Red Hat Advanced Cluster Management for Kubernetes 2.6

バックアップおよび復元

バックアップと復元の詳細について

Last Updated: 2023-11-01

Red Hat Advanced Cluster Management for Kubernetes 2.6 バックアップおよび復元

バックアップと復元の詳細について

法律上の通知

概要

バックアップと復元の詳細については、こちらをご覧ください。

目次

第1章 バックアップおよび復元

クラスターのバックアップおよび復元 Operator は、ハブクラスターで実行され、Red Hat Advanced Cluster Management for Kubernetes ハブクラスターの障害に対する災害復旧ソリューションを提供します。ハブクラスターに障害が発生すると、すべてのマネージドクラスターが引き続き正常に動作していても、ポリシー設定ベースのアラートやクラスターの更新などの一部の機能が動作しなくなります。ハブクラスターが利用できなくなったら、回復が可能かどうか、新しくデプロイメントされたハブクラスターからデータを回復する必要があるかどうかを判断するための回復計画が必要です。

アクティブ/パッシブハブクラスター設定を設定する方法について説明します。この設定では、最初のハブクラスターがデータをバックアップし、アクティブクラスターが使用できなくなったときにマネージドクラスターを制御するために 1 つ以上のパッシブハブクラスターがスタンバイになります。

また、メインハブクラスターが利用できず、復元操作が必要な場合に管理者に通知するように設定された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がアラートを送信する方法についても学びます。メインハブクラスターがアクティブでクラスターを管理している場合でも、バックアップソリューションが期待どおりに機能しない場合、同じポリシーが管理者に警告します。バックアップデータが生成されない問題、またはバックアップデータとハブクラスターが使用できなくなる可能性があるその他の問題が報告されます。

クラスターのバックアップと復元の Operator は、OADP Operator に依存して Velero をインストールし、ハブクラスターからデータが保存されているバックアップストレージの場所への接続を作成します。Velero は、バックアップおよび復元操作を実行するコンポーネントです。クラスターのバックアップおよび復元 Operator ソリューションは、マネージドクラスター、アプリケーション、ポリシー、ベアメタルアセットなどのすべての Red Hat Advanced Cluster Management ハブクラスターリソースのバックアップおよび復元サポートを提供します。

クラスターのバックアップおよび復元の Operator は、ハブクラスターのインストールを拡張するサードパーティーリソースのバックアップをサポートします。このバックアップソリューションを使用すると、指定した時間間隔で実行する cron ベースのバックアップスケジュールを定義できます。ハブクラスターがダウンしたら、新しいハブクラスターをデプロイし、バックアップされたデータを新しいハブクラスターに移動します。

次のトピックを読み続けて、バックアップおよび復元 operator の詳細を確認してください。

- アクティブ/パッシブ設定
- 障害復旧
- Operator アーキテクチャーのバックアップと復元
  - バックアップされるリソース
  - マネージドクラスターのアクティブ化時に復元されるリソース
  - リソース要求および制限のカスタマイズ
- マネージドクラスターのアクティベーションデータ
- アクティベーションデータを復元する前のクラスターの準備

1.1. アクティブ/パッシブ設定

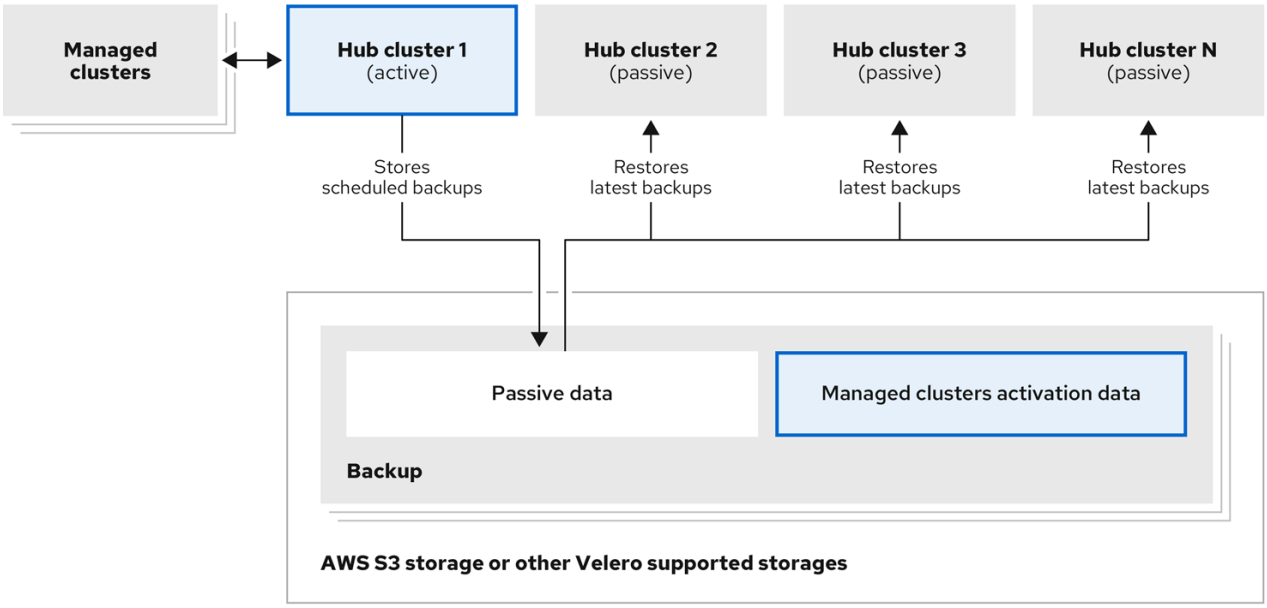
アクティブ/パッシブ設定では、アクティブなハブクラスターが 1 つと、パッシブなハブクラスターが複数あります。アクティブなハブクラスターは、プライマリーハブクラスターとも見なされ、プライマリーハブクラスターは、**BackupSchedule.cluster.open-cluster-management.io** リソースを使用し

て、クラスターを管理し、定義された時間間隔でリソースをバックアップします。

パッシブハブクラスターは、最新のバックアップを継続的に取得し、パッシブデータを復元します。パッシブハブは、**Restore.cluster.open-cluster-management.io** リソースを使用して、新規バックアップデータが利用可能な場合に、プライマリーハブクラスターからパッシブデータを復元します。これらのハブクラスターは、プライマリーハブクラスターがダウンした時にプライマリーハブに切り替えられるように、スタンバイ状態にあります。

アクティブ/パッシブのハブクラスターは同じストレージの場所に接続されており、プライマリーハブクラスターは、プライマリーハブクラスターは、バックアップにアクセスするために、パッシブハブクラスターのデータをバックアップします。この自動復元の設定方法の詳細については、バックアップを確認しながら、パッシブリソースを復元する セクションを参照してください。

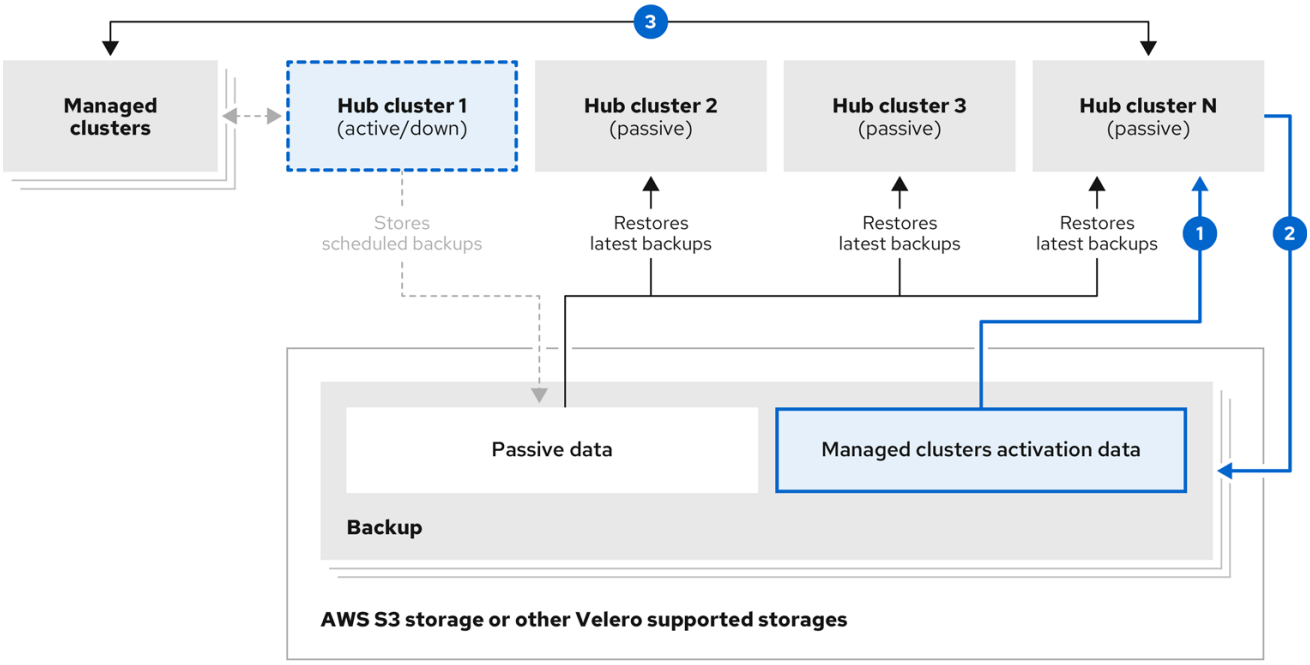
以下の図は、アクティブなハブクラスターがローカルクラスターを管理し、ハブクラスターデータを一定間隔でバックアップします。



