Commvault

Protecting VMs on Red Hat OpenShift Virtualization Using Kubernetes

Commvault

Table of Contents

Commvault

Protecting VMs on Red Hat Openshift Virtualization Using Commvault Kubernetes

You can back up and restore virtual machines (VMs) running on the Red Hat OpenShift Virtualization platform using the Commvault Kubernetes solution. This enables you to easily discover, protect, and recover VMs alongside containerized applications within your Kubernetes cluster, thereby minimizing downtime and eliminating additional costs associated with protecting VMs.

Note: This feature is part of the Commvault Early Adopter program. The Commvault Early Adopter program was created to engage customer feedback on specific features. Commvault works with select customers to discuss, plan, and help deploy the feature release, and to proactively assist with any issues. If you are interested in becoming part of the Commvault Early Adopter program, please contact us at earlyadopter@commvault.com.

Procedure

1. Creating an Application Group
2. Backing Up Cluster, Applications and Virtual Machines
3. Restoring Workloads or Restoring Virtual Machines
4. Excluding Workloads and Virtual Machines from Back Up

Creating an Application Group

To protect VMs deployed in the Red Hat OpenShift cluster, you must configure an application group in Commvault. An application group is a set of data that you want to protect. For Kubernetes, the data is the Kubernetes applications, namespaces, namespaced objects, non-namespaced objects, virtual machines and persistent volume data that you want to protect.

Go to the Add Application Group Wizard

1. From the Command Center navigation pane, go to **Protect** > **Kubernetes**.

   The **Overview** page appears.
2. Go to the **Application groups** tab.
3. In the upper-right area of the page, click **Add application group**.

   The **Select Cluster** page of the configuration wizard appears.

Select the Cluster and Backup Plan

1. From the Cluster list, select the cluster to create the application group for.
2. Click **Next**.

   The **Plan** page of the configuration wizard appears.
3. Select the backup plan to back up the cluster and workloads.

   If you don't already have a backup plan that you can use, to create one, click the add button +.

4. Click **Next**.

   The **Add Application Group** page appears.

5. In the **Application group name** box, enter a descriptive name for the application group.

Select the Resources to Back Up

You can select resources to back up by workload type or by label.

Select the Resources to Back Up by Workloads

When you select by workload, you can select the cluster, namespaces, Pods, DaemonSets, and other resources.

1. Click **Add**, and then select **Workloads**.

   The **Add Kubernetes workloads** dialog box appears.

2. From the **Browse** list, select the option that displays the resources or objects that you want to select:
   - **All workloads**: Displays the cluster, each namespace, and Pods, DaemonSets, Deployments, StatefulSets, Helm-deployed applications, and virtual machines within the namespace.

     Note: To protect the entire cluster, select *only* the cluster.
   - **Virtual machines**: Displays the cluster, each namespace, and virtual machines within the namespace.
   - **Volumes**: Displays the cluster, each namespace, and any PersistentVolumeClaims (PVCs) within the namespace. If a namespace does not contain any PersistentVolumeClaim (PVC) objects, the namespace is displayed as empty. PersistentVolume (PV) objects that do not have an associated PersistentVolumeClaim (PVC) are not displayed.
3. Select the resources to back up.
4. Click **Done**.

Select the Resources to Back Up by Label

When you select by label, you can specify labels and values to select resources/objects that have those labels and values.

1. Click **Add**, and then select **Label selectors**.

   The **Add label selector** dialog box appears.

2. From the **Type** list, select **Application**, **Namespaces**, or **Volumes**.
3. For **Value**, enter the label value.

   For example:
   - To select resources in the default namespace, enter **enable.backup=true**. You can also enter multiple labels as a comma-separated list like **enable.backup=true,env=prod**.
   - To select resources in all namespaces, enter **enable.backup=true --all-namespaces** or **enable.backup=true,env=prod --all-namespaces**.

