Set Up a Compliant Archive

November 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Introduction 1

Step 1: Create an AWS Account 1

Step 2: Create a New Vault 1

Step 3: Specify a Compliance Policy for Your Vault 4

Example 1: Deny Deletion Permissions for Archives Less Than 365 Days Old 5

Example 2: Deny Deletion Permissions Based on a Tag 6

Additional Resources 7

Introduction

This tutorial guides you through the following tasks.

- Create a New Vault for Regulatory/Compliance Archives
- Complete the Vault Lock Process
- Set up Flexible Access Controls in the Vault Access Policy

This tutorial is not meant for production environments and does not discuss options in depth. After you complete the steps, you can find more in-depth information in the Additional Resources section.

Step 1: Create an AWS Account

If you already have an AWS account, you can skip this prerequisite and use your existing account. To create an AWS account if you do not already have one:

1. Go to http://aws.amazon.com/.
2. Choose **Create an AWS Account**.
3. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

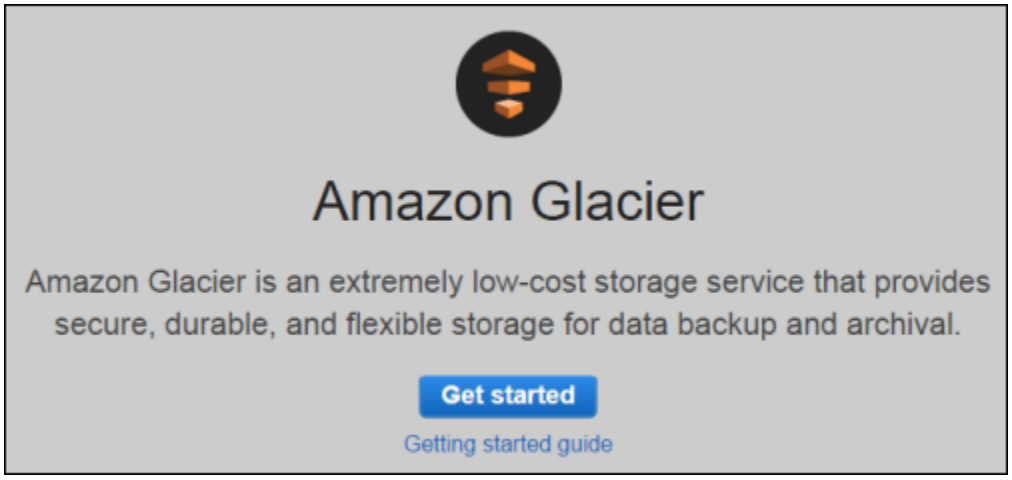
Step 2: Create a New Vault

A vault is a container for storing archives. Your first step is to create a vault in one of the supported AWS regions. In this getting started exercise, you create a vault in the US West (Oregon) region. For a list of the AWS regions supported by Amazon Glacier, go to Regions and Endpoints in the AWS General Reference.

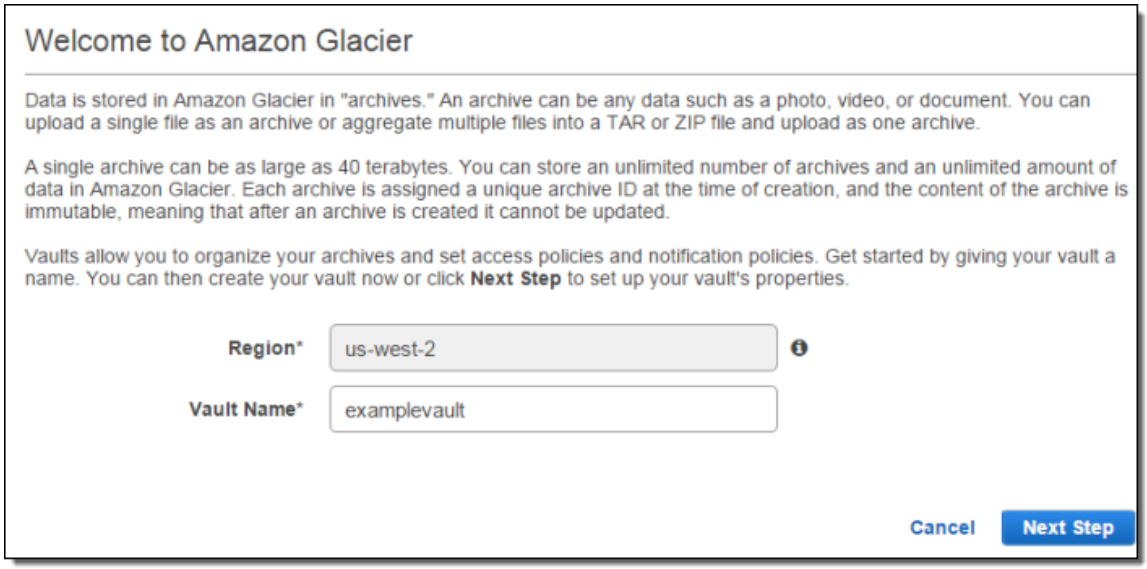
You can create vaults programmatically or by using the Amazon Glacier console. This section uses the console to create a vault.

