# Table of Contents

What is AWS Backup? ................................................................. 1  
Supported AWS resources and third-party applications ................................................................. 1  
Features available for all supported resources ................................................................. 2  
Feature availability by resource ................................................................. 2  
Feature availability by AWS Region ................................................................. 4  
Feature overview ........................................................................ 7  
  Centralized backup management ................................................................. 7  
  Policy-based backup ........................................................................ 7  
  Tag-based backup policies ........................................................................ 7  
Life cycle management policies ................................................................. 7  
Cross-Region backup ........................................................................ 8  
Cross-account management and cross-account backup ................................................................. 8  
Auditing and reporting with AWS Backup Audit Manager ................................................................. 8  
Incremental backups ........................................................................ 8  
Full AWS Backup management ........................................................................ 9  
Backup activity monitoring ........................................................................ 9  
Secure your data in backup vaults ........................................................................ 9  
Support for compliance obligations ........................................................................ 10  
Getting started ........................................................................ 10  
How it works ........................................................................ 11  
  Working with supported AWS services ........................................................................ 11  
    Opt in to managing services with AWS Backup ........................................................................ 12  
    Working with Amazon S3 data ........................................................................ 12  
    Working with VMware virtual machines ........................................................................ 12  
    Working with Amazon DynamoDB ........................................................................ 13  
    Working with Amazon FSx file systems ........................................................................ 13  
    Working with Amazon EC2 ........................................................................ 14  
    Working with Amazon EFS ........................................................................ 14  
    Working with Amazon EBS ........................................................................ 15  
    Working with Amazon RDS and Aurora ........................................................................ 15  
    Working with AWS Backup ........................................................................ 16  
    Working with AWS Storage Gateway ........................................................................ 16  
    Working with Amazon DocumentDB ........................................................................ 16  
    Working with Amazon Neptune ........................................................................ 16  
    Working with Amazon Timestream ........................................................................ 16  
    Working with AWS Organizations ........................................................................ 16  
    Working with AWS CloudFormation ........................................................................ 17  
    Working with AWS Backup, AWS Systems Manager for SAP, and SAP HANA ........................................................................ 17  
How AWS services back up their own resources ........................................................................ 17  
Metering, costs, and billing ........................................................................ 17  
  AWS Backup pricing ........................................................................ 17  
  AWS Backup billing ........................................................................ 18  
Cost allocation tags ........................................................................ 18  
AWS Backup Audit Manager pricing ........................................................................ 18  
Amazon Aurora pricing ........................................................................ 18  
Blogs, videos, tutorials, and other resources ........................................................................ 18  
Setting up AWS for the first time ........................................................................ 21  
  Sign up for AWS ........................................................................ 21  
  Create an IAM user ........................................................................ 21  
  Create an IAM role ........................................................................ 22  
Getting started ........................................................................ 24  
Prerequisites ........................................................................ 24  
Getting started 1: Service Opt-in ........................................................................ 25  
Next steps ........................................................................ 25
## Getting started 2: Create an on-demand backup

Next steps

---

## Getting started 3: Create a scheduled backup

Step 1: Create a backup plan based on an existing one

Step 2: Assign resources to a backup plan

Step 3: Create a backup vault

Next steps

---

## Getting started 4: Create Amazon EFS automatic backups

Next steps

---

## Getting started 5: View your backup jobs and recovery points

View the status of backup jobs

View all backups in a vault

View details of protected resources

Next steps

---

## Getting started 6: Restore a backup

Next steps

---

## Getting started 7: Create an audit report

Next steps

---

## Getting started 8: Clean up resources

Step 1: Delete restored AWS resources

Step 2: Delete the backup plan

Step 3: Delete the recovery points

Step 4: Delete the backup vault

Step 5: Delete the report plan

Step 6: Delete the reports

---

## Managing backup plans

---

## Creating a backup plan

Creating backup plans using the AWS Backup console

Creating backup plans using a JSON document and the AWS Backup CLI

Backup plan options and configuration

AWS CloudFormation templates for backup plans

---

## Assigning resources

Assigning resources using the console

Assigning resources programmatically

Assigning resources using AWS CloudFormation

Quotas on resource assignment

---

## Deleting a backup plan

---

## Updating a backup plan

---

## Backup vaults

---

## Logically air-gapped vaults (preview)

Overview

Use case

Compare and contrast with a standard backup vault

Create a logically air-gapped vault from the console

View logically air-gapped vault details in the console

Copy from a standard backup vault to a logically air-gapped vault in the console

Share a logically air-gapped vault from the console

Restore a backup from a logically air-gapped vault using the console

Delete a logically air-gapped vault using the console

Logically air-gapped vaults through CLI/API

---

## Create a backup vault

Creating a backup vault (console)

Creating a backup vault (programmatically)

Backup vault name

AWS KMS encryption key

Backup vault tags

Set access policies on backup vaults
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access to a resource type in a backup vault</td>
<td>63</td>
</tr>
<tr>
<td>Deny access to a backup vault</td>
<td>63</td>
</tr>
<tr>
<td>Deny access to delete recovery points in a backup vault</td>
<td>64</td>
</tr>
<tr>
<td><strong>AWS Backup Vault Lock</strong></td>
<td></td>
</tr>
<tr>
<td>Vault lock modes</td>
<td>65</td>
</tr>
<tr>
<td>Vault lock benefits</td>
<td>65</td>
</tr>
<tr>
<td>Lock a backup vault using the console</td>
<td>66</td>
</tr>
<tr>
<td>Lock a backup vault programatically</td>
<td>66</td>
</tr>
<tr>
<td>Review a backup vault for its AWS Backup Vault Lock configuration</td>
<td>67</td>
</tr>
<tr>
<td>Vault lock removal during grace time (Compliance mode)</td>
<td>68</td>
</tr>
<tr>
<td>AWS account closure with a locked vault</td>
<td>69</td>
</tr>
<tr>
<td>Additional security considerations</td>
<td>69</td>
</tr>
<tr>
<td>Delete a backup vault</td>
<td>70</td>
</tr>
<tr>
<td><strong>Working with backups</strong></td>
<td></td>
</tr>
<tr>
<td>Creating a backup</td>
<td>71</td>
</tr>
<tr>
<td>Creating automatic backups</td>
<td>71</td>
</tr>
<tr>
<td>Creating on-demand backups</td>
<td>71</td>
</tr>
<tr>
<td>Backup job statuses</td>
<td>72</td>
</tr>
<tr>
<td>How incremental backups work</td>
<td>72</td>
</tr>
<tr>
<td>Access to source resources</td>
<td>72</td>
</tr>
<tr>
<td>On-demand backups</td>
<td>73</td>
</tr>
<tr>
<td>Point-in-time recovery</td>
<td>74</td>
</tr>
<tr>
<td>Amazon S3 backups</td>
<td>79</td>
</tr>
<tr>
<td>Virtual machine backups</td>
<td>83</td>
</tr>
<tr>
<td>Advanced DynamoDB backup</td>
<td>107</td>
</tr>
<tr>
<td>Amazon Timestream backups</td>
<td>111</td>
</tr>
<tr>
<td>SAP HANA on Amazon EC2 backups</td>
<td>112</td>
</tr>
<tr>
<td>Amazon Redshift backups</td>
<td>117</td>
</tr>
<tr>
<td>Amazon RDS Multi-AZ backups</td>
<td>119</td>
</tr>
<tr>
<td>CloudFormation stack backups</td>
<td>120</td>
</tr>
<tr>
<td>Creating Windows VSS backups</td>
<td>124</td>
</tr>
<tr>
<td>Amazon EBS multi-volume, crash-consistent backups</td>
<td>125</td>
</tr>
<tr>
<td>Copying tags onto backups</td>
<td>125</td>
</tr>
<tr>
<td>Stopping a backup job</td>
<td>126</td>
</tr>
<tr>
<td><strong>Copying a backup</strong></td>
<td></td>
</tr>
<tr>
<td>Cross-Region backup</td>
<td>126</td>
</tr>
<tr>
<td>Cross-account backup</td>
<td>128</td>
</tr>
<tr>
<td><strong>Viewing a list of backups</strong></td>
<td></td>
</tr>
<tr>
<td>Listing backups by protected resource in the console</td>
<td>136</td>
</tr>
<tr>
<td>Listing backups by backup vault in the console</td>
<td>136</td>
</tr>
<tr>
<td>Listing backups programatically</td>
<td>136</td>
</tr>
<tr>
<td><strong>Editing a backup</strong></td>
<td></td>
</tr>
<tr>
<td>Deleting backups</td>
<td>137</td>
</tr>
<tr>
<td>Deleting backups manually</td>
<td>138</td>
</tr>
<tr>
<td>Troubleshooting manual deletions</td>
<td>138</td>
</tr>
<tr>
<td><strong>Restoring a backup</strong></td>
<td></td>
</tr>
<tr>
<td>How to restore</td>
<td>139</td>
</tr>
<tr>
<td>Non-destructive restores</td>
<td>139</td>
</tr>
<tr>
<td>Copy tags during a restore</td>
<td>139</td>
</tr>
<tr>
<td>Restore job statuses</td>
<td>141</td>
</tr>
<tr>
<td>Restoring S3 data</td>
<td>142</td>
</tr>
<tr>
<td>Restoring a virtual machine</td>
<td>144</td>
</tr>
<tr>
<td>Restoring an FSX file system</td>
<td>147</td>
</tr>
<tr>
<td>Restoring an Amazon EBS volume</td>
<td>151</td>
</tr>
<tr>
<td>Restoring an EFS file system</td>
<td>153</td>
</tr>
<tr>
<td>Restoring a DynamoDB table</td>
<td>155</td>
</tr>
<tr>
<td>Restoring an RDS database</td>
<td>157</td>
</tr>
</tbody>
</table>
Audit backups and create reports with AWS Backup Audit Manager ........................................ 8
  Working with audit frameworks ........................................................................................................ 177
    Choosing your controls ..................................................................................................................... 177
    Turning on resource tracking ......................................................................................................... 179
    Creating frameworks using the AWS Backup console ................................................................. 183
    Creating frameworks using the AWS Backup API ........................................................................ 184
    Viewing framework compliance status ........................................................................................... 192
    Finding non-compliant resources .................................................................................................. 193
    Updating audit frameworks ............................................................................................................ 193
  Deleting audit frameworks ............................................................................................................... 194
  Working with audit reports ................................................................................................................. 194
    Choosing your report template ........................................................................................................ 195
    Creating report plans using the AWS Backup console ............................................................... 199
    Creating report plans using the AWS Backup API ........................................................................ 201
    Creating on-demand reports .......................................................................................................... 203
    Viewing audit reports .................................................................................................................... 203
    Updating report plans .................................................................................................................... 203
    Deleting report plans ..................................................................................................................... 204

Using AWS CloudFormation to deploy AWS Backup Audit Manager resources ................................ 204
  Turn on resource tracking ............................................................................................................... 183
  Deploy default controls .................................................................................................................... 208
  Exempt IAM roles from control evaluation ...................................................................................... 209
  Create a report plan ........................................................................................................................... 209
  Using AWS Backup Audit Manager with AWS Audit Manager ...................................................... 210

AWS Backup Audit Manager controls and remediation ................................................................. 210
  Backup resources are protected by a backup plan ........................................................................... 211
  Backup plan minimum frequency and minimum retention ............................................................ 211
  Vaults prevent manual deletion of recovery points ....................................................................... 211
  Recovery points are encrypted ......................................................................................................... 212
  Minimum retention established for recovery point ......................................................................... 212
  Cross-Region backup copy is scheduled ......................................................................................... 212
  Cross-account backup copy is scheduled ....................................................................................... 213
  Backups are protected by AWS Backup Vault Lock ....................................................................... 213
  Last recovery point was created ....................................................................................................... 214

Manage multiple accounts with AWS Organizations ........................................................................ 215
  Creating a management account in Organizations ........................................................................ 216
  Enabling cross-account management .............................................................................................. 216

Delegated administrator .................................................................................................................... 216
  Prerequisites .................................................................................................................................... 217
  Register a member account as a delegated administrator account .................................................. 218
  Deregister a member account .......................................................................................................... 218
  Delegate AWS Backup policies through AWS Organizations ....................................................... 219

Creating a backup policy ................................................................................................................... 219
  Monitoring activities in multiple AWS accounts ............................................................................. 222

Resource opt-in rules .......................................................................................................................... 223
  Defining policies, policy syntax, and policy inheritance ................................................................ 223

AWS Backup and AWS CloudFormation ........................................................................................... 224
  In general ........................................................................................................................................... 224
What is AWS Backup?

