



Red Hat Advanced Cluster Management for Kubernetes 2.5

リリースノート

新機能、エラータの更新、既知の問題、非推奨と削除、および GDPR と FIPS の準備に関する製品の考慮事項に関するリリースノートの詳細をお読みください。

Red Hat Advanced Cluster Management for Kubernetes 2.5 リリースノート

新機能、エラータの更新、既知の問題、非推奨と削除、および GDPR と FIPS の準備に関する製品の考慮事項に関するリリースノートの詳細をお読みください。

法律上の通知

Copyright © 2023 Red Hat, Inc.

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

新機能、エラータの更新、既知の問題、非推奨と削除、および GDPR と FIPS の準備に関する製品の考慮事項に関するリリースノートの詳細をお読みください。

目次

第1章 リリースノート	3
1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES の新機能	3
1.2. 既知の問題	7
1.3. エラータの更新	29
1.4. 非推奨と削除	32
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	37
1.6. FIPS READINESS	43

第1章 リリースノート

重要: Red Hat Advanced Cluster Management の 2.5 以前のバージョンは削除され、サポートされなくなりました。バージョン 2.5 以前のドキュメントは更新されていません。ドキュメントはそのまま利用できますが、エラータやその他の更新はなく、非推奨となります。

ベストプラクティス: Red Hat Advanced Cluster Management の最新バージョンにアップグレードします。

- [Red Hat Advanced Cluster Management for Kubernetes の新機能](#)
- [エラータの更新](#)
- [既知の問題と制限](#)
- [非推奨と削除](#)
- [GDPR に対応するための Red Hat Advanced Cluster Management for Kubernetes での考慮事項](#)
- [FIPS readiness](#)

1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES の新機能

Red Hat Advanced Cluster Management for Kubernetes では、可観測性を提供し、ビルトインされたガバナンス、クラスターおよびアプリケーションライフサイクル管理で、Kubernetes ドメイン全体を可視化します。今回のリリースでは、より多くの環境でのクラスター管理、アプリケーション向けの GitOps 統合などが可能になりました。

重要: 一部の機能およびコンポーネントは [テクノロジープレビュー](#) として指定され、リリースされません。

詳細は、本リリースの新機能を参照してください。

- [Red Hat Advanced Cluster Management for Kubernetes へようこそ](#) から Red Hat Advanced Cluster Management for Kubernetes の概要を確認してください。
- オープンソースの **Open Cluster Management** リポジトリでは、オープンコミュニティからの貢献、コミュニケーションや展開への準備が整いました。[open-cluster-management.io](#) を参照してください。詳細は [GitHub リポジトリ](#) でも確認できます。
- 製品の主要なコンポーネントについては、[マルチクラスターアーキテクチャー](#) のトピックを参照してください。
- [スタートガイド](#) では、(本製品を使用開始するための) 一般的なタスク、さらに [トラブルシューティングガイド](#) について言及します。
- [Web コンソール](#)
 - [可観測性](#)
- [クラスター](#)
- [アプリケーション](#)
- [ガバナンス](#)

1.1.1. Web コンソール

- サイドバーナビゲーションは、他の製品と合わせることでユーザーエクスペリエンスが向上されました。ナビゲーションから、さまざまな製品機能にアクセスできます。また、**検索**は **Home** タブからナビゲーションで利用でき、ヘッダーからは検索できなくなります。
- [Red Hat OpenShift Container Platform 4.10 リリース](#) および、よりハイブリッドなコンソールで、動的プラグインを使用できます。実行時にロードされるクラスターにダイナミックプラグインを作成してデプロイするには、[OpenShift Container Platform ウェブコンソールへのダイナミックプラグインの追加](#) に関する OpenShift Container Platform のドキュメントを参照してください。
- **注:** OpenShift Container Platform バージョン 4.8 から 4.10 でプラグインが有効になっていない場合、Red Hat Advanced Cluster Management は **パースペクティブスイッチャー** で使用できます。Red Hat Advanced Cluster Management コンソールの詳細は、[コンソールの概要](#) を参照してください。
- Red Hat Advanced Cluster Management プラグインは、通常、OpenShift Container Platform コンソールから有効にできます。[コンソールの概要](#) で有効にする方法を説明しています。

1.1.1.1. 可観測性

- Red Hat Advanced Cluster Management は OpenShift Container Platform バージョン 3.11 Grafana ダッシュボードをサポートします。詳細は、[可観測性の有効化で MultiClusterObservability CR の作成](#) セクションを参照してください。
- 可観測性サービスに使用するオブジェクトストアにアクセスするための証明書をカスタマイズします。詳細は、[オブジェクトストアにアクセスするための証明書のカスタマイズ](#) を参照してください。
- Security Service Token 認証情報を使用して可観測性サービスを設定します。設定内容の詳細は、[Observability API](#) を参照してください。
- 可観測性サービスを使用すると、メトリクスを外部エンドポイントにエクスポートできます。詳細は、[メトリクスの外部エンドポイントへのエクスポート](#) を参照してください。
- 単一ノード OpenShift (SNO) クラスターの動的メトリクス収集がサポートされます。詳しくは、[単一ノード OpenShift クラスターの動的メトリック](#) を参照してください。

1.1.2. クラスター

- Red Hat Advanced Cluster Management を使用して Submariner マルチネットワークサービスを統合する機能の一部が一般提供されています。詳細は、[Submariner マルチクラスターネットワークワーキングおよびサービスディスカバリー](#) を参照してください。
- Submariner アドオンを有効にするときに、Globalnet コントローラーが重複する CIDR を解決できるようにします。詳細は、[Globalnet](#) を参照してください。
- ハブクラスターをホストし、Advanced RISC Machines (ARM) アーキテクチャーでクラスターをインポートして管理します。
- Central Infrastructure Management は、ベアメタル、Red Hat OpenStack Platform、VMware vSphere 環境、またはユーザープロビジョニングインフラストラクチャー (UPI) 方式を使用してインストールされ、プラットフォームが **None** の場合に、Metal3 をサポートするようになりました。

- クラスター作成プロセスで、ホストを検出してインフラストラクチャー環境に追加できます。詳細は、[オンプレミス環境でのクラスターの作成](#) を参照してください。
- 一般提供が開始された **ManagedClusterSet** を使用して、グループ内のすべての管理対象クラスターへのアクセスをまとめて管理します。**ManagedClusterSet** は、セットに特に割り当てられていないマネージドクラスターの **デフォルト** のマネージドクラスターセットを作成します。詳細は、[ManagedClusterSets の作成および管理](#) を参照してください。
- すぐに要求できるクラスタープール内のクラスターの数指定します。詳細は、[クラスタープールのスケールリング](#) を参照してください。
- Red Hat Advanced Cluster Management を使用して、Red Hat Virtualization に OpenShift Container Platform クラスターを作成します。詳細は、[Red Hat Virtualization でのクラスターの作成](#) を参照してください。
- テイントおよび容認を使用して、マネージドクラスターおよびマネージドクラスターセットの配置を制御します。詳細は、[テイントおよび容認を使用したマネージドクラスターの場所](#) を参照してください。
- 拡張可能なスケジューリングを使用して、クラスターの配置を制御します。詳細は、[Extensible scheduling](#) を参照してください。
- **backup-restore-enabled** ポリシーを使用してバックアップおよび復元コンポーネントを復元する方法を説明します。詳細は、[ポリシーを使用したバックアップの検証](#) を参照してください。
- Red Hat Advanced Cluster Management の検出を使用して、[OpenShift Cluster Manager](#) で利用可能な OpenShift 4 クラスターを検索します。検出は一般に利用可能で、API は **v1alpha1** から **v1** に更新されます。
 - 検出後に、クラスターをインポートして管理できます。Discovery サービスは、バックエンドおよびコンソールでの用途に Discover Operator を使用します。[Discovery service introduction](#) を参照してください。
- Red Hat Advanced Cluster Management コンソールを使用して VMware vSphere または Red Hat OpenStack Platform のクラスターを作成する際に、接続されていないクラスターのプロパティを認証情報で指定できるようになりました。詳細は、[VMware vSphere の認証情報の作成](#) および [Red Hat OpenStack の認証情報の作成](#) を参照してください。

認証情報にプロキシ接続のプロパティを指定します。詳細は、[認証情報の管理](#) のインフラストラクチャープロバイダーの認証情報のトピックを参照してください。

- **マルチクラスターエンジン Operator** は、クラスターのフリート管理を強化するソフトウェア Operator として一般提供されています。マルチクラスターエンジン Operator は、クラウドおよびデータセンター全体の Red Hat OpenShift Container Platform および Kubernetes クラスターライフサイクル管理をサポートします。Red Hat OpenShift Container Platform は、マルチクラスターエンジン Operator の前提条件です。

テクノロジープレビュー:

テクノロジープレビューとして利用できる以下のクラスター機能を確認してください。

- **Managed-ServiceAccount** コンポーネントを使用すると、マネージドクラスターでサービスアカウントを作成し、削除できます。コンポーネントはデフォルトで無効になっています。
 - 詳細は、[Multicluster engine Operator](#) ドキュメントの [ManagedServiceAccount アドオン \(テクノロジープレビュー\) の有効化](#) を参照してください。

- 詳細は、Red Hat Advanced Cluster Management ドキュメントの [MultiClusterHub の詳細設定](#) を参照してください。
- **hypershift** アドオンは、スケーリング時に OpenShift Container Platform コントロールプレーンをホストするのに役立ちます。コンポーネントはデフォルトで無効になっています。
 - 詳細は、**Multicluster Engine Operator** ドキュメントの [Hypershift add-on \(テクノロジープレビュー\)](#) を参照してください。
 - 詳細は、Red Hat Advanced Cluster Management ドキュメントの [Hypershift アドオン \(テクノロジープレビュー\)](#) および [ホストされたコントロールプレーンクラスターの使用 \(テクノロジープレビュー\)](#) を参照してください。
 - HyperShift を使用して、ホストされるコントロールプレーンクラスターを管理し、プロビジョニングします。詳細は、[ホストされているコントロールプレーンクラスターの使用 \(テクノロジープレビュー\)](#) を参照してください。