1. Sign into the AWS Management Console and open the Amazon Glacier console at https://console.aws.amazon.com/glacier/.

2. Select a region from the region selector. In this getting started exercise, we use the US West (Oregon) region.
3. If you are using Amazon Glacier for the first time, click **Get started**. (Otherwise, click **Create Vault**.)

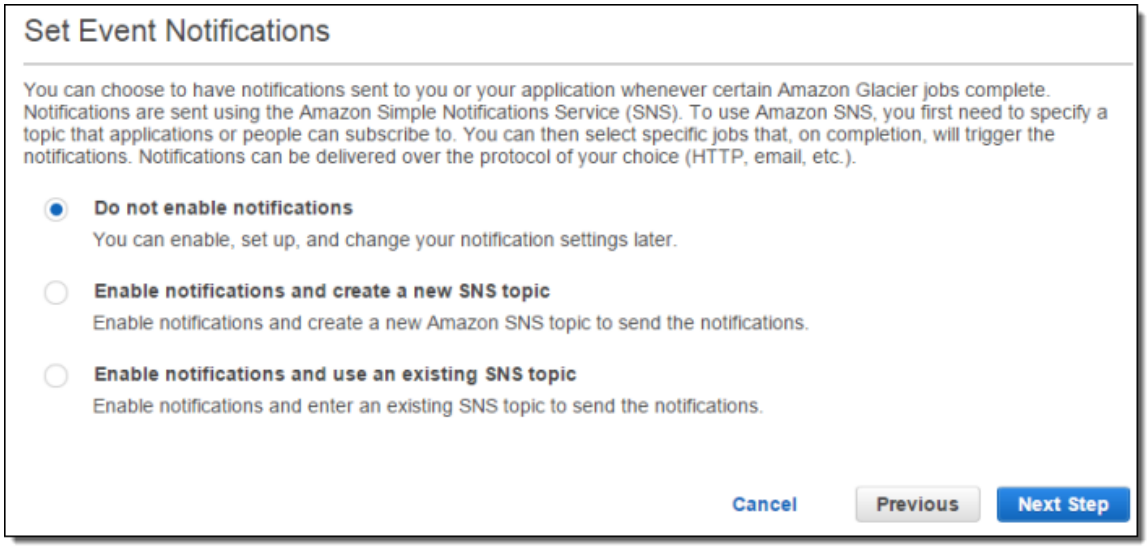


4. Enter **examplevault** as the vault name in the **Vault Name** field and then click **Next Step**. There are guidelines for naming a vault. For more information, see Creating a Vault in Amazon Glacier.

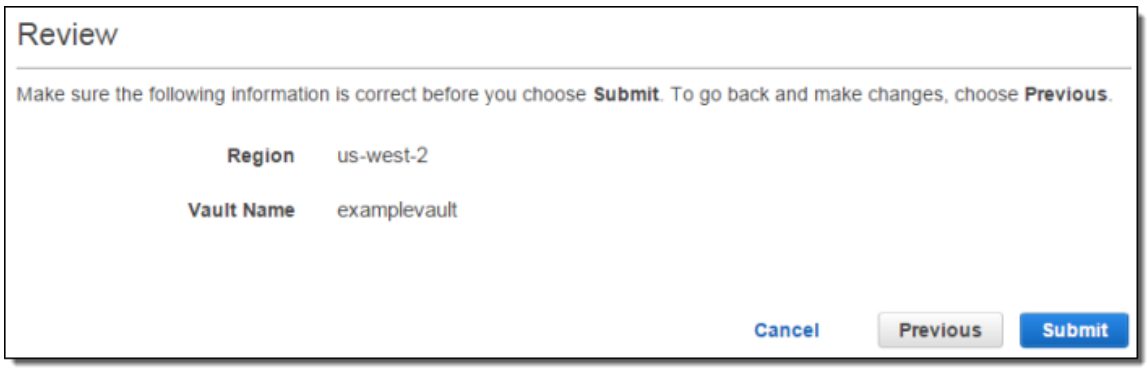


5. Select **Do not enable notifications**. For this getting started exercise, you will not configure notifications for the vault. If you wanted to have notifications sent to you or your application whenever certain Amazon Glacier jobs complete, you would select **Enable notifications and create a new SNS topic** or **Enable notifications and use an**

existing SNS topic to set up Amazon Simple Notification Service (Amazon SNS) notifications. In subsequent steps, you upload an archive and then download it using the high-level API of the AWS SDK. Using the high-level API does not require that you configure vault notification to retrieve your data.



