** は削除されません。

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: placement-policy-etcdencryption
spec:
  clusterConditions:
  - status: "True"
    type: ManagedClusterConditionAvailable
  clusterSelector:
    matchExpressions:
      - {key: environment, operator: In, values: ["test"]}
```

```
spec:
  clusterConditions:
  - status: "True"
    type: ManagedClusterConditionAvailable
  clusterSelector:
    matchExpressions: []
    matchLabel: {}
```

#### 1.3.6.3. IAM ポリシーコントローラーではグループユーザーが考慮されない

指定の **ClusterRole** に対するパーミッションがあるユーザー数を決定すると、IAM ポリシーコントローラーは Kubernetes **User** リソースのみをチェックし、Kubernetes **Group** リソースのユーザーを考慮しません。

#### 1.3.6.4. ログアウトできません

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。

#### 1.3.6.5. 管理者クラスターマネージャーが自動化ポリシーを作成できない

**open-cluster-management:cluster-manager-admin** へのクラスター全体のロールバインディングを持つユーザーは自動化ポリシーを作成できません。この問題を修正するには、ロールを自動化ポリシーに手動で追加する必要があります。

クラスターロール(**ClusterRole**)を作成または更新して、**Ansible** リソースの **cluster-manager-admin** ロールにルールを追加します。YAML は以下のファイルのようになります。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: add-ansible-rules
  labels:
    rbac.authorization.k8s.io/aggregate-to-ocm-cluster-manager-admin: "true"
rules:
- apiGroups: ["tower.ansible.com"]
  resources: ["ansiblejobs"]
  verbs: ["create","get", "list", "watch", "update", "delete", "deletecollection", "patch"]
```

#### 1.3.6.6. 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、「Upgrading gatekeeper and the gatekeeper operator」を参照してください。

#### 1.3.6.7. 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。

## 1.4. 非推奨と削除

Red Hat Advanced Cluster Management for Kubernetes から削除されるか、または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 2.1 バージョンが **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がなくても非推奨になります。以前のバージョンのドキュメントもサポートされていません。
- Red Hat Advanced Cluster Management の最新バージョンへのアップグレードがベストプラクティスです。

### 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従います。このポリシーの詳細については、「Kubernetes の非推奨ポリシー」を参照してください。

Red Hat Advanced Cluster Management API が非推奨または削除となるのは、以下のタイムライン以外のみです。

- **V1** API はすべて、12 ヶ月間または リリース 3 回分 (いずれか期間が長い方) 一般公開され、サポート対象です。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。
- **ベータ版** API はすべて、9ヶ月間またはリリース 3 回分 (いずれか期間が長い方) 一般公開されます。ベータ版 API は、この過ぎても削除されません。
- **アルファ版** 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。

### 1.4.2. 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 |
|---|---|---|---|---|
| アプリケーション | **HelmRepo** チャネル仕様: **insecureSkipVerify: "true"** は **configMapRef** 内では使用しません。 | 2.2 | **configMapRef** のないチャネルで **insecureSkipVerify: "true"** を使用します。 | 変更については、YAML サンプル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 Hive 設定 | 2.2 | インストールして、**oc edit hiveconfig hive** コマンドで直接 **hiveconfig** を編集します。 | なし |
| klusterlet Operator | **release-2.3** チャネルが更新を受信しない | 2.3 以降 | Red Hat OpenShift 専用クラスターをインポートして管理するには、アップグレードする必要があります。 | 「Operator を使用したアップグレード」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** の別の cert-manager の設定 | 2.3 | なし | なし |
| ガバナンス | カスタムポリシーコントローラー | 2.3 | 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 |
|---|---|---|---|---|
| 可観測性トポロジー | **Observe 環境** からのトポロジーアクセスを完全に削除 | 2.2 | なし | アプリケーショントポロジーは **アプリケーション管理** に配置されるようになり、**可観測性コンソール** には表示されなくなります。 |
| アプリケーション | Namespace のチャネルタイプを完全に削除 | 2.2 | なし | 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 |
| 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 |

| 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 | cert-manager の内部証明書管理 | 2.3 | アクションは不要です。 | なし |

## 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
- 遵守しない場合には多額の罰金が課される可能性がある
- 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良く理解するには、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、複数の技術データを扱いますが、その内、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、個人データの使用は、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、機微な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。このような全情報には、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を使用するかまたは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームノードにログインしたシステム管理者のみがアクセスできます。

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なストアで、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、「シークレットの管理」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ー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ース (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ースは、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 に管理者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

The 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、管理者ー、オペレーター、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ース (API)、およびユーザーインターフェー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、複数の技術データを扱いますが、その内、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。