Red Hat Advanced Cluster Management for Kubernetes 2.0

リリースノート

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

Last Updated: 2023-03-07

Red Hat Advanced Cluster Management for Kubernetes 2.0 リリースノート

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

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

Red Hat Advanced Cluster Management for Kubernetes リリースノート、新機能、および既知の問題

目次

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

- Red Hat Advanced Cluster Management for Kubernetes の新機能
- 修正パッケージの更新
- 既知の問題と制限
- 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 が一般提供されるようになりました。バージョン 2.0 で提供されている機能をご確認ください。

Red Hat Advanced Cluster Management for Kubernetes では、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。

- 「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

Operator ベースのインストールでは、Amazon Web Services など、設定済みのクラウドプロバイダーに、Red Hat OpenShift Container Platform クラスターを 10 分未満でインストールできます。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. クラスター管理

- 各種 Kubernetes サービスプロバイダーにクラスターを作成します。選択した Kubernetes クラウドサービスプロバイダーで Red Hat OpenShift Container Platform クラスターをプロビジョニングし、管理できます。詳細は、「Red Hat Advanced Cluster Management for Kubernetes でのクラスターの作成」を参照してください。
- 既存の Kubernetes クラスターをインポートします。一般的なクラウドサービスプロバイダーまたはプライベートクラウドでホストされる既存の Kubernetes クラスターをインポートして、クラスターを扱いやすいように一箇所で管理します。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。
- 1 つのインターフェースで Red Hat OpenShift Container Platform クラスターのアップグレードをすべて管理します。インポートおよびプロビジョニングされた Red Hat OpenShift Container Platform クラスターは、コンソールを使用して個別で、またはまとめて、アップグレードできます。

1.1.3. アプリケーション管理

クラスター全体に分散されているビジネスアプリケーションをデプロイして維持します。アプリケーションの管理は、サブスクリプションベースの自動化を使用して実行できます。

コンソールのトポロジーページからアプリケーションやリソースのステータスの全体図も確認できます。

- サブスクリプションは、定義セットとして機能する Kubernetes リソースで、アノテーション、ラベル、バージョンを使用してチャネル内の Helm チャートと、Kubernetes リソース (GitHub、Objectstores またはハブクラスターの deployable) を特定します。
- アプリケーションリソースを使用して、アプリケーション全体でコンポーネントをグループ化して表示します。
- 配置ルールは、アプリケーションをサブスクライブする場所と方法を定義します。配置ルールを使用すると、マルチクラスターでのデプロイメントが容易になります。
- チャネルリソースは、アプリケーションコンポーネントを取得するためにサブスクライブするソースを定義します。(Git、Objectstore、Helm リポジトリーまたはハブ上にあるテンプレート (deployable))

詳細は、「アプリケーションの管理」を参照してください。

1.1.4. セキュリティーおよびコンプライアンス

Red Hat Advanced Cluster Management for Kubernetes は複数のロールをサポートし、Kubernetes 承認メカニズムを使用します。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。

製品ガバナンスフレームワークを使用して、マネージドクラスターのセキュリティーを強化します。ガバナンスおよびリスクダッシュボードでは、お使いのクラスターおよびアプリケーションでのセキュリティーリスクおよびポリシー違反の数を表示して管理できます。

カスタムのポリシーコントローラーを作成して、クラスター上のポリシーコンプライアンスを報告し、検証します。デフォルトでインストールされる以下のポリシーコントローラーを有効にして管理します。

- 証明書ポリシーコントローラー
- Kubernetes 設定ポリシーコントローラー
- IAM ポリシーコントローラー

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。

ポリシーの作成時に、ポリシーの要素である **templates** を使用して、リソースの定義方法を記述します。ポリシーの要素の詳細は、「セキュリティーポリシーの管理」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。