パッシブハブクラスターは、マネージドクラスターをパッシブハブクラスターに移動するマネージドクラスターアクティベーションデータを除いて、このデータを復元します。パッシブハブクラスターは、パッシブデータを継続的に復元できます。バックアップを確認しながら、パッシブリソースを復元する セクションを参照してください。パッシブハブクラスターは、パッシブデータを 1 回限りの操作で復元できます。詳細については、パッシブリソースを復元する セクションを参照してください。

1.2. 障害復旧

プライマリーハブクラスターに障害が発生した場合、管理者はパッシブハブクラスターを選択してマネージドクラスターを引き継ぎます。以下のイメージでは、管理者は **ハブクラスター N** を新しいプライマリーハブクラスターとして使用するように決めます。



ハブクラスター N は、マネージドクラスターのアクティブ化データを復元します。この時点で、マネージドクラスターは、**ハブクラスター N** に接続されます。管理者は、**BackupSchedule.cluster.open-cluster-management.io** リソースを作成し、最初のプライマリーハブクラスターと同じストレージの場所にバックアップを保存することにより、新しいプライマリーハブクラスターである **ハブクラスター N** のバックアップをアクティブ化します。

その他のパッシブハブクラスターはすべて、新しいプライマリーハブクラスターで作成したバックアップデータを使用してパッシブデータを復元するようになりました。**ハブクラスター N** がプライマリーハブクラスターとなり、クラスターの管理とデータのバックアップを行います。

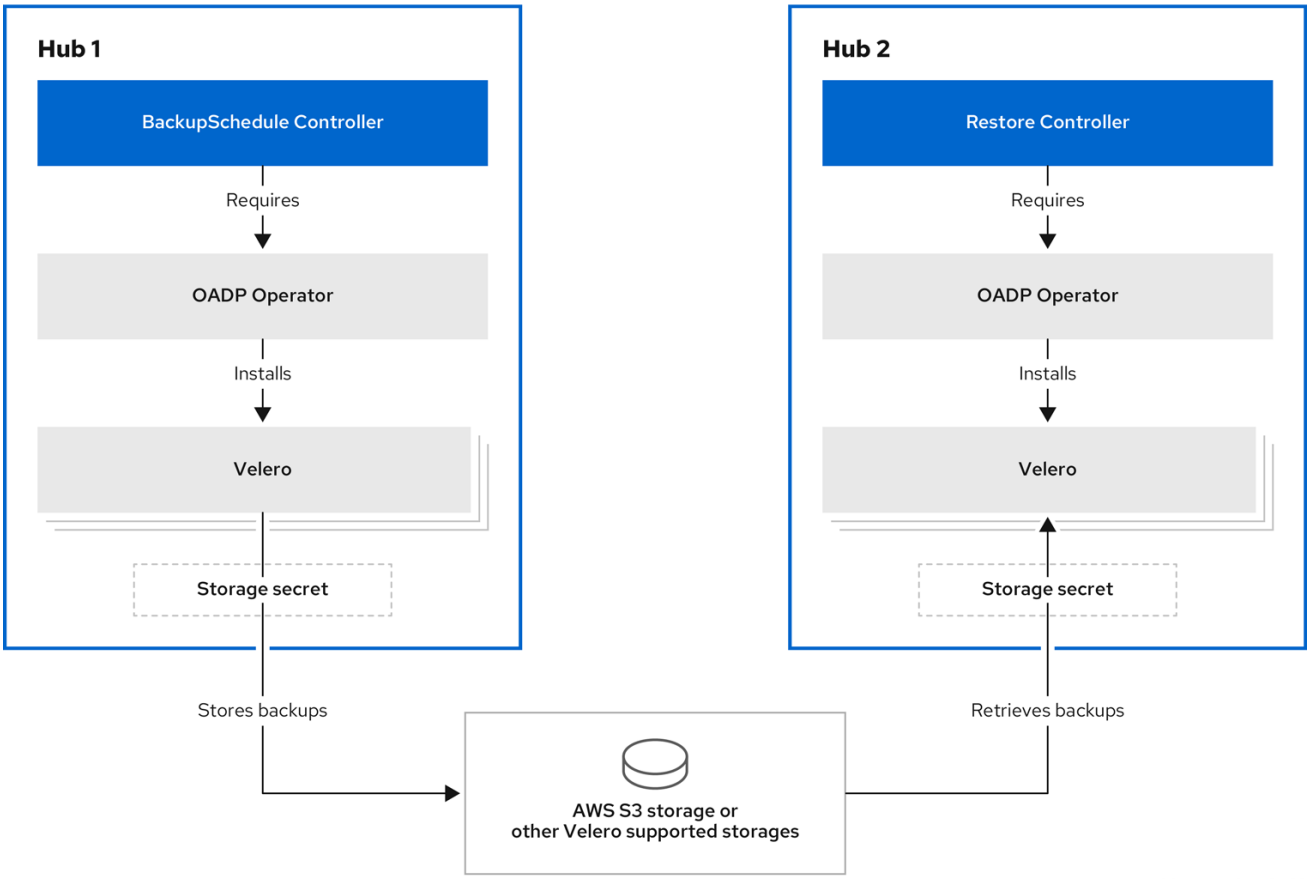
注記:

- 前の図のプロセス 1 は自動化されていません。これは、プライマリーハブクラスターに障害が発生して交換する必要があるかどうか、ハブクラスターとマネージドクラスターの間にネットワーク通信エラーがあるかどうかを管理者が判断する必要があるためです。また、管理者は、どのパッシブハブクラスターがプライマリーハブクラスターになるかを決定します。Ansible ジョブとのポリシー統合は、バックアップポリシーがバックアップエラーを報告したときに Ansible ジョブを実行することで、このステップを自動化するのに役立ちます。

- 前の図のプロセス 2 は手動です。管理者が新しいプライマリーハブクラスターからバックアップを作成しない場合、cron ジョブとしてアクティブに実行されているバックアップを使用して、管理者に通知されます。

1.3. OPERATOR アーキテクチャーのバックアップと復元

Operator は、プロセスに使用されている **backupSchedule.cluster.open-cluster-management.io** リソース (Red Hat Advanced Cluster Management のバックアップスケジュールの設定に使用) と **restore.cluster.open-cluster-management.io** リソース (バックアップの処理と復元に使用) を定義します。Operator は、対応する Velero リソースを作成し、リモートクラスターと、復元を必要とする他のハブクラスターリソースのバックアップに必要なオプションを定義します。次の図を表示します。



1.3.1. バックアップされるリソース

クラスターのバックアップと復元の Operator ソリューションは、マネージドクラスター、アプリケーション、ポリシー、ベアメタルアセットなど、すべてのハブクラスターリソースのバックアップおよび復元のサポートを提供します。このソリューションを使用して、基本的なハブクラスターのインストールを拡張するサードパーティーリソースをバックアップできます。このバックアップソリューションを使用すると、cron ベースのバックアップスケジュールを定義できます。これは、指定された時間間隔で実行し、ハブクラスターのコンテンツの最新バージョンを継続的にバックアップします。