他のクラスターについては、[クラスターの管理](#) を参照してください。

1.1.3. アプリケーション

- 配置および配置デシジョン API は **v1alpha1** から **v1beta1** にアップグレードされます。配置を使用して、サブスクリプションおよびアプリケーションセットが配信される **ClusterSet** にサブスクリプションする必要のあるターゲットクラスターを定義します。これらの情報は、コンソールの [詳細設定](#) から確認できます。
- 単一アプリケーション概要の個別のタブからトポロジにアクセスし、すべてを同時に表示できるようにします。各トポロジ要素の詳細は、[トポロジの読み取り方法](#) を参照してください。
- **ApplicationSet** が Argo CD アプリケーションのマルチクラスターサポートを追加する Argo CD のサブプロジェクトとして一般提供されるようになりました。製品コンソールエディターから **ApplicationSet** を作成できます。[アプリケーションモデルおよび定義](#) を参照してください。
- ハブクラスターのマネージドクラスターおよび **subscriptionReports** のステータスは軽量で、よりスケーラブルなものになります。以下の 3 種類のサブ状態レポートを参照してください。
 - パッケージレベルの **SubscriptionStatus**: これは、マネージドクラスター上のアプリケーションパッケージのステータスであり、アプリケーションによって **appsub** namespace にデプロイされるすべてのリソースの詳細なステータスが含まれます。
 - クラスターレベルの **SubscriptionReport**: 特定のクラスターにデプロイされているすべてのアプリケーションに関する全体的なステータスレポートです。
 - アプリケーションレベルの **SubscriptionReport**: これは、特定のアプリケーションがデプロイされたすべてのマネージドクラスターの全体的なステータスレポートです。詳細は、[サブスクリプションレポート](#) を参照してください。

他のアプリケーションのトピックについては、[アプリケーションの管理](#) を参照してください。

1.1.4. ガバナンス

- オプションの YAML フィールド **metadataComplianceType** を使用して、オブジェクトのラベルとアノテーションを他のフィールドとは異なる方法で処理します。詳細は、[ポリシー API](#) を参照してください。

- ポリシーをグループ化するためのポリシーセットを作成します。[ポリシーセットコントローラー](#)を参照してください。
- ポリシーセットの生成がポリシージェネレーターでサポートされるようになりました。[Policy generator](#)を参照してください。
- **protect** 機能を使用して、ハブクラスターポリシーテンプレートにある機密データのセキュリティを確保できます。また、**fromSecret** 機能がハブクラスターポリシーテンプレートで利用できるようになりました。詳細は、[protect function](#) セクションを参照してください。

ダッシュボードとポリシーフレームワークに関する詳細は、[ガバナンス](#)を参照してください。

1.1.5. アドオン

- Red Hat OpenStack Platform クラスターで Submariner をデプロイします。詳細は、[Submariner 向けの Red Hat OpenStack Platform の準備](#)を参照してください。

詳細は、[リリースノート](#)を参照してください。

1.2. 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。

- [ドキュメントの既知の問題](#)
- [インストールの既知の問題](#)
- [Web コンソールの既知の問題](#)
 - [可観測性の既知の問題](#)
- [クラスター管理の既知の問題](#)
- [アプリケーション管理の既知の問題](#)
- [ガバナンスの既知の問題](#)
- [バックアップおよび復元の既知の問題](#)
- [Submariner の既知の問題](#)

1.2.1. ドキュメントの既知の問題

1.2.1.1. カスタマーポータルドキュメントリンクは、上位レベルのセクションにリンクしている場合がある

場合によっては、カスタマーポータル Red Hat Advanced Cluster Management ドキュメントの他のセクションへの内部リンクが指定されたセクションに直接リンクしないことがあります。最上位のセクションにリンクされる場合もあります。

これが発生した場合は、指定されたセクションを手動で見つけるか、次の手順を実行して解決できません。

1. 解決されていないリンクを正しいセクションにコピーして、ブラウザのアドレスバーに貼り付けます。たとえば、https://access.redhat.com/documentation/ja-jp/red_hat_advanced_cluster_management_for_kubernetes/2.5/html/clusters/index#volsync のようになります。
2. リンクの **html** を **html-single** に置き換えます。新しい URL は https://access.redhat.com/documentation/ja-jp/red_hat_advanced_cluster_management_for_kubernetes/2.5/html-single/clusters/index#volsync のようになります。
3. 新しい URL にリンクして、ドキュメントで指定されたセクションを見つけます。

1.2.2. インストールの既知の問題

1.2.2.1. Red Hat Advanced Cluster Management のアップグレード後に Pod が復旧しないことがある

Red Hat Advanced Cluster Management を新しいバージョンにアップグレードした後、**StatefulSet** に属するいくつかの Pod が **failed** 状態のままになることがあります。このまれなイベントは、[Kubernetes の既知の問題](#) が原因です。

この問題の回避策として、失敗した Pod を削除します。Kubernetes は、正しい設定で自動的に再起動します。

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

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

1.2.2.3. アップグレード後、2つのクラスターキュレーターコントローラーが同時に実行されている

2.4.x から 2.5.0 にアップグレードした後、2つのクラスターキュレーターコントローラーが同時に実行される場合があります。クラスターライフサイクル Ansible 統合の一部のプリフックおよびポストフックに対して、2つ以上の **AnsibleJob** が作成されました。この問題を解決するには、次の手順を参照してください。

1. 2つのクラスターキュレーターコントローラーが実行されているかどうかを確認します。multicluster engine Operator からの **multicluster-engine** namespace と **open-cluster-management** namespace を含む次のコマンドを実行します。

```
kubectl -n multicluster-engine get deploy cluster-curator-controller
```

```
kubectl -n open-cluster-management get deploy cluster-curator-controller
```

2. 2つのクラスターキュレーターコントローラーが実行されている場合は、**open-cluster-management** namespace の **cluster-curator-controller** を削除します。以下のコマンドを実行します。

```
kubectl -n open-cluster-management delete deploy cluster-curator-controller
```

1.2.2.4. MultiClusterEngine の作成ボタンが機能しない

Red Hat OpenShift Container Platform コンソールに Red Hat Advanced Cluster Management for Kubernetes をインストールすると、ポップアップウィンドウに次のメッセージが表示されます。

MultiClusterEngine required

Create a MultiClusterEngine instance to use this Operator.

ポップアップウィンドウメッセージの **Create MultiClusterEngine** ボタンが機能しない場合があります。この問題を回避するには、提供された API セクションの MultiClusterEngine タイルで **インスタンスの作成** を選択します。

1.2.3. Web コンソールの既知の問題

1.2.3.1. Red Hat Advanced Cluster Management バージョン 2.5.x ではダークモードはサポートされていません

Red Hat Advanced Cluster Management バージョン 2.5.2 以降の 2.5.x バージョンは Red Hat OpenShift Container Platform バージョン 4.11 でサポートされていますが、Red Hat Advanced Cluster Management 2.5.x ではダークモードはサポートされていません。設定でダークモードを無効にするか、Red Hat Advanced Cluster Management バージョン 2.6 にアップグレードしてダークモードを有効にします。

1.2.3.2. ダークモードは、Kubernetes Operator バージョン 2.0.x のマルチクラスターエンジンではサポートされていません

Kubernetes Operator バージョン 2.0.2 およびそれ以降の 2.0.x バージョンのマルチクラスターエンジンは Red Hat OpenShift Container Platform バージョン 4.11 でサポートされますが、ダークモードは Kubernetes Operator 2.0.x のマルチクラスターエンジンではサポートされません。設定でダークモードを無効にするか、Kubernetes Operator バージョン 2.1 のマルチクラスターエンジンにアップグレードしてダークモードを有効にします。

1.2.3.3. LDAP ユーザー名の大文字と小文字が区別される

LDAP ユーザー名は、大文字と小文字が区別されます。LDAP ディレクトリーで設定したものと全く同じ名前を使用する必要があります。

1.2.3.4. 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。

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

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

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

1.2.3.6. 検索クエリーの解析エラー

環境が大規模になり、スケーリングのためにさらに多くのテストが必要になると、検索クエリーがタイムアウトになり、解析エラーメッセージが表示されることがあります。このエラーは、検索クエリーを 30 秒間待機した後に表示されます。

次のコマンドでタイムアウト時間を延長します。

```
kubectl annotate route multicloud-console haproxy.router.openshift.io/timeout=Xs
```

1.2.3.7. クラスターセットのネームスペースバインディングを編集できない

admin ロールを使用してクラスターセットの namespace バインディングを編集すると、次のメッセージのようなエラーが発生する場合があります。

ResourceError: managedclustersetbindings.cluster.open-cluster-management.io "<cluster-set>" is forbidden: User "<user>" cannot create/delete resource "managedclustersetbindings" in API group "cluster.open-cluster-management.io" in the namespace "<namespace>".

この問題を解決するには、バインドする namespace で **ManagedClusterSetBinding** リソースを作成または削除する権限も持っていることを確認してください。ロールバインディングでは、クラスターセットを namespace にバインドすることしかできません。

1.2.3.8. クラスターの詳細で誤ったスケーリングアラートが表示される

コンソールでクラスターの詳細を表示すると、**ノード** タブまたは **マシンプール** タブに次のメッセージが表示される場合があります。

Worker nodes are currently being removed from this cluster. Click the View machines button to see the status of the scaling operations (it may take a few minutes for the changes to be reflected on this console).