- Red Hat OpenShift Container Platform 4.7 は、2.0.x のエラータではサポートされません。

1.2.1. Errata 2.0.11

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.11 の更新について以下に一覧としてまとめています。

重要： Red Hat OpenShift Container Platform 4.5 は 2.0.11 ではサポートされません。Red Hat OpenShift Container Platform バージョン 4.6 を実行して、Red Hat Advanced Cluster Management バージョン 2.0.11 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 2.0.10 を使用できます。

1. Kubernetes **selfLink** の削除の結果として他のフィールドのデータを使用するように Search コードを更新。これにより、これらのフィールドに依存する Search ロジックに影響が及びました。(GitHub 11904)

2. **Policy** list ページに予期しないポリシーが表示される原因となっていた問題が修正されました。(GitHub 11853)

3. 廃止された変換されたコンソールコンテンツを削除。(GitHub 12640)

1.2.2. Errata 2.0.10

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.10 の更新について以下に一覧としてまとめています。

1. インポートされたクラスターディストリビューターバージョンを表示する **Clusters** ページが修正されました。(GitHub 11776)

2. 新規クラスターの作成時に利用可能な Red Hat OpenShift リリース **ClusterImageSets** を更新。(GitHub 10928)

3. ベアメタルアセットで誤ったステータスを報告する問題を修正(GitHub 10009)

1.2.3. Errata 2.0.9

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.9 は、コンテナーのアップグレード要件を解決しました。

1.2.4. Errata 2.0.8

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.8 の更新について以下に一覧としてまとめています。

1. **spec.SecretRef** のみが定義されているプライベート Helm リポジトリーチャネルからリソースをサブスクライブするために Helm サブスクリプションが作成されると、ハブクラスターのサブスクリプションがクラッシュする問題が修正されました。プライベート Helm リポジトリーチャネルシークレットは、同じチャネル namespace に定義する必要があります。(Bugzilla 1925281)

2. **cert-manager-webhook** Pod がパーミッションの問題により起動に失敗する問題が修正されました。イメージが更新され、特定のユーザーパーミッションの依存関係がなくなりました。(GitHub 9913)

3. spec.replicas が含まれない **Deployment** kind テンプレートで Helm サブスクリプションの Pod クラッシュや、整数ではない **spec.replicas** 値が含まれる問題が修正されました。(Bugzilla 1921531)

1.2.5. エラータ 2.0.7

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.7 は、特定されたセキュリティー CVE を解決しました。

1.2.6. エラータ 2.0.6

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.6 の更新について以下に一覧としてまとめています。

1. Google Cloud Platform でのクラスターの破棄が、すべてのサービスアカウントをクリーンアップしていなかった問題を修正しました。(GitHub 5948)
2. マネージドクラスターをデタッチした後に、create resources ページで一時的なエラーが発生する問題が修正されました。(GitHub 6299)
3. クラスターの追加に失敗した後に、Microsoft Azure マネージドクラスターの完全な破棄またはデタッチを妨げていた問題が修正されました。(GitHub 6353)
4. メモリーエラーが原因でベアメタルクラスターが 2.1.0 へのアップグレードに失敗する問題が修正されました。(GitHub 6898) (Bugzilla 1895799)
5. 新しい Visual Web ターミナルセッションの開始時に PATH エラーが修正されました。(GitHub 6928)
6. スケジュールされた時間に、**blocking** と **unblocking** 間の移行が時々妨げられていたサブスクリプション **timewindow** 関数の問題を解決しました。(GitHub 7337)

1.2.7. エラータ 2.0.5

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.5 の更新について以下に一覧としてまとめています。

1. セキュリティーコンポーネントの証明書を更新しました。(GitHub 6368)
2. Red Hat OpenShift Container Platform 4.6.1 のサポートが強化されました。(GitHub 6545)
3. Red Hat OpenShift Container Platform バージョン 4.6.1 の ClusterImageSet リソースが追加されました。(GitHub 6696)
4. ポリシーのアプリケーションフローが改善されました。(1890827)

1.2.8. エラータ 2.0.4

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.4 の更新について以下に一覧としてまとめています。

1. アップグレードする **search-operator** Pod のデフォルトメモリーを増加しました。(1882748)
2. クラッシュを防ぐために検索 Pod コレクターのソリューションを提供しました。(1883694)

