Red Hat Advanced Cluster Management for Kubernetes 2.1

リリースノート

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

Last Updated: 2022-01-31

Red Hat Advanced Cluster Management for Kubernetes 2.1 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

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Release_notes.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

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

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。
- 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
  - 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、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

- ハブクラスターを管理できるようになりました。Red Hat Advanced Cluster Management をインストールすると、ハブクラスターが自動的にインポートされ、管理されます。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. Web コンソール

- Web コンソールを使用して、集約ビューでクラスターへのアクセス、表示、管理を行います。Red Hat OpenShift Container Platform から Red Hat Advanced Cluster Management コンソールにアクセスし、クラスターデータおよび詳細を監視し、クラスター全体の検索コンポーネントを使用し、Visual Web ターミナルを使用してクラスターラベルを管理できます。コンソールコンポーネントの詳細は、「Web コンソール」を参照してください。
- マルチクラスター可観測性サービス (**multicluster-observability-operator**) を有効化して、マネージドクラスターのヘルスの表示と最適化が可能になりました。マネージドクラスターから収集したメトリクスデータおよびログを確認できます。詳細は、「環境の監視」を参照してください。

1.1.3. クラスター管理

- ベアメタル環境でクラスターを作成して管理できるようになりました。詳細は、「ベアメタルでのクラスターの作成」を参照してください。
- さらに、Red Hat Advanced Cluster Management を使用して、VMware vSphere 上で Red Hat OpenShift Container Platform クラスターを作成して、管理できます。詳細は、「VMware vSphere でのクラスターの作成」を参照してください。
- ManagedClusterSet リソースを作成して、クラスターをグループ化し、そのグループへのアクセス権をユーザーに付与できるようになりました。詳細は、「ManagedClusterSets」を参照してください。
- Red Hat OpenShift Update Service Operator と Red Hat Advanced Cluster Management for Kubernetes を統合すると、非接続環境でマネージドクラスターをアップグレードできます。詳細は、「非接続クラスターのアップグレード」を参照してください。

1.1.4. アプリケーション管理

- Red Hat Advanced Cluster Management for Kubernetes アプリケーションの管理では、リソース管理のコンソール設定で使用性が改善されました。コンソールでサポートされるチャネルを使用したアプリケーションの作成、アプリケーションの編集、シークレットオプションの設定などが可能になりました。アプリケーションリソースの管理 を参照してください。
- **Advanced configuration** から **Subscriptions**、**Placement rules** または **Channels** を選択して、表内のリソースを表示できます。表から、これらのリソースを YAML として編集することもできます。
- Red Hat Advanced Cluster Management for Kubernetes と Ansible Tower の統合はテクノロジープレビュー機能として利用できます。この機能を使用して、コンソールから Ansible ジョブをデプロイし、管理できます。また、**リソーストポロジー** でジョブのステータスを表示することもできます。「アプリケーションコンソール」を参照してください。
- アプリケーション管理の一環として、Ansible Tower のジョブを Git サブスクリプションに統合できます。タスクを自動化し、Slack や PagerDuty サービスなどの外部サービスと統合します。Ansible の使用に関する詳細は、「Ansible Tower タスクの設定 (テクノロジープレビュー機能)」を参照してください。

アプリケーション管理の変更およびドキュメントの改善についてはすべて、「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 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。
- 証明書ポリシーコントローラーでは、**disallowedSANPattern** パラメーターを使用して、パターンに対して DNS 名を照合できます。詳細は、「証明書ポリシーコントローラーの YAML の表」を参照してください。
- 製品ガバナンスフレームワークでポリシーを追加して、オープンソースコミュニティー (**open-cluster-management/policy-collection**) に貢献できるようになりました。サードパーティーのポリシー (guardkeeper など) を統合できます。詳細は、「サードパーティーポリシーコントローラーの統合」を参照してください。

- 設定ポリシーコントローラーを使用して ETCD 暗号化ポリシーを作成できるようになりました。ETCD 暗号化ポリシーを使用して機密データの暗号化を有効にします。詳細は、「ETCD 暗号化ポリシーの管理」を参照してください。
- クラスターバインディングとして **local-cluster** を選択して、自己管理のハブクラスター (ローカルハブクラスター) のポリシーを作成できるようになりました。詳細は、「セキュリティーポリシーの作成」を参照してください。
- これで **Status** タブからポリシー違反の履歴を表示できるようになりました。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。