ハブクラスターを交換する必要がある場合、またはハブクラスターに障害が発生したときに災害シナリオにある場合は、新しいハブクラスターをデプロイし、バックアップデータを新しいハブクラスターに移動できます。

バックアップデータを識別するために、次のクラスターバックアップおよび復元プロセスの順序付きリストを表示します。

- **MultiClusterHub** namespace のすべてのリソースを除外します。これは、現在のハブクラスター ID にリンクされているため、バックアップする必要のないインストールリソースのバックアップを回避するためです。
- API バージョンの接尾辞が **.open-cluster-management.io** のすべての CRD をバックアップします。この接尾辞は、すべての Red Hat Advanced Cluster Management リソースがバックアップされることを示します。
- API グループ (**argoproj.io**、**app.k8s.io**、**core.observatorium.io**、**hive.openshift.io**) からすべての CRD をバックアップします。
- API グループ (**admission.cluster.open-cluster-management.io**、**admission.work.open-cluster-management.io**、**internal.open-cluster-management.io**、**operator.open-cluster-**

management.io, **work.open-cluster-management.io**、**search.open-cluster-management.io**、**admission.hive.openshift.io**、**velero.io**) からすべての CRD を除外します。

- 含まれる API グループの一部である CRD (**clustermanagementaddon**、**observabilityaddon**、**applicationmanager**、**certpolicycontroller**、**iampolicycontroller**、**policycontroller**、**searchcollector**、**workmanager**、**backupschedule**、**restore**、**clusterclaim.cluster.open-cluster-management.io**) を除外しますが、これらは必要ないか、所有者リソースによって再作成されます。これらもバックアップされます。

- ラベル (**cluster.open-cluster-management.io/type**、**hive.openshift.io/secret-type**、**cluster.open-cluster-management.io/backup**) のいずれかを使用してシークレットと ConfigMap をバックアップします。

- バックアップが必要で、前述の基準に含まれていないその他のリソースには、**cluster.open-cluster-management.io/backup** ラベルを使用します。以下の例を参照してください。

```
apiVersion: my.group/v1alpha1
kind: MyResource
 metadata:
   labels:
    cluster.open-cluster-management.io/backup: ""
```

注意: hive.openshift.io.ClusterDeployment リソースによって使用されるシークレットはバックアップする必要があり、クラスターがコンソールを使用して作成された場合にのみ、**cluster.open-cluster-management.io/backup** ラベルで自動的に注釈が付けられます。代わりに GitOps を使用して Hive クラスターをデプロイする場合は、**cluster.open-cluster-management.io/backup** ラベルを **ClusterDeployment** で使用されるシークレットに手動で追加する必要があります。

- バックアップしたくない特定のリソースを除外します。たとえば、バックアッププロセスから Velero リソースを除外するには、次の例を参照してください。

```
apiVersion: my.group/v1alpha1
kind: MyResource
 metadata:
  labels:
    velero.io/exclude-from-backup: "true"
```

1.3.2. マネージドクラスターのアクティブ化時に復元されるリソース

cluster.open-cluster-management.io/backup ラベルをリソースに追加すると、リソースは **acm-resources-generic-schedule** バックアップで自動的にバックアップされます。いずれかのリソースを復元する必要がある場合は、ラベル値を **cluster-activation** に設定する必要があります。これは、マネージドクラスターが新しいハブクラスターに移動された後、復元されたリソースで **veleroManagedClustersBackupName:latest** が使用された場合に限ります。これにより、マネージドクラスターのアクティブ化が呼び出されない限り、リソースが復元されなくなります。以下の例を参照してください。

```
apiVersion: my.group/v1alpha1
kind: MyResource
 metadata:
  labels:
    cluster.open-cluster-management.io/backup: cluster-activation
```

cluster.open-cluster-management.io/backup: cluster-activation ラベルを使用して識別され、**acm-resources-generic-schedule** バックアップによって保存されるアクティベーションデータリソースとは別に、クラスターのバックアップおよび復元 Operator には、デフォルトでは、アクティベーションセット内のいくつかのリソースが含まれます。次のリソースは、**acm-managed-clusters-schedule** バックアップによってバックアップされます。

- **managedcluster.cluster.open-cluster-management.io**
- **managedcluster.clusterview.open-cluster-management.io**
- **klusterletaddonconfig.agent.open-cluster-management.io**
- **managedclusteraddon.addon.open-cluster-management.io**
- **managedclusterset.cluster.open-cluster-management.io**
- **managedclusterset.clusterview.open-cluster-management.io**
- **managedclustersetbinding.cluster.open-cluster-management.io**
- **clusterpool.hive.openshift.io**
- **clusterclaim.hive.openshift.io**
- **clustercurator.cluster.open-cluster-management.io**

1.3.3. リソース要求および制限のカスタマイズ

Velero の初回インストール時に、Velero Pod は以下のサンプルで定義されるデフォルトの CPU およびメモリー制限に設定されます。

```
resources:
 limits:
   cpu: "1"
   memory: 256Mi
 requests:
   cpu: 500m
   memory: 128Mi
```

前のサンプルの制限は一部のシナリオでうまく機能しますが、クラスターが多数のリソースをバックアップする場合には更新する必要がある場合があります。たとえば、2000 クラスターを管理するハブクラスターでバックアップを実行すると、out ofmemory error (OOM) が原因で Velero Pod がクラッシュします。以下の設定では、このシナリオでバックアップを完了できます。

```
  limits:
    cpu: "2"
    memory: 1Gi
  requests:
    cpu: 500m
    memory: 256Mi
```

Velero Pod リソースの制限および要求を更新するには、**DataProtectionApplication** リソースを更新し、Velero Pod の **resourceAllocation** テンプレートを挿入する必要があります。以下のサンプルを参照してください。

```
apiVersion: oadp.openshift.io/v1alpha1
kind: DataProtectionApplication
metadata:
  name: velero
  namespace: open-cluster-management-backup
spec:
...
  configuration:
...
    velero:
      podConfig:
        resourceAllocations:
          limits:
            cpu: "2"
            memory: 1Gi
          requests:
            cpu: 500m
            memory: 256Mi
```

DataProtectionApplication パラメーターの詳細は、Velero リソース要求および制限のカスタマイズ を参照してください。

1.4. マネージドクラスターのアクティベーションデータ

マネージドクラスターアクティベーションデータまたはその他のアクティベーションデータは、バックアップリソースです。アクティベーションデータが新しいハブクラスターに復元すると、マネージドクラスターは、復元が実行するハブクラスターによりアクティブに管理されます。**cluster.open-cluster-management.io/backup: cluster-activation** ラベルを使用すると、アクティベーションデータリソースは、マネージドクラスターのバックアップおよび resource-generic バックアップにより保存されます。

Operator の使用方法については、バックアップと復元の Operator の管理 を参照してください。

1.5. アクティベーションデータを復元する前のクラスターの準備

新しいハブクラスターでアクティベーションデータを復元する前に、次の手順を実行して、データの破損やクラスターの損失を回避します。

1. プライマリークラスターをシャットダウンします。
   詳細は、プライマリークラスターのシャットダウン を参照してください。

2. 既存のマネージドクラスターを復元ハブとして使用する場合は、**MultiClusterHub** で **disableHubSelfManagement** を **true** に設定します。
   詳細は、disableHubSelfManagement トピックを参照してください。

   次の例を参照してください。この例では、**spec.disableHubSelfManagement** を **true** に設定しています。

   ```
   apiVersion: operator.open-cluster-management.io/v1
   kind: MultiClusterHub
   metadata:
     name: multiclusterhub
     namespace: <namespace>
   spec:
     disableHubSelfManagement: true
   ```

注記: アクティベーションデータを復元ハブクラスターに移動する前に復元ハブクラスターで自己管理オプションを無効にしていないと、**local-cluster** klusterlet とマネージドクラスター namespace 内の klusterlet が競合します。その結果、復元ハブクラスターは、マネージドクラスターおよび復元されたマネージドクラスターを使用して自己管理されます。デタッチ操作の一部としてマネージドクラスターをデタッチすると、マネージドクラスターはプロビジョニング解除リクエストを受信し、その結果、復元ハブクラスター自体が削除されます。