AWS Backup is a fully-managed service that makes it easy to centralize and automate data protection across AWS services, in the cloud, and on premises. Using this service, you can configure backup policies and monitor activity for your AWS resources in one place. It allows you to automate and consolidate backup tasks that were previously performed service-by-service, and removes the need to create custom scripts and manual processes. With a few clicks in the AWS Backup console, you can automate your data protection policies and schedules.

AWS Backup does not govern backups you take in your AWS environment outside of AWS Backup. Therefore, if you want a centralized, end-to-end solution for business and regulatory compliance requirements, start using AWS Backup today.

Supported AWS resources and third-party applications

The following are AWS resources and third-party applications that you can back up and restore using AWS Backup.

<table>
<thead>
<tr>
<th>Supported resource</th>
<th>Supported resource type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
<td>Amazon EC2 instances (excluding store-backed AMIs)</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td>Amazon S3 data</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (Amazon EBS)</td>
<td>Amazon EBS volumes</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>Amazon DynamoDB tables</td>
</tr>
<tr>
<td>Amazon Relational Database Service (Amazon RDS)</td>
<td>Amazon RDS database instances (including all database engines); Multi-Availability Zone clusters</td>
</tr>
<tr>
<td>Amazon Aurora</td>
<td>Aurora clusters</td>
</tr>
<tr>
<td>Amazon Elastic File System (Amazon EFS)</td>
<td>Amazon EFS file systems</td>
</tr>
<tr>
<td>FSx for Lustre</td>
<td>FSx for Lustre file systems</td>
</tr>
<tr>
<td>FSx for Windows File Server</td>
<td>FSx for Windows File Server file systems</td>
</tr>
<tr>
<td>Amazon FSx for NetApp ONTAP</td>
<td>FSx for ONTAP file systems</td>
</tr>
<tr>
<td>Amazon FSx for OpenZFS</td>
<td>FSx for OpenZFS file systems</td>
</tr>
<tr>
<td>AWS Storage Gateway (Volume Gateway)</td>
<td>AWS Storage Gateway volumes</td>
</tr>
<tr>
<td>Amazon DocumentDB</td>
<td>Amazon DocumentDB clusters</td>
</tr>
</tbody>
</table>
Features available for all supported resources

To use an AWS Backup feature, it must be offered for your supported resource and AWS Region. Use the following sections and tables to determine feature availability.

AWS Backup offers the following features for ALL its supported AWS services and third-party applications it supports.

- Automated backup schedules and retention management
- Centralized backup monitoring
- Incremental backups, except for DynamoDB, Aurora, DocumentDB, and Neptune.
- AWS KMS-integrated backup encryption
- Cross-account management with AWS Organizations
- Automated backup audits and reports with AWS Backup Audit Manager
- Write-once, read-many (WORM) with AWS Backup Vault Lock

Feature availability by resource

To use AWS Backup with a supported AWS service in a particular Region, the service must be available in the Region. To determine service availability in a Region, view the service's endpoints in the AWS General Reference.

<table>
<thead>
<tr>
<th>AWS Backup supports</th>
<th>Cross-Region backup</th>
<th>Cross-account backup</th>
<th>AWS Backup Audit Manager</th>
<th>Increment backup</th>
<th>Continuous backup and point-in-time restore (PITR)</th>
<th>Full AWS Backup management</th>
<th>Lifecycle to cold storage</th>
<th>Item-level restore‡</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>S3</td>
<td>✓^</td>
<td>✓^</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EBS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### AWS Backup Developer Guide

#### Feature availability by resource

<table>
<thead>
<tr>
<th><strong>AWS Backup supports</strong></th>
<th><strong>Cross-Region backup</strong></th>
<th><strong>Cross-account backup</strong></th>
<th><strong>AWS Backup Audit Manager</strong></th>
<th><strong>Incremental backup</strong></th>
<th><strong>Continuous backup and point-in-time restore (PITR)</strong></th>
<th><strong>Full AWS Backup management</strong></th>
<th><strong>Lifecycle to cold storage</strong></th>
<th><strong>Item-level restore‡</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>RDS single instance</td>
<td>✓*</td>
<td>✓*</td>
<td>✓**</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDS cluster</td>
<td>✓*</td>
<td>✓*</td>
<td>✓**</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aurora</td>
<td>✓*</td>
<td>✓*</td>
<td>✓</td>
<td>✓</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSx for Lustre</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSx for Windows File Server</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSx for ONTAP</td>
<td>✓†</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSx for OpenZFS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Gateway</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DocumentDB*</td>
<td>✓*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neptune</td>
<td>✓*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Timestream✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows VSS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Virtual machines</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>CloudFormation templates</td>
<td>✓</td>
<td>✓*</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓*</td>
</tr>
<tr>
<td>DynamoDB without AWS Backup advanced features</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Feature availability by AWS Region

AWS Backup is available in all the following AWS Regions. AWS Backup features are available in all these Regions unless otherwise noted in the following table.

<table>
<thead>
<tr>
<th>AWS Backup supports</th>
<th>Cross-Region backup</th>
<th>Cross-account backup</th>
<th>AWS Backup Audit Manager</th>
<th>Increment backup</th>
<th>Continuous backup and point-in-time restore (PITR)</th>
<th>Full AWS Backup management</th>
<th>Lifecycle to cold storage</th>
<th>Item-level restore‡</th>
</tr>
</thead>
<tbody>
<tr>
<td>DynamoDB ✓ with AWS Backup advanced features</td>
<td>✓ ✓</td>
<td>✓</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP HANA databases on Amazon EC2 instances</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

^ Destination copies from S3 buckets and RDS databases with PITR are not Point-in-Time restorable (PITR).

* RDS, Aurora, DocumentDB, and Neptune do not support a single copy action that performs both cross-Region AND cross-account backup. You can choose one or the other. You can also use a AWS Lambda script to listen for the completion of your first copy, perform your second copy, then delete the first copy. RDS multi availability zone (Multi-AZ) database instances can be copied, but Multi-AZ clusters do not currently support cross-Region or cross-account copy.

+ AWS Backup supports Aurora snapshots, billed as incremental or full backups.

** See RDS multi-availability zone backups for Regions where Backup Audit Manager support is available.

† AWS Backup Audit Manager supports this resource across all controls except cross-account copy and cross-Region copy.

‡ The "item" in an item-level restore varies depending on the supported resource. For example, a file system item is a file or directory, whereas an S3 item is an S3 object. A VMware item is a disk. For more information, see the Restoring a backup (p. 139) section for the supported resource.

‡ In CloudFormation stack backups, nested resources retain their source resources' features. However, resources within the stack do not retain Point-in-Time Restore (PITR) functionality (such as S3 and RDS). Properties within the matrix above apply just to CloudFormation templates and not to the resources within the stack.
## Feature availability by AWS Region

<table>
<thead>
<tr>
<th>AWS Backup supports</th>
<th>Cross-Region backup</th>
<th>Cross-account management</th>
<th>Cross-account backup</th>
<th>AWS Backup Audit Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>South America (São Paulo) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Sydney) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (Ireland) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>US East (Ohio) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (London) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>US West (Oregon) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>US West (N. California) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (Paris) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (Stockholm) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Singapore) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Canada (Central) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Seoul) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>US East (N. Virginia) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (Frankfurt) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Jakarta) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>China (Beijing) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS Backup supports</td>
<td>Cross-Region backup</td>
<td>Cross-account management</td>
<td>Cross-account backup</td>
<td>AWS Backup Audit Manager</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>China (Ningxia) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middle East (Bahrain) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong) Region</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town) Region</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Milan) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Osaka) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Middle East (UAE) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Spain) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Zurich) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Hyderabad) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Melbourne) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-West) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AWS GovCloud (US-East) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

AWS Backup support for **Amazon S3** is available in all Regions except China (Beijing) and China (Ningxia). Cross-account and Cross-Region backup of S3 resources is not available in Middle East (Bahrain) Region, Asia Pacific (Hong Kong) Region Africa (Cape Town) Region Europe (Milan) Region, Asia Pacific (Osaka) Region, Middle East (UAE) Region, Europe (Spain) Region, Europe (Zurich) Region, Asia Pacific (Hyderabad) Region, and Asia Pacific (Melbourne) Region.

AWS Backup support for **Amazon FSx for Windows File Server** and Lustre is available in all Regions except Asia Pacific (Jakarta). AWS Backup support for **FSx for ONTAP** is available in all Regions except US West (N. California), Asia Pacific (Jakarta), Beijing and Ningxia, and Asia Pacific (Osaka). AWS Backup support for **FSx for OpenZFS** is only available in Asia Pacific (Sydney), Asia Pacific (Tokyo), Europe (Ireland), Europe (London), US East (Ohio), US West (Oregon), Asia Pacific (Singapore), Canada (Central), US East (N. Virginia), and Europe (Frankfurt) Regions.

AWS Backup support for **Storage Gateway** is available in all Regions except Asia Pacific (Osaka).
AWS Backup support for **VMware** is available in all Regions except Asia Pacific (Jakarta), China (Beijing) or China (Ningxia).

AWS Backup support for **Amazon Timestream** is available in US East (N. Virginia), US East (Ohio), US West (Oregon), Europe (Ireland), Europe (Frankfurt), Asia Pacific (Sydney), and Asia Pacific (Tokyo) Regions.

AWS Backup support for **SAP HANA** databases on Amazon EC2 instances are not currently supported in these Regions: Asia Pacific (Jakarta), AWS GovCloud (US-West), AWS GovCloud (US-East), China (Beijing), China (Ningxia) and Europe (Spain), Europe (Zurich), Asia Pacific (Hyderabad), Asia Pacific (Melbourne) Region.

**Feature overview**

AWS Backup provides many features and capabilities, including:

**Centralized backup management**

AWS Backup provides a centralized backup console, a set of backup APIs, and the AWS Command Line Interface (AWS CLI) to manage backups across the AWS services that your applications use. With AWS Backup, you can centrally manage backup policies that meet your backup requirements. You can then apply them to your AWS resources across AWS services, enabling you to back up your application data in a consistent and compliant manner. The AWS Backup centralized backup console offers a consolidated view of your backups and backup activity logs, making it easier to audit your backups and ensure compliance.

**Policy-based backup**

With AWS Backup, you can create backup policies known as **backup plans**. Use these backup plans to define your backup requirements and then apply them to the AWS resources that you want to protect across the AWS services that you use. You can create separate backup plans that each meet specific business and regulatory compliance requirements. This helps ensure that each AWS resource is backed up according to your requirements. Backup plans make it easy to enforce your backup strategy across your organization and across your applications in a scalable manner.

For all the configuration options for backup plans, see [Backup plan options and configuration (p. 37)](#).

**Tag-based backup policies**

You can use AWS Backup to apply backup plans to your AWS resources in a wide variety of ways, including tagging them. Tagging makes it easier to implement your backup strategy across all your applications and to ensure that all your AWS resources are backed up and protected. AWS tags are a great way to organize and classify your AWS resources. Integration with AWS tags enables you to quickly apply a backup plan to a group of AWS resources, so that they are backed up in a consistent and compliant manner.

For all the ways you can assign your resources to backup plans, see [Assigning resources to a backup plan (p. 43)](#).

**Lifecycle management policies**

AWS Backup enables you to meet compliance requirements while minimizing backup storage costs by storing backups in a low-cost cold storage tier (backups to cold storage are full backups). You can
configure lifecycle policies that automatically transition backups from warm storage to cold storage according to a schedule that you define.

AWS Backup lifecycles data (that is, transitions data from warm to cold storage) that is no longer referenced by warm backups. Data in cold backups that is only referenced by other cold backups are billed at cold storage tier prices. Others continue at warm storage tier pricing.

For which resources support tiering to cold storage, see Feature availability by resource (p. 2). The cold storage expression is ignored for other backups.