マシンプールが存在しない場合 (ユーザープロビジョニングインフラストラクチャー (UPI) インストールを使用するプロバイダーの場合) は、誤ったアラートを無視してください。コントロールプレーンの一部ではないワーカーノードがある場合に、このアラートが表示されます。マシンプールをスケーリングするのではなく、ワーカーノードが直接クラスターに追加された場合には、インストーラーでプロビジョニングされるインフラストラクチャー (IPI) のインストールを使用してプロビジョニングされたクラスターに対して、誤ったアラートが表示されることもあります。

1.2.4. 可観測性の既知の問題

1.2.4.1. サービスレベルの概要ダッシュボードでローカルクラスターが重複する

さまざまなハブクラスターが同じ S3 ストレージを使用して Red Hat Advanced Cluster Management の可観測性をデプロイする場合、**重複する local-clusters** は **Kubernetes/Service-Level Overview/API Server** ダッシュボード内で検出および表示できます。重複クラスターは、**Top Clusters**、**Number of clusters that has exceeded the SLO**、および **Number of clusters that are meeting the SLO** のパネル内の結果に影響を及ぼします。**local-clusters** は、共有 S3 ストレージに関連付けられた一意のクラスターです。複数の **local-clusters** がダッシュボード内で表示しないようにするには、一意のハブクラスターごとに、ハブクラスター専用の S3 バケットを使用して可観測性をデプロイすることが推奨されません。

1.2.4.2. 可観測性エンドポイント Operator がイメージのプルに失敗する

可観測性エンドポイント Operator は、MultiClusterObservability CustomResource (CR) へのデプロイにプルシークレットを作成したにもかかわらず、**open-cluster-management-observability**

namespace にプルシークレットがない場合に問題が発生します。新しいクラスターをインポートする場合、または Red Hat Advanced Cluster Management で作成された Hive クラスターをインポートする場合は、マネージドクラスターにプルイメージシークレットを手動で作成する必要があります。

詳細は、[可観測性の有効化](#) を参照してください。

1.2.4.3. ROKS クラスターおよび HyperShift クラスターからのデータはありません

Red Hat Advanced Cluster Management の可観測性は、組み込みダッシュボードで、ROKS クラスターおよび HyperShift 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 および HyperShift が管理するサーバーからの API サーバーメトリック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/Namespaces(Workload)** の ROKS クラスターおよび HyperShift クラスターをサポートしないパネルが含まれます。

1.2.4.4. ROKS クラスターおよび HyperShift クラスターからの etcd データはありません

ROKS クラスターおよび HyperShift クラスターの場合、Red Hat Advanced Cluster Management の可観測性は、ダッシュボードの **etcd** パネルにデータを表示しません。

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

1000 のクラスターを管理するハブクラスターで検索を無効にすると、メモリー不足 (OOM) が原因で **search-collector** Pod がクラッシュします。以下の手順を実行します。

1. ハブクラスターで検索が無効にされている場合、**search-redisgraph-pod** はデプロイされないため、**search-collector** デプロイメントを **0** レプリカにスケールダウンしてメモリーの使用量を削減します。
2. ハブクラスターで検索が有効になっている場合 (**search-redisgraph-pod** がデプロイされていることを意味する) は、**search-collector** デプロイメントを編集して割り当てられるメモリーを増やします。

1.2.4.6. 証明書が無効な場合に検索 Pod が TLS ハンドシェイクを完了できない

まれに、検索 Pod は証明書の変更後に自動的に再デプロイされない場合があります。これにより、サービス Pod 全体で証明書が一致なくなるため、転送レイヤーセキュリティ (TLS) ハンドシェイクが失敗します。この問題を修正するには、検索 Pod を再起動して証明書をリセットします。

1.2.4.7. 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"

ブラウザを更新し、ハブクラスターにログインしていることを確認します。

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

no project or cluster found

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

1.2.4.8. マネージドクラスターでの Prometheus データ喪失

デフォルトでは、OpenShift の Prometheus は一時ストレージを使用します。Prometheus は、再起動されるたびにすべてのメトリクスデータを失います。

Red Hat Advanced Cluster Management が管理する OpenShift Container Platform マネージドクラスターで可観測性を有効または無効にすると、可観測性エンドポイント Operator は、ローカルの Prometheus を自動的に再起動する alertmanager 設定を追加して **cluster-monitoring-config ConfigMap** を更新します。

1.2.4.9. Out-of-order サンプルの取り込みエラー

Observability **receive** Pod では、以下のエラーをレポートします。

Error on ingesting out-of-order samples

このエラーメッセージは、マネージドクラスターがメトリック収集間隔中に送信した時系列データが、以前の収集間隔中に送信した時系列データよりも古いことを意味します。この問題が発生した場合には、データは Thanos レシーバーによって破棄され、Grafana ダッシュボードに表示されるデータにギャップが生じる場合があります。エラーが頻繁に発生する場合は、メトリクスコレクションの間隔をより大きい値に増やすことが推奨されます。たとえば、間隔を 60 秒に増やすことができます。

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

1.2.4.10. マネージドクラスターで Grafana のデプロイが失敗する

マニフェストのサイズが 50,000 バイトを超えると、Grafana インスタンスはマネージドクラスターにデプロイされません。可観測性をデプロイした後、**local-cluster** のみが Grafana に表示されます。

1.2.5. クラスター管理の既知の問題

クラスター管理に関する次の既知の問題と制限を参照してください。

1.2.5.1. クラスター作成用の切断されたインストール設定は入力できないか、入力しても無視される

ベアメタルプロバイダーと切断されたインストールを使用してクラスターを作成する場合、**切断されたインストールの設定** セクションの資格情報にすべての設定を保存する必要があります。クラスター作成コンソールエディターでそれらを入力することはできません。

VMware vSphere または Red Hat OpenStack Platform プロバイダーを使用してクラスターを作成し、切断されたインストールを行う場合、ミラーレジストリーにアクセスするために証明書が必要な場合は、**切断されたインストールの設定セクションの資格情報の追加の信頼バンドル** フィールドに証明書を入力する必要があります。その証明書をクラスター作成コンソールエディターに入力すると、無視されます。

1.2.5.2. 切断されたインストーラーの資格情報は、証明書を区別しない

ベアメタル、VMware vSphere、または Red Hat OpenStack Platform プロバイダーの資格情報を作成する場合、インストーラーは証明書を区別しないため、**切断されたインストールのプロキシ** と **設定の追**

加の信頼バンドルフィールドには同じ値が含まれていることに注意してください。これらの機能を個別に使用することもできます。また、プロキシインストールと非接続インストールで異なる証明書が必要な場合は、フィールドに複数の証明書を入力できます。

1.2.5.3. アドオンの削除時にマネージドクラスターで必要な VolSync CSV の手動削除

ハブクラスターから VolSync **ManagedClusterAddOn** を削除すると、マネージドクラスターの VolSync Operator サブスクリプションが削除されますが、クラスターサービスバージョン (CSV) は削除されません。マネージドクラスターから CSV を削除するには、VolSync を削除する各マネージドクラスターで以下のコマンドを実行します。

```
oc delete csv -n openshift-operators volsync-product.v0.4.0
```

別のバージョンの VolSync がインストールされている場合は、**v0.4.0** をインストール済みバージョンに置き換えます。

1.2.5.4. sushy-tools の使用時にベアメタルマネージドクラスターのプロビジョニングに失敗する

sushy-tools を使用してベアメタルにマネージドクラスターをプロビジョニングすると、**virtual media cd query return 500** エラーでプロビジョニングに失敗する場合があります。sushy-tools の使用は、長時間稼働するクラスターでの信頼性を保証するものではありません。

sushy-tools が最新バージョンであることを確認して、sushy エミュレーターを再起動して問題を回避します。

1.2.5.5. デュアルスタックハブを使用する場合に OpenShift Container Platform 4.10 でのベアメタルクラスターのプロビジョニングに失敗する

OpenShift Container Platform バージョン 4.10 を実行しているデュアルスタックハブでベアメタルクラスターをプロビジョニングすると、プロビジョニングが失敗し、ノードの検査中に 'timeout reached during the node' というエラーメッセージが表示されます。この問題を回避するには、以下の例にあるように、**install-config.yaml** ファイルでプロビジョニングネットワークを無効にします。

```
platform:
  baremetal:
    provisioningNetwork: "Disabled"
```

プロビジョニングネットワークの詳細は、OpenShift Container Platform ドキュメントの [プロビジョニングネットワークなしでのデプロイ](#) を参照してください。

1.2.5.6. マネージドクラスターセットを削除してもそのラベルが自動的に削除されない

ManagedClusterSet を削除した後に、クラスターセットに関連付ける各マネージドクラスターに追加されるラベルは自動的に削除されません。削除したマネージドクラスターセットに含まれる各マネージドクラスターからラベルを手動で削除します。ラベルは **cluster.open-cluster-management.io/clusterSet:<ManagedClusterSet Name>** のようになります。

1.2.5.7. ClusterClaim エラー

ClusterPool に対して Hive **ClusterClaim** を作成し、**ClusterClaimspec** の有効期限のフィールドを無効な golang タイム値に手動で設定すると、Red Hat Advanced Cluster Management は不正な要求だけでなく、すべての **ClusterClaims** の実行および調整を停止します。

このエラーが発生すると、**clusterclaim-controller** Pod ログに以下の内容が表示されます。これは、プール名と、無効な有効期限が含まれた特定の例です。

```
E0203 07:10:38.266841      1 reflector.go:138] sigs.k8s.io/controller-runtime/pkg/cache/internal/informers_map.go:224: Failed to watch *v1.ClusterClaim: failed to list *v1.ClusterClaim: v1.ClusterClaimList.Items: [[v1.ClusterClaim: v1.ClusterClaim.v1.ClusterClaim.Spec: v1.ClusterClaimSpec.Lifetime: unmarshalerDecoder: time: unknown unit "w" in duration "1w", error found in #10 byte of ...|time:"1w"}],{"apiVe|..., bigger context ...|clusterPoolName":"policy-aas-hubs","lifetime":"1w"}], {"apiVersion":"hive.openshift.io/v1","kind":"Cl|...
```

無効な要求を削除できます。

不正な要求が削除されると、要求は追加の対話なしに正常に調整を開始します。

1.2.5.8. 製品チャンネルが、プロビジョニングされたクラスターと同期されない

clusterimageset は **fast** チャンネルに置かれますが、プロビジョニングされたクラスターは **stable** チャンネルにあります。現時点で、製品は **channel** をプロビジョニングされた OpenShift Container Platform クラスターと同期しません。

OpenShift Container Platform コンソールで適切なチャンネルに切り替えます。**Administration > Cluster Settings > Details Channel** の順にクリックします。

1.2.5.9. カスタム CA 証明書を使用した管理対象クラスターの、復元されたハブクラスターへの接続の復元は失敗する可能性がある

カスタム CA 証明書を使用してクラスターを管理したハブクラスターのバックアップを復元した後、管理対象クラスターとハブクラスター間の接続が失敗する場合があります。これは、復元されたハブクラスターで CA 証明書がバックアップされなかったためです。接続を復元するには、管理対象クラスターの namespace にあるカスタム CA 証明書情報を、復元されたハブクラスターの **<managed_cluster>-admin-kubeconfig** シークレットにコピーします。

ヒント: バックアップコピーを作成する前にこの CA 証明書をハブクラスターにコピーする場合は、バックアップコピーにシークレット情報が含まれます。将来、バックアップコピーを使用して復元する場合、ハブと管理対象クラスター間の接続は自動的に完了します。