3. プロビジョニングしたベアメタルクラスターが **Pending import** 状態のままの問題に対する解決策を提示しました。(1860233)

4. **ManagedClusterAction** リソースにビューアーの制限が追加されました。(GitHub 5843)

5. エージェントの証明書更新プロセスの強化。(GitHub 4914)

1.2.9. エラータ 2.0.3

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.3 の更新について以下に一覧としてまとめています。

1. アップグレードおよびインストールの改善および修正が追加されました。

2. システムを不安定にする **open-cluster-management** でリソースリークを修正しました。

3. ワーカーノードは必要ないため、ベアメタルのワークロードメッセージングが改善されました。

4. 他のベアメタルのユーザビリティーに関する問題に加えて、ベアメタルプロバイダー接続の編集機能が修正されました。

5. アンインストールの失敗の原因となっていた Webhook 検証エラーを解決しました。

6. Klusterlet 検索 Pod クラッシュが修正されました。

7. ポリシーの改善点の追加。

8. コンソールで、以下の不整合を修正し、以下の改善点を追加しました。

    a. **Application overview** ページのアプリケーション一覧における不安定性を修正しました。

    b. ポリシーアノテーションがない場合の **Governance and risk** ページの失敗を解決しました。

    c. ポリシー違反の **トポロジー** 不整合が修正されました。

    d. ポリシー違反ページの更新設定が修正されました。

    e. 伝播されたがコンソールで失敗したサブスクリプションが修正されました。

    f. クラウドプロバイダーの一覧へスクロールを追加し、ベアメタルオプションを表示します。

    g. ベアメタルクラスター作成コンソールの DNS VIP フィールドを有効化しました。

1.2.10. エラータ 2.0.2

エラータ 2.0.2 は、バージョン 2.0.0 からバージョン 2.0.1 にアップグレードした後に、一部のマネージドクラスターのインポートがまれに失敗していた問題を解決しています。エラータ 2.0.2 にアップグレードする前に、エラータ 2.0.1 にアップグレードする必要があります。

1.2.11. エラータ 2.0.1

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.0.1 の更新について以下に一覧としてまとめています。

1. クラスターのインポートプロセスが改善されました。
2. **oc** および **kubectl** CLI が Visual Web ターミナルの最新バージョンにアップグレードされました。
3. マネージドクラスターの Pod ログへの管理者 (**admin**) ロールアクセスが修正されました。
4. 製品のアンインストールプロセスが改善されました。
5. **Importing a cluster** ページのクラウドのフィールドオプションに **Bare metal** のラベルが追加されました。
6. クラスター作成時のデフォルトの **Network type** が OpenShiftSDN から OVNKubernetes に更新されました。
7. サブスクリプションは、インラインパッチの内容が文字列 1 つの **kustomization.yaml** ファイルをサポートするようになりました。
8. クラウドプロバイダーによる機密データの管理方法が改善されました。
9. クラスター作成のフローから DNS 仮想 IP パラメーターが削除されました。
10. クラスターのデタッチ時に概要ページが空白にならなくなりました。

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。

- 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. コンソールでリソースの作成に失敗する

Welcome ページで **Create resource** ボタンを選択すると、リソースの作成時に発生するエラーに関するアラートが表示される可能性があります。

この問題を解決するには、以下の手順を実行します。

1. ブラウザーキャッシュおよび Cookie を消去します。
2. Red Hat Advanced Cluster Management コンソールにログインします。
3. **Create resource** をクリックして再試行します。

重要: 入力した情報は、**Create resource** ページを更新すると失われます。

1.3.3. クラスター管理の既知の問題

1.3.3.1. 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。

1.3.3.2. 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。

1.3.3.3. klusterlet がデタッチされたクラスターで実行される

オンラインクラスターをアタッチした直後にデタッチすると、Klusterlet は **manifestwork** が同期する前に、デタッチされたクラスターで稼働し始めます。ハブクラスターからマネージドクラスターを削除しても、Klusterlet はアンインストールされません。問題を解決するには以下の手順を実行します。