Cross-Region backup

Using AWS Backup, you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region backup is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data. For more information, see Creating backup copies across AWS Regions.

Cross-account management and cross-account backup

You can use AWS Backup to manage your backups across all AWS accounts inside your AWS Organizations structure. With cross-account management, you can automatically use backup policies to apply backup plans across the AWS accounts within your organization. This makes compliance and data protection efficient at scale and reduces operational overhead. It also helps eliminate manually duplicating backup plans across individual accounts. For more information, see Managing AWS Backup resources across multiple AWS accounts.

You can also copy backups to multiple different AWS accounts inside your AWS Organizations management structure. This way, you can “fan in” backups to a single repository account, then “fan out” backups for greater resilience. Creating backup copies across AWS accounts.

Before you can use the cross-account management and cross-account backup features, you must have an existing organization structure configured in AWS Organizations. An organizational unit (OU) is a group of accounts that can be managed as a single entity. AWS Organizations is a list of accounts that can be grouped into organizational units and managed as a single entity.

Auditing and reporting with AWS Backup Audit Manager

AWS Backup Audit Manager helps you simplify data governance and compliance management of your backups across AWS. AWS Backup Audit Manager provides built-in, customizable controls that you can align with your organizational requirements. You can also use these controls to automatically track your backup activities and resources.

AWS Backup Audit Manager can help you locate specific activities and resources that are not yet compliant with the controls that you defined. It also generates daily reports that you can use to demonstrate evidence of compliance with your controls over time.

To include your backup compliance alongside your overall compliance posture, you can automatically import AWS Backup Audit Manager findings into AWS Audit Manager.

Incremental backups

AWS Backup efficiently stores your periodic backups incrementally. The first backup of an AWS resource backs up a full copy of your data. For each successive incremental backup, only the changes to your AWS
resources are backed up. Incremental backups enable you to benefit from the data protection of frequent backups while minimizing storage costs (backups to cold storage are full backups).

For a list of which resources support incremental backups, see Feature availability by resource (p. 2).

**Full AWS Backup management**

Some resource types support full AWS Backup management. The benefits of full AWS Backup management include:

- **Independent encryption.** AWS Backup automatically encrypts your backups with the KMS key of your AWS Backup vault, instead of using the same encryption key as your source resource. This increases your layers of defense. See Encryption for backups in AWS Backup (p. 227) for more information.

- **awsbackup Amazon Resource Names (ARNs).** Backup ARNs begin with `arn:aws:backup` instead of `arn:aws:source-resource`. This allows you to create access policies that apply specifically to backups and not the source resources. See Access control (p. 240) for more information.

- **Centralized backup billing and Cost Explorer cost allocation tags.** Charges for AWS Backup (including storage, data transfers, restores, and early deletion) appear under "Backup" in your Amazon Web Services bill, instead of appearing under each supported resource. You can also use Cost Explorer cost allocation tags to track and optimize your backup costs. See Metering, costs, and billing (p. 17) for more information.

To see which resource types are eligible for full AWS Backup management, see Feature availability by resource (p. 2).

**Backup activity monitoring**

AWS Backup provides a dashboard that makes it simple to audit backup and restore activity across AWS services. With just a few clicks on the AWS Backup console, you can view the status of recent backup jobs. You can also restore jobs across AWS services to ensure that your AWS resources are properly protected.

AWS Backup integrates with Amazon CloudWatch and Amazon EventBridge. CloudWatch allows you to track metrics and create alarms. EventBridge allows you to view and monitor AWS Backup events. For more information, see Monitoring AWS Backup events using EventBridge and Monitoring AWS Backup metrics with CloudWatch.

AWS Backup integrates with AWS CloudTrail. CloudTrail gives you a consolidated view of backup activity logs that make it quick and easy to audit how your resources are backed up. AWS Backup also integrates with Amazon Simple Notification Service (Amazon SNS), providing you with backup activity notifications, such as when a backup succeeds or a restore has been initiated. For more information, see Logging AWS Backup API calls with CloudTrail and Using Amazon SNS to track AWS Backup events.

**Secure your data in backup vaults**

The content of each AWS Backup backup is immutable, meaning that no one can alter that content. AWS Backup further secures your backups in backup vaults, which separates them safely from their source instances. For example, your vault will retain your Amazon EC2 and Amazon EBS backups according to the lifecycle policy you choose, even if you delete the source Amazon EC2 instance and Amazon EBS volumes.

Backup vaults offer encryption and resource-based access policies that let you define who has access to your backups. You can define access policies for a backup vault that define who has access to the backups within that vault and what actions they can take. This provides a simple and secure way to control access to your backups across AWS services. To review AWS and customer managed policies for AWS Backup, see Managed policies for AWS Backup.
You can use AWS Backup Vault Lock to prevent anyone (including you) from deleting backups or altering their retention period. AWS Backup Vault Lock helps you enforce a write-once-read-many (WORM) model and add another layer of defense to your defense in depth. To get started, see AWS Backup Vault Lock.

Support for compliance obligations

AWS Backup helps you meet your global compliance obligations. AWS Backup is in scope of the following AWS compliance programs:

- FedRAMP High
- GDPR
- SOC 1, 2, and 3
- PCI
- HIPAA
- and many more

Getting started

To learn more about AWS Backup, we recommend that you start with Getting started with AWS Backup (p. 24).
AWS Backup: How it works

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backing up of data across AWS services. With AWS Backup, you can create backup policies called backup plans. You can use these plans to define your backup requirements, such as how frequently to back up your data and how long to retain those backups.

AWS Backup lets you apply backup plans to your AWS resources by simply tagging them. AWS Backup then automatically backs up your AWS resources according to the backup plan that you defined.

The following sections describe how AWS Backup works, its implementation details, and security considerations.

Topics
- How AWS Backup works with supported AWS services (p. 11)
- Metering, costs, and billing (p. 17)
- AWS Backup blogs, videos, tutorials, and other resources (p. 18)

How AWS Backup works with supported AWS services

Some AWS Backup-supported AWS services offer their own, stand-alone backup features. Those features are available to you independent of whether you use AWS Backup. However, the backups other AWS services create are not available for central governance through AWS Backup.

To configure AWS Backup to centrally manage data protection for all your supported services, you must opt in to managing that service with AWS Backup, create an on-demand backup or schedule backups using a backup plan, and store your backups in backup vaults.

Topics
- Opt in to managing services with AWS Backup (p. 12)
- Working with Amazon S3 data (p. 12)
- Working with VMware virtual machines (p. 12)
- Working with Amazon DynamoDB (p. 13)
- Working with Amazon FSx file systems (p. 13)
- Working with Amazon EC2 (p. 14)
- Working with Amazon EFS (p. 15)
- Working with Amazon EBS (p. 15)
- Working with Amazon RDS and Aurora (p. 15)
- Working with AWS BackInt (p. 16)
- Working with AWS Storage Gateway (p. 16)
- Working with Amazon DocumentDB (p. 16)
- Working with Amazon Neptune (p. 16)
Opt in to managing services with AWS Backup

When new AWS services become available, you must enable AWS Backup to use those services. If you try to create an on-demand backup or backup plan using resources from a service that is not enabled, you receive an error message and cannot complete the process.

Note
Service opt-in settings are Region-specific. If you change the AWS Region that you're using, you must reconfigure the services that you use with AWS Backup.

To configure the services used with AWS Backup

2. In the navigation pane, choose Settings.
3. On the Service opt-in page, choose Configure resources.
4. Use the toggle switches to enable or disable the services used with AWS Backup.
   
   Important
   RDS, Aurora, Neptune, and DocumentDB share the same Amazon Resource Name (ARN). Opting in to manage one of these resource types with AWS Backup opts in to all of them when assigning it to a backup plan. Regardless, we recommend you opt in all of them to accurately represent your opt-in status.

5. Choose Confirm.

Working with Amazon S3 data

AWS Backup offers fully-managed backup and restore for Amazon S3 backups. To learn more, see Amazon S3 backups (p. 79).

- How to back up resources: Getting started with AWS Backup (p. 24)
- How to restore Amazon S3 data using AWS Backup: Restoring S3 data (p. 142)

For detailed information about S3 data, see the Amazon S3 documentation.

Working with VMware virtual machines

AWS Backup supports centralized and automated data protection for on-premises VMware virtual machines (VMs) along with VMs in the VMware Cloud™ (VMC) on AWS. You can back up from your on-premises and VMC virtual machines to AWS Backup. Then, you can restore from AWS Backup to either on-premises or VMC.

Backup gateway is downloadable AWS Backup software that you deploy to your VMware VMs to connect them to AWS Backup. The gateway connects to your VM management server to discover VMs, discovers your VMs, encrypts data, and efficiently transfers data to AWS Backup. The following diagram illustrates how Backup gateway connects to your VMs:
AWS Backup supports backing up and restoring Amazon DynamoDB tables. DynamoDB is a fully-managed NoSQL database service that provides fast and predictable performance with seamless scalability.

Since its launch, AWS Backup has always supported DynamoDB. Starting November 2021, AWS Backup also introduced advanced features for DynamoDB backups. Those advanced features include copying your backups across AWS Regions and accounts, tiering backups to cold storage, and using tags for permissions and cost management.

New AWS Backup customers onboarding after November 2021 will have advanced DynamoDB backup features enabled by default.

We recommend all existing AWS Backup customers enable advanced features for DynamoDB. There is no difference in warm backup storage pricing after you enable advanced features, and you can save money by tiering backups to cold storage and optimize your costs by using cost allocation tags.

For a full list of advanced features and how to enable them, see Advanced DynamoDB backup (p. 107).

- How to back up resources: Getting started with AWS Backup (p. 24)
- How to restore DynamoDB resources: Restoring an Amazon DynamoDB table (p. 155)

For detailed information about DynamoDB, see What is Amazon DynamoDB? in the Amazon DynamoDB Developer Guide.

Working with Amazon FSx file systems

AWS Backup supports backing up and restoring Amazon FSx file systems. Amazon FSx provides fully managed third-party file systems with the native compatibility and feature sets for workloads. AWS Backup uses the built-in backup functionality of Amazon FSx. So backups taken from the AWS Backup console have the same level of file system consistency and performance, and the same restore options as backups that are taken through the Amazon FSx console.

If you use AWS Backup to manage these backups, you gain additional functionality, such as unlimited retention options, and the ability to create scheduled backups as frequently as every hour. In addition, AWS Backup retains your backups even after the source file system is deleted. This protects against accidental or malicious deletion.
Use AWS Backup to protect Amazon FSx file systems if you want to configure backup policies and monitor backup tasks from a central backup console that also extends support for other AWS services.

- How to back up resources: Getting started with AWS Backup (p. 24)
- How to restore Amazon FSx resources: Restoring an FSx file system (p. 147)

For detailed information about Amazon FSx file systems, see the Amazon FSx documentation.

## Working with Amazon EC2

Using AWS Backup, you can schedule or perform on-demand backup jobs that include entire EC2 instances and Windows applications running on Amazon EC2, along with associated configuration data. This limits the need for you to interact with the storage (Amazon EBS) volume. Similarly, you can restore an entire Amazon EC2 instance from a single recovery point. A backup job can only have one resource. So you can have a job to back up an EC2 instance, and it will back up the root volume, all data volumes, and the associated instance configurations.

AWS Backup does not reboot EC2 instances at any time.

### Backing Up Amazon EC2 resources

When backing up an Amazon EC2 instance, AWS Backup takes a snapshot of the root Amazon EBS storage volume, the launch configurations, and all associated EBS volumes. AWS Backup stores certain configuration parameters of the EC2 instance, including instance type, security groups, Amazon VPC, monitoring configuration, and tags. The backup data is stored as an Amazon EBS volume-backed Amazon Machine Image (AMI).

You can also back up and restore your VSS-enabled Microsoft Windows applications. You can schedule application-consistent backups, define lifecycle policies, and perform consistent restores as part of an on-demand backup or a scheduled backup plan. For more information, see Creating Windows VSS backups (p. 124).

AWS Backup does not back up the following:

- Configuration of the Elastic Inference accelerator, if it is attached to the instance.
- User data used when the instance was launched.