1.2.5.10. ローカルクラスターが自動的に再作成されない場合がある

disableHubSelfManagement が **false** に設定されている場合、local-cluster は **MulticlusterHub Operator** によって再作成されます。ローカルクラスターをデタッチした後、ローカルクラスターが自動的に再作成されない場合があります。

- この問題を解決するには、**MulticlusterHub** によって監視されるリソースを変更します。以下の例を参照してください。

```
oc delete deployment multiclusterhub-repo -n <namespace>
```

- local-cluster を適切にデタッチするには、**MultiClusterHub** で **disableHubSelfManagement** を true に設定します。

1.2.5.11. オンプレミスクラスターを作成する場合は、サブネットを選択する必要がある

Red Hat Advanced Cluster Management コンソールを使用してオンプレミスクラスターを作成する場合は、クラスターで使用可能なサブネットを選択する必要があります。必須フィールドとしてマークされていません。

1.2.5.12. 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、以下のエラーが発生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 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。

1.2.5.13. Infrastructure Operator を使用したクラスターのプロビジョニングに失敗する

Infrastructure Operator を使用して OpenShift Container Platform クラスターを作成する場合、ISO イメージのファイル名は長すぎる可能性があります。長いイメージ名により、イメージのプロビジョニングとクラスターのプロビジョニングが失敗します。この問題が生じるかどうかを確認するには、以下の手順を実行します。

1. 以下のコマンドを実行して、プロビジョニングするクラスターのベアメタルホスト情報を表示します。

```
oc get bmh -n <cluster_provisioning_namespace>
```

2. **describe** コマンドを実行して、エラー情報を表示します。

```
oc describe bmh -n <cluster_provisioning_namespace> <bmh_name>
```

3. 以下の例と同様のエラーは、ファイル名の長さが問題であることを示します。

```
Status:
Error Count: 1
Error Message: Image provisioning failed: ... [Errno 36] File name too long ...
```

この問題が発生する場合、これは通常 OpenShift Container Platform の以下のバージョンで発生します。インフラストラクチャー Operator がイメージサービスを使用していないためです。

- 4.8.17 以前
- 4.9.6 以前

このエラーを回避するには、OpenShift Container Platform をバージョン 4.8.18 以降、または 4.9.7 以降にアップグレードしてください。

1.2.5.14. Azure Government クラスターを休止状態にできない

Azure Government クラスターを休止状態にしようとすると、以下のエラーがプロビジョニング Pod ログに追加されてハイバネートに失敗します。

Confidential Client is not supported in Cross Cloud request

1.2.5.15. 別の名前で再インポートした後に **local-cluster** のステータスがオフラインになる

local-cluster という名前のクラスターを、誤って別の名前のクラスターとして再インポートしようとすると、**local-cluster** と再インポートしたクラスターのステータスが **offline** と表示されます。

このケースから回復するには、以下の手順を行います。

1. ハブクラスターで以下のコマンドを実行して、ハブクラスターの自己管理の設定を一時的に編集します。

```
oc edit mch -n open-cluster-management multiclusterhub
```

2. **spec.disableSelfManagement=true** の設定を追加します。
3. ハブクラスターで以下のコマンドを実行し、**local-cluster** を削除し、再デプロイします。

```
oc delete managedcluster local-cluster
```

4. 以下のコマンドを実行して **local-cluster** 管理設定を削除します。

```
oc edit mch -n open-cluster-management multiclusterhub
```

5. 前の手順で追加した **spec.disableSelfManagement=true** を削除します。

1.2.5.16. Ansible 自動化を使用したクラスタープロビジョニングがプロキシ環境で失敗する

マネージドクラスターを自動的にプロビジョニングするように設定された AnsibleJob テンプレートは、以下の条件の両方が満たされると失敗する可能性があります。

- ハブクラスターで、クラスター全体のプロキシが有効になっている。
- Ansible Tower には、プロキシを介してのみアクセスできる。

1.2.5.17. klusterlet Operator のバージョンは、ハブクラスターと同じである必要がある

klusterlet Operator をインストールしてマネージドクラスターをインポートする場合には、klusterlet Operator のバージョンは、ハブクラスターのバージョンと同じでなければなりません。そうでないと、klusterlet Operator は動作しません。

1.2.5.18. マネージドクラスター namespace を手動で削除できない

マネージドクラスターの namespace を手動で削除できません。マネージドクラスター namespace は、マネージドクラスターの割り当てを解除した後に自動的に削除されます。マネージドクラスターの割り当てを解除する前に手動でマネージドクラスター namespace を削除する場合は、マネージドクラスターの削除後にマネージドクラスターに継続的な終了ステータスが表示されます。この終了マネージドクラスターを削除するには、割り当てを解除したマネージドクラスターからファイナライザーを手動で削除します。

1.2.5.19. バージョン 2.3 にアップグレードした後にクラスターの認証情報を変更できない

Red Hat Advanced Cluster Management をバージョン 2.3 にアップグレードすると、アップグレード前に Red Hat Advanced Cluster Management で作成して管理されていたマネージドクラスターの認証情報シークレットが変更できなくなります。

1.2.5.20. 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。

1.2.5.21. IBM OpenShift Container Platform Kubernetes Service クラスターの特定のバージョンのインポートはサポートされていない

IBM OpenShift Container Platform Kubernetes Service バージョン 3.11 のクラスターをインポートすることはできません。IBM OpenShift Kubernetes Service の 3.11 よりも後のバージョンはサポート対象です。

1.2.5.22. OpenShift Container Platform 3.11 の割り当てを解除しても **open-cluster-management-agent** が削除されない

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
```

1.2.5.23. 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。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、使用している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}" } ]'
```

1.2.5.24. 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。

1.2.5.25. 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。

1.2.5.26. OpenShift Container Platform Dedicated でコンソールを使用して OpenShift Container Platform マネージドクラスターをアップグレードできない

Red Hat Advanced Cluster Management コンソールを使用して、OpenShift Container Platform Dedicated 環境にある OpenShift Container Platform マネージドクラスターをアップグレードすることはできません。

1.2.5.27. 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。

1.2.5.28. IBM Power または IBM Z システムハブクラスターとの Ansible Tower 統合は使用できない

[Ansible Automation Platform Resource Operator](#) では **ppc64le** イメージまたは **s390x** イメージが提供されないため、IBM Power または IBM Z システムで Red Hat Advanced Cluster Management for Kubernetes ハブクラスターが実行されている場合には、Ansible Tower 統合を使用できません。

1.2.5.29. Red Hat OpenShift Container Platform 以外のマネージドクラスターでは、LoadBalancer が有効にされている必要がある

Red Hat OpenShift Container Platform および OpenShift Container Platform 以外のクラスターの両方は Pod ログ機能をサポートしますが、OpenShift Container Platform 以外のクラスターでは、この機能を使用できるように **LoadBalancer** が有効にされている必要があります。**LoadBalancer** を有効にするには、以下の手順を実行します。

1. クラウドプロバイダーごとに **LoadBalancer** 設定が異なります。詳細は、クラウドプロバイダーのドキュメントを参照してください。
2. **managedClusterInfo** のステータスで **loggingEndpoint** をチェックして、**LoadBalancer** が Red Hat Advanced Cluster Management で有効にされているかどうかを確認します。
3. 以下のコマンドを実行して、**loggingEndpoint.IP** または **loggingEndpoint.Host** に有効な IP アドレスまたはホスト名が設定されていることを確認します。

```
oc get managedclusterinfo <clusterName> -n <clusterNamespace> -o json | jq -r '.status.loggingEndpoint'
```

LoadBalancer のタイプについての詳細は、[Kubernetes のドキュメント](#) の Service ページを参照してください。

1.2.5.30. アップグレード後に Cluster-proxy-addon が起動しない

バージョン 2.4.x から 2.5.0 にアップグレードした後、**cluster-proxy-addon** が起動せず、**cluster-proxy-addon-manager** が nil ポインター例外を発生させます。

この問題を回避するには、以下の手順を実行します。

1. **cluster-proxy-addon** を無効にします。詳細は、[高度な設定](#) を参照してください。
2. **open-cluster-management** namespace から **cluster-proxy-signer** シークレットを削除します。
3. **cluster-proxy-addon** を有効にします。

1.2.6. アプリケーション管理の既知の問題

アプリケーションライフサイクルコンポーネントについては、次の既知の問題を参照してください。

1.2.6.1. アプリケーション ObjectBucket チャンネルタイプは、許可リストと拒否リストを使用できない

subscription-admin ロールの ObjectBucket チャンネルタイプで許可リストと拒否リストを指定することはできません。他の種類のチャンネルでは、サブスクリプションの許可リストと拒否リストによって、デプロイできる Kubernetes リソースとデプロイできない Kubernetes リソースが示されます。

1.2.6.2. Argo アプリケーションを 3.x OpenShift Container Platform 管理対象クラスターにデプロイできない

Infrastructure.config.openshift.io API は 3.x では使用できないため、コンソールから Argo **ApplicationSet** を 3.x OpenShift Container Platform 管理対象クラスターにデプロイすることはできません。

1.2.6.3. multicluster_operators_subscription イメージへの変更は自動的に有効にならない

マネージドクラスターで実行している **application-manager** アドオンは、以前は **klusterlet Operator** により処理されていましたが、サブスクリプション Operator により処理されるようになりました。サブスクリプション Operator は **multicluster-hub** で管理されていないため、**multicluster-hub** イメージマニフェスト ConfigMap の **multicluster_operators_subscription** イメージへの変更は自動的に有効になりません。

サブスクリプション Operator が使用するイメージが、**multicluster-hub** イメージマニフェスト ConfigMap の **multicluster_operators_subscription** イメージを変更することによってオーバーライドされた場合、マネージドクラスターの **application-manager** アドオンは、サブスクリプション Operator Pod が再起動するまで新しいイメージを使用しません。。Pod を再起動する必要があります。

1.2.6.4. アプリケーショントポロジで誤ったアプリケーションが表示される

同じ名前の **ApplicationSet** が異なる Gitops インスタンスに作成されると、アプリケーショントポロジは誤ったアプリケーションを表示します。複数の Gitops インスタンスがインストールされている場合に、各 Gitops インスタンスに同じ名前の **ApplicationSets** が設定され、**ApplicationSets** のトポロジが正しく表示されません。これは、作成される **ApplicationSets** の namespace をトポロジで区別していないことが原因です。

