Red Hat Advanced Cluster Management for Kubernetes 2.2

リリースノート

新機能、エラータ更新、既知の問題、非推奨化および削除、および GDPR および FIPS に対応する製品に関する考慮事項については、『リリースノート』を参照してください。

Last Updated: 2023-02-22

Red Hat Advanced Cluster Management for Kubernetes 2.2 リリースノート

新機能、エラータ更新、既知の問題、非推奨化および削除、および GDPR および FIPS に対応する製品に関する考慮事項については、『リリースノート』を参照してください。

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、エラータ更新、既知の問題、非推奨化および削除、および GDPR および FIPS に対応する製品に関する考慮事項については、『リリースノート』を参照してください。

目次

第1章 RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES のリリースノート

重要:

- Red Hat Advanced Cluster Management の 2.1 バージョンは **削除され、サポートさ** れなくなりました。ドキュメントはそのまま利用できますが、エラータやその他の更新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。
  - 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。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。
- 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。

1.1.1. インストール

Red Hat OpenShift Dedicated 環境にハブクラスターをインストールできるようになりました。詳細は、「ネットワーク接続時のオンラインインストール」を参照してください。

1.1.2. Web コンソール

検索永続性のストレージ設定を定義できるようになりました。永続性は、**searchCustomization** カスタムリソースでデフォルトで有効化されます。詳細は、「コンソールでの検索」を参照してください。

1.1.2.1. 環境の監視

- 可観測性の証明書は、有効期限前に自動的に更新されます。詳細は、「可観測性の証明書」を参照してください。

- 以下のメトリクスが Red Hat Advanced Cluster Management に追加され、テレメトリーに同梱されていますが、Red Hat Advanced Cluster Management Observe 環境の概要ダッシュボードには表示されません。
  - **visual_web_terminal_sessions_total**
  - **acm_managed_cluster_info**
- カスタムメトリクスを可観測性サービスに追加して、マネージドクラスターから収集できるようになりました。詳細は、「カスタムスケジューラーの追加」を参照してください。
- 可観測性は、マネージドクラスターの可観測性リソース (**observability-xxx**) の設定変更を自動的に制限し、クラスターが必要な状態であることを確認します。これは、ハブクラスターでも適用されます。必要ない更新は元に戻されます。可観測性サービスのカスタマイズ方法については、「可観測性のカスタマイズ」を参照してください。
- クラスターの Grafana ダッシュボードを設計できるようになりました。詳細は「Grafana ダッシュボード」を参照してください。
- OpenShift Container Storage は、可観測性サービスでサポートされるストレージソリューションになりました。詳細は、「可観測性サービスの有効化」を参照してください。

可観測性の詳細は、「環境の監視の紹介」を参照してください。

1.1.3. クラスター管理

- Red Hat OpenShift Dedicated 環境でクラスターをインポートして管理できます。また、IBM Z マネージドクラスターを管理することもできます。詳細は、「ハブクラスターへのターゲットのマネージドクラスターのインポート」を参照してください。
- **clusterclaims** を使用して、クラスターに固有の情報を表示でき ます。詳細は、「ClusterClaims」を参照してください。
- **テクノロジープレビュー:** Submariner は、Red Hat Advanced Cluster Management が管理するクラスター全体で直接ネットワーク接続できるように統合されています。詳しい情報は、Submariner を参照してください。
- **clusterrole** を作成して割り当てることで、マネージドクラスターの作成、管理、およびインポートを行うパーミッションを特定のグループに制限できるようになりました。詳細は、「特定のクラスター管理ロールの設定」を参照してください。
- クラスターイメージセットの一覧は自動的に更新され、クラスターイメージの一覧を最新の状態に保ちます。詳細は、「接続時におけるリリースイメージのカスタム一覧の管理」を参照してください。
- AnsibleTower タスクを自動化して、一台または複数のクラスターで AnsibleJob を作成して実行します。詳細は、「マネージドクラスターの AnsibleJob の作成 」を参照してください。