**Note**

For all instance types, only Amazon EBS-backed EC2 instances are supported. Ephemeral storage instances (that is, instance store-backed instances) are not supported.

When an AWS Backup managed Amazon EC2 AMI (Amazon Machine Image) or Amazon EBS snapshot is deleted via AWS Backup and you have the Amazon EC2 recycle bin configured, the image or snapshot might incur charges per the Amazon EC2 recycle bin policy. Snapshots and images in the Amazon EC2 recycle bin are no longer managed by AWS Backup and will not be managed by AWS Backup policies if you restore them from the recycle bin.

AWS Backup can encrypt EBS snapshots associated with an Amazon EC2 backup. This is similar to how it encrypts EBS snapshots. AWS Backup uses the same encryption applied on the underlying EBS volumes when creating a snapshot of the Amazon EC2 AMI, and the configuration parameters of the original instance are persisted in the restore metadata.

A snapshot derives its encryption from the volume as you have defined, and the same encryption is applied to the corresponding snapshots. EBS snapshots of a copied AMI will always be encrypted. If you use a KMS key during the copy, the key will be applied. If you don't use a KMS key, a default KMS key is applied.
• How to back up resources: Getting started with AWS Backup (p. 24)
• How to restore Amazon EC2 resources: Restoring an Amazon EC2 instance (p. 160)

For detailed information about Amazon EC2, see What is Amazon EC2? in the Amazon EC2 User Guide for Windows Instances.

**Working with Amazon EFS**

AWS Backup supports Amazon Elastic File System (Amazon EFS).

• How to back up resources: Getting started with AWS Backup (p. 24)
• How to restore Amazon EFS resources: Restoring an Amazon EFS file system (p. 153)

For detailed information about Amazon EFS file systems, see What is Amazon Elastic File System? in the Amazon Elastic File System User Guide.

**Working with Amazon EBS**

AWS Backup supports Amazon Elastic Block Store (Amazon EBS) volumes.

• How to back up resources: Getting started with AWS Backup (p. 24)
• How to restore Amazon EBS volumes: Restoring an Amazon EBS volume (p. 151)

For detailed information about Amazon EBS volumes, see What is Amazon Elastic Block Store (Amazon EBS)? in the Amazon EC2 User Guide for Linux Instances.

For more information, see Creating an Amazon EBS Volume in the Amazon EC2 User Guide for Linux Instances.

**Working with Amazon RDS and Aurora**

AWS Backup supports Amazon RDS database engines and Aurora clusters.

• How to back up resources: Getting started with AWS Backup (p. 24)
• How to restore Amazon RDS resources: Restoring an RDS database (p. 157)
• How to restore Aurora clusters: Restoring an Amazon Aurora cluster (p. 158)

For more information about Amazon RDS, see What is Amazon Relational Database Service? in the Amazon RDS User Guide.

For detailed information about Aurora, see What is Amazon Aurora? in the Amazon Aurora User Guide.

**Note**

If you initiate a backup job from the Amazon RDS console, this can conflict with an Aurora clusters backup job, causing the error Backup job expired before completion. If this occurs, configure a longer backup window in AWS Backup.

**Note**

RDS Custom for SQL Server and RDS Custom for Oracle are not currently supported by AWS Backup.

**Note**

AWS does not charge for Aurora snapshots stored inside a backup vault as long as Aurora has automated backups enabled and the retention period for Aurora automated backups is more
than the retention period of Aurora snapshots. Any snapshots within the backup vault will be charged if the snapshots’ database is deleted (deletions may occur accidentally or during blue/green deployment). Large snapshots and frequent backups from a deleted database could result in significant storage charges. Visit the AWS Backup calculator to estimate potential AWS Backup charges.

Working with AWS BackInt

AWS Backup works with AWS Backint to support a preview of SAP HANA database backup and restore on Amazon EC2 instances.

- Instructions to backup and restore SAP HANA resources: Public Preview of SAP HANA Amazon EC2
- Set up AWS Backint Agent: AWS Backint Agent for SAP HANA

Working with AWS Storage Gateway

AWS Backup supports Storage Gateway Volume Gateway. You can also restore Amazon EBS snapshots as Storage Gateway volumes.

- How to back up resources: Getting started with AWS Backup (p. 24)
- How to restore Storage Gateway resources: Restoring a Storage Gateway volume (p. 162).

Working with Amazon DocumentDB

AWS Backup supports Amazon DocumentDB clusters.

- How to back up resources: Getting started with AWS Backup (p. 24)
- How to restore Storage Gateway resources: Restoring a DocumentDB cluster (p. 172).

Working with Amazon Neptune

AWS Backup supports Amazon Neptune clusters.

- How to back up resources: Getting started with AWS Backup (p. 24)
- How to restore Amazon Neptune clusters: Restoring a Neptune cluster (p. 173).

Working with Amazon Timestream

AWS Backup supports Amazon Timestream tables.

- How to backup Timestream tables.
- How to restore Timestream tables.

Working with AWS Organizations

AWS Backup works with AWS Organizations to simplify cross-account monitoring and management

- Create a management account in Organizations.
• Turn on cross-account management.
• Designate delegated administrator accounts and delegate policies.

Working with AWS CloudFormation

AWS Backup support AWS CloudFormation templates and application stacks

• Backing up AWS CloudFormation stacks

Working with AWS BackInt, AWS Systems Manager for SAP, and SAP HANA

AWS Backup works with AWS BackInt and with SSM for SAP to support SAP HANA backup and restore functions.

• SAP HANA databases on Amazon EC2 instances backup
• Get started with SSM for SAP
• Get started with AWS Backint Agent for SAP HANA

How AWS services back up their own resources

You might refer to the technical documentation for a specific AWS service's backup and restore process, particularly when, during a restore, you need to configure a new instance of that AWS service. The following is a list of documentation:

• Amazon EC2 Related Services
• Using AWS Backup with Amazon EFS
• On-Demand Backup and Restore for DynamoDB
• Amazon EBS Snapshots
• Backing Up and Restoring Amazon RDS DB Instances
  • Overview of Backing Up and Restoring an Aurora DB Cluster
• Using AWS Backup with FSx for Windows File Server
• Using AWS Backup with FSx for Lustre
• Backing Up Your Volumes in AWS Storage Gateway
• Backing Up and Restoring in Amazon DocumentDB
• Backing Up and Restoring an Amazon Neptune Cluster

Metering, costs, and billing

AWS Backup pricing

Current AWS Backup prices are available at AWS Backup pricing.

Important
To avoid additional charges, configure your retention policy with a warm storage duration of at least one week.
For example, assume you take daily backups and retain them for one day. Further, assume that your protected resources are so large it takes the entire day to complete your backup. AWS Backup implements your retention period of one day and removes your backup from warm storage when your backup job completes. The next day, AWS Backup cannot create an incremental backup because you have no backup in warm storage. Since this retention period did not follow best practices, you run the risk and expense of creating a full backup every day. Ask your technical account manager or solutions architect for guidance around your use case.

### AWS Backup billing

When a resource type supports full AWS Backup management, charges for AWS Backup activity (including storage, data transfers, restores, and early deletion) appear in the "Backup" section of your Amazon Web Services bill. For a list of services that support full AWS Backup management, see the Full AWS Backup management section in the Feature availability by resource (p. 2) table.

When a resource type does not support full AWS Backup management, some of your AWS Backup activity, such as storage costs for your backups, might be and billed by the respective AWS service.

**Copy job failures**

You will only be charged once a recovery point has been created in the destination vault. There is no charge when a copy job fails and no recovery point is created.

**Cost allocation tags**

You can use cost allocation tags to track and optimize AWS Backup costs on a detailed level, and view and filter those tags using AWS Cost Explorer (note this functionality is not currently supported for DynamoDB).

To use cost allocation tags, see Automating backups and optimizing backup costs for Amazon EFS using AWS Backup and Using Cost Allocation Tags.

### AWS Backup Audit Manager pricing

AWS Backup Audit Manager charges for usage based on the number of control evaluations. A control evaluation is the evaluation of one resource against one control. Control evaluation charges appear on your AWS Backup bill. For current control evaluation pricing, see AWS Backup pricing.

To use AWS Backup Audit Manager controls, you must enable AWS Config recording to track your backup activity. AWS Config charges for each configuration item recorded, and these charges appear on your AWS Config bill. For current configuration item recorded pricing, see AWS Config pricing.

### Amazon Aurora pricing

AWS Backup currently does not support direct integration with Aurora continuous backups. AWS Backup supports Aurora database cluster snapshots, billed as incremental or full backups. During the configured retention period for Aurora continuous backups (up to 35 days), account is billed incrementally for the continuous backup and snapshots are free of charge. Snapshots retained past this window are charged as full backups.

### AWS Backup blogs, videos, tutorials, and other resources

For more information about AWS Backup, see the following:
• **Backup and restore on-premises VMware virtual machines using AWS Backup**, With Olumuyiwa Koya and Ezekiel Oyerinde (June 2022).

• **Using AWS Backup to protect Amazon Aurora databases**, With Chris Hendon, Brandon Rubadou, and Thomas Liddle (May 2022).

• **Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups**, With Evan Peck and Sabith Venkitachalapathy (May 2022).


• **Obtain aggregated daily cross-account multi-Region AWS Backup reporting**, With Wali Akbari and Sabith Venkitachalapathy (Feb. 2022).


• **Optimizing SAS Grid on AWS with FSx for Lustre (and optimizing disaster recovery using AWS Backup)**, With Matt Saeger and Shea Lutton (Jan. 2022).

• **Centralizing data protection and compliance in Amazon Neptune with AWS Backup**, With Brian O’Keefe (Nov. 2021).

• **Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup**, With Karthik Vijayaraghavan (Nov. 2021).

• **Simplify auditing your data protection policies with AWS Backup Audit Manager**, With Jordan Bjorkman and Harshitha Putta (Nov. 2021).

• **Enhance the security posture of your backups with AWS Backup Vault Lock**, With Rolland Miller (Oct. 2021).


• **Managing access to backups using service control policies with AWS Backup**, With Sabith Venkitachalapathy and Ibukun Oyewumi (Aug. 2021).

• **Automate centralized backup at scale across AWS services using AWS Backup**, With Ibukun Oyewumi and Sabith Venkitachalapathy (Jul. 2021).


• **Automate data recovery validation with AWS Backup**, With Mahanth Jayadeva (Jun. 2021).

• **Configuring notifications to monitor AWS Backup jobs**, With Virgil Ennes (Jun. 2021).


• **Manage Amazon EFS backup costs: AWS Backup support for cost allocation tags**, With Aditya Maruvada (May 2021).

• **Create and share encrypted backups across accounts and Regions using AWS Backup**, With Prachi Gupta (May 2021).

• **AWS Backup is now FedRAMP High approved for your compliance and data protection needs**, With Andy Grimes (May 2021).

• **ZS Associates enhances backup efficiency with AWS Backup**, With Mitesh Naik, Hiranand Mulchandani, and Sushant Jadhav (May 2021).


• **Cross-region and cross-account backups for Amazon FSx using AWS Backup**, With Adam Hunter and Fathima Kamal (Apr. 2021).

• **Amazon CloudWatch Events and Metrics for AWS Backup**, With Rolland Miller (Mar. 2021).
• **Point-in-time recovery and continuous backup for Amazon RDS with AWS Backup.** With Kelly Griffin (Mar. 2021).
• **Automate AWS Backup with AWS Service Catalog.** with John Husemoller (Jan. 2021).
• **Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup.** With Cher Simon (Jan. 2021).
• **AWS re:Invent recap: Data protection and compliance with AWS Backup.** With Nancy Wang (Dec. 2020).
• **AWS Backup provides centralized data protection across your AWS resources.** With Nancy Wang (Nov. 2020).
• **Tech Talk: Data protection at scale with AWS Backup.** With Kareem Behairy (Sep. 2020).
• **Centralized cross-account management with cross-Region copy using AWS Backup.** With Cher Simon (Sep. 2020).
• **Video Tutorial: Managing backups at scale in your AWS Organizations using AWS Backup.** With Ildar Sharafeev (Jul. 2020).
• **Managing backups at scale in your AWS Organizations using AWS Backup.** With Nancy Wang, Avi Drabkin, Ganesh Sundaresan, and Vikas Shah (Jun. 2020).
• **Recover Amazon EFS files and folders with AWS Backup.** With Abrar Hussain and Gurudath Pai (May 2020).
• **Scheduling automated backups using Amazon EFS and AWS Backup.** With Rob Barnes (Dec. 2019).
• **Protecting your data with AWS Backup.** With Anthony Fiore (Jul. 2019).
• **Video: Introduction to AWS Backup.** With AWS Training and Certification.
Setting up AWS for the first time

Before you use AWS Backup for the first time, complete the following tasks:

1. Sign up for AWS (p. 21)
2. Create an IAM user (p. 21)
3. Create an IAM role (p. 22)

Sign up for AWS

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including AWS Backup. You are charged only for the services that you use.