各 Gitops インスタンスに異なる名前でも **ApplicationSet** を作成し、トポロジを正しく表示できるようにします。

1.2.6.5. サブスクリプション管理者以外はポリシーリソースをデプロイできない

Red Hat Advanced Cluster Management バージョン 2.4 では、デフォルトで **policy.open-cluster-management.io/v1** リソースがアプリケーションサブスクリプションによってデプロイされなくなりました。

サブスクリプション管理者は、このデフォルトの動作を変更するためにアプリケーションサブスクリプションをデプロイする必要があります。

詳細は、[サブスクリプション管理者としての許可リストおよび拒否リストの作成](#) を参照してください。以前の Red Hat Advanced Cluster Management バージョンの既存のアプリケーションサブスクリプションによってデプロイされた **policy.open-cluster-management.io/v1** リソースは、サブスクリプション管理者がアプリケーションサブスクリプションをデプロイしていない限り、ソースリポジトリに合わせて調整されません。

1.2.6.6. アプリケーション Ansible フックのスタンドアロンモード

Ansible フックのスタンドアロンモードはサポートされていません。サブスクリプションを使用してハブクラスターに Ansible フックをデプロイするには、次のサブスクリプション YAML を使用できます。

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
    name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    local: true
```

ただし、**spec.placement.local:true** ではサブスクリプションが **standalone** モードで実行されているため、この設定では Ansible インストールが作成されない可能性があります。ハブモードでサブスクリプションを作成する必要があります。

1. **local-cluster** にデプロイする配置ルールを作成します。以下のサンプルを参照してください。

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: <towhichcluster>
  namespace: hello-openshift
spec:
  clusterSelector:
    matchLabels:
      local-cluster: "true" #this points to your hub cluster
```

2. 使用しているサブスクリプションで、作成した配置ルールを参照します。以下を参照してください。

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
    name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    placementRef:
      name: <towhichcluster>
      kind: PlacementRule
```

両方を適用すると、ハブクラスターに作成された Ansible インスタンスが表示されます。

1.2.6.7. Editor ロールのアプリケーションエラー

Editor ロールで実行するユーザーは、アプリケーションで **read** または **update** の権限のみが割り当てられているにもかかわらず、誤ってアプリケーションの **create** および **delete** の操作ができてしまいます。OpenShift Container Platform Operator Lifecycle Manager のデフォルト設定により、当製品の設定が変更されてしまいます。この問題を回避するには、以下の手順を参照してください。

1. **oc edit clusterrole applications.app.k8s.io-v1beta2-edit -o yaml** を実行して、アプリケーションのクラスターロールの編集を開きます。
2. verbs リストから **create** および **delete** を削除します。
3. 変更を保存します。

1.2.6.8. 配置ルールの編集ロールエラー

Editor ロールで実行するユーザーは、配置ルールで **read** または **update** の権限のみが割り当てられているにもかかわらず、誤って **create** および **delete** の操作もできてしまいます。OpenShift Container Platform Operator Lifecycle Manager のデフォルト設定により、当製品の設定が変更されてしまいます。この問題を回避するには、以下の手順を参照してください。

1. **oc edit clusterrole placementrules.apps.open-cluster-management.io-v1-edit** を実行して、アプリケーションの編集クラスターロールを開きます。
2. verbs リストから **create** および **delete** を削除します。
3. 変更を保存します。

1.2.6.9. 配置ルールの更新後にアプリケーションがデプロイされない

配置ルールの更新後にアプリケーションがデプロイされない場合には、**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。

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

Red Hat OpenShift Container Platform SCC の詳細は、[Security Context Constraints \(SCC\) の管理](#) を参照してください。これは、マネージドクラスターで必要な追加設定です。

デプロイメントごとにセキュリティーコンテキストとサービスアカウントが異なります。サブスクリプション Operator は SCC 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
```

1.2.6.11. アプリケーションチャンネルには一意の namespace が必要

同じ namespace に複数のチャンネルを作成すると、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 タイプのチャンネルとしてインストーラーで使用するので、**charts-v1** に追加のチャンネルを作成します。一意の namespace でチャンネルを作成するようにしてください。すべてのチャンネルには個別の namespace が必要ですが、GitHub チャンネルは例外で、別 GitHub のチャンネルと namespace を共有できます。

1.2.6.12. Ansible Automation Platform ジョブが失敗する

互換性のないオプションを選択すると、Ansible ジョブの実行に失敗します。Ansible Automation Platform は、**-cluster-scoped** のチャンネルオプションが選択されている場合にのみ機能します。これは、Ansible ジョブを実行する必要があるすべてのコンポーネントに影響します。

1.2.6.13. Ansible Automation Platform Operator によるプロキシ外の Ansible Tower へのアクセス

Ansible Automation Platform(AAP)Operator は、プロキシ対応の OpenShift Container Platform クラスター外の Ansible Tower にアクセスできません。解決するには、Ansible tower をプロキシ内にインストールします。Ansible Tower が提供するインストール手順を参照してください。

1.2.6.14. バージョン 2.4 で Helm Argo アプリケーションを編集する場合、テンプレート情報は表示されません

Helm Argo アプリケーションを作成して編集すると、YAML ファイルが正しい間、テンプレート情報は空で表示されます。エラーを修正するには、エラータ 2.4.1 にアップグレードしてください。

1.2.6.15. アプリケーション名の要件

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

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

1.2.6.16. アプリケーションコンソールテーブルの制限事項

コンソールのさまざまな **アプリケーション** の表に対する以下の制限を確認してください。

- **Overview** ページの **Applications** の表と、 **Advanced configuration** ページの **Subscriptions** の表にある **Clusters** の列では、アプリケーションリソースのデプロイ先のクラスター数が表示されます。アプリケーションは、ローカルクラスターのリソースで定義されているため、実際のアプリケーションリソースがローカルクラスターにデプロイされているかどうかにかかわらず、ローカルのクラスターは検索結果に含まれます。
- **Subscriptions** の **Advanced configuration** 表にある **Applications** の列には、サブスクリプションを使用するアプリケーションの合計数が表示されますが、サブスクリプションが子アプリケーションをデプロイする場合には、これらも検索結果に含まれます。
- **Channels** の **Advanced configuration** 表にある **Subscriptions** の列には、対象のチャンネルを使用するローカルクラスター上のサブスクリプション合計数が表示されます。ただし、他のサブスクリプションがデプロイするサブスクリプションは検索結果には含まれますが、ここには含まれません。

1.2.6.17. アプリケーションコンソールトポロジーのフィルターリング機能がない

2.5 では **Application** の **Console** と **Topology** が変更されています。コンソールの **Topology** ページにフィルターリング機能はありません。

1.2.6.18. ApplicationSet リソースがトポロジーにステータスを表示しない

ApplicationSet YAML で定義された namespace とは異なる namespace にリソースをデプロイする **ApplicationSet** アプリケーションを作成すると、リソースのステータスがトポロジーに表示されません。

1.2.6.19. 許可リストと拒否リストがオブジェクトストレージアプリケーションで機能しない

allow リストおよび **deny** リストの機能は、オブジェクトストレージアプリケーションのサブスクリプションでは機能しません。

1.2.6.20. ApplicationSet ウィザードがパスを自動的にフェッチしない

以前に作成した **ApplicationSet** と同じ URL とブランチで新しい **ApplicationSet** を作成すると、ApplicationSet ウィザードはパスを自動的にフェッチしません。

この問題を回避するには、**Path** フィールドにパスを手動で入力します。

1.2.7. ガバナンスの既知の問題

1.2.7.1. Red Hat Advanced Cluster Management からログアウトできない

外部アイデンティティプロバイダーを使用して Red Hat Advanced Cluster Management にログインする場合は、Red Hat Advanced Cluster Management からログアウトできない可能性があります。これは、Red Hat Advanced Cluster Management に IBM Cloud および Keycloak をアイデンティティプロバイダーとしてインストールして使用する場合に発生します。

Red Hat Advanced Cluster Management からログアウトするには、外部アイデンティティプロバイダーからログアウトしておく必要があります。

1.2.7.2. Gatekeeper Operator のインストールに失敗する

Red Hat OpenShift Container Platform バージョン 4.9 に gatekeeper Operator をインストールする場合、インストールに失敗します。OpenShift Container Platform をバージョン 4.9.0. にアップグレードする前に、gatekeeper Operator をバージョン 0.2.0 にアップグレードする必要があります。詳細は、[gatekeeper](#) および [gatekeeper Operator のアップグレード](#) を参照してください。

1.2.7.3. namespace が Terminating 状態で停止している場合に、設定ポリシーが準拠と表示される

設定ポリシーで **complianceType** のパラメーターに **mustnothave**、**remediationAction** のパラメーターに **enforce** が設定されている場合に、ポリシーは Kubernetes API に削除要求が送信されてから、準拠と表示されます。そのため、ポリシーが準拠と表示されているにもかかわらず、Kubernetes オブジェクトは、**Terminating** の状態のままになってしまう可能性があります。

1.2.7.4. ポリシーでデプロイされた Operator が ARM をサポートしない

ARM 環境へのインストールはサポートされますが、ポリシーを使用してデプロイされる Operator は ARM 環境をサポートしない可能性があります。Operator をインストールする以下のポリシーは ARM 環境をサポートしません。

- [Quay Container Security Operator の Red Hat Advanced Cluster Management ポリシー](#)
- [コンプライアンス Operator 向けの Red Hat Advanced Cluster Management ポリシー](#)

1.2.7.5. ポリシーテンプレートの問題

設定ポリシーのポリシーテンプレートを編集すると、次の問題が発生する場合があります。

- 設定ポリシーの名前を新しい名前に変更すると、古い名前の設定ポリシーのコピーが残ります。
- ハブクラスターのポリシーから設定ポリシーを削除すると、設定ポリシーはマネージドクラスターに残りますが、その状態は提供されません。これを解決するには、ポリシーを無効にしてから再度有効にします。ポリシー全体を削除することもできます。

1.2.8. バックアップおよび復元の既知の問題

1.2.8.1. バックアップおよび復元機能が IBM Power および IBM Z で動作しない

ハブクラスターのバックアップおよび復元機能には、Data Protection (OADP) Operator の OpenShift API が必要です。OADP Operator は、IBM Power または IBM Z アーキテクチャーでは使用できません。