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: 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。

1.2.1. エラータ 2.1.13

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。

1.2.2. エラータ 2.1.12

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。

1.2.3. エラータ 2.1.11

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。

1.2.4. エラータ 2.1.10

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 2.1.9

イメージ内の一部のコンテナーが更新されました。

1.2.6. エラータ 2.1.8

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.1.8 の更新について以下に一覧としてまとめています。

重要： エラータ 2.1.7 以降にアップグレードするには、Red Hat OpenShift Container Platform バージョン 4.6 以降を実行する必要があります。Red Hat OpenShift Container Platform バージョン 4.5 をそれ以降のバージョン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 2.1.6 を使用できます。

- Red Hat OpenShift Container Platform 4.6.30 へのアップグレード後の **クラッシュループ状態の** Observability **thanos-store-shard** Pod の問題を解決します。(GitHub 13081)

- コンソールで無効なポリシー **を** 削除すると、placementrule および **placementbinding** が削除されない問題を修正します。(GitHub 12689)

- Kubernetes selfLink の削除の結果として他のフィールドからのデータを使用するように Search コードを更新し、それらのフィールドに依存する Search ロジックに影響を与えました。(GitHub 12701)

1.2.7. エラータ 2.1.7

重要： Red Hat Advanced Cluster Management バージョン 2.1.7 にアップグレードするには、Red Hat OpenShift Container Platform バージョン 4.6 以降を実行する必要があります。Red Hat OpenShift Container Platform バージョン 4.5 をそれ以降のバージョン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 2.1.6 を使用できます。

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.1.7 の更新について以下に一覧としてまとめています。

- Hive コントローラーログに正しくないバージョン情報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 12014)

- **ManagedClusterView** リソースを作成および削除するための **表示** パーミッションを持つユーザーの承認を追加。また、**表示** パーミッションを持つユーザーがマネージドクラスターリソースの YAML ファイルを表示できるようになりました。(GitHub 11243)

- **clusterimagesets** リソースで create、update、および delete 操作を実行するために **cluster-manager-admin** ロールバインディングを持つユーザーを有効化。この変更により、**cluster-manager-admin** 権限を持つユーザーは Red Hat Advanced Cluster Management でクラスターをプロビジョニングできます。(GitHub 11596)

1.2.8. エラータ 2.1.6

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.1.6 の更新について以下に一覧としてまとめています。

- 新規クラスターの作成時に、利用可能な Red Hat OpenShift Container Platform リリース ClusterImageSets の一覧を更新しました。(GitHub 10760)

- 生成された import コマンドに引用符を追加し、コマンドの実行時に考えられるエラーを回避します。(Bugzilla 1934184)(GitHub 9983)

1.2.9. エラータ 2.1.5

注記： OpenShift Container Platform バージョン 4.7 はベアメタルではサポートされません。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 ハブクラスターでベアメタルのマネージドクラスターを作成することはできません。

- **packageOverrides** がサブスクリプション CR に誤って指定される場合に発生したログエラーを修正エラーが正しくログに記録され、正しい **packageOverrides** 仕様が無視されるようになりました。(GitHub 10008)

- クラスターの追加に使用できる Azure リージョンの一覧を更新しました。Bugzilla 1932430

- **アプリケーショントポロジー** ページが予期しないエラーを表示する原因となっていた問題が修正されました。(GitHub 9377)

- **spec.SecretRef** のみが定義されているプライベート Helm チャネルからリソースのサブスクライブに使用される場合に、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。ハブクラスターのサブスクリプションは、このタイプの Helm サブスクリプションではクラッシュしなくなりました。プライベートの Helm リポジトリーチャネルのシークレットは、同じチャネル namespace に定義する必要があります。Bugzilla 1932430

- 作成した Ansible prehook および posthook ジョブが重複していた問題を修正これで、Ansible prehook および posthook ジョブが 1 つだけ作成され、アプリケーションのサブスクリプションにより実行されるようになりました。(Bugzilla 1920654)

- **Overview** ページを更新し、ハブクラスター(local-cluster)からのリソースを追加します。(Bugzilla 1903446)

1.2.10. エラータ 2.1.4

イメージ内の一部のコンテナーが更新されました。

1.2.11. エラータ 2.1.3

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.1.3 の更新について以下に一覧としてまとめています。

- **appsub** が正常にデプロイされるように **multicluster-operators-hub** Pod でのパニックエラーを修正しました (Bugzilla 1921531)。

