Red Hat Advanced Cluster Management for Kubernetes 2.4

リリースノート

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

Last Updated: 2022-10-02

Red Hat Advanced Cluster Management for Kubernetes 2.4 リリースノート

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

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

法律上の通知

概要

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

目次

第1章 リリースノート

Red Hat Advanced Cluster Management の 2.1 バージョンが **削除され**、サポートされなくなりました。ドキュメントはそのまま利用できますが、エラータやその他の更新がなくても非推奨になります。以前のバージョンのドキュメントもサポートされていません。

- Red Hat Advanced Cluster Management for Kubernetes の新機能
- エラータの更新
- 既知の問題と制限
- 非推奨と削除
- GDPR に対応するための Red Hat Advanced Cluster Management for Kubernetes での考慮事項
- 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、リリースされます。

詳細は、本リリースの新機能を参照してください。

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

1.1.1. Web コンソール

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

1.1.1.1. 可観測性

- 可観測性サービスに記録ルールを追加して、Kubernetes API サーバーのサービスレベルのインジケーター(SLI)およびサービスレベルの目的(SLO)を計算します。詳細は、カスタムルールの作成 を参照してください。
- Grafana ダッシュボードから、フリート内のクラスターの集計を表示して、Kubernetes API サーバーのサービスレベルの概要を確認できるようになりました。Kubernetes API サーバーダッシュボードのクラスターフリートサービスレベルの概要の表示 を 参照してください。
- Grafana ダッシュボードから 7 日または 30 日間の残りのエラー予算および時間を表示します。この場合、サービスは Kubernetes API サーバーのクラスターのサービスレベルの概要でダウンタイムを利用できます。Kubernetes API サーバーダッシュボードのクラスターサービスレベルの概要の表示 を 参照してください。
- Grafana 8.1.3 と Red Hat Advanced Cluster Management を使用してメトリクスを表示します。詳細は、環境の監視 を参照してください。
- Grafana ダッシュボードから、Kubernetes API サーバーのクラスターサービスレベルの概要を表示します。Kubernetes API サーバーダッシュボードのクラスターサービスレベルの概要の表示 を 参照してください。

1.1.2. クラスター

- 以下のプラットフォームで OpenShift Container Platform ハブクラスターをホストし、これらのプラットフォームでプロビジョニングされるクラスターを管理できるようになりました。
  - IBM Z および LinuxONE
  - IBM Power Systems
- Red Hat Advanced Cluster Management コンソールを使用して、Microsoft Azure Government クラスターを作成し、管理します。詳細は 、「Microsoft Azure の認証情報の作成 」を参照してください。
- オンプレミスクラスターを管理するためにインフラストラクチャー環境を作成します。詳細は、「 インフラストラクチャー環境の作成 」を参照してください。
- Red Hat Advanced Cluster Management コンソールを使用して、インフラストラクチャー環境でオンプレミスクラスターを作成します。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。
- アドオンのステータスに基づいてマネージドクラスターを選択します。詳細は、Add-on status を参照してください。
- クラスターの作成時に、Red Hat Advanced Cluster Management コンソールでクラスターのプロキシー情報を設定できるようになりました。詳細は、クラスターの作成 で作成するクラスターの作成トピック を 参照してください。

テクノロジープレビュー：

- クラスターのバックアップおよび復元 Operator を使用して、クラスターリソースのバックアップおよび復元をスケジュールします。詳細は、クラスターのバックアップおよび復元 Operator （テクノロジープレビュー） を参照してください。

- ゼロタッチプロビジョニングを使用して、複数の SNO クラスターをデプロイします。詳細は、OpenShift Container Platform ドキュメントのDeploying distributed units at scale in a disconnected environmentを参照してください。

- VolSync を使用して永続ボリュームを複製します。これにより、永続ボリューム上のデータのコピーを作成できます。詳細は、Replicating persistent volumes with VolSync を参照してください。

1.1.3. アプリケーション

Application コンソールの **Create application** ドロップダウンメニューから、作成するアプリケーションのタイプを選択します。Git リポジトリー、Helm リポジトリー、または Object Storage リポジトリーのサブスクリプションを作成するオプションがあります。サブスクリプションは、チャネル内の Kubernetes リソース（ソースリポジトリー）です。

テクノロジープレビュー：同じドロップダウンメニューから Argo CD ApplicationSet を作成し、大規模なクラスターで Argo CD アプリケーションを管理できるようになりました。