For more information about AWS Backup usage rates, see the AWS Backup Pricing page.

If you have an AWS account already, skip to the next task. If you don’t have an AWS account, use the following procedure to create one.

To create an AWS account

2. Follow the online instructions.
   - Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.
   - When you sign up for an AWS account, an AWS account root user is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to an administrative user, and use only the root user to perform tasks that require root user access.

Note your AWS account number, because you’ll need it for the next task.

Create an IAM user

Services in AWS, such as AWS Backup, require that you provide credentials when you access them, so that the service can determine whether you have permissions to access its resources. AWS recommends that you do not use the AWS account root user to make requests. Instead, create an IAM user, and grant that user full access. We refer to these users as administrator users. You can use the admin user credentials, instead of the AWS account root user credentials, to interact with AWS and perform tasks, such as create a bucket, create users, and grant them permissions. For more information, see AWS account Root User Credentials vs. IAM User Credentials in the AWS General Reference and IAM Best Practices in the IAM User Guide.

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console.

To create an administrator user, choose one of the following options.
Choose one way to manage your administrator

<table>
<thead>
<tr>
<th>To</th>
<th>By</th>
<th>You can also</th>
</tr>
</thead>
<tbody>
<tr>
<td>In IAM Identity Center (Recommended)</td>
<td>Use short-term credentials to access AWS.</td>
<td>Following the instructions in Getting started in the AWS IAM Identity Center (successor to AWS Single Sign-On) User Guide.</td>
</tr>
<tr>
<td>In IAM (Not recommended)</td>
<td>Use long-term credentials to access AWS.</td>
<td>Following the instructions in Creating your first IAM admin user and user group in the IAM User Guide.</td>
</tr>
</tbody>
</table>

To sign in as this new IAM user, sign out of the AWS Management Console. Then use the following URL, where your_aws_account_id is your AWS account number without the hyphens (for example, if your AWS account number is 1234-5678-9012, your AWS account ID is 123456789012):

https://your_aws_account_id.signin.aws.amazon.com/console/

Enter the IAM user name and password that you just created. When you’re signed in, the navigation bar displays your_user_name@your_aws_account_id.

If you don’t want the URL for your sign-in page to contain your AWS account ID, you can create an account alias. From the IAM dashboard, click Create Account Alias and enter an alias, such as your company name. To sign in after you create an account alias, use the following URL:

https://your_account_alias.signin.aws.amazon.com/console/

To verify the sign-in link for IAM users for your account, open the IAM console and check under AWS account Alias on the dashboard.

Create an IAM role

You can use the IAM console to create an IAM role that grants AWS Backup permissions to access supported resources. After you create the IAM role, you will create and attach policies to the role.

To create an IAM role with the console

1. Sign in to the AWS Management Console and open the IAM console.
2. In the IAM console, choose Roles in the navigation pane, and choose Create role.
3. Choose AWS Service Roles, and then choose Select for AWS Backup. Choose Next: Permissions.
4. On the **Attach permissions policies** page, check both AWSBackupServiceRolePolicyForBackup, and AWSBackupServiceRolePolicyForRestores. These AWS managed policies grant AWS Backup permission to back up and restore all supported AWS resources. To learn more about managed policies and view examples, see [Managed Policies](#).

Then, choose **Next: Tags**.

5. Choose **Next: Review**.

6. For **Role Name**, type a name that describes the purpose of this role. Role names must be unique within your AWS account. Because various entities might reference the role, you cannot edit the name of the role after you create it.

   Choose **Create Role**.

7. On the Roles page, choose the role that you created to open its details page.
Getting started with AWS Backup

This tutorial shows you the generic steps for using AWS Backup features and functionality. As with any part of this technical documentation, you should follow along with the AWS Management Console in the other window.

You can also learn how to use AWS Backup with a specific service by reading these tutorials:

- Amazon Relational Database Service (Amazon RDS) Backup and Restore using AWS Backup
- Tutorial: Amazon EBS Backup and Restore using AWS Backup

Topics

- Prerequisites (p. 24)
- Getting started 1: Service Opt-in (p. 25)
- Getting started 2: Create an on-demand backup (p. 25)
- Getting started 3: Create a scheduled backup (p. 27)
- Getting started 4: Create Amazon EFS automatic backups (p. 29)
- Getting started 5: View your backup jobs and recovery points (p. 30)
- Getting started 6: Restore a backup (p. 31)
- Getting started 7: Create an audit report (p. 32)
- Getting started 8: Clean up resources (p. 34)

Prerequisites

Before you begin, ensure that you have the following:

- An AWS account. For more information, see Setting up AWS for the first time (p. 21).
- At least one resource supported by AWS Backup.
- You should be familiar with the AWS services and resources that you are backing up. See the list of supported AWS resources and third-party applications.

When new AWS services become available, enable AWS Backup to use those services.

To configure the AWS services to use with AWS Backup

2. In the navigation pane, choose Settings.
3. On the Service opt-in page, choose Configure resources.
4. On the Configure resources page, use the toggle switches to enable or disable the services that are used with AWS Backup. Choose Confirm when your services are configured. Make sure that the AWS service you're opting in is available in your AWS Region. For information about supported Regions, see Service endpoints and quotas in the AWS General Reference.
Note
If you set up automatic backups after enabling Amazon EFS for AWS Backup, your automatic backups will continue even if you opt out or disable Amazon EFS for AWS Backup. For more information, see Getting started 4: Create Amazon EFS automatic backups (p. 29). To disable automatic backups, use the Amazon EFS console or API.

- Make sure that the resources you're backing up are all in the same AWS Region.

To complete this tutorial, you can use your AWS account root user to sign in to the AWS Management Console. However, AWS Identity and Access Management (IAM) recommends that you not use the AWS account root user. Instead, create an administrator in your account and use those credentials to manage resources in your account. For more information, see Setting up AWS for the first time (p. 21).

The AWS Backup console provides different options to back up your resources. You can create a backup on-demand, schedule and configure how you want the resource backed up, or configure resources to back up automatically when the resource is created.

Getting started 1: Service Opt-in

To use AWS Backup to protect some AWS services, you must affirmatively opt in. For example, you must opt in to have AWS Backup manage Amazon EC2 AMIs and Amazon EBS snapshots. Opt-in choices apply to the specific account and AWS Region, so you might have to opt in to multiple Regions using the same account.

As AWS Backup supports more and more AWS services and third-party applications, you might need to revisit this step to opt in to those newly-supported resources.

If you do not opt in, AWS Backup does not govern backups you take in your AWS environment outside of AWS Backup.

To opt in to use AWS Backup to protect all supported resource types

2. In the left navigation pane, choose Settings.
3. Under Service opt-in, choose Configure resources.
4. Opt in to all AWS Backup-supported Resources by moving all the toggles to the right.
5. Choose Confirm.

Next steps

To create an on-demand backup using AWS Backup, proceed to Getting started 2: Create an on-demand backup (p. 25).

Getting started 2: Create an on-demand backup

On the AWS Backup console, the Protected resources page lists resources that have been backed up by AWS Backup at least once. If you’re using AWS Backup for the first time, there aren’t any resources, such as Amazon EBS volumes or Amazon RDS databases, listed on this page. This is true even if that resource was assigned to a backup plan if that backup plan has not run a scheduled backup job at least once.
In this first step, you create an on-demand backup of one of your resources. You will then see this resource listed on the Protected resources page.

**To create an on-demand backup**

2. Using the navigation pane, choose Protected resources, and then Create on-demand backup.
3. On the Create on-demand backup page, choose the resource type that you want to back up; for example, choose DynamoDB for Amazon DynamoDB tables.
4. Choose the name or ID of the resource that you want to protect. Make sure that the resource you chose is the one you want.
   
   **Note**
   
   For Amazon FSx for Lustre, Persistent and Persistent_2 deployment types are supported.
5. Ensure that Create backup now is selected. This initiates a backup immediately and enables you to see your saved resource sooner on the Protected resources page.
6. Specify a transition to cold storage value (if appropriate) and an expire value.
   
   **Note**
   
   - To see the list of resources that you can transition to cold storage, see the "Lifecycle to cold storage" section of the Feature availability by resource (p. 2) table. All other resource types are saved to warm storage, and ignore the transition to cold storage expression. The Expire value is valid for all resource types.
   - When backups expire and are marked for deletion as part of your lifecycle policy, AWS Backup deletes the backups at a randomly chosen point over the following 8 hours. This window helps ensure consistent performance.
7. Choose an existing backup vault. Choosing Create new backup vault opens a new page to create a vault and then returns you to the Create on-demand backup page when you are finished.
8. Under IAM role, choose Default role.
   
   **Note**
   
   If the AWS Backup default role is not present in your account, a role is created for you with the correct permissions.
9. If you want to assign one or more tags to your on-demand backup, enter a key and optional value, and choose Add tag.
   
   **Note**
   
   - For Amazon EC2 resources, AWS Backup automatically copies existing group and individual resource tags, in addition to any tags that you add to this backup. For more information, see Copying tags onto backups (p. 125).
   - When creating a tag-based backup plan, if you choose a role other than Default role, make sure that it has the necessary permissions to back up all tagged resources. AWS Backup tries to process all resources with the selected tags. If it encounters a resource that it doesn't have permission to access, the backup plan fails.
10. Choose Create on-demand backup. This takes you to the Jobs page, where you will see a list of jobs.
11. If your resource type is EC2, the Advanced backup settings section will appear. Choose Windows VSS if your EC2 instance is running Microsoft Windows. This enables you to take application-consistent Windows VSS backups.
   
   **Note**
   
   AWS Backup currently supports application-consistent backups of resources running on Amazon EC2 only. Not all instance types or applications are supported for Windows VSS backups. For more information, see Creating Windows VSS backups (p. 124).
12. Choose the Backup job ID for the resource that you chose to back up to see the details of that job.
Next steps

To automate your backup activity, proceed to Getting started 3: Create a scheduled backup (p. 27).

Getting started 3: Create a scheduled backup

In this step of the AWS Backup tutorial, you create a backup plan, assign resources to it, and then create a backup vault.

Before you begin, ensure that you have the required prerequisites. For more information, see Getting started with AWS Backup (p. 24).

Topics
- Step 1: Create a backup plan based on an existing one (p. 27)
- Step 2: Assign resources to a backup plan (p. 28)
- Step 3: Create a backup vault (p. 28)
- Next steps (p. 29)

Step 1: Create a backup plan based on an existing one

A backup plan is a policy expression that defines when and how you want to back up your AWS resources, such as Amazon DynamoDB tables or Amazon Elastic File System (Amazon EFS) file systems. You assign resources to backup plans, and AWS Backup then automatically backs up and retains backups for those resources according to the backup plan. For more information, see Managing backups using backup plans (p. 36).

There are two ways to create a new backup plan: You can build one from scratch or build one based on an existing backup plan. This example uses the AWS Backup console to create a backup plan by modifying an existing backup plan.

To create a backup plan from an existing one

2. From the dashboard, choose Manage Backup plans. Or, using the navigation pane, choose Backup plans and choose Create Backup plan.
3. Choose Start with template, choose a plan from the list (for example, Daily-Monthly-1yr-Retention), and enter a name in the Backup plan name box.
   
   **Note**
   If you try to create a backup plan that is identical to an existing plan, you get an AlreadyExistsException error.