- VMware で作成され、ワーカープール CPU、メモリー、またはディスクサイズに指定された値を使用しないマネージドクラスターの問題が修正されました。(GitHub 8930)

- ポリシーのセレクターと一致する作成済みまたは削除済みの namespace が証明書ポリシーコントローラーで検出されない問題が修正されました。(GitHub 7639)

- Grafana ClusterRoleBinding オブジェクトの問題が修正されました。(GitHub 7621)

- ポリシーの処理時に設定ポリシーコントローラーがクラッシュする問題が修正されました。(GitHub 7569)

- 既存のプロバイダー接続の編集時に namespace が欠落する問題が修正されました。(GitHub 7501)

- ポリシーが存在しない URL に移動すると、アニメーションが読み込まれる代わりにポリシーページに **No resource** と表示されるルーティングの問題が修正されました。(GitHub 7445)

- コンテンツのコピーアンドペースト時にポリシーエディターがクラッシュする問題と、カスタム仕様があることを表示するフォームが更新されない場合に **.spec.policyTemplate** でエラーが発生する問題が修正されました。(GitHub 7380)

- チャネル接続の失敗に関するメッセージがサブスクリプションステータスに追加されました。(GitHub 7177)

- コンソールの **Delete application** モーダルに表示されていた削除可能なアプリケーションリソースからチャネルが除外されました。このモーダルではチャネルを削除できなくなりました。今回の修正で、このモーダルで削除できるのはサブスクリプションと配置ルールのみになりました。(GitHub 7153)

- NIST コンテンツに合わせて、全ポリシー要素で一貫性が保たれるように NIST カテゴリー、標準、制御の表示が修正されました。(GitHub 6954)

- 介入なしに最大のワークロードを処理できるように、デフォルトのインストール設定での検索 Pod メモリーの要求と上限が増やされました (**redisgraph** Pod が 4GB、検索 API および Redisgraph Pod のメモリー要求が 128MB)。(GitHub 6890)

- **secretRef** がないことが原因でプライベート Git への Git チャンネルの接続に失敗し、**multicluster-operators-hub-subscription** Pod がクラッシュする問題が修正されました。(GitHub 8764)

- OpenShift Container Platform 4.6.10 インストールのパーミッションの問題が原因で、**cert-manager-webhook** の起動に失敗する問題が修正されました。(GitHub 8517)

- 多数のコンパクターが競合する高可用性設定が修正され、コンパクターが 1 つだけ実行されるようになりました。(GitHub 7676)

- Grafana ダッシュボードがメトリクス消去の間隔よりも短い間隔で自動更新され、パフォーマンスに影響を与える可能性のある問題が修正されました。(GitHub 7665)

- 管理向けの Red Hat OpenShift on IBM Cloud クラスターのインポートがサポートされるようになりました。(Bugzilla 1894778)

- サブスクリプションを使用して選択した Git リポジトリーリソースをターゲットクラスターにデプロイする Git Webhook 通知機能が修正されました。(GitHub 6785)

- 正常にデプロイされるにも拘らず、オフラインでアクセスできないアプリケーショントポロジーリソースの問題が修正されました。リモートクラスターがオフラインの場合に、ステータスが Failed とクラスターノードに表示されるようになりました。(GitHub 6298)

1.2.12. エラータ 2.1.2

Red Hat Advanced Cluster Management for Kubernetes の エラータ 2.1.2 の更新について以下に一覧としてまとめています。

- 登録エージェント証明書の更新要求をハブクラスターが拒否し、1 ヶ月後に登録エージェントの一部がオフラインになるという問題が修正されました。(GitHub 5628)

- Red Hat Advanced Cluster Management のアップグレード時に一部のクラスターイメージセット間で競合を引き起こしていた問題が修正されました。(GitHub 7527)

- アップグレード時に一部の証明書が削除される原因となっていた問題が修正されました。(GitHub 7533)

1.2.13. エラータ 2.1.1

Red Hat Advanced Cluster Management の エラータ 2.1.1 の更新について以下に一覧としてまとめています。

- **certificate** および **iam** ポリシーコントローラーを更新し、ポリシー違反の履歴を正しく維持できない問題を修正しました。(GitHub 6014)

- VMware マネージドクラスターのデフォルトのワーカーノード値を増やし (4 CPU、2 コア、16384 MB メモリー)、他のプロバイダーに合わせました。(GitHub 6206)