1. **cleanup-managed-cluster** スクリプトを **deploy** Git リポジトリーからダウンロードします。
2. 以下のコマンドを入力して **cleanup-managed-cluster.sh** スクリプトを実行します。

```
./cleanup-managed-cluster.sh
```

1.3.3.4. 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。

1.3.3.5. OpenShift Container Platform 3.11 の割り当てを解除しても open-cluster-manangement-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** namesapce 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
```

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

クラウドプロバイダー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。クラウドプロバイダーでアクセスキーを更新するには、以下のコマンドを実行します。

- 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)

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

- Microsoft Azure

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

1.3.3.7. オフラインのマネージドクラスターをデタッチした後もリソースが残る

オフライン状態のマネージドクラスターをデタッチすると、マネージドクラスターから削除できないリソースがあります。これらのリソースを削除するには、以下の手順を実行します。

1. **oc** コマンドラインインターフェースが設定されていることを確認してください。
2. また、マネージドクラスターに **KUBECONFIG** が設定されていることを確認してください。**oc get ns | grep open-cluster-management-agent** を実行すると、2 つの namespace が表示されるはずです。

```
open-cluster-management-agent         Active   10m
open-cluster-management-agent-addon   Active   10m
```

3. **cleanup-managed-cluster** スクリプトを **deploy** Git リポジトリーからダウンロードします。
4. 以下のコマンドを入力して **cleanup-managed-cluster.sh** スクリプトを実行します。

```
./cleanup-managed-cluster.sh
```

5. 以下のコマンドを実行して、namespace が両方削除されていることを確認します。

```
oc get ns | grep open-cluster-management-agent
```

1.3.3.8. 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。

1.3.3.9. 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. アプリケーション管理の既知の問題

1.3.4.1. YAML マニフェストで複数のリソースを作成できない

managedclusteraction で複数のリソースはサポートされません。コンソールのリソース作成機能から、複数のリソースで、 YAML マニフェストを適用することはできません。

1.3.4.2. コンソールパイプラインカードで異なるデータが表示される場合がある

パイプラインの検索結果では、正確なリソース数を返しますが、パイプラインカードでは、アプリケーションで使用されていないリソースを表示するので、この数はカードの数と異なる場合があります。

たとえば、**kind:channel** の検索後に、チャネルが 10 件表示されるにも拘らず、コンソールのパイプラインカードでは使用されているチャネル 5 件だけが表示される可能性があります。

1.3.4.3. 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
```

1.3.4.4. namespace チャネルの deployable リソース

チャネル namespace 内で deployable リソースを手作業で作成する必要があります。

deployable リソースを正しく作成するには、deployable に必要な以下のラベル 2 つをサブスクリプションコントローラーに追加して、このコントローラーで追加する deployable リソースを特定します。

```
labels:
    apps.open-cluster-management.io/channel: <channel name>
    apps.open-cluster-management.io/channel-type: Namespace
```

各 deployable の **spec.template.metadata.namespace** でテンプレートの namespace を指定しないでください。

namespace タイプのチャネルおよびサブスクリプションの場合は、deployable テンプレートがすべてマネージドクラスターのサブスクリプション namespace にデプロイされます。そのため、サブスクリプション namespace 以外で定義される deployable テンプレートは省略されます。

詳細は、「チャネルの作成および管理」を参照してください。

1.3.4.5. 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。

1.3.4.6. 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。

1.3.4.7. 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します。

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。

1.3.4.8. 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。

使用している namespace で SCC CR を手動で作成するには、以下を実行します。

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

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

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

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

1.3.4.9. 一意の namespace でのアプリケーションチャネル

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 に各チャネルを作成することを推奨します。ただし、Git チャネルは、Git、Helm、Kubernetes namespace、オブジェクトストアなどの別のチャネルタイプで namespace を共有できます。