4. On the plan summary page, choose the backup rule you want and then choose Edit.
5. Review and choose the values that you want for your rule. For example, you can extend the retention period of the backup in the Monthly rule to three years instead of one year. If your plan includes Amazon EFS backups, you can configure lifecycle policies that automatically transition these backups from warm storage to cold storage according to a schedule that you define.
6. For the backup vault, choose Default or choose Create new Backup vault to create a new vault.
7. (Optional) Choose an AWS Region from the list in **Destination region** to copy the backup to different Region. To add more Regions, choose **Add copy**.

8. When you have finished editing the rule, choose **Save Backup rule**.

On the **Summary** page, choose **Assign resources** to prepare for the next section.

**Step 2: Assign resources to a backup plan**

After you create a backup plan, you must assign your AWS resources to that backup plan. For more information about assigning resources, see Assigning resources to a backup plan (p. 43).

If you don’t already have existing AWS resources that you want to assign to a backup plan, create some new resources to use for this exercise. Create one or two resources using supported AWS resources and third-party applications.

**To assign resources to a backup plan**

1. The previous steps should have taken you to the **Assign resources** page.
2. Type in a **Resource assignment name**.
3. For IAM role, choose **Default role**. If you choose another role, it must have permissions to back up all the resources you assign.
4. In the **Assign resources** section, choose **Include all resource types**. A **resource type** is an AWS Backup-supported AWS service or third-party application. This backup plan will now protect all resource types that you have opted in to protect using AWS Backup.
5. Choose **Assign resources**.

You return to the backup plan **Summary** page. Choose **Create backup plan** to deploy your first backup plan!

**Step 3: Create a backup vault**

Instead of using the default backup vault that is automatically created for you on the AWS Backup console, you can create specific backup vaults to save and organize groups of backups in the same vault.

For more information about backup vaults, see Backup vaults (p. 54).

**To create a backup vault**

1. On the AWS Backup console, in the navigation pane, choose **Backup vaults**.
   
   **Note**
   
   If the navigation pane is not visible on the left side, you can open it by choosing the menu icon in the upper-left corner of the AWS Backup console.

2. Choose **Create backup vault**.
3. Enter a name for your backup vault. You can name your vault to reflect what you will store in it, or to make it easier to search for the backups you need. For example, you could name it **FinancialBackups**.
4. Select an AWS Key Management Service (AWS KMS) key. You can use either a key that you already created, or select the default AWS Backup KMS key.
   
   **Note**
   
   The AWS KMS key that is specified here applies only to backups of services that support AWS Backup independent encryption. To see the list of resource types that support AWS KMS encryption, see List of resource types that support AWS KMS encryption.
Backup independent encryption, see the "Full AWS Backup management" section of the Feature availability by resource (p. 2) table.

5. Optionally, add tags that will help you search for and identify your backup vault. For example, you could add a **BackupType:Financial** tag.

6. Choose **Create Backup vault**.

7. In the navigation pane, choose **Backup vaults**, and verify that your backup vault has been added.

**Note**
You can now edit a backup rule in one of your backup plans to store backups created by that rule in the backup vault you just created.

**Next steps**

To back up Amazon EFS file systems specifically, proceed to [Getting started 4: Create Amazon EFS automatic backups](p. 29).

---

**Getting started 4: Create Amazon EFS automatic backups**

When you create an Amazon Elastic File System (Amazon EFS) file system using the Amazon EFS console, automatic backups are turned on by default. If you want to automatically back up an existing Amazon EFS file system, you can do so using the Amazon EFS console, API, or CLI.

**To automatically back up an existing Amazon EFS file system using the console**

2. On the **File systems** page, choose a file system to turn on automatic backups.
3. Choose **Edit** in the **General** settings panel.
4. To turn on automatic backups, choose **Enable automatic backups**.

The default backup plan setting is **daily** backups, **35-day retention**. The default backup window (the time frame when the backup will run) is set to start at 5 AM UTC (Coordinated Universal Time) and lasts 8 hours.

**Note**
The Amazon EFS automatic backup vault aws/efs/automatic-backup-vault is reserved for those automatic backups only. If you use it as a destination for other backup plans, you will receive an "insufficient privileges" error.

AWS Backup creates a service-linked role on your behalf in your account. This role has the permissions required to perform Amazon EFS backups. For detailed information about service-linked roles, see [Using service-linked roles for AWS Backup](p. 333).

For step-by-step instructions on how to turn automatic backups on or off using the Amazon EFS console, API, or CLI, see [Automatic backups](https://docs.aws.amazon.com/efs/latest/ug/automated-backups.html) in the [Amazon Elastic File System User Guide](https://docs.aws.amazon.com/efs/latest/ug/)

**Next steps**

To view the backups that you've created, proceed to [Getting started 5: View your backup jobs and recovery points](p. 30).
Getting started 5: View your backup jobs and recovery points

With AWS Backup, you can view the status and other details of backup and restore activity across the AWS services that you use.

On the AWS Backup dashboard, you can manage backup plans, create on-demand backups, restore backups, and view the status of backup and restore jobs.

Topics
- View the status of backup jobs (p. 30)
- View all backups in a vault (p. 30)
- View details of protected resources (p. 30)
- Next steps (p. 31)

View the status of backup jobs

Use the AWS Backup dashboard to quickly view the status of your backup and restore activity.

To view backup job status

2. In the navigation pane, choose Dashboard.
3. To view the status of your backup jobs, choose Backup jobs details. This takes you to the Backup jobs page, where you can view tables containing backup jobs and restore jobs.
4. You can filter the jobs that are displayed by time. For example, jobs created in the last 24 hours, the last week, or the last 30 days. You can also set the number of jobs to display per page by choosing the gear icon.

View all backups in a vault

Follow these steps to view the backups that were created in a specified vault in AWS Backup.

To view all backups in a vault

1. On the AWS Backup console, in the navigation pane, choose Backup vaults.
2. Choose the vault that you used when creating an on-demand or scheduled backup, and view all the backups that were created in this vault.

Note
Each backup has a Status, which is usually Completed. If for some reason AWS Backup can't delete a backup according to its lifecycle configuration, it marks this backup as Expired. You are billed for the storage that Expired backups consume and should delete them.

View details of protected resources

On the Protected resources page, you can explore details of the resources that are backed up in AWS Backup.
To view protected resources

1. On the AWS Backup console, in the navigation pane, choose **Protected resources**.
2. View the AWS resources that are being backed up. Choose a resource in the list to explore your backups for that resource.

Next steps

To restore a recovery point that you have viewed, proceed to **Getting started 6: Restore a backup** (p. 31).

Getting started 6: Restore a backup

After a resource has been backed up at least once, it is considered protected and is available to be restored using AWS Backup. Follow these steps to restore a resource using the AWS Backup console.

For information about restore parameters for specific services, or restoring a backup using the AWS CLI or the AWS Backup API, see **Restoring a Backup**.

To restore a resource

2. In the navigation pane, choose **Protected resources** and the resource ID you want to restore.
3. A list of your recovery points, including the resource type, is displayed by **Resource ID**. Choose a resource to open the **Resource details** page.
4. To restore a resource, in the **Backups** pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose **Restore**.
5. Specify the restore parameters. The restore parameters shown are specific to the resource type that is selected.
   
   **Note**
   
   If you only keep one backup, you can only restore to the state of the file system at the time you took that backup. You can’t restore to prior incremental backups.

   For instructions on how to restore specific resources, see **Restoring a backup**.

6. For **Restore role**, choose **Default role**.
   
   **Note**
   
   If the AWS Backup default role is not present in your account, a role is created for you with the correct permissions.

7. Choose **Restore backup**.

   The **Restore jobs** pane appears. A message at the top of the page provides information about the restore job.

   **Note**
   
   When you perform a restore to restore specific items within an Amazon EFS instance, you can restore those items to either a new or an existing file system. If you restore the items to an existing file system, AWS Backup creates a new Amazon EFS directory off of the root directory to contain the items. The full hierarchy of the specified items is preserved in the recovery directory. For example, if directory A contains subdirectories B, C, and D, AWS Backup retains the hierarchical structure when A, B, C, and D are recovered.
Regardless of whether you perform an Amazon EFS partial restore to an existing file system or to new file system, each restore attempt creates a new recovery directory off of the root directory to contain the restored files. If you attempt multiple restores for the same path, several directories containing the restored items might exist.

To restore an Amazon EFS instance

If you are restoring an Amazon EFS instance, you can perform a Full restore, which restores the entire file system. Or, you can restore specific files and directories using Item-level restore (item-level restores have limits. See Restoring an EFS file system for more information). For information about restoring other types of resources, see Restoring a backup.

Note
To restore an Amazon EFS instance, you must "Allow" backup:startrestorejob.

For detailed information about restoring a backup, see Restoring a backup (p. 139).

Next steps

With AWS Backup Audit Manager, you can audit your backup activity and resources. You can also create reports that you can use as evidence of your backup, restore, and copy jobs. To create a report, see Getting started 7: Create an audit report (p. 32).

Getting started 7: Create an audit report

In Getting started 5: View your backup jobs and recovery points (p. 30), you observed your backup activity in the AWS Backup Dashboard, Backup vault, and Protected Resources views. However, these views are dynamic and will update depending on when you visit them. These views are not necessarily the best evidence of continued compliance with your organizational data protection requirements and controls across time.

In this step, you will create an on-demand backup job report using AWS Backup Audit Manager.

AWS Backup Audit Manager delivers a variety of audit reports in CSV, JSON, or both formats daily and on-demand to your Amazon S3 bucket. You can audit the compliance of your backup activity and resources against a number of customizable controls. You can receive reports on your backup, copy, and restore jobs. The backup job report is evidence that your backup jobs took place.

The following is an example of a backup plan.

```json
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC00000",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7700000",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e6abcde",
      "creationDate": "2021-07-14T23:53:47.229Z",
      "completionDate": "2021-07-15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5aabcde",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 8589934592,
      "backupVaultName": "Default"
    }
  ]
}
```
To create a backup report (including an on-demand backup report), you first create a report plan to automate your reports and deliver them to an Amazon S3 bucket.

A report plan requires that you have an Amazon S3 bucket to receive your reports. For instructions on setting up a new S3 bucket, see Step 1: Create your first S3 bucket in the Amazon Simple Storage Service User Guide.

To create a report plan

2. In the left navigation pane, choose Reports.
3. Choose Create report plan.
4. Select Backup job report from the dropdown list.
5. For Report plan name, enter TestBackupJobReport.
6. For File format, choose both CSV and JSON.
7. For S3 bucket name, select the destination for your reports from the dropdown list.
8. Choose Create report plan.

Next, you must allow your S3 bucket to receive report from AWS Backup. AWS Backup Audit Manager automatically generates an S3 access policy for you.

To view and apply this access policy

1. In the left navigation pane, choose Reports.
2. Under Report plan name, choose the name of your report plan (TestBackupJobReport).
3. Choose Edit.
4. Choose View access policy for S3 bucket.
5. Choose Copy permissions.
6. Choose Edit bucket policy to edit your destination S3 bucket's policy to allow it to receive your backup job reports.
7. Copy or add the permissions to the destination S3 bucket policy.

Next, create your first backup job report.

To create an on-demand backup report

1. In the left navigation pane, choose Reports.
2. Under Report plan name, choose the name of your report plan (TestBackupJobReport).
3. Choose Create on-demand report.

Finally, view your report.

To view your report

1. In the left navigation pane, choose Reports.
2. Under **Report plan name**, choose the name of your report plan (`TestBackupJobReport`).
3. In the **Report jobs** section, choose the **S3 link**. Doing so takes you to your destination S3 bucket.
4. Choose **Download**.
5. Open the report using the program that you use to work with CSV or JSON files.

## Next steps

To clean up your getting started resources and avoid unwanted charges, proceed to **Getting started 8: Clean up resources** (p. 34).

### Getting started 8: Clean up resources

After you perform all the tasks in **Getting started with AWS Backup** (p. 24), you might want to clean up what you have created to avoid incurring any unnecessary charges.