- 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)

- アプリケーションの終了、変更、および再開後に、**Merge updates** オプションが **unset** に変更される問題が修正されました。(GitHub 6349)

- 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クリーンアップを妨げていた問題が修正されました。(GitHub 6353)

- **helm** タイプのアプリケーションを **local-cluster** にデプロイした後に、アプリケーショントポロジーが正しいリソースノードを表示できない問題が修正されました。アプリケーショントポロジーでは、すべてのタイプのアプリケーションが表示されるようになりました。(GitHub 6400)

- アプリケーションサブスクリプション: Git **kustomization.yaml** ファイルの **packageOverrides** YAML コンテンツを有効にし、デフォルトでサブスクリプションのアノテーションで識別されるパスを使用します。(GitHub 6476)

- 複数のサブスクリプションが同じ Git チャネルを同じブランチで共有した場合に、サブスクリプションの上書きが機能しない問題が修正されました。(GitHub 6476)

- オブジェクト一覧で、**musthave** コンプライアンスタイプを使用するポリシーが、**mustonlyhave** コンプライアンスタイプと同様の動作をする問題が修正されました。オブジェクト一覧のたった 1 つのフィールドを指定し、一覧内の 1 つのオブジェクトにポリシーで指定されたフィールドに一致するフィールドがある限り、**musthave** ポリシーはそのフィールドを準拠しているとマークできるようになりました。(GitHub 6492)

- すべての時系列に 3 つのコピーを保存できるように、すべての Thanos レシーバーを設定する問題を解決しました。また、ターゲットハッシュリングの少なくとも 2 つの Thanos レシーバーに、すべての時系列が正常に書き込まれるようにします。(GitHub 6547)

- **Create** ウィザードでアプリケーションを作成し、これをエディターで開いた際に、**merge update** 設定を選択すると、この設定が消去される問題が修正されました。(GitHub 6554)

- ポリシーが **noncompliant** 状態を表示する原因となっていた問題が修正されました。(GitHub 6630)

- Git Webhook がチャネルおよびサブスクリプションで有効化された場合に発生する問題が修正されましたが、サブスクライブしているリソースはターゲットクラスターに適用されませんでした。(GitHub 6785)

- 最初の読み込み時の **Forbidden** エラーで、**create resource** コマンドが失敗する可能性がある問題を解決しました。(GitHub 6798)

- 永続ボリューム用に、Red Hat Advanced Cluster Management 可観測性コンポーネントで、以下の追加のメトリクスを公開しました。

  - **kubelet_volume_stats_available_bytes**

  - **kubelet_volume_stats_capacity_bytes**

  - **kube_persistentvolume_status_phase**
    これらのメトリクスは、ダッシュボードまたはアラートルールで明示的に公開されていませんが、それらをクエリーし、カスタムアラートルールを設定することができます。(GitHub 6891)

- 新しいポリシーの作成時における選択および選択解除の不整合が修正されました。(GitHub 6897)

- 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)
- 可観測性コンポーネントを正常にインストールするために **open-cluster-management-observability** namespace でプルシークレットを必要とする問題が修正されました。この変更では、可観測性コンポーネントをインストールするためにプルシークレットを作成する必要はありません。(GitHub 6911)
- ガバナンスおよびリスクダッシュボードの読み込みに長い時間がかかる問題が修正されました。(GitHub 6925)
- 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)
- 可観測性 Operator がランタイム時に再起動される際に、マネージドクラスターでの可観測性コンポーネントが誤ったイメージを使用するよう変更されるというタイミングの問題を修正しました。(GitHub 6942)
- プライベート Git リポジトリーから失敗したアプリケーション作成を回避するために、修正を適用する手順が追加されました。(GitHub 6952) (Bugzilla 1896341)
- **open-cluster-management** namespace 以外の namespace にある場合に、 **klusterlet-addon-controller** が認識されないという問題が修正されました。(GitHub 6986)
- オブジェクトテンプレートが一覧を求めてフィールドをチェックしたところ、想定していた一覧とは違うものがそのフィールドに設定されていることに気づいた際に、設定ポリシーコントローラーがクラッシュする問題を修正しました。(GitHub 7135)
- すべてのオンラインクラスターにデプロイされたアプリケーションに変更を加える際に、テンプレートエディターの YAML が placementRule **status: 'True'** 設定を除外する問題を修正しました。
  更新されたアプリケーションを保存する前に、placementRule の YAML エディターで **status: 'True'** を手動で入力すると、設定は保持されます。(GitHub 7152)
- その他の一般的な変更や、記載されていないコードおよびドキュメントへのバグ修正が完了しました。