- To select resources in a specific namespace, enter **enable.backup=true -n** namespace_name or **enable.backup=true,env=prod -n** namespace_name.

  Note: Commvault does not support the following for label selectors:

  - Using -A as the short form of --all-namespaces. You must use --all-namespaces.
  - Using the --namespace parameter as the long form of -n. You must use -n.

Exclude the Resources from Backup

You can exclude Kubernetes workloads or resources from an application group so that they are not backed up.

For more information, see Excluding Workloads and Virtual Machines from Back Up.

Create the Application Group

1. Click **Submit**.

   The application group properties page appears.

2. To run an on-demand backup of the application group, in the upper-right area of the page, click **Back up**.

Backing Up Kubernetes Cluster, Applications and Virtual Machines

You can perform an on-demand backup for a Kubernetes cluster, application, virtual machine or PersistentVolumeClaim.

Procedure

1. From the Command Center navigation pane, go to **Protect** > **Kubernetes**.

   The **Overview** page appears.

2. Follow the steps for the entity that you want to back up:

   - Cluster: On the **Clusters** tab, in the row for the cluster, click the action button, and then select **Backup**.
   - Application: On the **Applications** tab, in the row for the application, click the action button, and then select **Backup**.
   - Virtual machine: On the **Applications** tab, in the row for the virtual machine, click the action button, and then select **Backup**.
   - Application group: On the **Application groups** tab, in the row for the application group, click the action button, and then select **Backup**.

   The **Backup options** dialog box appears.

3. In the **Backup type** field, leave **Incremental** selected.

   If no full backup exists, Commvault automatically performs a full backup.

4. Click **Submit**.

Restoring Kubernetes Workloads

You can restore Kubernetes applications—which are supported API resources/objects (such as Secrets, ConfigMaps, Namespaces, and StorageClasses) that can be listed, created, or re-created using the Kubernetes API server—in place to the original cluster or out of place to a different cluster, distribution, and StorageClass. You can also restore VMs in the Kubernetes cluster to the original cluster or out of place to a different cluster.

By default, Kubernetes applications and VMs are restored to the original cluster, using the same access node used during the backup.

In Place Restore

Go to the Restore Wizard

1. From the Command Center navigation pane, go to **Protect** > **Kubernetes**.

   The **Overview** page appears.

2. On the **Application groups** tab, in the row for the application group that you want to restore, click the action button  , and then click **Restore**.

   The **Select restore type** page appears.

3. Click **Full workload**.

   The **Restore** page appears.

4. Select the applications and VMs to restore.

5. To select a specific backup copy to restore from, do the following:

   By default, Commvault restores content from the first available, valid backup copy that it finds.

   a. In the upper-right corner of the page, click **Change source**.

      The **Change source** dialog box appears.

   b. From the **MediaAgent** list, select the access node that contains the backup copy.

   c. From the **Source** list, select the backup copy.

   d. Click **OK**.

6. Click **Restore**.

   The **Destination** page of the configuration wizard appears.

Destination

1. For **Type**, select **In place**.

2. From the **Access node** list, select the access node to perform the restore.

   For optimal performance, select an access node that has low latency to the Kubernetes cluster and the backup copy.

3. Click **Next**.

   The **Applications** page of the configuration wizard appears.

Applications

1. Review the applications and VMs to restore.
2. Click **Next**.

   The **Restore Options** page of the configuration wizard appears.

Restore Options

1. To delete and overwrite existing data, move the **Unconditionally overwrite if it already exists** toggle key to the right, and then click **Yes** in the confirmation dialog box.

   If any data matching the restore data exists in the destination, Commvault deletes the existing data before starting the restore process.
2. To use resource modifiers to add, delete, and modify fields in the Kubernetes resource YAMLs that you restore, under **Additional options**, do the following:
   - To use an existing resource modifier, from the **Select modifiers** list, select the resource modifier.

     Note: For in-place restore, modifier from the source cluster will be used.
   - To specify a new resource modifier or to change an existing modifier, click **Edit Modifiers**.
3. Click **Next**.