1.1.4. アプリケーション管理

Git 接続の機能が改良され、自己署名証明書を使用してプライベートリポジトリーに接続できます。詳細は、「セキュアな Git 接続用のアプリケーションチャネルおよびサブスクリプションの設定」を参照してください。

Argo CD が統合され、任意のタイプのサポート対象マネージドクラスターを手動で同期できるようになりました。Argo CD クラスターコレクションを有効にして、アプリケーションを Argo CD からマネージドクラスターにデプロイできるようにします。Argo CD を有効にする方法については、「Argo CD

のマネージドクラスターの設定」を参照してください。

アプリケーション管理の全変更およびドキュメントについては、「アプリケーションの管理」を参照してください。

1.1.5. セキュリティーおよびコンプライアンス

- Red Hat Advanced Cluster Management gatekeeper Operator ポリシーを使用して、gatekeeper をインストールできるようになりました。詳細は、「gatekeeper Operator ポリシーを使用した gatekeeper のインストール」を参照してください。
- コンプライアンスオペレーターポリシーを使用して Red Hat OpenShift Container Platform コンプライアンスオペレーターをインストールできるようになりました。詳細については、「コンプライアンスオペレーターポリシー」を参照してください。
- Essential 8 (E8) スキャンポリシーを作成して適用し、マスターノードとワーカーノードをスキャンして E8 プロファイルに準拠しているかどうかを確認できるようになりました。詳細については、「E8スキャンポリシー」を参照してください。
- 内部管理証明書をローテーションできるようになりました。詳細は、「証明書」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、「ガバナンスおよびリスク」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:

- Red Hat OpenShift Container Platform 4.5 は、2.2.4 以降のエラータリリースではサポートされません。OpenShift Container Platform バージョン 4.6 で稼働し、Red Hat Advanced Cluster Management バージョン 2.2.4 以降にアップグレードする必要があります。Red Hat OpenShift Container Platform のバージョンを 4.6 にアップグレードできない場合は、引き続き Red Hat Advanced Cluster Management バージョン 2.2.3 を使用できます。
- 参照用として 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。

1.2.1. Errata 2.2.13

このエラータリリースは、1 つ以上の製品コンテナーイメージにセキュリティー修正と更新を提供します。

1.2.2. Errata 2.2.12

このエラータリリースは、1 つ以上の製品コンテナーイメージにセキュリティー修正と更新を提供します。

1.2.3. Errata 2.2.11

- サポートされていないバージョンの OpenShift Container Platform を利用可能なクラスターイメージセットの一覧から削除します。(Bugzilla 2030859)

- **observabilityAddon** のステータスが **degraded** 状態であるために可観測性が無効になるとマネージドクラスターのアップグレードが妨げられる問題が修正されました。今回の修正により、可観測性が無効になっている場合に **observabilityAddon** がマネージドクラスターから削除され、アップグレードを完了できるようになりました。(GitHub 19636)

このエラータリリースは、1 つ以上の製品コンテナーイメージにセキュリティー修正と更新を提供します。

1.2.4. エラータ 2.2.10

このエラータリリースは、製品コンテナーイメージの更新を提供します。

1.2.5. エラータ 2.2.9

このエラータリリースは、製品コンテナーイメージの更新を提供します。

1.2.6. エラータ 2.2.8

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.2.8 の更新について以下に一覧としてまとめています。

- 調整時にアプリケーションが削除される原因となっていた問題を修正します。削除は、サブスクライブされた Git リポジトリーの誤った kustomization など、誤って設定されたアプリケーションマニフェストによって生じました。今回の修正により、マニフェストを誤って設定しても、デプロイされたアプリケーションが削除されない場合に、アプリケーショントポロジーのユーザーインターフェースにエラーメッセージが表示されます。(Bugzilla 1972947)

- 作成される不要なシークレットの数を減らすことで、**cert manager** をより少ないメモリー消費で起動できます。(GitHub 13127)

- 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。

1.2.7. エラータ 2.2.7

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.2.7 の更新について以下に一覧としてまとめています。