1.2.8.2. バックアップの競合の回避

ハブクラスターは passive から primary クラスターに戻されると、異なるクラスターが同じストレージの場所にあるデータをバックアップできます。これにより、バックアップの競合が発生します。つまり、最新のバックアップが passive ハブクラスターによって生成されたことを意味します。

BackupSchedule.cluster.open-cluster-management.io リソースがハブクラスターで有効になっているため、passive ハブクラスターはバックアップを生成しますが、このハブクラスターは primary ハブクラスターでなくなったため、バックアップデータは書き込みできるべきではありません。以下のコマンドを実行して、バックアップの競合があるかどうかを確認します。

```
oc get backupschedule -A
```

以下のステータスが返される場合があります。

```

NAMESPACE   NAME                PHASE          MESSAGE
openshift-adp schedule-hub-1 BackupCollision Backup acm-resources-schedule-
20220301234625, from cluster with id [be97a9eb-60b8-4511-805c-298e7c0898b3] is using the same
storage location. This is a backup collision with current cluster [1f30bfe5-0588-441c-889e-
eaf0ae55f941] backup. Review and resolve the collision then create a new BackupSchedule resource
to resume backups from this cluster.
```

BackupSchedule.cluster.open-cluster-management.io リソースの **status** を **BackupCollision** に設定して、バックアップの競合を回避します。**BackupSchedule** リソースによって作成される **Schedule.velero.io** リソースは自動的に削除されます。

バックアップの競合は、**hub-backup-pod** ポリシーにより報告されます。管理者は、どのハブクラスターが対象のストレージの場所にデータを書き込んでいるかを確認する必要があります。次に、passive ハブクラスターから **BackupSchedule.cluster.open-cluster-management.io** リソースを削除し、primary ハブクラスターに新しい **BackupSchedule.cluster.open-cluster-management.io** リソースを再作成して、バックアップを再開します。

詳細は、[クラスターのバックアップおよび復元オペレーター](#) を参照してください。

1.2.8.3. Velero 復元の制限

以下の復元の制限を確認してください。

- 初期ハブクラスターにバックアップデータを復元する前に、新しいハブクラスターに既存のポリシーが存在する場合、データの復元先の初期ハブクラスターと新規ハブクラスターは同じにはなりません。このポリシーは、バックアップリソースで利用できないポリシーであるため、新しいハブクラスターで実行しないでください。
- Velero は既存のリソースを省略するため、新しいハブクラスターのポリシーは変更されません。したがって、ポリシーは、最初のハブクラスターでバックアップしたポリシーと同じではありません。
- ユーザーが新しいハブクラスターのバックアップを再適用する場合には、新しいハブクラスターには、アクティブなハブクラスターとは異なる設定があります。ハブクラスターに以前の復元からの既存のポリシーがあるため、復元されません。バックアップに想定された更新が含

まれている場合でも、ポリシーのコンテンツは、新しいハブクラスターの Velero によって更新されません。

前述の制限に対応するために、**restore.cluster.open-cluster-management.io** リソースが作成されると、クラスターのバックアップおよび復元 Operator は、Velero 復元の開始前にハブクラスターを削除して復元の準備を行う一連の手順を実行します。詳細は、[復元前にハブクラスターのクリーニング](#)を参照してください。

1.2.8.4. インポートされたマネージドクラスターが表示されない

プライマリーハブクラスターに手動でインポートされたマネージドクラスターは、パッシブハブクラスターでアクティベーションデータが復元された場合にのみ表示されます。

1.2.8.5. クラスターのバックアップおよび復元のアップグレードの制限

enableClusterBackup パラメーターを **true** に設定してクラスターを 2.4 から 2.5 にアップグレードすると、次のメッセージが表示されます。

```
When upgrading from version 2.4 to 2.5, cluster backup must be disabled
```

クラスターをアップグレードする前に、**enableClusterBackup** パラメーターを **false** に設定して、クラスターのバックアップおよび復元を無効にします。**MultiClusterHub** リソースの **components** セクションは、次の YAML ファイルのようになります。

アップグレードが完了したら、バックアップおよび復元のコンポーネントを再度有効にすることができます。以下のサンプルを参照してください。

```
overrides:
  components:
    - enabled: true
      name: multiclusterhub-repo
    - enabled: true
      name: search
    - enabled: true
      name: management-ingress
    - enabled: true
      name: console
    - enabled: true
      name: insights
    - enabled: true
      name: grc
    - enabled: true
      name: cluster-lifecycle
    - enabled: true
      name: volsync
    - enabled: true
      name: multicluster-engine
    - enabled: false
      name: cluster-proxy-addon
    - enabled: true <<<<<<<<
      name: cluster-backup
  separateCertificateManagement: false
```

OADP を手動でインストールした場合は、アップグレードする前に OADP を手動でアンインストールする必要があります。アップグレードが成功し、バックアップおよび復元が再度有効になると、OADP が自動的にインストールされます。

1.2.8.6. マネージドクラスターリソースが復元されない

local-cluster 管理対象クラスター リソースの設定を復元し、新しいハブクラスターで **local-cluster** データを上書きすると、設定が正しく設定されません。リソースにはクラスター URL の詳細など、**local-cluster** 固有の情報が含まれているため、以前のハブクラスター **local-cluster** のコンテンツはバックアップされません。

復元されたクラスターの **local-cluster** リソースに関連するすべての設定変更を手動で適用する必要があります。詳細については、[新しいハブクラスターの準備](#) を参照してください。

1.2.8.7. prepareForBackup は、Velero スケジュールが最初に作成されたときにのみ呼び出されます

prepareForBackup 関数で定義されたラベルは、スケジュールの作成後に作成されたリソースには追加されません。これは、バックアップが開始する前にラベル付けされている Red Hat OpenShift シークレットの Hive および Infrastructure Operator に影響します。

影響を受けるリソースのリストを表示します。

- **clusterDeployments** によって使用され、クラスター要求によって作成されるシークレット
- クラスタープールのシークレット
- **agent-install.openshift.io/watch** および **environment.metal3.io** のラベルが付いたシークレット

BackupSchedule、**veleroSchedule**、または **veleroTTL** の値を更新して、新しい一連のスケジュールを開始します。次に、結果のバックアップを復元に使用します。これは、バックアップの最新のリソースにラベルを付けるように定義されています。

1.2.8.8. 復元された Hive マネージドクラスターは、新しいハブクラスターに接続できない場合がある

Hive マネージドクラスターの変更またはローテーションされた認証局 (CA) のバックアップを新しいハブクラスターで復元すると、マネージドクラスターは新しいハブクラスターへの接続に失敗します。このマネージドクラスターの **admin kubeconfig** シークレット (バックアップで使用可能) が無効になっているため、接続は失敗します。

新しいハブクラスター上のマネージドクラスターの復元された **admin kubeconfig** シークレットを手動で更新する必要があります。

1.2.9. Submariner の既知の問題

1.2.9.1. 現時点で Submariner が CNI ネットワークプロバイダーとしてサポートしているのは OpenShift SDN のみ

OpenShiftSDN のみが CNI ネットワークプロバイダーとしてサポートされています。OVN は現在サポートされていません。

1.2.9.2. Submariner はワーカーノードとして、一部の **Red Hat Enterprise Linux** ノードをサポートしていない

カーネルバージョンが 4.18.0-359.el8.x86_64 から 4.18.0-372.11.1.el8_6.x86_64 の Red Hat Enterprise Linux ワーカー ノードを含むクラスターに Submariner をデプロイすると、アプリケーションワークロードがリモートクラスターとの通信に失敗します。

1.2.9.3. Red Hat Advanced Cluster Management で管理可能なインフラストラクチャプロバイダーは **Submariner** でサポートされていない場合がある

Submariner は、Red Hat Advanced Cluster Management が管理できるすべてのインフラストラクチャプロバイダーでサポートされているわけではありません。サポートされているプロバイダーの一覧は、[Red Hat Advanced Cluster Management のサポートマトリックス](#) を参照してください。

1.2.9.4. Submariner は、**Red Hat Advanced Cluster Management** コンソールからの **Red Hat OpenStack Platform** インフラストラクチャーの準備をサポートしていない

Red Hat OpenStack クラスターの自動クラウド準備は、product-title-short} コンソールの Submariner ではサポートされていません。Red Hat Advanced Cluster Management API を使用して、クラウドを手動で準備できます。

1.2.9.5. Submariner は **Globalnet** でヘッドレスサービスをサポートしていない

Submariner は、Globalnet でヘッドレスサービスをサポートします。ただし、**clusterset.local** ドメイン名を使用して、同じクラスター内に存在するクライアントからエクスポートされたヘッドレスサービスにアクセスすると、ヘッドレスサービスに関連付けられている **globalIP** がクライアントに返され、クラスター内でルーティングできません。

cluster.local ドメイン名を使用して、ローカルのヘッドレスサービスにアクセスできます。

1.2.9.6. Submariner はエアギャップクラスターをサポートしていない

Submariner は、エアギャップ環境でプロビジョニングされたクラスターに対して検証されていません。

1.2.9.7. 多数のゲートウェイをデプロイできない

複数のゲートウェイを展開することはできません。

1.2.9.8. NAT が有効な場合、Submariner は VXLAN をサポートしない

VXLAN ケーブルドライバーを使用する Submariner は、現在、非 NAT 展開でのみサポートされています。

1.2.9.9. グローバルネットの制限

Globalnet は、Red Hat OpenShift Data Foundation ディザスタリーカバリーソリューションではサポートされていません。局地的なディザスタリーカバリーシナリオでは、各クラスター内のクラスターとサービスネットワークに重複しない範囲のプライベート IP アドレスを使用するようにしてください。

1.3. エラータの更新

デフォルトでは、エラータの更新はリリース時に自動的に適用されます。詳細は、[Operator を使用したアップグレード](#)を参照してください。

重要: 参照できるように、[エラータ](#) リンクと GitHub 番号がコンテンツに追加され、内部で使用される可能性があります。ユーザーは、アクセス権が必要なリンクを利用できない可能性があります。