**Topics**

- Step 1: Delete restored AWS resources (p. 34)
- Step 2: Delete the backup plan (p. 34)
- Step 3: Delete the recovery points (p. 35)
- Step 4: Delete the backup vault (p. 35)
- Step 5: Delete the report plan (p. 35)
- Step 6: Delete the reports (p. 35)

### Step 1: Delete restored AWS resources

To delete AWS resources that you restored from a recovery point, such as Amazon Elastic Block Store (Amazon EBS) volumes or Amazon DynamoDB tables, you use the console for that service. For example, to delete an Amazon Elastic File System (Amazon EFS) file system, use the Amazon EFS console.

**Note**

This information refers to restored resources, not to recovery points stored in a backup vault.

### Step 2: Delete the backup plan

If you don’t want to create scheduled backups, you should delete your backup plans. Before you can delete a backup plan, you must delete all resource assignments to that backup plan.

Follow these steps to delete a backup plan:

**To delete a backup plan**

2. In the navigation pane, choose **Backup plans**.
3. On the **Backup plans** page, choose the backup plan that you want to delete. This takes you to the details page for that backup.
4. To delete the resource assignments for your plan, choose the radio button next to the assignment name, and then choose **Delete**.
5. To delete the backup plan, choose **Delete** in the upper-right corner of the page.
6. On the confirmation page, enter the plan name, and choose **Delete plan**.
Step 3: Delete the recovery points

Next, you can delete the backup recovery points that are in your backup vault.

To delete the recovery points

1. On the AWS Backup console, in the navigation pane, choose Backup vaults.
2. On the Backup vaults page, choose the backup vault where you stored the backups.
3. Check the recovery point and choose Delete.
4. If you are deleting more than one recovery point, follow these steps:
   a. If your list contains a continuous backup, choose whether to keep or delete your continuous backup data.
   b. To delete all the recovery points listed, type delete, and then choose Delete recovery points.

Keep your browser tab open until you see the green success banner at the top of the page. Prematurely closing this tab will end the deletion process and might leave behind some of the recovery points you wanted to delete. For more information, see Deleting backups.

Step 4: Delete the backup vault

You can't delete the default backup vault in AWS Backup. However, if you created a different backup vault, empty the backup vault by deleting the backups. Then select the backup vault and choose Delete.

Step 5: Delete the report plan

Your report plan automatically sends a new report daily. To prevent this, delete the report plan.

To delete the report plan

1. On the AWS Backup console, in the navigation pane, choose Reports.
2. Under Report plan name, choose the name of your report plan.
3. Choose Delete.
4. Enter your report plan name, and choose Delete report plan.

Step 6: Delete the reports

You can delete your reports by following the instructions for Deleting a single object for each of your reports. If you no longer need your destination S3 bucket, after deleting all the objects from the bucket, you can delete the bucket by following the instructions for Deleting a bucket.
Managing backups using backup plans

In AWS Backup, a backup plan is a policy expression that defines when and how you want to back up your AWS resources, such as Amazon DynamoDB tables or Amazon Elastic File System (Amazon EFS) file systems. You can assign resources to backup plans, and AWS Backup automatically backs up and retains backups for those resources according to the backup plan. You can create multiple backup plans if you have workloads with different backup requirements.

AWS Backup efficiently stores your periodic backups incrementally. The first backup of an AWS resource backs up a full copy of your data. For each successive incremental backup, only the changes to your AWS resources are backed up. Incremental backups enable you to benefit from the data protection of frequent backups while minimizing storage costs.

AWS Backup also seamlessly manages your backup chain, allowing you to restore at any time. This includes after your backup plan's lifecycle automatically deletes your only full backup because it has exceeded the retention period you defined.

The following sections provide the basics of managing your backup strategy in AWS Backup.

Topics
- Creating a backup plan (p. 36)
- Assigning resources to a backup plan (p. 43)
- Deleting a backup plan (p. 53)
- Updating a backup plan (p. 53)

Creating a backup plan

You can create a backup plan using the AWS Backup console, API, CLI, SDK, or an AWS CloudFormation template.

Topics
- Creating backup plans using the AWS Backup console (p. 36)
- Creating backup plans using a JSON document and the AWS Backup CLI (p. 37)
- Backup plan options and configuration (p. 37)
- AWS CloudFormation templates for backup plans (p. 41)

Creating backup plans using the AWS Backup console

AWS Backup provides different ways to get started using the AWS Backup console:

- Start from an existing plan — You can create a new backup plan based on the configurations in an existing plan. Existing plans provided by AWS Backup are based on best practices and common backup policy configurations. When you select an existing backup plan to start from, the configurations from that backup plan are automatically populated for your new backup plan. You can then change any of these configurations according to your backup requirements.
Creating backup plans using a JSON document and the AWS Backup CLI

You can also define your backup plan in a JSON document and provide it using the AWS Backup console or AWS CLI. The following JSON document contains a sample backup plan that creates backups hourly on the hour. It automatically deletes a backup after retaining it for one year.

```
{
  "BackupPlan":{
    "BackupPlanName":"test-plan",
    "Rules": [
      {
        "RuleName":"test-rule",
        "TargetBackupVaultName":"test-vault",
        "ScheduleExpression":"cron(15 * * * *)",
        "StartWindowMinutes":60,
        "CompletionWindowMinutes":600,
        "Lifecycle":{
          "DeleteAfterDays":365
        }
      }
    ]
  }
}
```

Assuming you store the preceding JSON document as test-backup-plan.json, You can use the following CLI command to create it in AWS Backup.

```
aws backup create-backup-plan --cli-input-json file:///PATH-TO-FOLDER/test-backup-plan.json
```

Backup plan options and configuration

When you define a backup plan in the AWS Backup console, you configure the following options:

**Backup plan name**

You must provide a unique backup plan name.

If you choose name that is identical to the name of an existing plan, you will receive an error message.

**Backup rules**

Backup plans are composed of one or more backup rules. To add backup rules to a backup plan, or to edit existing rules in a backup plan:
1. From the AWS Backup console, in the left navigation pane, choose **Backup plans**.
2. Under **Backup plan name**, select a backup plan.
3. Under the **Backup rules** section:
   - To add a backup rule, choose **Add backup rule**.
   - To edit an existing backup rule, select a rule, then choose **Edit**.

**Note**
If you have a backup plan with multiple rules if the time frame of the two rules overlap, AWS Backup optimizes the backup and takes a backup for the rule with the longer retention time. The optimization takes into account the full start window, not just when the daily backup is taken.

Each backup rule consists of the following elements.

**Backup rule name**
Backup rule names are case sensitive. They must contain from 1 to 50 alphanumeric characters or hyphens.

**Backup frequency**
The backup frequency determines how often AWS Backup creates a snapshot backup. Using the console, you can choose a frequency of every hour, 12 hours, daily, weekly, or monthly. You can also create a cron expression that creates snapshot backups as frequently as hourly. Using the AWS Backup CLI, you can schedule snapshot backups as frequently as hourly.

If you select weekly, you can specify which days of the week you want backups to be taken. If you select monthly, you can choose a specific day of the month.

You can also check the **Enable continuous backups for supported resources** checkbox to create a point-in-time restore (PITR)-enabled continuous backup rule. Unlike snapshot backups, continuous backups allow you to perform point-in-time restore. To learn more about continuous backups, see **Point-in-Time Recovery**.

**Backup window**
Backup windows consist of the time that the backup window begins and the duration of the window in hours. Backup jobs are started within this window. If you are unsure what backup window to use, you can choose to use the default backup window that AWS Backup recommends. The default backup window is set to start at 5 AM UTC (Coordinated Universal Time) and lasts 8 hours.

**Note**
You can customize the backup frequency and backup window start time using a cron expression. To see the six fields of AWS cron expressions, see **Schedule Expressions for Rules** in the *Amazon CloudWatch Events User Guide*. Two examples of AWS cron expressions are `15 * ? * * *` (take a backup every hour at 15 minutes past the hour) and `0 12 * * ? *` (take a backup every day at 12 noon UTC). For a table of examples, click the preceding link and scroll down the page.

AWS Backup evaluates cron expressions between 00:00 and 23:59 UTC. If you create a backup rule for "every 12 hours" but provide a start time of later than 11:59, it will only run once per day.

**Note**
In general, AWS database services cannot start backups 1 hour before or during their maintenance window and Amazon FSx cannot start backups 4 hours before or during their maintenance window or automatic backup window (Amazon Aurora is exempt from this maintenance window restriction). Snapshot backups scheduled during those times will fail. One
exception: when you opt in to using AWS Backup for both snapshot and continuous backups for a supported service, you no longer need to worry about those windows because AWS Backup will schedule them for you. See Point-in-Time Recovery for a list of supported services and instructions on how to use AWS Backup to take continuous backups.

Overlapping backup rules

On occasion, a backup plan might contain multiple, overlapping rules. When the start windows of different rules overlap, AWS Backup retains the backup under the rule with the longer retention period. For example, consider a backup plan with two rules:

1. Backup hourly, with a 1-hour start window, and retain for 1 day.
2. Backup every 12 hours, with an 8-hour start window, and retain for 1 week.

After 24 hours, the second rule creates two backups (because it has the longer retention period). The first rule creates eight backups (because the second rule's 8-hour start window prevented more hourly backups from running). Specifically:

<table>
<thead>
<tr>
<th>During this Start Window</th>
<th>This Rule Creates 1 Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midnight to 8AM</td>
<td>12 hours</td>
</tr>
<tr>
<td>8 to 9</td>
<td>Hourly</td>
</tr>
<tr>
<td>9 to 10</td>
<td>Hourly</td>
</tr>
<tr>
<td>10 to 11</td>
<td>Hourly</td>
</tr>
<tr>
<td>11 to Noon</td>
<td>Hourly</td>
</tr>
<tr>
<td>Noon to 8PM</td>
<td>12 hours</td>
</tr>
<tr>
<td>8 to 9</td>
<td>Hourly</td>
</tr>
<tr>
<td>9 to 10</td>
<td>Hourly</td>
</tr>
<tr>
<td>10 to 11</td>
<td>Hourly</td>
</tr>
<tr>
<td>11 to Midnight</td>
<td>Hourly</td>
</tr>
</tbody>
</table>

During the start window, the backup job status remains in CREATED status until it has successfully begun or until the start window time has run out. If within the start window time AWS Backup receives an error that allows the job to be retried, AWS Backup will automatically retry to begin the job at least every 10 minutes until the backup successfully begins (the job status changes to RUNNING) or until the job status changes to EXPIRED (which is expected to occur when the start window time is over).

Lifecycle

The lifecycle defines when a backup is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.

AWS Backup lifecycles data (that is, transitions data from warm to cold storage) that is no longer referenced by warm backups. Data in cold backups that is only referenced by other cold backups are billed at cold storage tier prices. Others continue at warm storage tier pricing.

You can specify how long AWS Backup should store your backups. In order to save you storage costs, AWS Backup automatically deletes your backups at the end of this period. The retention period for
snapshots can range between 1 day and 100 years (or indefinitely if you don't enter one), while the retention period for continuous backups can range from 1 day to 35 days.

If you want your backups to be incremental, you must have at least one warm backup. Because each backup to cold storage is a full backup, AWS Backup recommends that you set your lifecycle settings to not move your backup to cold storage until after at least 8 days.

If you set your lifecycle to back up to cold storage after 1 day, each of those backups will be a full backup. This might be less cost effective than a less regular transfer to cold storage.

Backups that are transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, on the console, the “retention” setting must be 90 days longer than the “transition to cold after days” setting. You can't change the “transition to cold after days” setting after a backup has been transitioned to cold.

Note
- To see the list of resources that you can transition to cold storage, see the "Lifecycle to cold storage" section of the Feature availability by resource (p. 2) table. The cold storage expression is ignored for other resources.
- When backups reach the end of their lifecycle and are marked for deletion as part of your lifecycle policy, AWS Backup deletes the backups at a randomly chosen point over the following 8 hours. This 8-hour window helps ensure consistent performance for deletion.

Backup vault
A backup vault is a container to organize your backups in. Backups created by a backup rule are organized in the backup vault that you specify in the backup rule. You can use backup vaults to set the AWS Key Management Service (AWS KMS) encryption key that is used to encrypt backups in the backup vault and to control access to the backups in the backup vault. You can also add tags to backup vaults to help you organize them. If you don't want to use the default vault, you can create your own. For step-by-step instructions for creating a backup vault, see Step 3: Create a backup vault (p. 28).