このエラータリリースは、製品コンテナーイメージの更新を提供します。

1.2.8. エラータ 2.2.6

重要: 前の注記の情報を参照してください。

Red Hat OpenShift Container Platform 4.8 は 2.2.6 以降でサポートされます。*重要: ベアメタル用 Red Hat OpenShift Container Platform 4.8 は本リリースでは機能しません。

Red Hat Advanced Cluster Management for Kubernetes の エラータが提供する修正を一覧としてまとめています。

- インポートされたクラスターの問題を修正します。メトリクス可視性で OpenShift Container Platform 3.11 からのインポートされたクラスターは、他の OpenShift Container Platform クラスターとして表示されます。(GitHub 13162)

- カスタム CA 証明書を使用する Git リポジトリーサーバーから Helm チャートにサブスクライブするアプリケーションでデプロイメントの失敗を修正します。カスタム CA 検証を回避するた

めに **insecureSkipVerify: true** のいずれかを使用してアプリケーションチャネルを設定するか、カスタム CA 証明書をチャネル設定に追加します。(GitHub 14467)

- メタデータと仕様の更新に対して RedisGraph StatefulSet を更新し、アップグレードの問題を修正します。(GitHub 13661)
- 設定ポリシーコントローラーの比較およびソート機能を修正し、ポリシーコントローラーで設定されるマネージドクラスターの Kubernetes リソースを継続的に増加するようにします。(Bugzilla 1973772)
- 選択した namespace が **NonCompliant** の場合は、設定ポリシーの namespace 選択を更新し、ポリシーを **NonCompliant** として識別します。(Bugzilla 1969845)
- OpenShift Container Platform 4.8 との互換性のために **cert-manager** の **SelfLink** 属性の使用を削除します。(GitHub 13121)
- **SecurityConstraintContext** ポリシーの問題を修正し、検索 Operator Pod の起動を阻止しました。デフォルトでは root 以外のユーザーで実行される Docker イメージを更新し、root 以外のユーザーでコンテナーを開始する **runAsNonRoot** で、検索オペレーターデプロイメントのセキュリティーコンテキストを更新します。(Bugzilla 1967953)
- さまざまなコンテナー更新を追加します。
- ベアメタルアセットフィールドが正しく入力されない問題を修正します。(GitHub 9850)

1.2.9. エラータ 2.2.5

重要: 前の注記の情報を参照してください。

Red Hat Advanced Cluster Management for Kubernetes の エラータが提供する修正を一覧としてまとめています。

- 複数の証明書の問題を修正します。
- 証明書の更新時に Pod が自動的に再起動されるように、Search redisgraph StatefulSet にラベルを追加します。(GitHub 12299)

1.2.10. エラータ 2.2.4

重要: 前の注記の情報を参照してください。

Red Hat Advanced Cluster Management for Kubernetes の エラータが提供する修正を一覧としてまとめています。

- コンソールで無効なポリシーが削除された場合に、**placementrule** と **placementbinding** が削除されないという問題を修正しました。(GitHub 12689)
- 製品システム namespace で作成されたチャネルロールおよびロールバインディングを削除します。今回の修正により、システムシークレットがマネージドクラスターサービスアカウントに公開されなくなりました。(GitHub 12319)
- **endpoint-observability-operator** Pod の可観測性で問題を解決します。ハブクラスターが IBM クラウドにインストールされている場合に、マネージドクラスターからハブクラスターへの通信が原因で、**不明な認証局で署名された証明書** エラーが発生していました。(GitHub 11125)
- 正しいバージョンが表示されない Hive コントローラーの問題を修正します。(GitHub 12013)

- 可観測性クラッシュの問題を修正します。(Bugzilla 1967890)

