Create a lifecycle policy

Use the following procedure to create a lifecycle policy.

To create a lifecycle policy

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Elastic Block Store**, **Lifecycle Manager**, then choose **Create snapshot lifecycle policy**.
3. Provide the following information for your policy as needed:

- **Description**–A description of the policy.
- **Resource type**–The type of resource to back up. Use `Volume` to create snapshots of individual volumes or use `Instance` to create multi-volume snapshots from the volumes for an instance.
- **Target with these tags**–The resource tags that identify the volumes or instances to back up.
- **Lifecycle policy tags**–The tags for the lifecycle policy.
- **Schedule name**–A name for the schedule.
- **Frequency**–The interval between policy runs. You can configure policy runs on a daily, weekly, monthly, or yearly schedule. Alternatively, choose **Custom cron expression** to specify an interval of up to 1 year. For more information, see Cron expressions in the *Amazon CloudWatch Events User Guide*.
- **Starting at** *hh*:*mm* **UTC**–The time at which the policy runs are scheduled to start. The first policy run starts within an hour after the scheduled time.
- **Retention type**–You can retain snapshots based on either the total count of snapshots or the age of each snapshot. For retention based on the count, the range is 1 to 1000. After the maximum count is reached, the oldest snapshot is deleted when a new one is created. For age-based retention, the range is 1 day to 100 years. After the retention period of each snapshot expires, it is deleted. The retention period should be greater than or equal to the creation interval.
- **Tagging information**–Choose whether to copy all user-defined tags on a source volume to the snapshots created by this policy. You can also specify additional tags for the snapshots in addition to the tags applied by Amazon Data Lifecycle Manager. If the resource type is `INSTANCE`, you can choose to automatically tag your snapshots with the following variable tags: `instance-id` and `timestamp`. The values of the variable tags are determined when the tags are added.
- **Fast snapshot restore**–Choose whether to enable fast snapshot restore for all snapshots created by this policy. If you enable fast snapshot restore, you must choose the Availability Zones in which to enable it. You are billed for each minute that fast snapshot restore is enabled for a

snapshot in a particular Availability Zone. Charges are pro-rated with a minimum of one hour. You can also specify the maximum number of snapshots that can be enabled for fast snapshot restore.

- **Enable cross Region copy**–You can copy each snapshot to up at three additional Regions. You must ensure that you do not exceed the number of concurrent snapshot copies per Region. For each Region, you can choose different retention policies and whether to copy all tags or no tags. If the source snapshot is encrypted or if encryption by default is enabled, the snapshots copies are encrypted. If the source snapshot is unencrypted, you can enable encryption. If you do not specify a CMK, the snapshots are encrypted using the default key for EBS encryption in each destination Region. If you specify a CMK for the destination Region, you must have access to the CMK.

- **IAM role**–An IAM role that has permissions to create, delete, and describe snapshots, and to describe volumes. AWS provides a default role, **AWSDataLifecycleManagerDefaultRole**, or you can create a custom IAM role.

- **Policy status after creation**–Choose **Enable policy** to start the policy runs at the next scheduled time or **Disable policy** to prevent the policy from running.

4. Choose **Create Policy**.

View a lifecycle policy

Use the following procedure to view a lifecycle policy.

To view a lifecycle policy

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Elastic Block Store**, **Lifecycle Manager**.
3. Select a lifecycle policy from the list. The **Details** tab displays information about the policy.

Modify a lifecycle policy

Use the following procedure to modify a lifecycle policy.

To modify a lifecycle policy

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Elastic Block Store**, **Lifecycle Manager**.
3. Select a lifecycle policy from the list.
4. Choose **Actions**, **Modify Snapshot Lifecycle Policy**.

5. Modify the policy settings as needed. For example, you can modify the schedule, add or remove tags, or enable or disable the policy.
6. Choose **Update policy**.

Delete a lifecycle policy

Use the following procedure to delete a lifecycle policy.

To delete a lifecycle policy

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Elastic Block Store**, **Lifecycle Manager**.
3. Select a lifecycle policy from the list.
4. Choose **Actions**, **Delete Snapshot Lifecycle Policy**.
5. When prompted for confirmation, choose **Delete Snapshot Lifecycle Policy**.