YAML Editor を使用すると、フィールドの変更時にアプリケーションを作成または編集する際にファイルの更新を確認できます。

アプリケーションの作成時または後に、セカンダリーチャネルを指定できます。セカンダリーチャネルを作成すると、アプリケーションはプライマリーに障害が発生した場合にセカンダリーを使用します。

サブスクリプション管理者は、許可リストおよび拒否リストを作成できます。同じロールで、すべてのアプリケーションリソースをサブスクリプションの名前空間にデプロイできるようになりました。サブスクリプション管理者タスクやその他の高度な設定トピックについては、Application advanced configuration を参照してください。

他のアプリケーション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

- **Governance** ページから表示される新しい列を使用できます。コンソールから **Source** 列を使用して、GitOps を使用してデプロイされるポリシーを特定します。**Status** 列を使用して、ポリシーの有効化を確認します。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。

- FIPS に対応した Red Hat Advanced Cluster Management クラスターを使用できるようになりました。詳細は、FIPS readinessを参照してください。

- Red Hat Insights およびガバナンスの統合を使用して、ガバナンス違反のアラートを送信します。違反を送信するコンポーネントを特定することもできます。詳細は、Insight PolicyReports の管理 を参照してください。

- 一括アクションをサポートする新しいフィルターオプションで、ダッシュボードをカスタマイズします。詳細は、Customize the Governance page を参照してください。

- **policy_governance_info** メトリックを使用してトレンドを表示し、ポリシーの失敗を分析します。詳細は、ガバナンスのメトリクス を参照してください。

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

詳細は、『リリースノート』を参照してください。

1.2. エラータの更新

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

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

FIPS の通知:**spec.ingress.sslCiphers** で独自の暗号を指定しない場合、**multiclusterhub-operator** は暗号のデフォルトリストを提供します。2.4 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。

1.2.1. Errata 2.4.7

- 一部の Grafana ダッシュボードのデータが表示されない問題を修正します。
- 1 つ以上の製品コンテナーイメージに更新を配信します。

1.2.2. Errata 2.4.6

- 空の Applications **Overview** ページで生じる可能性のある問題を修正します。(Bugzilla #2036197)
- クラスター作成プロセスから非推奨の API を削除します。(Bugzilla #2041540)
- VMware vSphere クラスターの作成時に、ネットワーク名に空白スペースを使用できるようになりました。(Bugzilla #2074766)
- Red Hat Advanced Cluster Management の **local-cluster** を更新する不足しているオプションを解決し、OpenShift Container Platform コンソールを使用して更新が手動で適用されたときに同じクラスターがハングする原因となっていた問題を解決します。(Bugzilla #2079418)
- Red Hat Advanced Cluster Management バージョン 2.2 から段階的にアップグレードした後、Red Hat Advanced Cluster Management 2.4 を使用してクラスターを作成できない問題が修正されました。(Bugzilla #2089490)
- プロビジョニングネットワーク設定は、プロビジョニングネットワークを必要としないベアメタルのデプロイメントをサポートするためにオプションになりました。(Bugzilla #2096406)
- 既存クラスターと同じ名前と namespace でクラスタープールを作成しようとすると、既存のクラスターが破棄される原因となっていた問題が修正されました。(Bugzilla #2102436)
- 1 つ以上の製品コンテナーイメージに更新を配信します。

1.2.3. Errata 2.4.5

- 可観測性のアップグレードの問題を修正します。(Bugzilla #2087277)
- Redis で利用できない検索と失敗を解決し、大量のエラーログが生じました。ヘルスモニタリングが修正され、検索コンポーネントが回復し、ログの詳細度を減らすことができます。(Bugzilla #2065318)
- フィードバックなしにフェーズを作成しない管理 VMware クラスターを **作成** する際の問題を修正します。(Bugzilla #1937078)

1.2.4. Errata 2.4.4

- クラスターに提供された無効な情報により作成が失敗しても、クラスターのステータスが **Creating** for a cluster に表示される問題を修正します。(Bugzilla #1995380)
- 追加のログインページにリンクした問題を解決します。これにより、1 時間後にログインまたは自動ログインオフ時に無限ループが発生することがありました。(Bugzilla #2061958)
- 1 つ以上の製品コンテナーイメージに更新を配信します。