1.2.11. エラータ 2.2.3

Red Hat Advanced Cluster Management for Kubernetes の エラータが提供する修正を一覧としてまとめています。

- コンプライアンス Operator ポリシーに制御カテゴリーを追加します。(GitHub 11234)
- YAML エディターを更新して、無効な **imageSetRef** が **ClusterDeployment** に指定されるとエラーが表示されるようにします。(Bugzilla 1946244)
- インポートしたクラスターのコンソール問題を修正します。(GitHub 11119)
- YAML ファイルの **name** および **namespace** に引用符を追加して、値が文字列として入力されるようにします。(Bugzilla 1936883)
- Kustomize API モジュールバージョンを **0.8.5** にアップグレードし、Kubernetes-sigs の修正に対応します。(GitHub 11362)
- マネージドクラスターにアクセスするために、管理者以外のユーザーに **GET** クラスターロールのサポートを追加します。**PlacementRule** によって作成および返されるクラスター一覧には、ユーザーがアクセス可能なクラスターのみが含まれます (Bugzilla 1946244)。
- Gatekeeper および Gatekeeper Operator ベースイメージのアップグレードを追加します。(Github 12038)

1.2.12. エラータ 2.2.2

Red Hat Advanced Cluster Management for Kubernetes の エラータが提供する修正を一覧としてまとめています。

- このエラータは、複数のセキュリティーの問題およびコンテナーイメージの更新に対応します。
- **create policy** フォームの既存のポリシーで空白ページが表示されていた問題を解決します。(Bugzilla 1940588)
- **Create policy**仕様のドロップダウンメニューで、gatekeeper Operator ポリシーを追加します。(GitHub 10447)
- **アプリケーショントポロジー** のデプロイメントステータスの問題を修正します。カスタムエイリアスがパッケージ名と一致しない場合に Helm リソースチャートには、リソースデプロイメントステータスが表示されるようになりました。(GitHub 10401)
- **terminating** ステータスの **ObservabilityAddon** に関する問題を修正します。(GitHub 10012)
- 可能なリージョンすべてに Azure クラスターを作成する機能を追加します。(GitHub 9700)
- ハブクラスターでのカスタム認証局に関連する問題を修正します。Submariner エージェントが接続できるようになりました。(GitHub 9894)
- サブスクリプション CR に誤って指定されていた **packageOverrides** の問題を修正します。ハブクラスターの Pod またはマネージドクラスターの **klusterlet-addon-appmgr** Pod でエラーが発生していました。ログは上書きを無視するようになりました。(GitHub 9700)

- Visual Web ターミナル CLI を更新することで、OpenShift Container Platform バージョン 4.7 をサポートするようになりました。(GitHub 9640)
- 二重引用符を使用してエスケープされていない文字を処理するように、クラスターのインポートコマンドを更新します。**-d** オプションで base64 を使用するようにしてください。(GitHub 10748)
- クラスター YAML エディターの問題を修正します。(Bugzilla 1941778)
- NodeJS バージョン 12 だけでなく、14 のサポートを追加し、ベースイメージの脆弱性を抑えます。(GitHub 9540)
- ベースイメージの **ServiceExport** API バージョンを更新します。(Bugzilla 1936528)
- **clusterdeployment** で参照されていたアセットが別の **clusterdeployment** で再利用できない、ベアメタルアセットの問題を修正します。(GitHub 9272)
- 更新の頻度が多すぎるベアメタルの問題を修正します。(GitHub 9463)
- アプリケーション管理のデフォルト調整レートを 15 分に変更します。調整レートが設定可能になりました。(GitHub 10644)
- **KubeAPIServerLatency** ルールを削除して、デフォルトのアラートマネージャーでリソースの問題を修正します。(GitHub 10693)
- ロールベースのアクセス制御を更新します。**ManagedClusterView** リソースを作成および削除する**Viewer** ロールと、Pod のログを **取得** および表示する **cluster-manager-admin** ユーザーの権限が追加されました。(GitHub 11243, 11242)

1.2.13. エラータ 2.2.1

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.2.1 の更新について以下に一覧としてまとめています。

このエラータリリースは、コンテナーイメージの新しいセットを提供します。

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
- 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
- セキュリティーの既知の問題