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。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。

- アップグレードの既知の問題
- インストールの既知の問題
- Web コンソールの既知の問題
- 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. アップグレードの既知の問題

1.3.1.1. 可観測性アドオンにより、バージョン 2.1.x から 2.3.2 へのアップグレードの低下

2.1.x から 2.3.2 へのアップグレード後、可観測性アドオンの準備が整わないか、またはアップグレード時にイメージマニフェスト ConfigMap が正しく読み込まれないため、一部のクラスターのパフォーマンスが低下してしまう可能性があります。これにより、誤ったイメージが生じます。

この問題を修正するには、以下のコマンドを実行して **multicluster-observability-operator** Pod を再起動します。

oc delete pod multicluster-observability-operator -n open-cluster-management

1.3.1.2. 2.1.x にアップグレードすると、証明書が失われます。

Red Hat Advanced Cluster Management をバージョン 2.0 から 2.1 にアップグレードした後、アプリケーションテンプレートエディターを開いて変更を行う際に、アプリケーションをデプロイする場所を指定する設定は事前に選択されません。アプリケーションテンプレートエディターでアプリケーション設定を変更した場合には、エディターを保存して閉じる前に、アプリケーションのデプロイメント設定を選択する必要があります。

1.3.1.3. 2.1.1 へのアップグレードにより証明書が失われます。

クラスターを Red Hat Advanced Cluster Management バージョン 2.1.1 にアップグレードすると、クラスター上の証明書の一部またはすべてが失われます。以下のコマンドのいずれかを入力すると、この状況を確認できます。

```
oc get certificates -n open-cluster-management
```

または

```
oc get pods -n open-cluster-management | grep -vE "Completed|Running"
```

最初のコマンドの実行時に想定よりも少ない証明書が返された場合、または 2 番目のコマンドの実行後に複数の Pod が返された場合は、 **generate-update-issue-cert-manifest.sh** スクリプト を実行して証明書を更新します。

1.3.1.4. バージョン 2.1.1 へのアップグレードは、ClusterImageSet エラーにより完了しません。

Red Hat Advanced Cluster Management for Kubernetes バージョン 2.1.0 を Red Hat Advanced Cluster Management バージョン 2.1.1 にアップグレードしても完了せず、以下のエラーと同様のエラーが表示される場合があります。

```
failed to get candidate release: rendered manifests contain a resource
that already exists. Unable to continue with update: ClusterImageSet "img4.6.1-x86-64"
in namespace "" exists and cannot be imported into the current release: invalid
ownership metadata; label validation error: missing key "app.kubernetes.io/managed-by":
must be set to "Helm"; annotation validation error: missing key "meta.helm.sh/release-name":
must be set to "console-chart-c4cb5"; annotation validation error: missing key
"meta.helm.sh/release-namespace": must be set to "open-cluster-management"
```

これは、既存バージョンの 1 つまたは複数の ClusterImageSets に、アップグレードと共に追加されるバージョンと同じ名前を持つ場合に生じます。これにより、競合が生じます。この問題を回避するには、以下の手順を実行します。

1. 実行中のアップグレードを停止します。
2. エラーメッセージで特定されるローカル環境から、ClusterImageSet または ClusterImageSets を削除します。
3. アップグレードを再起動します。

1.3.1.5. 2.1.1 へのアップグレードにより、klusterletaddonconfig CRD が無効になります。

Red Hat Advanced Cluster Management をバージョン 2.1.0 から 2.1.1 にアップグレードすると、アップグレード中に **klusterletaddonconfig** カスタムリソース定義 (CRD) が再インストールされる可能性があります。再インストールされる場合、すべてのアドオンは **Cluster settings** ページに **Disabled** ステータスを表示します。問題を診断し、klusterletaddonconfig CRD を復元するには、以下の手順を実行します。

1. **oc login** コマンドを使用して、ハブクラスターにログオンします。
2. 以下のコマンドを実行して、**klusterletaddonconfig** CRD が削除されたのは、CRD の再インストールが原因であることを確認します。