1.2.5. Errata 2.4.3

- ecdsa-sha2-nistp521 ssh キーの使用時にクラスターが Red Hat Advanced Cluster Management が作成できないようにする問題を修正します。(Bugzilla #2048500)
- 1 つ以上の製品コンテナーイメージに更新を配信します。

1.2.6. エラータ 2.4.2

- **LimitRange** をサポートするポリシーの一部が Pod の再起動後の属性の変更を受け入れることを妨げる問題を修正します。(GitHub #19160)
- 1 つ以上の製品コンテナーイメージに更新を配信します。

1.2.7. エラータ 2.4.1

- ポリシーの数がそのページの他の場所に表示されるため、マネージドクラスターの詳細ビューに表示される **PolicyReport** データからガバナンスおよびリスクを取得するすべてのポリシーをフィルタリングします。(GitHub #17438)
- Operatorhub Installation コンソールのオプションの **imagepullsecret** パラメーターのサンプルを削除し、クラスターに存在しないプルシークレットが誤って使用されるのを防ぎます。(GitHub #17884)
- クラスターを破棄し、マネージドクラスターのステータスが **Unknown** になる場合に、クラスタープールが **Detaching** 状態でハングする状態が生じる原因となっていた問題を修正します。ACM 2.4.1 へのアップグレード後、**Detaching** ステータスでハングしたすべてのクラスターが namespace と共に自動的に終了し、予想される動作を再開します。これらのクラスターまたはハブクラスター上の名前空間をクリーンアップするために、手動による介入は必要ありません。(GitHub #18249)
- 機能ゲートが中央インフラストラクチャー管理 (CIM) 環境を追加できるようにするために必要な手順を削除します。
- 失敗した **ClusterDeployment** が **ClusterPool** コンソールで発生した検証エラーを妨げていた問題を修正します。(Bugzilla #1995380)
- 1 つ以上の製品コンテナーイメージに更新を配信します。

1.3. 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 known issues」を参照してください。

1.3.1. ドキュメントの既知の問題

1.3.1.1. カスタマーポータルの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ります

場合によっては、カスタマーポータルの 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。場合によっては、リンクは最上位のセクションに解決されます。

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す。

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、ブラウザー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/2.4/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/2.4/html-single/clusters/index#volsync** を読み込む必要があります。

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。

1.3.2. インストールの既知の問題

1.3.2.1. Red Hat Advanced Cluster Management のアップグレード後に Pod が復旧されない可能性がある

Red Hat Advanced Cluster Management を新しいバージョンにアップグレードすると、**StatefulSet** に属する Pod の一部が **failed** 状態のままになる可能性があります。この頻繁に発生するイベントは、既知の Kubernetes 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 が正しい設定で自動的に再起動します。

1.3.2.2. 2.2.x から 2.3.4 にアップグレードすると、klusterlet が削除される可能性があります

2.2.x から 2.3.4 にアップグレードすると、Klusterlet が削除される場合があります。この問題を回避するには、次の手順を参照してください。

1. 作業エージェントを 2.3.3 にアップグレードします。
   a. 以下の JSON コンテンツで JSON ファイル **work-image-override.json** を作成します。

```
[
  {
    "image-name": "work-rhel8",
    "image-remote": "registry.redhat.io/rhacm2",
    "image-digest":
"sha256:b6606f6bb6504acfb48f13cd5296473c17088caf380097ff7ce316f781c4f196",
    "image-key": "work"
  }
]
```

   b. ハブクラスターでイメージオーバーライド用の ConfigMap を作成します。

```
kubectl -n open-cluster-management create configmap work-image-override --from-
file=./work-image-override.json
```

   c. ハブクラスターに **mch** のアノテーションを付けて、イメージのオーバーライドを有効にします。

```
kubectl -n open-cluster-management annotate mch multiclusterhub --overwrite mch-
imageOverridesCM=work-image-override
```

   d. **multiclusterhub-operator** を再起動して変更を適用します。

```
kubectl -n open-cluster-management delete pod multiclusterhub-operator-xxxxx-xxxxx
```

   約 30 分待って、すべての管理対象クラスターで実行されている作業エージェントが、オーバーライドされたイメージで再始動されたことを確認します。
2. 2.2.x から 2.3.4 にアップグレードします。
3. work-agent のイメージオーバーライドを無効にします。
4. アップグレードが完了したら、work-agent のイメージオーバーライドを安全に削除できます。

```
kubectl -n open-cluster-management annotate mch multiclusterhub mch-imageOverridesCM-
--overwrite
kubectl -n open-cluster-management delete configmap work-image-override
```