1.3.1. インストールの既知の問題

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

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

1.3.1.2. インストール時に証明書マネージャーを配置してはいけない

Red Hat Advanced Cluster Management for Kubernetes をインストールする時に、クラスター上に証明書マネージャーを配置させることはできません。

証明書マネージャーがクラスターに存在すると、Red Hat Advanced Cluster Management for Kubernetes のインストールに失敗します。

この問題を解決するには、以下のコマンドを実行して、証明書マネージャーがクラスターに存在するかどうかを確認します。

```
kubectl get crd | grep certificates.certmanager
```

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** の結果々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
```

1.3.2.8. YAML ファイルが Search ページに表示されない

Safari v14.0.3 Web ブラウザーを使用する場合は、**Search** ページから YAML ファイルは表示されません。サポート対象の他のブラウザーについては Supported browsers を参照してください。または、Safari バージョンをアップグレードしてください。

1.3.2.9. redisgraph StatefulSet および Pod を再起動します。

2.2.z から 2.2.5 にアップグレードすると、**redisgraph** StatefulSet および Pod はリフレッシュされません。変更が反映されるように、**redisgraph** StatefulSet を手動で削除する必要があります。問題を解決するには以下の手順を実行します。

1. Red Hat Advanced Cluster Management 2.2.4 をインストールします。
2. Red Hat Advanced Cluster Management 2.2.5 にアップグレードします。
3. 管理者としてログインし、以下のコマンドを実行して **redisgraph** StatefulSet を確認します。

   ```
   oc get statefulset search-redisgraph -n open-cluster-management
   ```

4. StatefulSet および Pod が再起動しなかったことに注意してください。
5. 以下のコマンドを使用して **redisgraph** StatefulSet を削除します。

   ```
   oc delete statefulset search-redisgraph -n open-cluster-management
   ```

6. **redisgraph** Pod が以下のコマンドで正常に実行しているかどうかを確認します。

   ```
   oc get pod search-redisgraph-0 -n open-cluster-management
   ```

redisgraph StatefulSet および Pod が再起動しました。

1.3.2.10. 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。

1.3.2.11. 可観測性アドオンが終了しない

マネージドクラスターを強制的にデタッチすると、クラスター namespace にある **ObservabilityAddon** リソース (**observability-addon**) が **Terminating** の状態のままになり、削除できません。また、クラスター namespace も削除できません。

この問題を修正するには、クラスター namespace の **ObervabilityAddon** リソースを更新してください。メタデータの **finalizers** パラメーターを削除してリソースを更新します。以下のコマンドを実行します。