1.6. バックアップおよびリストア OPERATOR の管理

クラスターのバックアップおよび復元 Operator は自動的にインストールされません。**MultiClusterHub** リソースで **cluster-backup** パラメーターを **true** に設定して、バックアップコンポーネントを有効にします。有効にすると、クラスターのバックアップと復元のオペレーターが **open-cluster-management-backup** namespace にインストールされます。クラスターバックアップオペレーターをインストールすると、クラスターバックアップおよび復元オペレーターと同じ namespace に OADP Operator も自動的にインストールされます。

注記:

- OADP Operator 1.0 はマルチアーキテクチャービルドをサポートしなくなり、公式リリース用に x86_64 ビルドのみを生成します。その結果、**x86_64** 以外のアーキテクチャーを使用している場合は、バックアップコンポーネントでインストールされた OADP Operator を正しいバージョンに置き換える必要があります。バージョンを置き換えるには、OADP Operator をアンインストールし、アーキテクチャーに一致するオペレーターを見つけてからインストールします。

- 以前に OADP Operator をハブクラスターにインストールして使用していた場合は、バックアップコンポーネントの namespace とは異なる namespace で、このバージョンをアンインストールしてください。これは、バックアップコンポーネントが、コンポーネントの namespace にインストールされた OADP で動作するようになったためです。バックアップコンポーネントでインストールされた OADP Operator が所有する **DataProtectionApplication** リソースと同じストレージの場所を使用します。これは、前回の Operator と同じバックアップデータにアクセスします。Velero バックアップリソースが、このハブクラスターの新しい OADP Operator namespace 内に読み込まれるようになりました。

Velero は、Red Hat Advanced Cluster Management ハブクラスターの OADP Operator と共にインストールされます。Velero は、Red Hat Advanced Cluster Management ハブクラスターリソースのバックアップおよび復元に使用されます。

Velero のサポートされるストレージプロバイダーの一覧は、S3-Compatible オブジェクトストアプロバイダー を参照してください。

- 前提条件
- バックアップおよびリストア Operator の有効化
- バックアップおよびリストア Operator の使用
- Extending backup data
- Scheduling a cluster backup
- バックアップの復元
  - Preparing the new hub cluster
  - 復元前のハブクラスターのクリーニング

- Restoring passive resources while checking for backups
- Restoring passive resources
- Restoring all resources
- Restoring imported managed clusters
- 他の復元サンプルの使用
- 復元イベントの表示
- Shutting down the primary cluster

- Validating your backup or restore configurations
- サーバー側の暗号化を使用したデータの保護

1.6.1. 前提条件

バックアップおよび復元 operator を有効にして使用するには、次の前提条件を満たしている必要があります。

- バックアップの保存先となるクラウドストレージの 認証情報シークレットの作成 手順を必ず実行します。シークレットリソースは、バックアップコンポーネントの namespace にある OADP Operator の namespace に作成する必要があります。
- **アクティブ/パッシブハブクラスターの両方の場合**:
  - Red Hat OpenShift Container Platform クラスターから、Red Hat Advanced Cluster Management for Kubernetes Operator バージョン 2.6.x をインストールします。**MultiClusterHub** リソースは、Red Hat Advanced Cluster Management のインストール時に自動的に作成され、**Running** のステータスを表示します。
  - クラスターのバックアップおよび復元 Operator は手動でインストールする必要があります。クラスターのバックアップおよび復元 Operator (**cluster-backup**) を有効にします。**cluster-backup** パラメーターを **true** に設定して **MultiClusterHub** リソースを編集します。これにより、バックアップコンポーネントと同じネームスペースに OADP オペレータがインストールされます。
- **パッシブハブクラスターの場合**:
  - パッシブハブクラスターで復元操作を実行する前に、ハブクラスターを手動で設定し、すべての Operator をアクティブなハブクラスターと同じ namespace にインストールする必要があります。
  - Red Hat Advanced Cluster Management Operator が、初期ハブクラスターと同じ namespace にインストールされていることを確認します。次に **DataProtectionApplication** リソースを作成し、初期ハブクラスターがデータをバックアップしたのと同じストレージの場所に接続します。
- **DataProtectionAppliation** リソースの作成時に作成したシークレットを使用します。
  以下の手順を実行して、**DataProtectionApplication** リソースのインスタンスを作成します。
  1. Red Hat OpenShift Container Platform コンソールから、**Operators** > **Installed Operators** を選択します。

2. DataProtectionApplication の下の **Create instance** をクリックします。

3. {ocp-short) コンソールを使用して設定を選択するか、**DataProtectionApplication** の例で説明されているように YAML ファイルを使用して、Velero インスタンスを作成します。

4. **DataProtectionApplication** namespaceを **open-cluster-management-backup** に設定します。

5. **DataProtectionApplication** リソースの仕様 (**spec:**) 値を適切に設定します。次に、**Create** をクリックします。
デフォルトのバックアップストレージの場所を使用する場合は、**backupStorageLocations** セクションで値 **default: true** を設定します。以下の **DataProtectionApplication** リソースの例を確認します。

```
apiVersion: oadp.openshift.io/v1alpha1
kind: DataProtectionApplication
metadata:
  name: dpa-sample
spec:
  configuration:
    velero:
      defaultPlugins:
      - openshift
      - aws
    restic:
      enable: true
  backupLocations:
    - name: default
      velero:
        provider: aws
        default: true
        objectStorage:
          bucket: my-bucket
          prefix: my-prefix
        config:
          region: us-east-1
          profile: "default"
        credential:
          name: cloud-credentials
          key: cloud
  snapshotLocations:
    - name: default
      velero:
        provider: aws
        config:
          region: us-west-2
          profile: "default"
```

DataProtectionApplication リソース を作成する例を参照してください。

- 復元操作を実行する前に、Ansible Automation Platform、Red Hat OpenShift Container Platform GitOps、または証明書マネージャーなどの他の Operator がインストールされていることを確認します。これにより、新しいハブクラスターが初期のハブクラスターと同じように設定されます。

- パッシブハブクラスターは、バックアップと復元 Operator、および前のハブクラスターで設定された他の Operator をインストールするときに、最初のハブクラスターと同じ namespace 名を使用する必要があります。

1.6.2. バックアップおよびリストア Operator の有効化

クラスターのバックアップおよび復元 Operator は、**MultiClusterHub** リソースの初回作成時に有効にできます。**cluster-backup** パラメーターは **true** に設定します。Operator を有効にすると、Operator リソースがインストールされます。

MultiClusterHub リソースがすでに作成されている場合には、**MultiClusterHub** リソースを編集して、クラスターバックアップ Operator をインストールまたはアンインストールできます。クラスターバックアップ Operator をアンインストールする場合は、**cluster-backup** を **false** に設定します。

バックアップおよび復元 Operator が有効にされている場合には、**MultiClusterHub** リソースは以下の YAML ファイルのようになります。

```
apiVersion: operator.open-cluster-management.io/v1
  kind: MultiClusterHub
  metadata:
    name: multiclusterhub
    namespace: open-cluster-management
  spec:
    availabilityConfig: High
    enableClusterBackup: false
    imagePullSecret: multiclusterhub-operator-pull-secret
    ingress:
      sslCiphers:
        - ECDHE-ECDSA-AES256-GCM-SHA384
        - ECDHE-RSA-AES256-GCM-SHA384
        - ECDHE-ECDSA-AES128-GCM-SHA256
        - ECDHE-RSA-AES128-GCM-SHA256
    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: true <<<<<<<<
          name: cluster-backup
    separateCertificateManagement: false
```

1.6.3. バックアップおよびリストア Operator の使用

バックアップをスケジュールおよび復元するには、以下の手順を実行します。

1. バックアップおよび復元 Operator **backupschedule.cluster.open-cluster-management.io** を使用してバックアップスケジュールを作成し、**restore.cluster.open-cluster-management.io** リソースを使用してバックアップを復元します。

2. 次のコマンドを実行して、**backupschedule.cluster.open-cluster-management.io** リソースを作成します。

```
kubectl create -f cluster_v1beta1_backupschedule.yaml
```

cluster_v1beta1_backupschedule.yaml リソースは、次のファイルのようになる場合があります。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: BackupSchedule
metadata:
  name: schedule-acm
  namespace: open-cluster-management-backup
spec:
  veleroSchedule: 0 */2 * * * # Create a backup every 2 hours
  veleroTtl: 120h # deletes scheduled backups after 120h; optional, if not specified, the
maximum default value set by velero is used - 720h
```

backupschedule.cluster.open-cluster-management.io spec プロパティーに関する以下の説明を確認してください。

- **veleroSchedule** は必須のプロパティーで、バックアップをスケジュールする cron ジョブを定義します。

- **veleroTtl** は任意のプロパティーで、スケジュールされているバックアップリソースの有効期限を定義します。指定されていない場合には、Velero で設定された最大デフォルト値 (**720h**) が使用されます。

3. **backupschedule.cluster.open-cluster-management.io** リソースの状態をチェックします。3 つの **schedule.velero.io** リソースの定義が表示されます。以下のコマンドを実行します。