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

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

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

-

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

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

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

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

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

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

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

1.3.4. 可観測性の既知の問題

1.3.4.1. 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

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す。

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

可観測性エンドポイントオペレーターは、MultiClusterObservability CustomResource (CR) へのデプロ

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

詳細は、可観測性の有効化 を参照してください。

1.3.4.3. ROKS クラスターにはデータがありません

Red Hat Advanced Cluster Management の可観測性は、組み込みダッシュボードで、ROKS クラスターのデータが表示されないパネルがあります。これは、ROKS が、管理対象サーバーからの API サーバーメトリクスを公開しないためです。以下の Grafana ダッシュボードには、**Kubernetes/API server**、**Kubernetes/Compute Resources/Workload**、**Kubernetes/Compute Resources/Namespace(Workload)** の ROKS クラスターをサポートしないパネルが含まれます。

1.3.4.4. ROKS クラスターに etcd データがない

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

1.3.4.5. 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てください。

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します）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。

1.3.4.6. 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しなくなるため、転送レイヤーセキュリティー (TLS) ハンドシェイクが失敗します。この問題を修正するには、検索 Pod を再起動して証明書をリセットします。

1.3.4.7. 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。

1.3.4.8. 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。

1.3.4.9. 順不同サンプルの取得エラー

可観測性を **受け取る** Pod は以下のエラーメッセージを報告します。

```
Error on ingesting out-of-order samples
```

エラーメッセージとは、メトリクスコレクションの間隔が以前のコレクション間隔で送信された時系列データよりも古い場合に、マネージドクラスターによって送信される時系列データを示すことを意味します。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高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認識されます。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、この問題は表示されません。

1.3.5. クラスター管理の既知の問題

1.3.5.1. Cluster および **clusterimageset** チャネルが自動的に同期されない

clusterimageset は **"fast"** チャ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ネルに切り替えます (**Administration** > **Cluster Settings** > **Details Channel**)。

1.3.5.2. 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ります

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、マネージドクラスターの 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。

1.3.5.3. 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

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。

1.3.5.4. 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ります

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。

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

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

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

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

1.3.5.6. 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。

1.3.5.7. 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
```

1.3.5.8. 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、ハブクラスターの自己管理の設定を一時的に編集します。

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

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

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

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

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

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

1.3.5.9. 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ー環境で失敗する

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ーが有効になっている。
- Ansible Tower には、プロキシーを介してのみアクセスできる。

1.3.5.10. 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。

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

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

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

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

1.3.5.13. 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。

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

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

1.3.5.15. 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
```

1.3.5.16. プロビジョニングされたクラスターのシークレットの自動更新はサポート対象外

クラウドプロバイダーのアクセスキーを変更しても、プロビジョニングされたクラスターのアクセスキーは、namespace で更新されません。これは、マネージドクラスターがホストされ、マネージドクラスターの削除を試みるクラウドプロバイダーで認証情報の有効期限が切れる場合に必要です。このような場合は、以下のコマンドを実行して、クラウドプロバイダーでアクセスキーを更新します。

- Amazon Web Services (AWS)

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

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

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

  CLUSTER-NAME は、お使いのクラスター名に置き換えます。

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

- Microsoft Azure

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

- VMware vSphere

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

1.3.5.17. 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。

1.3.5.18. 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。

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

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

1.3.5.20. ワークマネージャーのアドオン検索の詳細

特定のマネージドクラスターにある特定のリソースの検索詳細ページで問題が発生する可能性があります。マネージドクラスターの work-manager アドオンが **Available** ステータスであることを確認してから検索する必要があります。

1.3.5.21. アーキテクチャー全体でクラスターを作成する際に、手動で作成されたリリースイメージが必要です。

ハブクラスターのアーキテクチャーとは異なるアーキテクチャーでマネージドクラスターを作成するには、両方のアーキテクチャーのファイルが含まれるリリースイメージ(**ClusterImageSet**)を作成する必要があります。たとえば、**ppc64le** または **s390x** のハブクラスターから **x86_**64 クラスターを作成する場合は、リリースイメージを作成する必要があります。両方のファイルセットでリリースイメージを作成する場合、新規のリリースイメージにより OpenShift Container Platform リリースレジストリーがマルチアーキテクチャーイメージマニフェストを提供できるので、クラスターの作成は成功します。