FIPS の通知: **spec.ingress.sslCiphers** で独自の暗号を指定しない場合、**multiclusterhub-operator** は暗号のデフォルトリストを提供します。2.4 の場合には、この一覧には、FIPS 承認されていない暗号が 2 つ含まれます。バージョン 2.4.x 以前からアップグレードし、FIPS コンプライアンスが必要な場合は、**multiclusterhub** リソースから、以下の 2 つの暗号 (**ECDHE-ECDSA-CHACHA20-POLY1305** および **ECDHE-RSA-CHACHA20-POLY1305**) を削除します。

1.3.1. Errata 2.5.9

- 1 つ以上の製品コンテナイメージとセキュリティー修正プログラムの更新を提供します。

1.3.2. Errata 2.5.8

- **must-gather** コマンドは Red Hat OpenShift Container Platform のバージョン番号を収集するようになりました。(ACM-2857)
- **MEMCACHED** インデックスの **max_item_size** 設定がすべての **MEMCACHED** クライアントに変更を反映しない原因となった問題を修正します。(ACM-4683)
- 名前にドットが含まれるポリシーのポリシーステータスがより速く更新されるようになりました。(ACM-4736)

1.3.3. エラータ 2.5.7

- コンソールの **Edit time ウィンドウ** のリンクを修正します。リンクが正しい編集ページを開くようになります。(ACM-2647)
- アプリケーションの作成時にトポロジーノードがアプリケーションコンソールに表示される問題を修正します。(ACM-3340)

1.3.4. エラータ 2.5.6

- 1 つ以上の製品コンテナイメージとセキュリティー修正プログラムの更新を提供します。

1.3.5. エラータ 2.5.5

- 特定のキーと値を持つカスタムラベルをポリシーに追加すると、すべてのポリシーでサービス拒否が発生する問題を修正します。

1.3.6. エラータ 2.5.4

- 1 つ以上の製品コンテナイメージとセキュリティー修正プログラムの更新を提供します。

1.3.7. エラータ 2.5.3

- サポートされていない **--validate-cluster-security** フラグを **HypershiftDeployment** コントローラー引数として使用する場合の権限の問題を修正します。(Bugzilla 2109544)

- 検索アグリゲーターのロジックを更新して、マネージドクラスターからの同時同期要求を回避します。(Bugzilla 2092863)
- 1つ以上の製品コンテナイメージとセキュリティー修正プログラムの更新を提供します。

1.3.8. エラータ 2.5.2

- Red Hat Advanced Cluster Management バージョン 2.5.2 以降では、Red Hat OpenShift Container Platform バージョン 4.11 で Red Hat Advanced Cluster Management バージョン 2.5.x がサポートされます。
- Red Hat OpenShift Container Platform バージョン 4.11 では、Kubernetes Operator バージョン 2.0.2 のマルチクラスターエンジンから始まり、Kubernetes Operator バージョン 2.0.x のそれ以降のマルチクラスターエンジンがサポートされます。
- Submariner Globalnet がオンプレミスクラスターとパブリッククラスター間で接続に失敗する原因となった MTU の問題を修正します。(Bugzilla 2074547)
- インストール後に management-ingress Pod が開始されない問題に対処します。(Bugzilla 2082254)
- 大文字を含むラベルを持つ **ClusterClaim** を作成するときに、マネージドクラスターログでエラーが発生するバグを修正します。(Bugzilla 2095481)
- Red Hat OpenShift Container Platform へのインストール時に、**MultiClusterHub** がインストール フェーズで停止する可能性がある問題を解決しました。(Bugzilla 2099503)
- カスタムメトリック **allowlist** でカスタマイズされたメトリックの制限を増やし、マネージドクラスターからより多くのメトリックを収集できるようにします。(Bugzilla 2099808)
- コンソールでポリシーのメモリー値を更新した後、**enforce** するように設定された LimitRange ポリシーが **non-compliant** の状態を表示する原因となったバグを修正します。(Bugzilla 2100036)
- サブスクリプションアプリケーションで **app-of-apps** パターンを使用すると、**This application has no subscription match selector (spec.selector.matchExpressions)** エラーが発生する問題を修正します。(Bugzilla 2101577)
- Red Hat Advanced Cluster Management クラスターのバックアップおよび復元 Operator を使用して Hub クラスターをリカバリーした後、クラスターが「unknown」状態のままになる問題を解決しました。(Bugzilla 2103653)
- **NodePool.Release.Image** のデフォルト値が、**HostedClusterSpec.Release.Image** に指定されていない場合に、指定されたリリースイメージに設定します。(Bugzilla 2105436)
- SSH を使用して非公開でホストされている Git サーバーに接続したアプリケーションサブスクリプションが失敗する原因となった問題を解決します。この修正により、非公開でホストされている Git サーバーへの SSH 接続が有効になります。(Bugzilla 2105885)
- コンソールを使用してポリシーを削除したときに、関連する **PolicyAutomation** および **AnsibleJob** オブジェクトが削除されないというバグを修正しました。(Bugzilla 2116060)

1.3.9. エラータ 2.5.1

- マネージドクラスターにデプロイされた一部のアプリケーションを削除するバグを修正します。(Bugzilla 2101453)

- **Overview** ページで **The backend service is unavailable** と表示されていたコンソールエラーを解決しました。(Bugzilla 2096389)
- ポリシーアドオンの異常な状態または障害を伴うクラスターアドオンコンソールの問題を解決します。(Bugzilla 2088270)

1.4. 非推奨と削除

Red Hat Advanced Cluster Management for Kubernetes から削除されるか、または非推奨となった製品の一部について説明します。**推奨アクション** および詳細にある、代替りのアクションを検討してください。これについては、現在のリリースおよび、1つ前のリリースと2つ前のリリースの表に記載されています。

重要:

- Red Hat Advanced Cluster Management の 2.4 以前のバージョンは **削除** され、サポートされなくなりました。ドキュメントはそのまま利用できますが、エラーやその他の更新はなく、非推奨となります。
- 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。

1.4.1. API の非推奨と削除

Red Hat Advanced Cluster Management は、Kubernetes の API 非推奨ガイドラインに準拠します。このポリシーの詳細については、[Kubernetes の非推奨ポリシー](#) を参照してください。Red Hat Advanced Cluster Management API は、以下のタイムライン以外でのみ非推奨または削除されます。

- **V1** API はすべて、12 ヶ月間またはリリース 3 回分 (いずれか長い方) の期間は一般公開され、サポート対象となります。V1 API は削除されませんが、この期間を過ぎると非推奨になる可能性があります。
- **Beta** 版 API はすべて、9 ヶ月間またはリリース 3 回分 (いずれか長い方) の期間は一般公開されます。Beta 版 API は、この期間を過ぎても削除されません。
- **Alpha** 版 API はサポートの必要はありませんが、ユーザーにとってメリットがある場合には、非推奨または削除予定として記載される場合があります。

1.4.1.1. API の非推奨化

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
検出	DiscoveredCluster および DiscoveryConfig v1alpha1 API が非推奨になりました。Discovery API が V1 にアップグレードされました。	2.5	V1 を使用してください。	なし

製品またはカテゴリ	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
Placements	v1alpha1 は非推奨となったため、 v1alpha1 API は v1beta1 にアップグレードされます。	2.5	V1beta1 を使用してください。	Placement API v1alpha1 の spec.prioritizerPolicy.configurations.name フィールドが削除されました。 v1beta1 の spec.prioritizerPolicy.configurations.scoreCoordinate.builtIn を使用します。
PlacementDecisions	v1alpha1 は非推奨となったため、 v1alpha1 API は v1beta1 にアップグレードされます。	2.5	V1beta1 を使用してください。	なし
アプリケーション	v1alpha1 API は完全に廃止されます。GitOps クラスター API が V1beta1 にアップグレードされます。	2.5	V1beta1 の使用	なし
アプリケーション	deployables.apps.open-cluster-management.io	2.5	なし	deployable API は、アップグレードパスにのみ残ります。deployable CR の作成、更新、または削除は調整されません。
CertPolicyController	v1 API は非推奨になりました。	2.5	この API は使用しないでください。	CertPolicyController.agent.open-cluster-management.io
ApplicationManager	v1 API は非推奨になりました。	2.5	この API は使用しないでください。	ApplicationManager.agent.open-cluster-management.io

製品またはカテゴリ	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
IAMPolicyController	v1 API は非推奨になりました。	2.5	この API は使用しないでください。	IAMPolicyController.agent.open-cluster-management.io
PolicyController	v1 API は非推奨になりました。	2.5	この API は使用しないでください。	PolicyController.agent.open-cluster-management.io
SearchCollector	v1 API は非推奨になりました。	2.5	この API は使用しないでください。	SearchCollector.agent.open-cluster-management.io
WorkManager	v1 API は非推奨になりました。	2.5	この API は使用しないでください。	WorkManager.agent.open-cluster-management.io
ManagedClusterSets	v1alpha1 は非推奨となったため、 v1alpha1 API は v1beta1 にアップグレードされます。	2.4	V1beta1 を使用してください。	なし
ManagedClusterSetBindings	v1alpha1 は非推奨となったため、 v1alpha1 API は v1beta1 にアップグレードされます。	2.4	V1beta1 を使用してください。	なし

1.4.2. Red Hat Advanced Cluster Management の非推奨機能

非推奨のコンポーネント、機能またはサービスはサポートされますが、使用は推奨されておらず、今後のリリースで廃止される可能性があります。以下の表に記載されている **推奨アクション** と詳細の代替アクションについて検討してください。

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
-----------	------------	-------	------------	----------

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
クラスター	ベアメタルアセットを使用したクラスターの作成。	2.5	コンソールでインフラ環境を作る	影響を受ける非推奨領域は、 ベアメタル資産の作成および変更 および ベアメタルでのクラスターの作成 を参照してください。手順は、 オンプレミス環境でのクラスターの作成 を参照してください。
アドオン Operator	ビルトインのマネージドクラスターアドオンのインストール	2.5	なし	なし
可観測性	data.custom_rules.yaml.groups.rules が非推奨になりました。	2.5	data.custom_rules.yaml.groups.recording_rules を使用してください。	可観測性のカスタマイズ を参照してください。
インストーラー	operator.open-cluster-management.io_multiclusterhubs_crd.yaml の enableClusterProxyAddon および enableClusterBackup フィールド	2.5	なし	インストールの設定については、 高度な設定 を参照してください。
klusterlet Operator	release-2.4 、 release-2.3 チャンネルは更新を受信しません	2.3 以降	Red Hat OpenShift Dedicated クラスターをインポートして管理するには、2.5 にアップグレードして更新を受け取る必要があります。	Operator を使用したアップグレード を参照してください。
アプリケーション	シークレットの管理	2.4	代わりに、シークレットにポリシーハブテンプレートを使用してください。	セキュリティポリシーの管理 を参照してください。