   The **Summary** page of the configuration wizard appears.

Summary

1. Review the selected workloads and restore options.
2. Click **Submit**.

Out of Place Restore

Go to the Restore Wizard

1. From the Command Center navigation pane, go to **Protect** > **Kubernetes**.

   The **Overview** page appears.
2. On the **Application groups** tab, in the row for the application group that you want to restore, click the action button  , and then click **Restore**.

   The **Select restore type** page appears.
3. Click **Full workload**.

   The **Restore** page appears.
4. Select the applications and VMs to restore.
5. To select a specific backup copy to restore from, do the following:

   By default, Commvault restores content from the first available, valid backup copy that it finds.

   a. In the upper-right corner of the page, click **Change source**.

The **Change source** dialog box appears.

b. From the **MediaAgent** list, select the access node that contains the backup copy.

c. From the **Source** list, select the backup copy.

d. Click **OK**.

6. Click **Restore**.

   The **Destination** page of the configuration wizard appears.

Destination

1. For **Type**, select **Out of place**.
2. For **Destination cluster**, select the cluster to restore the content to.

   You can select any Kubernetes cluster that is added to Commvault.
3. From the **Access node** list, select the access node to perform the restore.

   For optimal performance, select an access node that has low latency to the Kubernetes cluster and the backup copy.
4. Click **Next**.

   The **Applications** page of the configuration wizard appears.

Applications

1. To modify the application, select the check box next to the application or VM and then click **Configure restore options**.
2. Select the namespace to restore the application to:
   - To restore to an existing namespace, from the **Namespace** list, select the namespace.
   - To create a namespace, click the **Add** option, and then enter a name for the namespace.
3. From the **Storage class** list, select the StorageClass to provision PersistentVolumes from.

   If you intend to back up the restored application with Commvault, select a StorageClass that has a CSI provisioner, an attacher, and a snapshotter.
4. Click **Save**.
5. In the **Change display name to** box, enter a name for the restored application.
6. To configure restore exclusions, click **Exclude resources**.

   The **Restore exclusions** window appears.
7. From **Filter** list, select an existing restore filter from either the source or destination cluster or click **+** to add a new filter.

   If you add a new resource filter during restore operation, then it is added to the cv-config namespace.

   Note: Commvault needs the cv-config namespace and a custom CRD cvresourcefilters.k8s.cv.io to be present on the cluster. If the namespace and CRD are not present, when you create your resource filter, the software

automatically creates a new namespace called cv-config and deploys a new CustomResourceDefinition (CRD) to your cluster.

8. In the **Exclusions** area, from the **Exclude** list, select **Exclude by rule**.

   The **Add rule** dialog box appears.

9. From the list, select **Kind**, **Group**, **Version**, **Namespace**, **Name**, and then specify the rule.
10. Click **Save**.
11. To exclude the application-related API resources, move the **Exclude sub-resources** toggle key to the right.

    The **Exclude sub-resources** area appears.

12. From the **Exclude** list, select **Exclude by Rule**

    The **Add rule** dialog box appears.

13. From the list, select **Kind**, **Group**, **Version**, **Namespace**, **Name**, and then specify the rule.
14. Click **Save**.
15. Click **Save**.
16. Click **Next**.

    The **Restore Options** page of the configuration wizard appears.

Restore Options

1. To delete and overwrite existing data, move the **Unconditionally overwrite if it already exists** toggle key to the right, and then click **Yes** in the confirmation dialog box.

   If any data matching the restore data exists in the destination, Commvault deletes the existing data before starting the restore process.

2. To use resource modifiers to add, delete, and modify fields in the Kubernetes resource YAMLs that you restore, under **Additional options**, do the following:
   - To use an existing resource modifier from either the source or destination cluster, select the resource modifier.
   - To specify a new resource modifier or to change an existing modifier, click **Edit Modifiers**.
3. Click **Next**.