1.3.5. セキュリティーの既知の問題

1.3.5.1. コンソールへのログイン時の内部エラー 500

Red Hat Advanced Cluster Management for Kubernetes がインストールされ、OpenShift Container Platform がカスタム Ingress 証明書でカスタマイズされると、**500 Internal Error** メッセージが表示されます。OpenShift Container Platform 証明書が Red Hat Advanced Cluster Management for Kubernetes の管理 Ingress に含まれていないため、コンソールにアクセスできません。以下の手順を実行して OpenShift Container Platform 証明書を追加します。

1. 新しい証明書に署名するために使用される認証局が含まれる ConfigMap を作成します。ConfigMap は **openshift-config** namespace で作成されたものと同じである必要があります。以下のコマンドを実行します。

```
oc create configmap custom-ca \
    --from-file=ca-bundle.crt=</path/to/example-ca.crt> \
    -n open-cluster-management
```

2. 以下のコマンドを実行して **multiclusterhub** YAML ファイルを編集します。

```
oc edit multiclusterhub multiclusterhub
```

   a. **customCAConfigmap** のパラメーター値を編集して **spec** セクションを更新します。パラメーターは次のような内容になります。

```
customCAConfigmap: custom-ca
```

上記の手順が完了したら、変更がチャートに伝播されるまで数分待ち、ログインし直します。OpenShift Container Platform 証明書が追加されます。

1.3.5.2. クラスター名がポリシーの詳細パネルに表示されない

特定のポリシーの全クラスター違反がポリシーの詳細パネルに一覧表示されます。ユーザーにクラスターへのロールアクセスがない場合には、クラスター名は表示されません。クラスター名は、**-** の記号で表示されます。

1.3.5.3. ポリシーでの空のステータス

クラスターが実行されていない時にクラスターに適用されたポリシーは **NonCompliant** とみなされます。違反の詳細を表示すると、**status** パラメーターが空になっています。

1.3.5.4. 配置ルールとポリシーバインディングが空

ポリシーを作成または変更した後には、Red Hat Advanced Cluster Management コンソールのポリシー詳細で、配置ルールとポリシーバインディングが空になっている可能性があります。これは通常、ポリシーが無効になっているか、またはポリシーにその他の更新が加えられたことが原因となっています。YAML ビューのポリシーに対して、設定が正しく設定されていることを確認します。

1.3.5.5. helm リリースの削除後の cert-manager の復元

cert-manager および **cert-manager-webhook-helmreleases** を削除すると、Helm リリースがトリガーされ、チャートを自動的に再デプロイして新しい証明書を生成します。新しい証明書は、他の Red Hat Advanced Cluster Management コンポーネントを作成する他の helm チャートに同期する必要があります。ハブクラスターから証明書コンポーネントを復元するには、以下の手順を実行します。

1. 以下のコマンドを実行して、**cert-manager** の helm リリースを削除します。

   ```
   oc delete helmrelease cert-manager-5ffd5
   oc delete helmrelease cert-manager-webhook-5ca82
   ```

2. helm リリースが再作成され、Pod が実行されていることを確認します。

3. 以下のコマンドを実行して、証明書が生成されていることを確認します。

   ```
   oc get certificates.certmanager.k8s.io
   ```

   以下の応答が返される場合があります。

   ```
   (base) ➜  cert-manager git:(master) ✗ oc get certificates.certmanager.k8s.io
   NAME                        READY   SECRET                      AGE
   EXPIRATION
   multicloud-ca-cert          True    multicloud-ca-cert          61m   2025-
   09-27T17:10:47Z
   ```

4. **generate-update-issuer-cert-manifest.sh** スクリプト をダウンロードして実行し、この証明書を使用して他のコンポーネントを更新します。

5. **oc get certificates.certmanager.k8s.io** のシークレットの Ready 状態がすべて **True** となっていることを確認します。