```
oc get BackupSchedule -n open-cluster-management-backup
```

4. 注意: 復元操作は、復元シナリオ向けに別のハブクラスターで実行します。復元操作を開始するには、バックアップを復元するハブクラスターに **restore.cluster.open-cluster-management.io** リソースを作成します。
注意: 新しいハブクラスターにバックアップを復元する場合には、バックアップを作成した、前のバブクラスターがシャットダウンされていることを確認します。実行中の場合には、前のハブクラスターは、マネージドクラスターの調整機能により、マネージドクラスターが使用できなくなったことが検出されるとすぐに、マネージドクラスターの再インポートが試行されます。

   クラスターのバックアップおよび復元 Operator、backup **schedule.cluster.open-cluster-management.io** および **restore.cluster.open-cluster-management.io** リソースを使用して、バックアップまたは復元リソースを作成できます。**cluster-backup-operator** サンプル を参照してください。

5. 次のコマンドを実行して、**restore.cluster.open-cluster-management.io** リソースを作成します。

```
kubectl create -f cluster_v1beta1_backupschedule.yaml
```

リソースは以下のファイルのようになります。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm
  namespace: open-cluster-management-backup
spec:
  veleroManagedClustersBackupName: latest
  veleroCredentialsBackupName: latest
  veleroResourcesBackupName: latest
```

6. 以下のコマンドを実行して Velero **Restore** リソースを表示します。

```
oc get restore.velero.io -n open-cluster-management-backup
```

7. 次のコマンドを実行して、Red Hat Advanced Cluster Management **Restore** イベントを表示します。

```
oc describe restore.cluster.open-cluster-management.io -n open-cluster-management-backup
```

Restore YAML リソースのパラメーターとサンプルの説明については、Restoring a backup セクションを参照してください。

1.6.4. Extending backup data

cluster.open-cluster-management.io/backup ラベルをリソースに追加することで、クラスターのバックアップおよび復元を使用してサードパーティーのリソースをバックアップできます。ラベルの値は、空の文字列を含む任意の文字列にすることができます。バックアップするコンポーネントを識別するのに役立つ値を使用してください。たとえば、コンポーネントが IDP ソリューションによって提供される場合は、**cluster.open-cluster-management.io/backup: idp** ラベルを使用します。

注意: マネージドクラスターのアクティブ化リソースが復元されたときにリソースを復元する場合は、**cluster.open-cluster-management.io/backup** ラベルに **cluster-activation** 値を使用します。マネージドクラスターのアクティブ化リソースを復元すると、マネージドクラスターは、復元が開始されたハブクラスターによってアクティブに管理されます。

1.6.5. Scheduling a cluster backup

backupschedule.cluster.open-cluster-management.io リソースを作成すると、バックアップスケジュールが有効になります。以下の **backupschedule.cluster.open-cluster-management.io** サンプルを表示します。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: BackupSchedule
metadata:
  name: schedule-acm
  namespace: open-cluster-management-backup
```

```
spec:
  veleroSchedule: 0 */2 * * *
  veleroTtl: 120h
```

backupschedule.cluster.open-cluster-management.io リソースを作成したら、以下のコマンドを実行してスケジュールされたクラスターバックアップのステータスを取得します。

```
oc get BackupSchedule -n open-cluster-management-backup
```

1 つ前のコマンドの **<oadp-operator-ns>** パラメーターは、**BackupSchedule** が作成される namespace で、OADP Operator がインストールされている namespace と同じです。**backupschedule.cluster.open-cluster-management.io** リソースは、バックアップの生成に使用される **schedule.velero.io** リソースを 6 つ作成します。以下のコマンドを実行して、スケジュールされるバックアップの一覧を表示します。

```
os get schedules -A | grep acm
```

リソースは、以下のグループで個別にバックアップされます。

- **Credentials backup** は、Hive 認証情報、Red Hat Advanced Cluster Management、およびユーザー作成の認証情報と ConfigMap を保存するバックアップファイルです。
- **リソースバックアップ**: Red Hat Advanced Cluster Management リソースのバックアップと汎用リソース用のバックアップが含まれています。これらのリソースは、**cluster.open-cluster-management.io/backup** というラベルを使用します。
- **マネージドクラスターのバックアップ**。これには、バックアップが復元されるハブクラスターへのマネージドクラスター接続をアクティブにするリソースのみが含まれます。

注記: **リソースバックアップ** ファイルには、マネージドクラスター固有のリソースが含まれますが、マネージドクラスターをハブクラスターに接続するリソースのサブセットは含まれません。マネージドクラスターを接続するリソースは、アクティベーションリソースと呼ばれ、マネージドクラスターのバックアップに含まれます。新しいハブクラスターで **認証情報** および **リソース** のバックアップのみのバックアップを復元すると、新しいハブクラスターには、Hive API で作成されたすべてのマネージドクラスターが切り離された状態で表示されます。ただし、インポート操作を使用してプライマリーハブクラスターにインポートされたマネージドクラスターは、アクティベーションデータがパッシブハブクラスターに復元された場合にのみ表示されます。この時点で、マネージドクラスターは、バックアップファイルを作成した元のハブクラスターに引き続き接続されます。

アクティベーションデータが復元されると、Hive API を使用して作成されたマネージドクラスターのみが新しいハブクラスターに自動的に接続されます。他のすべてのマネージドクラスターは **保留** 状態で表示されるため、新しいクラスターに手動で再接続する必要があります。

1.6.6. バックアップの復元

一般的な復元のシナリオでは、バックアップが実行されるハブクラスターが利用できなくなり、バックアップデータを新しいハブクラスターに移動する必要があります。これには、新しいハブクラスターでクラスター復元操作を実行します。この場合、復元操作はバックアップが作成される場所とは異なるハブクラスターで実行します。

また、以前のスナップショットからのデータを復元できるように、バックアップデータを取得したハブクラスターでデータを復元するケースもあります。この場合、復元とバックアップ操作の両方が同じハブクラスターで実行されます。

ハブクラスターで **restore.cluster.open-cluster-management.io** リソースを作成した後に、**oc get**

restore -n open-cluster-management-backup のコマンドを実行して復元操作のステータスを取得できます。また、バックアップファイルに含まれるバックアップのリソースが作成されていることを確認できる必要があります。

注記: Restore passive resources セクションで説明されているように、**syncRestoreWithNewBackups** オプションを使用して **true** に設定しない限り、**restore.cluster.open-cluster-management.io** リソースは 1 回実行されます。復元操作の完了後に同じ復元操作を再度実行する場合は、同じ **spec** オプションで新しい **restore.cluster.open-cluster-management.io** リソースを作成する必要があります。

復元操作を使用して、バックアップ操作で作成される全バックアップタイプ 3 つを復元します。ただし、特定の種類のバックアップ (マネージドクラスターのみ、ユーザー資格情報のみ、またはハブクラスターリソースのみ) のみをインストールするように選択できます。

復元では、以下の 3 つの必要な **spec** プロパティーを定義します。ここでは、バックアップしたファイルのタイプに対して復元ロジックが定義されます。

- **veleroManagedClustersBackupName** は、マネージドクラスターのアクティベーションリソースの復元オプションを定義するのに使用されます。
- **veleroCredentialsBackupName** は、ユーザーの認証情報の復元オプションを定義するために使用されます。
- **veleroResourcesBackupName** は、ハブクラスターリソース (**Applications**、**Policy**、その他のハブクラスターリソース (マネージドクラスターパッシブデータなど)) の復元オプションを定義するのに使用されます。
  前述のプロパティーの有効な値は次のとおりです。
  - **latest**: このプロパティーは、このタイプのバックアップで使用可能な、最後のバックアップファイルを復元します。
  - **skip:** このプロパティーは、現在の復元操作でこのタイプのバックアップの復元は試行しません。
  - **<backup_name>**: このプロパティーは、名前で参照する指定のバックアップを復元します。

restore.cluster.open-cluster-management.io で作成された **restore.velero.io** リソースの名前は、**<restore.cluster.open-cluster-management.io name>-<velero-backup-resource-name>** のテンプレートルールを使用して生成されます。以下の説明を参照してください。

- **restore.cluster.open-cluster-management.io** は、復元を開始する現在の **restore.cluster.open-cluster-management.io** リソースの名前です。
- **Velero-backup-resource-name** は、データの復元に使用される Velero バックアップファイルの名前です。たとえば、**restore.cluster.open-cluster-management.io** リソース **restore-acm** は **restore.velero.io** 復元リソースを作成します。フォーマットについては、以下の例を参照してください。
  - **restore-acm-acm-managed-clusters-schedule-20210902205438** は、マネージドクラスターのアクティベーションデータのバックアップを復元するのに使用されます。このサンプルでは、リソースの復元に使用される **backup.velero.io** バックアップ名は **acm-managed-clusters-schedule-20210902205438** です。
  - **restore-acm-acm-credentials-schedule-20210902206789** は、認証情報バックアップの復元に使用されます。このサンプルでは、リソースの復元に使用される **backup.velero.io** バックアップ名は **acm-managed-clusters-schedule-20210902206789** です。

- **restore-acm-acm-resources-schedule-20210902201234** は、アプリケーション、ポリシー、およびマネージドクラスターパッシブデータバックアップなどの他のハブクラスターリソースを復元するのに使用されます。このサンプルでは、リソースの復元に使用される **backup.velero.io** バックアップ名は **acm-managed-clusters-schedule-20210902201234** です。

注記: skip がバックアップタイプに使用されている場合は、**restore.velero.io** は作成されません。

以下の YAML サンプルで、クラスターの **リストア** リソースを参照してください。この例では、利用可能な最新のバックアップファイルを使用して、3 つのタイプのバックアップファイルがすべて復元されています。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm
  namespace: open-cluster-management-backup
spec:
  veleroManagedClustersBackupName: latest
  veleroCredentialsBackupName: latest
  veleroResourcesBackupName: latest
```