   The **Summary** page of the configuration wizard appears.

Summary

1. Review the selected workloads and restore options.
2. Click **Submit**.

Restoring Kubernetes Virtual Machines

You can restore VMs, including VM configurations in the Kubernetes cluster to the original cluster or out of place to a different cluster for application migration or disaster recovery. By default, Kubernetes VMs are restored to the original cluster, using the same access node used during the backup.

In Place Restore

Go to the Restore Wizard

1. From the Command Center navigation pane, go to **Protect** > **Kubernetes**.

   The **Overview** page appears.

2. On the **Application groups** tab, in the row for the application group that you want to restore, click the action button  , and then click **Restore**.

   The **Select restore type** page appears.

3. Click **Full VM restore**.

   The **Restore** page appears.

4. Select the VMs to restore.

5. To select a specific backup copy to restore from, do the following:

   By default, Commvault restores content from the first available, valid backup copy that it finds.

   a. In the upper-right corner of the page, click **Change source**.

      The **Settings** dialog box appears.

   b. From the **MediaAgent** list, select the access node that contains the backup copy.

   c. From the **Source** list, select the backup copy.

   d. Click **OK**.

6. Click **Restore**.

   The **Destination** page of the configuration wizard appears.

Destination

1. For **Type**, select **In place**.

2. From the **Access node** list, select the access node to perform the restore.

   For optimal performance, select an access node that has low latency to the Kubernetes cluster and the backup copy.

3. Click **Next**.

   The **Applications** page of the configuration wizard appears.

Applications

1. Review the VMs to restore.
2. Click **Next**.

   The **Restore Options** page of the configuration wizard appears.

Restore Options

1. To automatically start the VM after the restore is complete, select **Power on VMs after restore**.
   - During the restore, the VM is briefly powered on, regardless of the value of this setting. This brief powering on of the VM is a necessary part of the restore process and cannot be changed.
   - The power state of the VM does not affect subsequent backups.
2. To delete and overwrite existing data, move the **Unconditionally overwrite if it already exists** toggle key to the right, and then click **Yes** in the confirmation dialog box.

   If any data matching the restore data exists in the destination, Commvault deletes the existing data before starting the restore process.
3. To use resource modifiers to add, delete, and modify fields in the Kubernetes resource YAMLs that you restore, under **Additional options**, do the following:
   - To use an existing resource modifier, from the **Select modifiers** list, select the resource modifier.

     Note: For in-place restore, modifier from the source cluster will be used.
   - To specify a new resource modifier or to change an existing modifier, click **Edit Modifiers**.
4. Click **Next**.

   The **Summary** page of the configuration wizard appears.

Summary

1. Review the selected VMs and restore options.
2. Click **Submit**.

Out of Place Restore

Go to the Restore Wizard

1. From the Command Center navigation pane, go to **Protect** > **Kubernetes**.

   The **Overview** page appears.
2. On the **Application groups** tab, in the row for the application group that you want to restore, click the action button  , and then click **Restore**.

   The **Select restore type** page appears.
3. Click **Full VM restore**.

   The **Restore** page appears.

4. Select the VMs to restore.
5. To select a specific backup copy to restore from, do the following:

   By default, Commvault restores content from the first available, valid backup copy that it finds.

   a. In the upper-right corner of the page, click **Change source**.

      The **Change source** dialog box appears.

   b. From the **MediaAgent** list, select the access node that contains the backup copy.

   c. From the **Source** list, select the backup copy.

   d. Click **Save**.
6. Click **Restore**.

   The **Destination** page of the configuration wizard appears.

Destination

1. For **Type**, select **Out of place**.
2. For **Destination cluster**, select the cluster to restore the content to.

   You can select any Kubernetes cluster that is added to Commvault.
3. From the **Access node** list, select the access node to perform the restore.

   For optimal performance, select an access node that has low latency to the Kubernetes cluster and the backup copy.
4. Click **Next**.