```
kubectl edit observabilityaddon observability-addon -n <CLUSTER_NAMESPACE>
```

CLUSTER_NAMESPACE は、デタッチされたクラスターの namespace です。

finalizers パラメーターを削除してから **ObervabilityAddon** リソースを削除します。

1.3.2.12. 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。

1.3.2.13. アップグレード後にメトリクスデータが収集されなくなる

Red Hat Advanced Cluster Management を 2.2.3 から 2.2.4 にアップグレードした後、**open-cluster-management-addon-observability** の **metrics-collector** がマネージドクラスターからデータの収集が停止してしまう可能性があります。これは、マルチクラスター可観測性 Operator のアップグレード後にイメージマニフェストの ConfigMap がアップグレードされたためです。

以下の Quay.io イメージが **endpoint-observabililty-operator** YAML ファイルで使用されることを確認できます (**quay.io/open-cluster-management/endpoint-monitoring-operator:2.2.0-6a5ea47fc39d51fb4fade6157843f2977442996e** および **quay.io/open-cluster-management/metrics-collector:2.2.0-ff79e6ec8783756b942a77f08b3ab763dfd2dc15**。

この問題を修正するには、ハブクラスターの **open-cluster-management** namespace にある **multicluster-observability-operator** Pod を削除します。新規 Pod が作成されると、適切なイメージで新しい **endpoint-observability-operator** デプロイメントがマネージドクラスターに作成されます。

1.3.2.14. MultiClusterObservability CR が誤ったステータスを表示する

Red Hat Advanced Cluster Management を 2.1 から 2.2.x にアップグレードした後に、**MultiClusterObservability** カスタムリソース (CR) は引き続き OpenShift Container Platform コンソールからの **Installing** を表示します。Grafana コンソールからメトリクスデータが表示されることを確認して、**MultiClusterObservability** が正常にデプロイされていることを確認できます。

1.3.2.15. 可観測性サービスメトリクスギャップ

一部のメトリクスデータは、Red Hat OpenShift Container Platform と 4.8 クラスターの Grafana ダッシュボードには表示されません。バージョン 2.3 にアップグレードする必要があります。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。

1.3.3. クラスター管理の既知の問題

1.3.3.1. 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。

1.3.3.2. クラスターのアップグレード時に、コンソールでクラスターのバージョンがすぐに更新されない

Cluster details ページでマネージドクラスターまたはローカルクラスターをアップグレードする場合に、アップグレードプロセスが完了してから、更新されたバージョン番号が **Cluster details** ページに表示されるまで最長 10 分かかることがあります。

1.3.3.3. OpenShift Container Platform バージョン 4.7 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 4.7 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。

1.3.3.4. 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。

1.3.3.5. 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。

1.3.3.6. コンソールでマネージドクラスターポリシーの矛盾が報告される場合がある

クラスターのインポート後に、インポートしたクラスターにログインして、Klusterlet でデプロイした Pod すべてが実行中であることを確認します。全 Pod が実行されていない場合に、コンソールで矛盾するデータが表示される可能性があります。

ポリシーコントローラーを実行していない場合など、**Governance and risk** ページと **Cluster status** で同じ違反結果が表示されない可能性があります。

たとえば、**Overview** ステータスで違反が 0 件と表示されているにも拘らず、**Governance and risk** ページで違反が 12 件報告される場合などです。

このような場合には、ページ間で不整合があると、マネージドクラスターの **policy-controller-addon** とハブクラスターのポリシーコントローラーが連携されていないことが分かります。また、マネージドクラスターには、すべての Klusterlet コンポーネントを実行するためのリソースが十分にない可能性があります。

その結果、ポリシーはマネージドクラスターに伝播されないことや、違反がマネージドクラスターから報告されないことがありました。

1.3.3.7. クラスターのインポートには 2 回試行する必要がある

Red Hat Advanced Cluster Management ハブクラスターで以前に管理されていて、デタッチされたクラスターをインポートすると、1 回目のインポートプロセスが失敗する可能性があります。クラスターのステータスは **pending import** となります。コマンドを再度実行すると、インポートが正常に実行されるはずです。

1.3.3.8. IBM Red Hat OpenShift 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 Red Hat OpenShift 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。

1.3.3.9. 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
```

1.3.3.10. 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}"} }]'
```

1.3.3.11. 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。

1.3.3.12. 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。

1.3.3.13. 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。

1.3.3.14. Red Hat OpenShift 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、Red Hat OpenShift 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。

1.3.3.15. 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。

1.3.3.16. ベアメタルクラスターが破棄された後に、関連するベアメタルアセットが破棄されない

ベアメタルアセットは、関連付けられたクラスターを破棄した後、孤立したアセットとして残る可能性があります。これは、クラスターを破棄するために必要なパーミッションはあるけれども、ベアメタルアセットを破棄するパーミッションがない場合に発生します。この問題を回避するには、クラスターデプロイメントを参照する Red Hat Advanced Cluster Management でベアメタルアセットを作成する際に、ファイナライザーを **ClusterDeployment** リソースに追加します。

```
kubectl patch clusterdeployments <name> -n <namespace> -p '{"metadata":{"finalizers":
["baremetalasset.inventory.open-cluster-management.io"]}}'
```

name は、お使いのクラスターデプロイメント名に置き換えます。

namespace は、お使いのクラスターリソースの namespace に置き換えます。

クラスターデプロイメントを削除する場合、以下のコマンドを入力してファイナライザーを手動で削除する必要があります。