注記 Hive API によって作成されたマネージドクラスターのみが、マネージドクラスターのバックアップからの **acm-managed-clusters** バックアップが別のハブクラスターに復元されるときに、新しいハブクラスターに自動的に接続されます。他のすべてのマネージドクラスターは **Pending Import** 状態のままであり、新しいハブクラスターにインポートし直す必要があります。詳細は、Restoring imported managed clusters (Technology Preview) を参照してください。

1.6.6.1. Preparing the new hub cluster

新しいハブクラスターで復元操作を実行する前に、ハブクラスターを手動で設定し、初期ハブクラスターと同じ Operator をインストールする必要があります。Red Hat Advanced Cluster Management Operator は、初期ハブクラスターと同じ namespace にインストールし、**DataProtectionApplication** リソースを作成してから、初期ハブクラスターがデータをバックアップしたのと同じストレージの場所に接続する必要があります。

MultiClusterEngine リソースへの変更を含め、Red Hat Advanced Cluster Management オペレーターによって作成された **MultiClusterHub** リソースの最初のハブクラスターと同じ設定を使用します。

たとえば、初期ハブクラスターに Ansible Automation Platform、Red Hat OpenShift GitOps、**cert-manager** などの他の Operator がインストールされている場合は、復元操作を実行する前にそれらをインストールする必要があります。これにより、新しいハブクラスターが初期のハブクラスターと同じ方法で設定されます。

1.6.6.2. 復元前のハブクラスターのクリーニング

Velero は現在、ハブクラスターの既存のバックアップリソースを省略します。これにより、新しいハブクラスターでハブクラスターデータを復元する時に使用可能なシナリオが制限されます。新しいハブクラスターが使用され、復元が複数回適用される場合は、復元が実行する前にデータがクリーンアップされない限り、ハブクラスターをパッシブ設定として使用することは推奨されません。新しいハブクラスターのデータは、復元されたリソースで利用可能なデータを反映していません。

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 は一連の手順を実行し、Velero 復元を開始する前にハブクラスターを消去して復元の準備を行います。

cleanup オプションは **cleanupBeforeRestore** プロパティーを使用して、クリーンアップするオブジェクトのサブセットを特定します。このクリーンアップには、以下の 3 つのオプションを設定できます。

- **None**: クリーンアップは必要なく、Velero の復元を開始するだけです。これは、新しいハブクラスターで使用されます。
- **CleanupRestored**: 以前の Red Hat Advanced Cluster Management の復元で作成されたすべてのリソースを消去します。このプロパティーは、**CleanupAll** プロパティーよりも影響範囲が少ないので、こちらを使用することが推奨されます。
- **CleanupAll**: 復元操作を実行してからリソースが作成されていなくても、Red Hat Advanced Cluster Management バックアップとして含まれている可能性のある、ハブクラスター上の全リソースを消去します。これは、ハブクラスターに追加のコンテンツが作成された場合にクリーンアップが必要となるため、使用されます。このオプションは、以前のバックアップではなく、ユーザーによって作成されたハブクラスター上のリソースを消去するため、このオプションは注意して使用してください。**CleanupRestored** オプションを使用し、ハブクラスターが災害シナリオのパッシブクラスターとして指定されている場合は、ハブクラスターのコンテンツを手動で更新しないことを強くお勧めします。最終的な選択肢として、**CleanupAll** オプションを使用するようにしてください。

注記:

- Velero は、復元されたバックアップにリソースがない場合に、velero 復元リソースのステータス **PartiallyFailed** を設定します。これは、対応するバックアップが空であるために作成された **restore.velero.io** リソースのいずれかによりリソースが復元されない場合には、**restore.cluster.open-cluster-management.io** リソースが **PartiallyFailed** ステータスになる可能性があることを意味します。
- **syncRestoreWithNewBackups:true** を使用して新規バックアップが利用可能な場合にパッシブデータの復元を継続しない限り、**restore.cluster.open-cluster-management.io** リソースは 1 回実行されます。この場合、同期サンプルで復元パッシブに従います。Restoring passive resources while checking for backups を参照してください。復元操作が完了し、同じハブクラスターで別の復元操作を実行する場合は、新しい **restore.cluster.open-cluster-management.io** リソースを作成する必要があります。
- 複数の **restore.cluster.open-cluster-management.io** リソースを作成できますが、いつでもアクティブにできるのは 1 つだけです。

1.6.6.3. Restoring passive resources while checking for backups

新しいバックアップが利用可能かどうかを引き続き確認し、それらを自動的に復元しながら、**restore-passive-sync** サンプルを使用してパッシブデータを復元します。新しいバックアップを自動的に復元するには、**syncRestoreWithNewBackups** パラメーターを **true** に設定する必要があります。また、最新のパッシブデータだけを復元する必要もあります。サンプルの例は、このセクションの最後にあります。

VeleroResourcesBackupName および **VeleroCredentialsBackupName** パラメーターを **latest** に設定し、**VeleroManagedClustersBackupName** パラメーターを省略して **スキップ** します。**VeleroManagedClustersBackupName** が **latest** に設定された直後に、マネージドクラスターは新しいハブクラスターでアクティベートされ、プライマリーハブクラスターになります。

アクティベートされたマネージドクラスターがプライマリーハブクラスターになると、復元リソースが **Finished** に設定され、**true** に設定されていても **syncRestoreWithNewBackups** は無視されます。

デフォルトでは、コントローラーは **syncRestoreWithNewBackups** が **true** に設定されると、30 分ごとに新規バックアップをチェックします。新しいバックアップが見つかった場合は、バックアップされたリソースを復元します。**restoreSyncInterval** パラメーターを更新してチェックの期間を変更できま

す。

たとえば、10 分ごとにバックアップをチェックする次のリソースを参照してください。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm-passive-sync
  namespace: open-cluster-management-backup
spec:
  syncRestoreWithNewBackups: true # restore again when new backups are available
  restoreSyncInterval: 10m # check for new backups every 10 minutes
  cleanupBeforeRestore: CleanupRestored
  veleroManagedClustersBackupName: skip
  veleroCredentialsBackupName: latest
  veleroResourcesBackupName: latest
```

1.6.6.4. Restoring passive resources

パッシブ設定でハブクラスターリソースを復元するには、**restore-acm-passive** サンプルを使用します。パッシブデータは、シークレット、ConfigMap、アプリケーション、ポリシー、およびすべてのマネージドクラスターカスタムリソースなどのバックアップデータで、マネージドクラスターとハブクラスター間の接続をアクティブ化しません。バックアップリソースは、認証情報のバックアップおよび復元リソースによりハブクラスターで復元されます。

以下のサンプルを参照してください。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm-passive
  namespace: open-cluster-management-backup
spec:
  cleanupBeforeRestore: CleanupRestored
  veleroManagedClustersBackupName: skip
  veleroCredentialsBackupName: latest
  veleroResourcesBackupName: latest
```