   The **Applications** page of the configuration wizard appears.

Applications

1. To modify the VM, select the check box next to the VM and then click **Configure restore options**.
2. Select the namespace to restore the application to:
   - To restore to an existing namespace, from the **Namespace** list, select the namespace.
   - To create a namespace, click the **Add** option, and then enter a name for the namespace.
3. From the **Storage class** list, select the StorageClass to provision PersistentVolumes from.

   If you intend to back up the restored application with Commvault, select a StorageClass that has a CSI provisioner, an attacher, and a snapshotter.
4. From the **Instance type** list, choose a pre-defined configuration of CPU and memory for the restored VM. To customize the resources manually, select **CPU and memory** and then specify the desired number of **CPU cores** and **Memory size**.
5. Specify the **Hostname** for the restored VM.
6. Click **Save**.
7. In the **Change display name to** box, enter a name for the restored application.

8. To configure restore exclusions, click **Exclude resources**.

   The **Restore exclusions** window appears.

9. From **Filter** list, select an existing restore filter from either the source or destination cluster or click **+** to add a new filter.

   If you add a new resource filter during restore operation, then it is added to the cv-config namespace.

   Note: Commvault needs the cv-config namespace and a custom CRD cvresourcefilters.k8s.cv.io to be present on the cluster. If the namespace and CRD are not present, when you create your resource filter, the software automatically creates a new namespace called cv-config and deploys a new CustomResourceDefinition (CRD) to your cluster.

10. In the **Exclusions** area, from the **Exclude** list, select **Exclude by rule**.

    The **Add rule** dialog box appears.

11. From the list, select **Kind**, **Group**, **Version**, **Namespace**, **Name**, and then specify the rule.
12. Click **Save**.
13. To exclude the application-related API resources, move the **Exclude sub-resources** toggle key to the right.

    The **Exclude sub-resources** area appears.

14. From the **Exclude** list, select **Exclude by Rule**

    The **Add rule** dialog box appears.

15. From the list, select **Kind**, **Group**, **Version**, **Namespace**, **Name**, and then specify the rule.
16. Click **Save**.
17. Click **Save**.
18. Click **Next**.

    The **Restore Options** page of the configuration wizard appears.

Restore Options

1. To automatically start the VM after the restore is complete, select **Power on VMs after restore**.
   - During the restore, the VM is briefly powered on, regardless of the value of this setting. This brief powering on of the VM is a necessary part of the restore process and cannot be changed.
   - The power state of the VM does not affect subsequent backups.
2. To delete and overwrite existing data, move the **Unconditionally overwrite if it already exists** toggle key to the right, and then click **Yes** in the confirmation dialog box.

   If any data matching the restore data exists in the destination, Commvault deletes the existing data before starting the restore process.

3. To use resource modifiers to add, delete, and modify fields in the Kubernetes resource YAMLs that you restore, under **Additional options**, do the following:

- To use an existing resource modifier from either the source or destination cluster, select the resource modifier.
- To specify a new resource modifier or to change an existing modifier, click **Edit Modifiers**.

4. Click **Next**.

   The **Summary** page of the configuration wizard appears.

Summary

1. Review the selected VMs and restore options.
2. Click **Submit**.

Excluding Workloads and Virtual Machines from Back Up

You can exclude Kubernetes workloads (virtual machines and applications) or resources from an application group so that they are not backed up.

Excluding workloads is particularly useful when you use namespace-centric protection to back up the entire cluster. With namespace-centric protection, you can exclude applications and virtual machines that do not require protection, while still ensuring that new workloads are discovered and protected.

Important: If you exclude a workload that is specifically selected or is the only content selected to back up, then the workload is still backed up. If you add content as namespace or label selector and exclude a single or multiple workloads, then the workload is excluded from back up.

Go to the Application Group

1. From the Command Center navigation pane, go to **Protect** > **Kubernetes**.

   The **Overview** page appears.