Manage backups using the AWS CLI

The following examples show how to use Amazon Data Lifecycle Manager to manage the backups of your EBS volumes using the AWS CLI.

Examples

- Create a lifecycle policy
- Display a lifecycle policy
- Modify a lifecycle policy
- Delete a lifecycle policy

Create a lifecycle policy

Use the create-lifecycle-policy command to create a lifecycle policy. To simplify the syntax, the example uses a JSON file, `policyDetails.json`, that includes the policy details.

This example uses a resource type of `VOLUME` to create snapshots of all volumes with the specified target tags. To create snapshots of all volumes for all instances with the specified target tags, use a resource type of `INSTANCE` instead.

```
aws dlm create-lifecycle-policy --description "My volume policy" --state
ENABLED --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole --policy-
details file://policyDetails.json
```

The following is an example of the `policyDetails.json` file.

```
{
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [
        {
            "Key": "costcenter",
            "Value": "115"
        }
    ],
    "Schedules":[
        {
            "Name": "DailySnapshots",
            "TagsToAdd": [
                {
                    "Key": "type",
                    "Value": "myDailySnapshot"
                }
            ],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "03:00"
                ]
            },
            "RetainRule": {
                "Count": 5
            },
```

```
        "CopyTags": false
      }
   ]
}
```

Upon success, the command returns the ID of the newly created policy. The following is example output.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Display a lifecycle policy

Use the get-lifecycle-policy command to display information about a lifecycle policy.

```
aws dlm get-lifecycle-policy --policy-id policy-0123456789abcdef0
```

The following is example output. It includes the information that you specified, plus metadata inserted by AWS.

```
{
   "Policy":{
      "Description": "My first policy",
      "DateCreated": "2018-05-15T00:16:21+0000",
      "State": "ENABLED",
      "ExecutionRoleArn":
"arn:aws:iam::210774411744:role/AWSDataLifecycleManagerDefaultRole",
      "PolicyId": "policy-0123456789abcdef0",
      "DateModified": "2018-05-15T00:16:22+0000",
      "PolicyDetails": {
         "PolicyType":"EBS_SNAPSHOT_MANAGEMENT",
          "ResourceTypes": [
              "VOLUME"
          ],
          "TargetTags": [
              {
```

```json
            "Value": "115",
            "Key": "costcenter"
        }
      ],
      "Schedules": [
        {
          "TagsToAdd": [
            {
              "Value": "myDailySnapshot",
              "Key": "type"
            }
          ],
          "RetainRule": {
            "Count": 5
          },
          "CopyTags": false,
          "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
              "03:00"
            ]
          },
          "Name": "DailySnapshots"
        }
      ]
    }
  }
}
```

Modify a lifecycle policy

Use the update-lifecycle-policy command to modify the information in a lifecycle policy. To simplify the syntax, this example references a JSON file, `policyDetailsUpdated.json`, that includes the policy details.

```
aws dlm update-lifecycle-policy --state DISABLED --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" --policy-
details file://policyDetailsUpdated.json
```

The following is an example of the `policyDetailsUpdated.json` file.

```
{
    "ResourceTypes":[
        "VOLUME"
    ],
    "TargetTags":[
        {
            "Key": "costcenter",
            "Value": "120"
        }
    ],
    "Schedules":[
        {
            "Name": "DailySnapshots",
            "TagsToAdd": [
                {
                    "Key": "type",
                    "Value": "myDailySnapshot"
                }
            ],
            "CreateRule": {
                "Interval": 12,
                "IntervalUnit": "HOURS",
                "Times": [
                    "15:00"
                ]
            },
            "RetainRule": {
                "Count" :5
            },
            "CopyTags": false
```

```
        }
    ]
}
```

To view the updated policy, use the `get-lifecycle-policy` command. You can see that the state, the value of the tag, the snapshot interval, and the snapshot start time were changed.

Delete a lifecycle policy

Use the delete-lifecycle-policy command to delete a lifecycle policy and free up the target tags specified in the policy for reuse.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```