1.6.6.5. アクティベーションリソースの復元

ハブクラスターでクラスターを管理する場合は、**restore-acm-passive-activate** サンプルを使用します。この場合、パッシブリソースを使用するハブクラスターで他のデータがすでに復元されていることを前提とします。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm-passive-activate
  namespace: open-cluster-management-backup
spec:
  cleanupBeforeRestore: CleanupRestored
  veleroManagedClustersBackupName: latest
  veleroCredentialsBackupName: skip
  veleroResourcesBackupName: skip
```

パッシブリソースを復元した方法に応じて、アクティベーションリソースを復元するいくつかのオプションがあります。

- Restore passive resources while checking for backups to restore passive dataセクションに記載されているように、**restore-acm-passive-sync cluster.open-cluster-management.io** リソースを使用した場合は、このリソースで **veleroManagedClustersBackupName** の値を **latest** の値に更新します。その結果、マネージドクラスターリソースと **restore-acm-passive-sync** リソースが復元されます。

- パッシブリソースを 1 回限りの操作で復元した場合、またはリソースをまだ復元していない場合は、**Restoring all resources** セクションで指定されているように、すべてのリソースを復元することを選択します。

1.6.6.6. Restoring all resources

一度にすべてのデータを復元し、ハブクラスターがマネージドクラスターを 1 つのステップで管理するようにする場合は、**restore-acm** サンプルを使用します。ハブクラスターに **restore.cluster.open-cluster-management.io** リソースを作成したら、次のコマンドを実行して復元操作のステータスを取得します。

```
oc get restore -n open-cluster-management-backup
```

サンプルは、次のリソースに酷似している可能性があります。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm
  namespace: open-cluster-management-backup
spec:
  cleanupBeforeRestore: CleanupRestored
  veleroManagedClustersBackupName: latest
  veleroCredentialsBackupName: latest
  veleroResourcesBackupName: latest
```

ハブクラスターから、バックアップファイルに含まれるバックアップされたリソースが作成されていることを確認します。

1.6.6.7. Restoring imported managed clusters

Hive API を使用してプライマリーハブクラスターに接続されたマネージドクラスターのみが、アクティベーションデータが復元される新しいハブクラスターに自動的に接続されます。これらのクラスターは、**Clusters** タブの **Create cluster** ボタンを使用して、プライマリーハブクラスター上に作成されています。**Import cluster** ボタンを使用して最初のハブクラスターに接続されたマネージドクラスターは、アクティベーションデータが復元されると **Pending Import** として表示され、新しいハブクラスターにインポートし直す必要があります。

Hive がマネージドクラスター **kubeconfig** をハブクラスターのマネージドクラスター namespace に格納するため、Hive マネージドクラスターを新しいハブクラスターに接続できます。これは、新しいハブクラスターでバックアップおよび復元されます。次に、インポートコントローラーは、復元された設定を使用してマネージドクラスターのブートストラップ **kubeconfig** を更新します。これは、Hive API を使用して作成されたマネージドクラスターでのみ使用できます。インポートされたクラスターでは使用できません。

インポートされたクラスターを新しいハブクラスターに正常に接続するには、復元操作の開始後に

インポートされたクラスターを新しいハブクラスターに再接続するには、復元操作の開始後に **auto-import-secret** リソースを手動で作成します。詳細は、Importing the cluster with the auto import secret を参照してください。

Pending Import 状態のクラスターごとに、マネージドクラスターの namespace に **auto-import-secret** リソースを作成します。インポートコンポーネントが新しいハブクラスターで自動インポートを開始するのに十分な権限を持つ **kubeconfig** またはトークンを使用します。マネージドクラスターに接続するには、トークンを使用して各マネージドクラスターにアクセスできる必要があります。トークンには、**klusterlet** ロールバインディングまたは同じアクセス権限を持つロールが必要です。

1.6.6.8. 他の復元サンプルの使用

次の復元セクションを参照して、さまざまな種類のバックアップファイルを復元するための YAML の例を確認してください。

- 3 種類のバックアップリソースをすべて復元します。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm
  namespace: open-cluster-management-backup
spec:
  veleroManagedClustersBackupSchedule: latest
  veleroCredentialsBackupSchedule: latest
  veleroResourcesBackupSchedule: latest
```

- マネージドクラスターリソースのみを復元します。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm
  namespace: open-cluster-management-backup
spec:
  veleroManagedClustersBackupName: latest
  veleroCredentialsBackupName: skip
  veleroResourcesBackupName: skip
```

- **acm-managed-clusters-schedule-20210902205438** バックアップを使用して、マネージドクラスターのリソースのみを復元します。

```
apiVersion: cluster.open-cluster-management.io/v1beta1
kind: Restore
metadata:
  name: restore-acm
  namespace: open-cluster-management-backup
spec:
  veleroManagedClustersBackupName: acm-managed-clusters-schedule-20210902205438
  veleroCredentialsBackupName: skip
  veleroResourcesBackupName: skip
```

注記:

  - **restore.cluster.open-cluster-management.io** リソースは 1 回実行されます。復元操作が

完了したら、オプションで同じハブクラスターで別の復元操作を実行できます。新しい復元操作を実行するには、**restore.cluster.open-cluster-management.io** リソースを新規作成する必要があります。

- 複数の **restore.cluster.open-cluster-management.io** を作成できますが、同時に実行できるのは 1 つのみです。

1.6.6.9. 復元イベントの表示

以下のコマンドを使用して、復元イベントに関する情報を取得します。

```
oc describe -n <oadp-n> <restore-name>
```

イベント一覧は以下の例のようになります。

```
Spec:
  Cleanup Before Restore:             CleanupRestored
  Restore Sync Interval:              4m
  Sync Restore With New Backups:      true
  Velero Credentials Backup Name:     latest
  Velero Managed Clusters Backup Name:  skip
  Velero Resources Backup Name:       latest
Status:
  Last Message:                       Velero restores have run to completion, restore will continue to sync
with new backups
  Phase:                              Enabled
  Velero Credentials Restore Name:  example-acm-credentials-schedule-20220406171919
  Velero Resources Restore Name:    example-acm-resources-schedule-20220406171920
Events:
  Type    Reason                 Age   From              Message
  ----    ------                 ----  ----              -------
  Normal  Prepare to restore:    76m   Restore controller  Cleaning up resources for backup acm-
credentials-hive-schedule-20220406155817
  Normal  Prepare to restore:    76m   Restore controller  Cleaning up resources for backup acm-
credentials-cluster-schedule-20220406155817
  Normal  Prepare to restore:    76m   Restore controller  Cleaning up resources for backup acm-
credentials-schedule-20220406155817
  Normal  Prepare to restore:    76m   Restore controller  Cleaning up resources for backup acm-
resources-generic-schedule-20220406155817
  Normal  Prepare to restore:    76m   Restore controller  Cleaning up resources for backup acm-
resources-schedule-20220406155817
  Normal  Velero restore created:  74m   Restore controller  example-acm-credentials-schedule-
20220406155817
  Normal  Velero restore created:  74m   Restore controller  example-acm-resources-generic-
schedule-20220406155817
  Normal  Velero restore created:  74m   Restore controller  example-acm-resources-schedule-
20220406155817
  Normal  Velero restore created:  74m   Restore controller  example-acm-credentials-cluster-
schedule-20220406155817
  Normal  Velero restore created:  74m   Restore controller  example-acm-credentials-hive-schedule-
20220406155817
  Normal  Prepare to restore:    64m   Restore controller  Cleaning up resources for backup acm-
resources-schedule-20220406165328
  Normal  Prepare to restore:    62m   Restore controller  Cleaning up resources for backup acm-
credentials-hive-schedule-20220406165328
```

```
  Normal  Prepare to restore:     62m   Restore controller  Cleaning up resources for backup acm-credentials-cluster-schedule-20220406165328
  Normal  Prepare to restore:     62m   Restore controller  Cleaning up resources for backup acm-credentials-schedule-20220406165328
  Normal  Prepare to restore:     62m   Restore controller  Cleaning up resources for backup acm-resources-generic-schedule-20220406165328
  Normal  Velero restore created: 61m   Restore controller  example-acm-credentials-cluster-schedule-20220406165328
  Normal  Velero restore created: 61m   Restore controller  example-acm-credentials-schedule-20220406165328
  Normal  Velero restore created: 61m   Restore controller  example-acm-resources-generic-schedule-20220406165328
  Normal  Velero restore created: 61m   Restore controller  example-acm-resources-schedule-20220406165328
  Normal  Velero restore created: 61m   Restore controller  example-acm-credentials-hive-schedule-20220406165328
  Normal  Prepare to restore:     38m   Restore controller  Cleaning up resources for backup acm-resources-generic-schedule-20220406171920
  Normal  Prepare to restore:     38m   Restore controller  Cleaning up resources for backup acm-resources-schedule-20220406171920
  Normal  Prepare to restore:     36m   Restore controller  Cleaning up resources for backup acm-credentials-hive-schedule-20220406171919
  Normal  Prepare to restore:     36m   Restore controller  Cleaning up resources for backup acm-credentials-cluster-schedule-20220406171919
  Normal  Prepare to restore:     36m   Restore controller  Cleaning up resources for backup acm-credentials-schedule-20220406171919
  Normal  Velero restore created: 36m   Restore controller  example-acm-credentials-cluster-schedule-20220406171919
  Normal  Velero restore created: 36m   Restore controller  example-acm-credentials-schedule-20220406171919
  Normal  Velero restore created: 36m   Restore controller  example-acm-resources-generic-schedule-20220406171920
  Normal  Velero restore created: 36m   Restore controller  example-acm-resources-schedule-20220406171920
  Normal  Velero restore created: 36m   Restore controller  example-acm-credentials-hive-schedule-20220406171919
```