```
kubectl patch clusterdeployments <name> -n <namespace> -p '{"metadata":{"finalizers":[]}}'
```

name は、お使いのクラスターデプロイメント名に置き換えます。

namespace は、お使いのクラスターリソースの namespace に置き換えます。

1.3.4. アプリケーション管理の既知の問題

1.3.4.1. Application デプロイメントウィンドウエラー

Active within specified interval に設定されたデプロイメントウィンドウでアプリケーションを作成する場合は、デプロイメントウィンドウが正しく計算されず、アプリケーションが未定義の時間でデプロイされることがあります。

1.3.4.2. 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。この数を超えると、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
```

1.3.4.3. 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。

1.3.4.4. 仕様がない deployable リソースが機能しない

仕様なしで Deployable リソースを適用すると、Pod の **multicluster-operators-application** コンテナー **multicluster-operators-deployable** をクラッシュします。deployable には仕様が含まれている必要があります。

仕様なしでリソースを誤って作成する場合は、不要な deployable を削除して、**multicluster-operators-application** Pod を再起動します。

空で Pod をクラッシュさせる以下の Deployable の例を参照してください。

```
apiVersion: apps.open-cluster-management.io/v1
kind: Deployable
metadata:
  labels:
    app: simple-app-tester
  name: simple-app-tester-deployable
  namespace: grp-proof-of-concept-acm
```

1.3.4.5. ReplicationController または ReplicaSet リソースのトポロジーがない

ReplicationController または **ReplicaSet** リソースを直接作成するアプリケーションをデプロイする場合には、Pod リソースは **アプリケーショントポロジー** に表示されません。Pod リソースを作成する代わりに、**Deployment** または **DeploymentConfig** リソースを使用できます。

1.3.4.6. アプリケーショントポロジーで誤った Ansible ジョブステータスが表示される

Ansible テストは、通常のタスクとしてではなく、サブスクリプションのフックとして実行されます。Ansible タスクは prehook および posthook フォルダーに保存する必要があります。Ansible タスクは、フックとしてではなく、通常のタスクとしてデプロイできますが、このような場合に、アプリケーショントポロジーの Ansible のジョブステータスが正しく報告されません。

1.3.4.7. 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。

1.3.4.8. 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。

1.3.4.9. 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
```

1.3.4.10. 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。Red Hat OpenShift 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-v1beta1-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。

1.3.4.11. 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。Red Hat OpenShift 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。

1.3.4.12. 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。

1.3.4.13. 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
```

1.3.4.14. 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. アプリケーション管理の制限事項

1.3.5.1. 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 の各表にある Clusters の列に、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アプリケーション、サブスクリプション、配置ルール、チャネルオブジェクト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. セキュリティーの既知の問題

1.3.6.1. 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。

重要:

- Red Hat Advanced Cluster Management の 2.1 バージョンは **削除され、サポートさ** れなくなりました。ドキュメントはそのまま利用できますが、エラータやその他の更新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。

注記: 固定化 されたアイテムは、製品のリリースから削除されたり、非推奨になることはありませんが、今後、更新や開発が行われることはありません。たとえば、API がリリースで新しいバージョンに置き換えられた場合に、**固定化** としてこのトピックに記載されます。この API は、非推奨または削除されるまでにリリース 1 回から 3 回ほど引き続き利用できます。

現在のリリースに安定している機能が記載されている場合のみ、**推奨アクション** にある代替アクションと、表で説明されている詳細について検討してください。

1.4.1. 非推奨

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
アプリケーション管理	**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

1.4.1.1. API の非推奨に関するガイダンス

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. 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。削除された機能に代わる代替機能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。
アプリケーション管理	Namespace のチャネルタイプを完全に削除	2.2	なし	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

- データのライフサイクル
- データの収集
- データストレージ
- データアクセス
- データ処理
- データの削除
- 個人データの使用を制限する機能
- 付録

1.5.3. GDPR

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

1.5.3.1. GDPR が重要な理由

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

- 個人の権利の追加および強化
- 個人データの定義の広義化
- データ処理者の義務の追加
- 遵守しない場合に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。