この問題を回避するには、アーキテクチャタイプについて次の例のような手順を実行します。

1. OpenShift Container Platform リリースレジストリー から、**x86_64**、**s390x**、および **ppc64le** リリースイメージを含む マニフェスト一覧 を作成します。

   a. Quay リポジトリーから両方のアーキテクチャーのマニフェスト一覧をプルします。

```
$ podman pull quay.io/openshift-release-dev/ocp-release:4.9.1-x86_64
$ podman pull quay.io/openshift-release-dev/ocp-release:4.9.1-ppc64le
$ podman pull quay.io/openshift-release-dev/ocp-release:4.9.1-s390x
```

   b. イメージを管理するプライベートリポジトリーにログインします。

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

   private-repo は、リポジトリーへのパスに置き換えます。

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

```
$ podman push quay.io/openshift-release-dev/ocp-release:4.9.1-x86_64 <private-repo>/ocp-release:4.9.1-x86_64
$ podman push quay.io/openshift-release-dev/ocp-release:4.9.1-ppc64le <private-
```

```
repo>/ocp-release:4.9.1-ppc64le
$ podman push quay.io/openshift-release-dev/ocp-release:4.9.1-s390x <private-
repo>/ocp-release:4.9.1-s390x
```

private-repo は、リポジトリーへのパスに置き換えます。

d. 新規情報のマニフェストを作成します。

```
$ podman manifest create mymanifest
```

e. 両方のリリースイメージへの参照をマニフェスト一覧に追加します。

```
$ podman manifest add mymanifest <private-repo>/ocp-release:4.9.1-x86_64
$ podman manifest add mymanifest <private-repo>/ocp-release:4.9.1-ppc64le
$ podman manifest add mymanifest <private-repo>/ocp-release:4.9.1-s390x
```

private-repo は、リポジトリーへのパスに置き換えます。

f. マニフェストリストの一覧を既存のマニフェストにマージします。

```
$ podman manifest push mymanifest docker://<private-repo>/ocp-release:4.9.1
```

private-repo は、リポジトリーへのパスに置き換えます。

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

a. 以下の例のような情報を含む **YAML** ファイルを作成します。

```
apiVersion: hive.openshift.io/v1
kind: ClusterImageSet
metadata:
  labels:
    channel: fast
    visible: "true"
  name: img4.9.1-appsub
spec:
  releaseImage: <private-repo>/ocp-release:4.9.1
```

private-repo は、リポジトリーへのパスに置き換えます。

b. ハブクラスターで以下のコマンドを実行し、変更を適用します。

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

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

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

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

1.3.5.22. IBM Power または IBM Z システムハブクラスターでは Argo CD はサポートされません。

Red Hat Advanced Cluster Management との Argo CD の統合は、利用可能な **ppc64le** イメージまたは **s390x** イメージがないため、IBM Power で実行されている Red Hat Advanced Cluster Management ハブクラスターでは機能しません。

1.3.5.23. IBM Power または IBM Z システムハブクラスターとの Ansible Tower 統合を使用できません。

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ので、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。

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

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

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

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

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

1.3.6. アプリケーション管理の既知の問題

1.3.6.1. サブスクリプション管理者による場合を除き、ポリシーリソースはデプロイされません

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、ソースリポジトリーに合わせて調整されません。

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

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

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

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

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

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

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

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

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

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

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

2. お使いのサブスクリプションで、作成した配置ルールを参照します。以下を参照してください。

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
```

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

両方を適用すると、Ansible インスタンスがハブクラスターに作成されているのが表示されるはずです。

1.3.6.4. Editor ロールのアプリケーションエラー

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

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

1.3.6.5. 配置ルールの編集ロールエラー

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

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

1.3.6.6. 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。

1.3.6.7. 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
```

1.3.6.8. 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。

1.3.6.9. 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。

1.3.6.10. Ansible Automation Platform Operator によるプロキシー外の Ansible Tower へのアクセス

Ansible Automation Platform(AAP)Operator は、プロキシー対応の 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 をプロキシー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。

1.3.6.11. 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。

1.3.6.12. アプリケーション名の要件

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

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

1.3.6.13. アプリケーションコンソールの表

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

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

1.3.7. ガバナンスの既知の問題

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

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

1.3.7.2. 配置リソースの制限

リマインダーとして、ポリシーは **PlacementRule** または **Placement** リソースを使用して、特定のマネージドクラスターへのポリシーのデプロイを制御する必要があります。**Placement** リソースを使用するポリシーを作成する場合には、以下の制限事項があります。