2. On the **Application groups** tab, click the application group.

   The application group properties page appears.

Exclude Resources by Application

When you select by application, you can exclude the namespaces, Pods, DaemonSets, and other resources in the cluster.

1. On the **Content** tab, in the **Content** section, click the edit button .

   The **Manage content** dialog box appears.

2. Move the **Exclude resources** toggle key to the right.

   The **Exclusions** area appears.

3. From the **Exclude** list, select **Applications**.

   The **Add exclusions** dialog box appears.

4. From the **Browse** list, select the option that displays the resources/objects that you want to select:

- **All workloads**: Displays the cluster, each namespace, and Pods, DaemonSets, Deployments, StatefulSets, Helm-deployed applications, and virtual machines within the namespace.
- **Virtual machines**: Displays the cluster, each namespace, and virtual machines within the namespace.
- **Volumes**: Displays the cluster, each namespace, and any PersistentVolumeClaims (PVCs) within the namespace.

If a namespace does not contain any PersistentVolumeClaim (PVC) objects, the namespace is displayed as empty.

PersistentVolume (PV) objects that do not have an associated PersistentVolumeClaim (PVC) are not displayed.

5. Select the resources to exclude from backup.
6. Click **Done**.

Exclude Resources by Label

When you select by label, you can select labels and values to exclude resources/objects that have those labels and values.

1. On the **Content** tab, in the **Content** section, click the edit button .

   The **Manage content** dialog box appears.
2. Move the **Exclude resources** toggle key to the right.

   The **Exclusions** area appears.
3. From the **Exclude** list, select **Label selectors**.

   The **Add label selector** dialog box appears.
4. From the **Type** list, select **Application**, **Namespaces**, or **Volumes**.
5. For **Value**, enter the label value. Supported format is key=value [-n <namespace> | --all-namespaces]. For example, usage=prod -n dev.
6. Click **Add**.

Exclude Resources by Rule

You can exclude Kubernetes resources from backups by configuring rule(s) based on the resource **Kind**, **Group**, **Version**, **Namespace**, **Name**, and **Label**. Applications such as Pod, Deployment, StatefulSet can be excluded from backups.

Note: Applications deployed via Helm charts cannot be excluded from backups.

1. On the **Content** tab, in the **Content** section, click the edit button .

   The **Manage content** dialog box appears.
2. Move the **Exclude resources** toggle key to the right.

   The **Exclusions** area appears.
3. From the **Exclude** list, select **Exclude by Rule**.

The **Add rule** dialog box appears.

4. From the list, select **Kind**, **Group**, **Version**, **Namespace**, **Name**, or **Label**, and then specify the rule.
5. Click **Save**.

Exclude Sub-Resources by Rule

You can exclude sub-resources of applications from backup such as ConfigMaps, Secrets, Services, PersistentVolumeClaims, etc.

Note: Sub-resources associated with applications deployed via Helm charts cannot be excluded from backups.

1. On the **Content** tab, in the **Content** section, click the edit button  .

   The **Manage content** dialog box appears.
2. Move the **Exclude sub-resources** toggle key to the right.

   The **Exclude sub-resources** area appears.
3. From the **Exclude** list, select **Exclude by Rule**

   The **Add rule** dialog box appears.
4. From the list, select **Kind**, **Group**, **Version**, **Namespace**, **Name**, or **Label**, and then specify the rule.
5. Click **Save**.

Exclude PVCs

You can exclude workload PVCs from back up.

1. On the **Content** tab, in the **Content** section, click the edit button  .

   The **Manage content** dialog box appears.
2. Move the **Exclude PVCs** toggle key to the right.

   The **Exclude PVCs** area appears.
3. To select a PVC manually, click **Browse**.

   In the **Browse workload PVCs** dialog box, select the PVC and click **OK**.
4. To add a filter, click **Add**.

   In the **Add PVC filter** dialog box, enter the **PVC name or pattern** and click **OK**.
5. Click **Save**.