6. If the region and vault name are correct, then click **Submit**.



7. Your new vault is listed on the **Amazon Glacier Vaults** page.

Step 3: Specify a Compliance Policy for Your Vault

Amazon Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual Amazon Glacier vaults with a vault lock policy. You can specify controls such as "write once read many" (WORM) in a vault lock policy and lock the policy from future edits. Once locked, the policy can no longer be changed.

Amazon Glacier enforces the controls set in the vault lock policy to help achieve your compliance objectives, for example, for data retention. You can deploy a variety of compliance controls in a vault lock policy using the AWS Identity and Access Management (IAM) policy language. For more information about vault lock policies, see Amazon Glacier Access Control with Vault Lock Policies.

A vault lock policy is different than a vault access policy. Both policies govern access controls to your vault. However, a vault lock policy can be locked to prevent future changes, providing strong enforcement for your compliance controls. You can use the vault lock policy to deploy regulatory and compliance controls, which typically require tight controls on data access. In contrast, you use a vault access policy to implement access controls that are not compliance related, temporary, and subject to frequent modification. Vault lock and vault access policies can be used together. For example, you can implement time-based data retention rules in the vault lock policy (deny deletes), and grant read access to designated third parties or your business partners (allow reads).

Locking a vault takes two steps:

- Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires.

- Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the Amazon Glacier API to lock a vault, see Locking a Vault by Using the Amazon Glacier API.

Here are two examples of vault lock policies you might want to use with your vault.

Note: For the purpose of this exercise we recommend you use "7 days" versus "365 days" so that you can easily check the policy and delete the archive, without incurring charges after 7 days.

Example 1: Deny Deletion Permissions for Archives Less Than 365 Days Old

Suppose that you have a regulatory requirement to retain archives for up to one year before you can delete them. You can enforce that requirement by implementing the following Vault Lock policy. The policy denies the `glacier:DeleteArchive` action on the `examplevault` vault if the archive being deleted is less than one year old. The policy uses the Amazon Glacier-specific condition key `ArchiveAgeInDays` to enforce the one-year retention requirement.

```
{
     "Version":"2012-10-17",
     "Statement":[
      {
         "Sid": "deny-based-on-archive-age",
         "Principal": "*",
         "Effect": "Deny",
         "Action": "glacier:DeleteArchive",
         "Resource": [
            "arn:aws:glacier:us-west-
2:123456789012:vaults/examplevault"
         ],
         "Condition": {
             "NumericLessThan" : {
                  "glacier:ArchiveAgeInDays" : "365"
             }
         }
      }
   ]
```

```
}
```

Example 2: Deny Deletion Permissions Based on a Tag

Suppose that you have a time-based retention rule that an archive can be deleted if it is less than a year old. At the same time, suppose that you need to place a legal hold on your archives to prevent deletion or modification for an indefinite duration during a legal investigation. In this case, the legal hold takes precedence over the time-based retention rule specified in the Vault Lock policy.

To put these two rules in place, the following example policy has two statements:

1. The first statement denies deletion permissions to everyone, locking the vault. This lock is performed by using the `LegalHold` tag.
2. The second statement grants deletion permissions when the archive is less than 365 days old. But even when archives are less than 365 days old, no one can delete them because the vault has been locked by the first statement.

```
{
     "Version":"2012-10-17",
     "Statement":[
      {
        "Sid": "no-one-can-delete-any-archive-from-vault",
        "Principal": "*",
        "Effect": "Deny",
        "Action": [
          "glacier:DeleteArchive"
        ],
        "Resource": [
          "arn:aws:glacier:us-west-
2:123456789012:vaults/examplevault"
        ],
        "Condition": {
          "StringLike": {
            "glacier:ResourceTag/LegalHold": [
              "true",
              ""
            ]
          }
        }
```

```
      },
      {
        "Sid": "you-can-delete-archive-less-than-1-year-
old",
        "Principal": "*",
        "Effect": "Allow",
        "Action": [
          "glacier:DeleteArchive"
        ],
        "Resource": [
          "arn:aws:glacier:us-west-
2:123456789012:vaults/examplevault"
        ],
        "Condition": {
          "NumericLessThan": {
            "glacier:ArchiveAgeInDays": "365"
          }
        }
      }
   ]
}
```

Additional Resources

We recommend that you continue to learn more about the concepts introduced in this guide with the following resources:

- Amazon Glacier Vault Lock
- Abort Vault Lock (DELETE lock-policy)
- Complete Vault Lock (POST lockId)
- Get Vault Lock (GET lock-policy)
- Initiate Vault Lock (POST lock-policy)