   ```
   % oc get klusterletaddonconfig --all-namespaces
   ```

   返されるコンテンツが **No resources found** の場合は、再インストールが原因である可能性が高いです。ステップ 3 に進みます。

3. 以下のスクリプトをファイルに保存します。この例では、ファイル名は **restore-addons.sh** です。

   ```
   KUBECTL=oc
   ACM_NAMESPACE=open-cluster-management

   ACM_VERSION=$(${KUBECTL} get -n ${ACM_NAMESPACE} `${KUBECTL} get mch -
   oname -n ${ACM_NAMESPACE} | head -n1` -ojsonpath='{.status.desiredVersion}')
   if [ "${ACM_VERSION}" = ""  ]; then
   ACM_VERSION=2.1.1
   fi

   echo "ACM version: ${ACM_VERSION}"

   for clusterName in `${KUBECTL} get managedcluster --ignore-not-found | grep -v "NAME" |
   awk '{ print $1 }'`; do
       echo "Checking klusterletaddonconfig in ${clusterName} namespace."
       ${KUBECTL} get klusterletaddonconfig ${clusterName} -n ${clusterName} >/dev/null 2>&1
       if [ "$?" != "0"  ]; then
           echo "  klusterletaddonconfig in ${clusterName} is missing."
           echo "  Creating..."
           printf "  "
           cat <<EOF | ${KUBECTL}  apply -f -
   apiVersion: agent.open-cluster-management.io/v1
   kind: KlusterletAddonConfig
   metadata:
     name: ${clusterName}
   ```

```
  namespace: ${clusterName}
spec:
  clusterLabels:
    cloud: auto-detect
    vendor: auto-detect
  clusterName: ${clusterName}
  clusterNamespace: ${clusterName}
  applicationManager:
    enabled: true
  certPolicyController:
    enabled: true
  iamPolicyController:
    enabled: true
  policyController:
    enabled: true
  searchCollector:
    enabled: true
  version: ${ACM_VERSION}
EOF

    fi
    echo "  Done."
done
```

open-cluster-management namespace に Red Hat Advanced Cluster Management をインストールしなかった場合は、**ACM_NAMESPACE** の値を namespace の名前に置き換えます。

4. CLI からスクリプトを実行します。コマンドは、以下のコマンドのようになるはずです。

```
chmod +x restore-addons.sh && ./restore-addons.sh
```

スクリプトを実行すると、削除された **klusterletaddonconfig** CRD が各マネージドクラスター namespace に再作成されます。

1.3.1.6. 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。

1.3.1.7. バージョン 2.0.4 から 2.1 にアップグレードすると、ClusterServiceVersion が保留状態のままになる

Red Hat Advanced Cluster Management バージョン 2.0.4 から 2.1 にアップグレードした後に、**oc get csv** コマンドを実行します。この出力で、Red Hat Advanced Cluster Management ClusterServiceVersion (CSV) の **PHASE** が **Pending** にも拘らず、**NAME** は **advanced-cluster-management.v2.1.0** に更新されています。

この問題を回避するには、以下の手順を実行し、 **clusterRole** カスタムリソースを検索して、このリソースがない場合には作成します。

1. 以下のコマンドを入力して、the Red Hat Advanced Cluster Management 2.1 CSV がデプロイした **clusterrolebinding** リソースすべてを検索します。

```
oc get clusterrolebinding |grep advanced-cluster-management
```

出力は次のような内容になるはずです。

```
advanced-cluster-management.v2.1.0-86dfdf7c5d          ClusterRole/advanced-cluster-
management.v2.1.0-86dfdf7c5d       9h
advanced-cluster-management.v2.1.0-cd8d57f64           ClusterRole/advanced-cluster-
management.v2.1.0-cd8d57f64        9h
```

2. 以下のようなコマンドを入力して、各 **clusterrolebinding** を開き、**open-cluster-management** サービスアカウントに関連付けられている **clusterRole** 名を検索します。

```
oc get clusterrolebinding advanced-cluster-management.v2.1.0-cd8d57f64 -o yaml
```

出力は次のような内容になるはずです。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: advanced-cluster-management.v2.1.0-cd8d57f64
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: advanced-cluster-management.v2.1.0-cd8d57f64
subjects:
- kind: ServiceAccount
  name: multicluster-operators
  namespace: open-cluster-management
```

3. 以下のコンテンツを **.yaml** ファイルに追加し、欠落している **clusterRole** エントリーを手作業で作成します。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: advanced-cluster-management.v2.1.0-cd8d57f64
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
```