1.4. 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

1.4.1. 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。

1.4.2. 目次

1.4.3. 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。

1.4.3.1. GDPR が重要な理由

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

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

1.4.3.2. GDPR の詳細情報

- EU GDPR の情報ポータル
- Red Hat GDPR の Web サイト

1.4.4. 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。

1.4.5. データのライフサイクル

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

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

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

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

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

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

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

1.4.5.2. オンラインの連絡先として使用される個人データ

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

- Slack チャネルがある場合は、Slack の公開コミュニティー
- 製品ドキュメントに関する公開コメントまたはチケット
- 技術コミュニティーでの公開会話

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

1.4.6. データの収集

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

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

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

- アプリケーションとの間で行き来するデータはどのように保護されるのか?移動中のデータは暗号化されているか?
- アプリケーションでデータはどのように保存されるのか?使用していないデータは暗号化されるのか?
- アプリケーションのアクセスに使用する認証情報はどのように収集され、保存されるのか?
- アプリケーションがデータソースへのアクセス時に使用する認証情報はどのように収集され、保存されるのか?

- アプリケーションが収集したデータを必要に応じて削除するにはどうすればよいか?

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

1.4.7. データストレージ

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

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

- **プラットフォームの設定データ:** Red Hat Advanced Cluster Management for Kubernetes プラットフォームの設定は、一般的な設定、Kubernetes、ログ、ネットワーク、Docker などの設定のプロパティーを使用して設定 YAML ファイルを更新し、カスタマイズできます。このデータは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームインストーラーへの入力情報として使用し、1 つまたは複数のノードをデプロイします。このプロパティーには、ブートストラップに使用される管理者ユーザー ID とパスワードも含まれます。

- **Kubernetes 設定データ:** Kubernetes クラスターの状態データは分散 Key-Value Store (KVS) (**etcd**) に保存されます。

- **ユーザー ID、パスワードなどのユーザー認証データ:** ユーザー ID およびパスワードの管理は、クライアントエンタープライズの LDAP ディレクトリーで対応します。LDAP で定義されたユーザーおよびグループは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームのチームに追加して、アクセスロールを割り当てることができます。Red Hat Advanced Cluster Management for Kubernetes プラットフォームでは、LDAP からメールアドレスとユーザー ID は保存されますが、パスワードは保存されません。Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、グループ名を保存し、ログイン時にユーザーが所属する利用可能なグループをキャッシュします。グループメンバーシップは、長期的に永続化されません。エンタープライズ LDAP で未使用時にユーザーおよびグループデータのセキュリティー確保について、考慮する必要があります。Red Hat Advanced Cluster Management for Kubernetes プラットフォームには、認証サービスと、エンタープライズディレクトリーと対応して、アクセストークンを管理する Open ID Connect (OIDC) が含まれます。このサービスは MongoDB 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。

1.4.8. データアクセス

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

- Web ユーザーインターフェイス (コンソール)

- Kubernetes の **kubectl** CLI

- Red Hat Advanced Cluster Management for Kubernetes CLI
- oc CLI

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

1.4.8.1. 認証

Red Hat Advanced Cluster Management for Kubernetes プラットフォームの認証マネージャーは、コンソールからのユーザーの認証情報を受け入れ、バックエンドの OIDC プロバイダーに認証情報を転送し、OIDC プロバイダーはエンタープライズディレクトリーに対してユーザーの認証情報を検証します。次に OIDC プロバイダーは認証クッキー (**auth-cookie**) を、JSON Web Token (**JWT**) のコンテンツと合わせて、認証マネージャーに返します。JWT トークンは、認証要求時にグループのメンバーシップに加え、ユーザー ID やメールアドレスなどの情報を永続化します。この認証クッキーはその後コンソールに返されます。クッキーはセッション時に更新されます。クッキーは、コンソールをサインアウトしてから、または Web ブラウザーを閉じてから 12 時間有効です。

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

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

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

1.4.8.2. 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。

1.4.8.3. 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、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。

1.4.8.4. 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。

1.4.9. 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。

1.4.10. データの削除

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

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

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

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

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

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

1.4.11. 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。

1.4.12. 付録

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

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