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
ガバナンスコンソール	pod-security-policy	2.4	なし	なし
インストーラー	operator.open-cluster-management.io_multiclusterhubs_crd.yaml の別の cert-manager の設定	2.3	なし	なし
ガバナンス	カスタムポリシーコントローラー	2.3	なし	なし

1.4.3. 削除

通常、**削除**された項目は、以前のリリースで非推奨となった機能で、製品では利用できなくなっています。削除された機能には、代替の方法を使用する必要があります。以下の表に記載されている **推奨アクション** と詳細の代替アクションについて検討してください。

製品またはカテゴリ	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	deployable コントローラー	2.5	なし	Deployable コントローラーが削除されました。
Red Hat Advanced Cluster Management コンソール	Visual Web ターミナル (テクノロジープレビュー)	2.4	代わりにターミナルを使用してください。	なし
アプリケーション	単一の ArgoCD インポートモード。ハブクラスターの Argo CD サーバーにインポートされるシークレット。	2.3	クラスターシークレットは、複数の ArgoCD サーバーにインポートできます。	なし
アプリケーション	ArgoCD クラスター統合: spec.applicationManager.argocdCluster	2.3	マネージドクラスターを登録する GitOps クラスターおよび配置カスタムリソースを作成します。	マネージドクラスターでの GitOps の設定

製品またはカテゴリ	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
ガバナンス	cert-manager の内部証明書管理	2.3	アクションは不要です。	なし

1.5. GDPR に対応するための RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES プラットフォームでの考慮事項

1.5.1. 注意

本書は、EU 一般データ保護規則 (GDPR: General Data Protection Regulation) への対応準備を容易化するために作成されました。本書では、GDPR に組織が対応する準備を整える際に考慮する必要のある Red Hat Advanced Cluster Management for Kubernetes プラットフォームの設定可能な機能や、製品のあらゆる用途について説明します。機能の選択、設定方法が多数ある上に、本製品は、幅広い方法で製品内だけでなく、サードパーティーのクラスターやシステムで使用できるので、本書で提示している情報は完全なリストではありません。

顧客は EU 一般データ保護規則など、さまざまな法律や規制を確実に遵守する責任を負います。顧客は、顧客の事業に影響を及ぼす可能性のある、関係する法律や規制の特定や解釈、およびこれらの法律や規制を遵守するために必要となる対応について、資格を持った弁護士の助言を受ける責任を単独で負います。

本書に記載されている製品、サービス、およびその他の機能は、すべての顧客の状況には適しておらず、利用が制限される可能性があります。Red Hat は、法律、会計または監査上の助言を提供するわけではなく、当社のサービスまたは製品が、お客様においていかなる法律または規制を順守していることを表明し、保証するものでもありません。

1.5.2. 目次

- [GDPR](#)
- [GDPR に準拠する製品の設定](#)
- [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
- 遵守しない場合に多額の罰金が課される可能性
- 情報流出の通知の義務付け

1.5.3.2. GDPR の詳細情報

- [EU GDPR の情報ポータル](#)
- [Red Hat GDPR の Web サイト](#)

1.5.4. GDPR に準拠する製品の設定

以下のセクションでは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームでのデータ管理のさまざまな点について説明し、GDPR 要件に準拠するための機能に関する情報を提供します。

1.5.5. データのライフサイクル

Red Hat Advanced Cluster Management for Kubernetes は、オンプレミスのコンテナ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、コンテナを管理するための統合環境です。

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

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

Red Hat Advanced Cluster Management for Kubernetes プラットフォームとそのデータフローを最もよく理解するには、Kubernetes、Docker および Operator がどのように機能するか理解する必要があります。このようなオープンソースコンポーネントは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームに不可欠です。Kubernetes デプロイメントは、アプリケーションのイン

スタンスを配置するのに使用します。これらのアプリケーションのインスタンスは、Docker イメージを参照する Operator に組み込まれます。Operator にはアプリケーションの詳細が含まれ、Docker イメージにはアプリケーションの実行に必要な全ソフトウェアパッケージが含まれます。

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

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

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

1.5.5.2. オンラインの連絡先として使用される個人データ

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

- Slack チャンネルがある場合は、Slack の公開コミュニティ
- 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
- 技術コミュニティでの公開会話

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

1.5.6. データの収集

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

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

コンテナ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のか？

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

1.5.7. データストレージ

Red Hat Advanced Cluster Management for Kubernetes プラットフォームでは、設定ファイルまたはデータベースとしてローカルまたはリモートファイルシステムのステートフルストアで、プラットフォームの設定や管理に関する技術データは永続化されます。使用されていない全データのセキュリティ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、アクセス権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 をバックエンドとして使用します。
- **ユーザー ID とパスワードなどのサービス認証データ:** コンポーネント間のアクセスに Red Hat Advanced Cluster Management for Kubernetes プラットフォームのコンポーネントが使用する認証情報は、Kubernetes Secret として定義します。Kubernetes リソース定義はすべて **etcd** の Key-Value データストアで永続化されます。初期の認証情報の値は、Kubernetes Secret の設定 YAML ファイルとして、プラットフォームの設定データで定義されます。詳細は、Kubernetes ドキュメントの [Secrets](#) を参照してください。

1.5.8. データアクセス

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

- Web ユーザーインターフェイス (コンソール)
- Kubernetes の **kubectl** CLI
- Red Hat Advanced Cluster Management for Kubernetes CLI
- oc CLI

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

1.5.8.1. 認証

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

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

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

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

1.5.8.2. ロールマッピング

Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、ロールベースのアクセス制御 (RBAC) をサポートします。ロールマッピングのステージでは、認証ステージで提示されたユーザー名がユーザーまたはグループロールにマッピングされます。認可時にロールを使用して、認証ユーザーがどのような管理者アクティビティーを実行できるか判断します。

1.5.8.3. 認可

Red Hat Advanced Cluster Management for Kubernetes プラットフォームのロールを使用して、クラスター設定アクション、カタログや Helm リソース、Kubernetes リソースへのアクセスを制御します。クラスター管理者、管理者、Operator、エディター、ビューワーなど、IAM (Identity and Access Management) ロールが複数含まれています。ロールは、チームへの追加時に、ユーザーまたはユーザーグループに割り当てられます。リソースへのチームアクセスは、namespace で制御できます。

1.5.8.4. Pod のセキュリティー

Pod のセキュリティーポリシーを使用して、Pod での操作またはアクセス権をクラスターレベルで制御できるように設定します。

1.5.9. データ処理

Red Hat Advanced Cluster Management for Kubernetes のユーザーは、システム設定を使用して、設定および管理に関する技術データをどのように処理して、データのセキュリティーを確保するかを制御できます。

ロールベースのアクセス制御 (RBAC) では、ユーザーがアクセスできるデータや機能を制御します。

転送中のデータは **TLS** を使用して保護します。**HTTPS (TLS の下層)** は、ユーザークライアントとバックエンドのサービス間でのセキュアなデータ転送を確保するために使用されます。インストール時に、使用するルート証明書を指定できます。

保管時のデータの保護は、**dm-crypt** を使用してデータを暗号化することでサポートされます。

Red Hat Advanced Cluster Management for Kubernetes プラットフォームの技術データの管理、セキュリティー確保と同じプラットフォームのメカニズムを使用して、ユーザーが開発したアプリケーションまたはユーザーがプロビジョニングしたアプリケーションの個人データを管理し、セキュリティーを確保することができます。クライアントは、独自の機能を開発して、追加の制御を実装できます。

1.5.10. データの削除

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

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

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

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

1.5.11. 個人データの使用を制限する機能

Red Hat Advanced Cluster Management for Kubernetes プラットフォームでは、エンドユーザーは本書でまとめられている機能を使用し、個人データとみなされるプラットフォーム内の技術データの使用を制限することができます。

GDPR では、ユーザーはデータへのアクセス、変更、取り扱いの制限をする権利があります。本ガイドの他の項を参照して、以下を制御します。

- アクセス権限

- Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、データへの個別アクセスを設定できます。
- Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人に対し、このプラットフォームが保持する個人データの情報を提供できます。
- 変更する権限
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人がデータを変更または修正できるようにします。
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人のデータを修正できます。
- 処理を制限する権限
 - Red Hat Advanced Cluster Management for Kubernetes プラットフォームの管理者は、Red Hat Advanced Cluster Management for Kubernetes プラットフォーム機能を使用して、個人データの取り扱いを停止できます。

1.5.12. 付録

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

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

1.6. FIPS READINESS

Red Hat Advanced Cluster Management for Kubernetes の FIPS readiness が完了しました。Red Hat Advanced Cluster Management は、同じツールを使用して、Red Hat OpenShift Container Platform で使用される Red Hat Enterprise Linux (RHEL) 認定暗号化モジュールに暗号化呼び出しが渡されるようにします。OpenShift の FIPS サポートの詳細は、[FIPS 暗号のサポート](#) を参照してください。

1.6.1. 制限事項

Red Hat Advanced Cluster Management および FIPS には以下の制限を確認してください。

- Red Hat OpenShift Container Platform は、**x86_64** アーキテクチャーでのみ FIPS をサポートします。
- Integrity Shield は、FIPS に対応していないテクノロジープレビューコンポーネントです。
- 検索および可観測性コンポーネントによって使用される Persistent Volume Claims (PVC) および S3 ストレージは、指定のストレージを設定する際に暗号化する必要があります。Red Hat Advanced Cluster Management はストレージの暗号化を提供しません。OpenShift Container Platform ドキュメント [Support for FIPS cryptography](#) を参照してください。

- Red Hat Advanced Cluster Management コンソールを使用してマネージドクラスターをプロビジョニングする場合は、マネージドクラスター作成の **Cluster details** セクションで以下のチェックボックスを選択して、FIPS 標準を有効にします。

FIPS with information text: Use the Federal Information Processing Standards (FIPS) modules provided with Red Hat Enterprise Linux CoreOS instead of the default Kubernetes cryptography suite file before you deploy the new managed cluster.