- コンソールからポリシーの詳細を表示すると、配置情報は表示されません。
- コンソールからポリシーを削除しても、配置情報は削除されません。
- コンソールからポリシーを編集しても、配置情報は更新されません。

Placement リソースの使用時には、コマンドラインインターフェース(CLI)を使用してポリシーの更新を行います。

1.3.7.3. 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。

1.3.7.4. namespace が Terminating 状態のままの場合の設定ポリシーが一覧表示されます。

complianceType パラメーターについて **mustnothave** で設定され、**remediationAction** パラメーターに **enforce** が設定されている設定ポリシーがある場合、ポリシーは Kubernetes API の削除要求が加えられた後に準拠済みとして一覧表示されます。そのため、ポリシーが準拠していると、Kubernetes オブジェクトは **Terminating** 状態のままにすることができます。

1.3.8. バックアップおよび復元の既知の問題

1.3.8.1. 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。

1.3.8.2. 復元操作後、アプリケーションとポリシーに管理対象クラスターのリソースステータスが表示されない

別のハブクラスターからバックアップされたデータを使用して、新しいハブクラスターで復元操作を実行すると、アプリケーションとポリシーは、管理対象クラスター上のリソースのステータスを表示しません。これは、検索アドオンとポリシーアドオンが新しいハブクラスターを指すようにリセットされていないために発生します。

新規ハブクラスターから、全マネージドクラスターの **addon-certpolicyctrl** および **addon-search** を再起動する必要があります。次のコマンドを実行して、Pod を再起動します。

```
oc get pods -n open-cluster-management-agent-addon | grep search | awk '{print $1}' | xargs kubectl delete pod
```

1.4. 非推奨と削除

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

重要:

- Red Hat Advanced Cluster Management の 2.1 バージョンが **削除され**、サポートされなくなりました。ドキュメントはそのまま利用できますが、エラータやその他の更新がなくても非推奨になります。以前のバージョンのドキュメントもサポートされていません。
- Red Hat Advanced Cluster Management の最新バージョンへのアップグレードがベストプラクティスです。

1.4.1. API の非推奨と削除

Red Hat Advanced Cluster Management は、Kubernetes の API 非推奨ガイドラインに従います。このポリシーの詳細については、 「Kubernetes の非推奨ポリシー」を参照してください。

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

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

1.4.1.1. API の非推奨化

製品またはカテゴリー	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
アプリケーション	**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。	2.4	**V1beta1** の使用	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ー	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
アプリケーション	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。	セキュリティーポリシーの管理 を参照してください。
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
klusterlet Operator	**release-2.4,release-2.3** チャネルは更新を受信しない	2.3 以降	Red Hat OpenShift 専用クラスターをインポートおよび管理するには、2.5 にアップグレードして更新を受信する必要があります。	「Operator を使用したアップグレード」を 参照してください。
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
アプリケーション	**HelmRepo** チャネル仕様: **insecureSkipVerify: "true"** は **configMapRef** 内では使用しません。	2.2	**configMapRef** のないチャネルで **insecureSkipVerify: "true"** を使用します。	変更については、YAML サンプルを参照してください。
インストーラー	**operator.open-cluster-management.io_multiclusterhubs_crd.yaml** の Hive 設定	2.2	インストールして、**oc edit hiveconfig hive** コマンドで直接 **hiveconfig** を編集します。	なし

1.4.3. 削除

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

製品またはカテゴリー	影響を受けるアイテム	バージョン	推奨されるアクション	詳細およびリンク
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
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
可観測性トポロジー	**Observe 環境** からのトポロジーアクセスを完全に削除	2.2	なし	アプリケーショントポロジーは **アプリケーション管理** に配置されるようになり、**可観測性コンソール** には表示されなくなります。
アプリケーション	Namespace のチャネルタイプを完全に削除	2.2	なし	なし

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

1.5.1. 注意

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

顧客は EU 一般データ保護規則など、さまざまな法律や規制を確実に遵守する責任を負います。顧客

は、顧客の事業に影響を及ぼす可能性のある、関係する法律や規制の特定や解釈、およびこれらの法律や規制を遵守するために必要となる対応について、資格を持った弁護士の助言を受ける責任を単独で負います。