1.3.2. インストールの既知の問題

1.3.2.1. 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
```

1.3.3. Web コンソールの既知の問題

1.3.3.1. 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。

1.3.3.2. 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。

1.3.3.3. 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。

1.3.3.4. 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。

1.3.3.5. 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。

1.3.3.6. 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
```

1.3.3.7. MultiClusterObservability CR 名が原因で可観測性が機能しない

一意の名前で **MultiClusterObservability** カスタムリソース(CR)をデプロイする場合、メトリクスデータは収集されません。**metrics-collector** が作成されないため、メトリクスは収集されません。可観測性のデプロイ時に、Red Hat Advanced Cluster Management は **MultiClusterObservability** CR のデフォルト名（ **可観測性** ）のみの使用をサポートします。

1.3.4. クラスター管理の既知の問題

1.3.4.1. 新規ベアメタルアセットオプションが表示されない

ベアメタルアセットを作成して保存した後に、テーブルでベアメタルアセットを選択し、選択したアクションを適用できます。この問題により、新しいベアメタルアセットを選択した後に利用可能なアク

ションが表示されない可能性があります。ブラウザーウィンドウを更新し、表の最初にアクションを復元します。

1.3.4.2. 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。

1.3.4.3. 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。

1.3.4.4. 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。

1.3.4.5. 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。

1.3.4.6. 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。

1.3.4.7. 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。

1.3.4.8. 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
```

1.3.4.9. 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、クラスターの名前に置き換えます。

  $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}"} }]'
  ```

1.3.4.10. 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。

1.3.4.11. 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。

1.3.4.12. 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。

1.3.4.13. 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。

1.3.5. アプリケーション管理の既知の問題

1.3.5.1. 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。

1.3.5.2. リソーストポロジーのステータスがデプロイされていない

Helm サブスクリプションに **packageAlias** が定義されていない場合には、リソーストポロジーはリモートクラスターリソースを **Not deployed** と表示します。

「パッケージの上書きの設定」を参照して、適切な **packageName** および **packageAlias** を定義してください。

1.3.5.3. 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。

1.3.5.4. アプリケーションの編集時にコンソールでの更新マージオプションの選択が解除される

アプリケーションコンソールで、アプリの編集時に **Merge update** の選択が解除されます。以前に選択したオプションがあり、更新のマージを継続する場合には、再度オプションを選択し直す必要があります。

更新のマージが正常に行われたことを確認するには、YAML サブスクリプションアノテーションに **reconcile-option: merge** が含まれていることを確認します。コンソールで以下の手順を実行します。

1. コンソールのリソーストポロジーの図で **Subscription** ノードをクリックします。
2. サブスクリプションの詳細のポップアップウィンドウで **View Resource YAML** ボタンをクリックします。
3. **apps.open-cluster-management.io/reconcile-option: merge** アノテーションがサブスクリプションの **.yaml** ファイルに作成されていることを確認します。

1.3.5.5. プライベートの Git URL が存在する場合に Git ブランチと URL パスのフィールドが生成されない

プライベート Git リポジトリーでアプリケーションを作成して **Create application** をクリックし、別の Git タイプを作成すると、コンソールのフィールドに以前の URL が入力されません。

このような場合には、アプリケーションエディターにチャネルの認証情報の詳細が表示されません。既存のチャネルリポジトリーのリポジトリー認証情報を変更すると、そのリポジトリーにサブスクライブする既存のアプリケーションを管理できません。

この問題を解決するには、チャネルリソースの認証情報を更新するか、チャネルを削除して再作成します。

YAML エディターを使用して、最新の認証情報でチャネルリソースを更新します。
link:../manage_applications#managing-apps-with-git-repositories[Managing apps with Git repositories] のサンプルのセクションを参照してください。

1.3.5.6. 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。

1.3.5.7. namespace チャネル

namespace チャネルは、コードでは機能する可能性がありますが、このオプションはまだドキュメント化されていません。

1.3.5.8. 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
```

1.3.5.9. 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。

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。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。

1.3.5.11. 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。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。

1.3.5.12. 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。

1.3.6. セキュリティーの既知の問題

1.3.6.1. 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。

1.3.6.2. 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

1.4.3.2. 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。

1.4.5.1. 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。

1.4.5.2. 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。

1.4.6. 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。

1.4.7. 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。

1.4.8. 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。

1.4.8.1. 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。

1.4.8.2. 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。

1.4.8.4. 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。

1.4.11. 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。