1.6.6.10. プライマリークラスターのシャットダウン

新しいハブクラスターにバックアップを復元する場合には、バックアップを作成した、前のバブクラスターがシャットダウンされていることを確認します。そのクラスターが実行中の場合には、前のハブクラスターは、マネージドクラスターの調整機能により、マネージドクラスターが使用できなくなったことが検出されると、マネージドクラスターの再インポートが試行されます。

1.6.7. バックアップまたは復元設定の検証

クラスターのバックアップおよび復元 Operator の Helm チャート (**cluster-backup-chart**) は、ハブクラスターに **backup-restore-enabled** ポリシーをインストールし m バックアップと復元のコンポーネントに関する問題について通知するために使用されます。**backup-restore-enabled** ポリシーには、以下の制約を確認するテンプレートセットが含まれます。

- **Pod の検証**
  以下のテンプレートは、Pod のステータスでバックアップコンポーネントおよび依存関係の有無を確認します。

- **acm-backup-pod-running** テンプレートは、バックアップおよび復元 Operator Pod が実行されているかどうかを確認します。
- **OADP-pod-running** テンプレートは、OADP Operator Pod が実行されているかどうかを確認します。
- **velero-pod-running** テンプレートは Velero Pod が実行されているかどうかを確認します。

- Data Protection Application の検証
  - **data-protection-application-available** テンプレートは、**DataProtectioApplicatio.oadp.openshift.io** リソースが作成されるかどうかを確認します。この OADP リソースは Velero 設定をセットアップします。

- **バックアップストレージの検証**
  - **backup-storage-location-available** テンプレートは、**BackupStorageLocation.velero.io** リソースが作成され、ステータス値が **Available** かどうかを確認します。これは、バックアップストレージへの接続が有効であることを意味します。

- BackupSchedule **競合検証**
  - **acm-backup-clusters-collision-report** テンプレートは、**BackupSchedule.cluster.open-cluster-management.io** が現在のハブクラスターに存在する場合に、ステータスが **BackupCollision** ではないことを検証します。これにより、バックアップデータをストレージの場所に書き込むときに、現在のハブクラスターが他のハブクラスターと競合していないことを確認できます。
    BackupCollision 状態の定義については、Backup Collisions セクションを参照してください。

- BackupSchedule **および復元ステータスの検証**
  - **acm-backup-phase-validation** テンプレートは、**BackupSchedule.cluster.open-cluster-management.io** が現在のクラスターに存在する場合に、ステータスが **Failed** でないこと、または **空** の状態であることを確認します。これにより、このクラスターがプライマリーハブクラスターであり、バックアップを生成している場合に **BackupSchedule.cluster.open-cluster-management.io** ステータスが正常であることが保証されます。
  - 同じテンプレートは、**Restore.cluster.open-cluster-management.io** が現在のクラスターに存在する場合に、ステータスが **失敗** でないこと、または **空** の状態にないことを確認します。これにより、このクラスターがセカンダリーハブクラスターであり、バックアップを復元する場合に、**Restore.cluster.open-cluster-management.io** のステータスが正常であることが保証されます。

- **バックアップの存在検証**
  - **acm-managed-clusters-schedule-backups-available** テンプレートは、**BackupStorageLocation.velero.io** で指定された場所で **Backup.velero.io** リソースが利用可能かどうかを確認し、バックアップが **BackupSchedule.cluster.open-cluster-management.io** リソースによって作成されるかどうかを確認します。これにより、バックアップが少なくとも 1 回実行され、バックアップと復元 Operator が検証されます。

- **完了するためのバックアップ**
  - **acm-backup-in-progress-report** テンプレートは、**Backup.velero.io** リソースが **InProgress** 状態で停止していないか確認します。この検証が追加されるのは、多数のリ

ソースがある場合、バックアップの実行中に velero Pod が再起動し、バックアップが完了せずに進行中のままになるためです。通常のバックアップ中、バックアップリソースは、実行中のどこかの時点で進行中になりますが、停止しているわけではなく、完了まで実行されます。スケジュールの実行中およびバックアップの進行中に **acm-backup-in-progress-report** テンプレートが警告を報告するのは正常です。

- **cron ジョブとしてアクティブに実行されるバックアップ**
  - **BackupSchedule.cluster.open-cluster-management.io** はアクティブに実行され、ストレージの場所に新しいバックアップを保存します。この検証は、**backup-schedule-cron-enabled** ポリシーテンプレートにより行われます。テンプレートは、ストレージの場所に **velero.io/schedule-name: acm-validation-policy-schedule** ラベルの付いた **Backup.velero.io** があることを確認します。
    acm-validation-policy-schedule バックアップは、バックアップ cron スケジュールの時刻が設定された後に期限切れになるように設定されています。バックアップを作成するために実行されている cron ジョブがない場合には、古い **acm-validation-policy-schedule** バックアップは期限切れになり、新しいバックアップが作成されないので削除されます。したがって、現在 **acm-validation-policy-schedule backups** が存在しない場合には、アクティブな cron ジョブがバックアップを生成することはありません。

    このポリシーは、ハブクラスターがアクティブで、バックアップを作成または復元するときに、バックアップの問題をハブクラスター管理者に通知することを目的としています。

1.6.8. サーバー側の暗号化を使用したデータの保護

サーバー側の暗号化は、保存場所でデータを受信するアプリケーションまたはサービスのデータ暗号化です。バックアップメカニズム自体は、転送中 (バックアップストレージの場所との間を移動するとき) または保存中 (バックアップストレージの場所のディスクに保存されている間) にデータを暗号化しません。代わりに、オブジェクトおよびスナップショットシステムのネイティブメカニズムに依存しています。

ベストプラクティス: 使用可能なバックアップストレージのサーバー側の暗号化を使用して、宛先でデータを暗号化します。バックアップには、認証情報や設定ファイルなど、ハブクラスターの外部に保存するときに暗号化する必要があるリソースが含まれています。

serverSideEncryption パラメーターおよび **kmsKeyId** パラメーターを使用して、Amazon S3 に保存されているバックアップの暗号化を有効にすることができます。詳細は、バックアップストレージの場所 YAML を参照してください。次のサンプルは、**DataProtectionApplication** リソースを設定するときに AWS KMS キー ID を指定します。

```
spec:
  backupLocations:
    - velero:
        config:
          kmsKeyId: 502b409c-4da1-419f-a16e-eif453b3i49f
          profile: default
          region: us-east-1
```

他のストレージプロバイダーの設定可能なすべてのパラメーターについては、Velero がサポートするストレージプロバイダー を参照してください。