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

1.5.2. 目次

1.5.3. GDPR

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

1.5.3.1. GDPR が重要な理由

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

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

1.5.3.2. GDPR の詳細情報

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

1.5.4. GDPR に準拠する製品の設定

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

1.5.5. データのライフサイクル

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

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

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

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

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

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

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

1.5.5.2. オンラインの連絡先として使用される個人データ

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

- Slack チャネルがある場合は、Slack の公開コミュニティー

- 製品ドキュメントに関する公開コメントまたはチケット
- 技術コミュニティーでの公開会話

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

1.5.6. データの収集

Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、機微な個人情報を収集しません。当製品は、管理者ユーザー ID とパスワード、サービスユーザー ID とパスワード、IP アドレス、Kubernetes ノード名など、個人データとみなされる可能性のある、技術データを作成し、管理します。また、Red Hat Advanced Cluster Management for Kubernetes プラットフォームは、プラットフォームの管理ユーザーに関する情報も扱います。このような全情報には、ロールベースのアクセス制御を使用した管理コンソールを使用するかまたは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームノードにログインしたシステム管理者のみがアクセスできます。

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

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

- アプリケーションとの間で行き来するデータはどのように保護されるのか?移動中のデータは暗号化されているか?
- アプリケーションでデータはどのように保存されるのか?使用していないデータは暗号化されるのか?
- アプリケーションのアクセスに使用する認証情報はどのように収集され、保存されるのか?
- アプリケーションがデータソースへのアクセス時に使用する認証情報はどのように収集され、保存されるのか?
- アプリケーションが収集したデータを必要に応じて削除するにはどうすればよいか?

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

1.5.7. データストレージ

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

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

- **プラットフォームの設定データ:** Red Hat Advanced Cluster Management for Kubernetes プラットフォームの設定は、一般的な設定、Kubernetes、ログ、ネットワーク、Docker などの設定のプロパティーを使用して設定 YAML ファイルを更新し、カスタマイズできます。このデー

タは、Red Hat Advanced Cluster Management for Kubernetes プラットフォームインストーラーへの入力情報として使用し、1 つまたは複数のノードをデプロイします。このプロパティーには、ブートストラップに使用される管理者ユーザー ID とパスワードも含まれます。

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

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

- **ユーザー ID とパスワードなどのサービス認証データ:** コンポーネント間のアクセスに Red Hat Advanced Cluster Management for Kubernetes プラットフォームのコンポーネントが使用する認証情報は、Kubernetes Secret として定義します。Kubernetes リソース定義はすべて **etcd** の Key-Value データストアで永続化されます。初期の認証情報の値は、Kubernetes Secret の設定 YAML ファイルとして、プラットフォームの設定データで定義されます。詳細は、「シークレットの管理」を参照してください。

1.5.8. データアクセス

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

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

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

1.5.8.1. 認証

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

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

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

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

1.5.8.2. ロールマッピング

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

1.5.8.3. 認可

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

1.5.8.4. Pod のセキュリティー

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

1.5.9. データ処理

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

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

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

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

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

1.5.10. データの削除

Red Hat Advanced Cluster Management for Kubernetes プラットフォームには、コマンド、アプリケーションプログラミングインターフェース (API)、およびユーザーインターフェースのアクションが含まれており、製品が作成または収集したデータを削除します。これらの機能により、サービスユーザー ID

およびパスワード、IP アドレス、Kubernetes ノード名、または他のプラットフォームの設定データ、プラットフォームを管理するユーザーの情報などの、技術データを削除できます。

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

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

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

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

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

1.5.11. 個人データの使用を制限する機能

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

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

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

1.5.12. 付録

Red Hat Advanced Cluster Management for Kubernetes はプラットフォームとして、複数の技術データ

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

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

1.6. FIPS READINESS

Red Hat Advanced Cluster Management for Kubernetes の FIPS readiness が完了します。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、「Support for FIPS cryptography」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、IBM Power(**ppc64le**)および IBM Z(**s390x**)アーキテクチャーで FIPS をサポートしません。
- 以下のテクノロジープレビューのコンポーネントは FIPS の準備が整っていません。
  - ストレージクラスターのバックアップおよび復元
  - Red Hat OpenShift のインフラストラクチャー Operator
  - Submariner
  - VolSync
- 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 Claim（永続ボリューム要求、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 からマネージドクラスターをプロビジョニングする場合は、新しいマネージドクラスターをデプロイする前に、**install-config.yaml** ファイルで **fips: true** を設定する必要があります。