Copy to Regions
As part of your backup plan, you can optionally create a backup copy in another AWS Region. For more information about backup copies, see Creating backup copies across AWS Regions.

When you define a backup copy, you configure the following options:

Destination Region
The destination Region for the backup copy.

(Advanced Settings) Backup vault
The destination backup vault for the copy.

(Advanced Settings) IAM Role
The IAM role that AWS Backup uses when creating the copy. The role must also have AWS Backup listed as a trusted entity, which enables AWS Backup to assume the role. If you choose Default and the AWS Backup default role is not present in your account, a role is created for you with the correct permissions.

(Advanced Settings) Lifecycle
Specifies when to transition the backup copy to cold storage and when to expire (delete) the copy. Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. You can't change this value after a copy has transitioned to cold storage.
**Expire** specifies the number of days after creation that the copy is deleted. This must be greater than 90 days beyond the Transition to cold storage value.

**Tags added to recovery points**

The tags that you list here are automatically added to backups when they are created.

**Tags added to backup plans**

These tags are associated with the backup plan itself to help you organize and track your backup plan.

**Advanced backup settings**

Enables application consistent backups for third-party applications that are running on Amazon EC2 instances. Currently, AWS Backup supports Windows VSS backups. AWS Backup excludes specific Amazon EC2 instance types from Windows VSS backups. For more information, see [Creating Windows VSS backups](p. 124).

**AWS CloudFormation templates for backup plans**

We provide two sample AWS CloudFormation templates for your reference. The first template creates a simple backup plan. The second template enables VSS backups in a backup plan.

**Note**

If you are using the default service role, replace `service-role` with `AWSBackupServiceRolePolicyForBackup`.

---

**Description:** backup plan template to back up all resources daily at 5am UTC, and tag all recovery points with backup:daily.

**Resources:**

**KMSKey:**
- **Type:** AWS::KMS::Key
- **Properties:**
  - **Description:** "Encryption key for daily"
  - **EnableKeyRotation:** True
  - **Enabled:** True
  - **KeyPolicy:**
    - **Version:** "2012-10-17"
    - **Statement:**
      - **Effect:** Allow
      - **Principal:**"AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
      - **Action:**"kms:*"
      - **Resource:** "*"

**BackupVaultWithDailyBackups:**
- **Type:** "AWS::Backup::BackupVault"
- **Properties:**
  - **BackupVaultName:** "BackupVaultWithDailyBackups"
  - **EncryptionKeyArn:** !GetAtt KMSKey.Arn

**BackupPlanWithDailyBackups:**
- **Type:** "AWS::Backup::BackupPlan"
- **Properties:**
  - **BackupPlan:**
    - **BackupPlanName:** "BackupPlanWithDailyBackups"
    - **BackupPlanRule:**
      - **RuleName:** "RuleForDailyBackups"
TargetBackupVault: !Ref BackupVaultWithDailyBackups
ScheduleExpression: "cron(0 5 ? * * *)"

DependsOn: BackupVaultWithDailyBackups
DDBTableWithDailyBackupTag:
  Type: "AWS::DynamoDB::Table"
  Properties:
    TableName: "TestTable"
    AttributeDefinitions:
      - AttributeName: "Album"
        AttributeType: "S"
    KeySchema:
      - AttributeName: "Album"
        KeyType: "HASH"
    ProvisionedThroughput:
      ReadCapacityUnits: "5"
      WriteCapacityUnits: "5"
    Tags:
      - Key: "backup"
        Value: "daily"

BackupRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "backup.amazonaws.com"
          Action:
            - "sts:AssumeRole"
        ManagedPolicyArns:
          - "arn:aws:iam::aws:policy/service-role/service-role"

TagBasedBackupSelection:
  Type: "AWS::Backup::BackupSelection"
  Properties:
    BackupSelection:
      SelectionName: "TagBasedBackupSelection"
      IamRoleArn: !GetAtt BackupRole.Arn
      ListOfTags:
        - ConditionType: "STRINGEQUALS"
          ConditionKey: "backup"
          ConditionValue: "daily"
        BackupPlanId: !Ref BackupPlanWithDailyBackups
        DependsOn: BackupPlanWithDailyBackups

Description: backup plan template to enable Windows VSS and add backup rule to take backup of assigned resources daily at 5am UTC.

Resources:
KMSKey:
  Type: AWS::KMS::Key
  Properties:
    Description: "Encryption key for daily"
    EnableKeyRotation: True
    Enabled: True
    KeyPolicy:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
Assigning resources to a backup plan

Resource assignment specifies which resources AWS Backup will protect using your backup plan. AWS Backup gives you both simple default settings and fine-grained controls to assign resources to your backup plan. Each time your backup plan runs, it scans your AWS account for all resources that match your resource assignment criteria. This level of automation allows you to define your backup plan and resource assignment exactly once. AWS Backup abstracts away the work of finding and backing up new resources that fit your earlier-defined resource assignment.

You can assign any AWS Backup-supported resource types that you have opted in for AWS Backup to manage. For instructions on how to opt in to more AWS Backup-supported resource types, see Getting started 1: Service Opt-in.

Your resource assignment can include (or exclude) resource types and resources.

- A resource type includes every instance or resource of an AWS Backup-supported AWS service or third-party application. For example, the DynamoDB resource type refers to all your DynamoDB tables.

- A resource is a single instance of a resource type, such as one of your DynamoDB tables. You can specify a resource using its unique resource ID.

You can further refine your resource assignment using tags and conditional operators.

Topics
- Assigning resources using the console (p. 44)
- Assigning resources programmatically (p. 45)
- Assigning resources using AWS CloudFormation (p. 50)
- Quotas on resource assignment (p. 53)
Assigning resources using the console

To navigate to the Assign resources page:
2. Choose Backup plans.
3. Choose Create Backup plan.
4. Select any template in the Choose template dropdown list, then choose Create plan.
5. Type in a Backup plan name.
6. Choose Create plan.
7. Choose Assign resources.

To begin your resource assignment, in the General section:
1. Type in a Resource assignment name.
2. Choose the Default role or Choose an IAM role.
   Note
   If you choose an IAM role, verify that it has permission to back up all the resources you are about assign. If your role encounters a resource that it doesn't have permission to back up, your backup plan will fail.

To assign your resources, in the Assign resources section, choose one of the two options under Define resource selection:

- Include all resource types. This option configures your backup plan to protect all current and future AWS Backup-supported resources assigned to your backup plan. Use this option to quickly and easily protect your data estate.
  When you choose this option, you can optionally Refine selection using tags as the next step.

- Include specific resource types. When you choose this option, you must Select specific resource types with the following steps:
  1. Using the Select resource types dropdown menu, assign one or more resource types.
     Important
     RDS, Aurora, Neptune, and DocumentDB share the same Amazon Resource Name (ARN). Opting in to manage one of these resource types with AWS Backup opts in to all of them when assigning it to a backup plan. To refine your selection, use tags and conditional operators.

     Once you finish, AWS Backup presents you the list of resource types you selected and its default setting, which is to protect all resources for each selected resource type.

   2. Optionally, if you want to exclude specific resources from a resource type you selected:
      1. Use the Choose resources dropdown menu and deselect the default option.
      2. Select the specific resources to assign to your backup plan.

   3. Optionally, you can Exclude specific resource IDs from the selected resource types. Use this option if you want to exclude one or a few resources out of many, because doing so might be faster than selecting many resources during the previous step. You must have including a resource type before excluding resources from that resource type. Exclude a resource ID with the following steps:
      1. Under Exclude specific resource IDs from the selected resource types, choose one or more of the resource types that you included using Select resource types.
2. For each resource type, use the **Choose resources** dropdown menu to select one or more resources to exclude.

In addition to your previous choices, you can make even more granular selections using the optional **Refine selection using tags** feature. This feature allows you to refine your current selection to include a subset of your resources using tags.

Tags are key-value pairs that you can assign to specific resources to help you identify, organize, and filter your resources. Tags are case sensitive. For more information, see [Tagging AWS resources](https://docs.aws.amazon.com/general/latest/securityguide/security-tagging-resource-labels.html) in the AWS General Reference.

When you refine your selection using two or more tags, the effect is an AND condition. For example, if you refine your selection using two tags, `env: prod` and `role: application`, you only assign resources with BOTH tags to your backup plan.

**To refine your selection using tags:**

1. Under **Refine selection using tags**, choose a **Key** from the dropdown list.
2. Choose a **Condition for value** from the dropdown list.
   - **Value** refers to the next input, the value of your key-value pair.
   - **Condition** can be `Equals`, `Contains`, `Begins with`, or `Ends with`, or their inverse: `Does not equal`, `Does not contain`, `Does not begin with`, or `Does not end with`.
3. Choose a **Value** from the dropdown list.
4. To further refine using another tag, choose **Add tag**.

### Assigning resources programmatically

You can define a resource assignment in a JSON document. This sample resource assignment assigns all Amazon EC2 instances to the backup plan `BACKUP-PLAN-ID`:

```json
{
  "BackupPlanId": "BACKUP-PLAN-ID",
  "BackupSelection": {
    "SelectionName": "resources-list-selection",
    "IamRoleArn": "arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources": [
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

Assuming this JSON is stored as `backup-selection.json`, you can assign these resources to your backup plan using the following CLI command:

```bash
aws backup create-backup-selection --cli-input-json file:///PATH-TO-FILE/backup-selection.json
```

The following table lists a number of example resource assignments along with the corresponding JSON document that preforms the assignment using the AWS Backup API, CLI, or SDK. To make this table easier for you to read, the examples omit the fields "BackupPlanId", "SelectionName", and "IamRoleArn". The wildcard `*` represents zero or more non-whitespace characters.
<table>
<thead>
<tr>
<th>Resource assignment</th>
<th>JSON</th>
</tr>
</thead>
</table>
| Select all resources in my account.                                                | `{  
|                                               
|   "BackupSelection":{
|       "Resources":[
|           "*"
|       ]
|   }
|                                               
| }                                                                                   |
| Select all resources in my account, but exclude EBS volumes.                       | `{  
|                                               
|   "BackupSelection":{
|       "Resources":[
|           "*"
|       ],
|       "NotResources":[
|           "arn:aws:ec2:*:*:volume/*"
|       ]
|   }
|                                               
| }                                                                                   |
| Select all resources tagged with "backup": "true" in my account, but exclude EBS volumes. | `{  
|                                               
|   "BackupSelection":{
|       "Resources":[
|           "*"
|       ],
|       "NotResources":[
|           "arn:aws:ec2:*:*:volume/*"
|       ],
|       "Conditions":{
|           "StringEquals":[
|               {
|                   "ConditionKey":"aws:ResourceTag/backup",
|                   "ConditionValue":"true"
|               }
|           ]
|       }
|   }
|                                               
| }                                                                                   |
| Select all EBS volumes and RDS DB instances tagged with both "backup": "true" and "stage": "prod". | `{  
|                                               
|   "BackupSelection":{
|       "Resources":[
|           "arn:aws:ec2:*:*:volume/*",
|           "arn:aws:rds:*:*:db:*"
|       ],
|       "Conditions":{
|           "StringEquals":[
|               {
|                   "ConditionKey":"aws:ResourceTag/backup",
|                   "ConditionValue":"true"
|               },
|               {
|                   "ConditionKey":"aws:ResourceTag/stage",
|                   "ConditionValue":"prod"
|               }
|           ]
|       }
|   }
|                                               
| }                                                                                   |
### Assigning resources programmatically

#### Resource assignment

<table>
<thead>
<tr>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>```json</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>Note</td>
</tr>
</tbody>
</table>
The Boolean arithmetic is similar to that in IAM policies, with those in "Resources" combined using a Boolean OR and those in "Conditions" combined with a Boolean AND.

Note
The "Resources" expression "arn:aws:rds:*:*:db:*" only selects RDS DB instances because there are no corresponding Aurora, Neptune, or DocumentDB resources.

Select all EBS volumes and RDS instances tagged with "backup": "true" but not "stage": "test".

```json |
{ |
"BackupSelection": |
"Resources": |
[ "arn:aws:ec2:*:*:volume/*", |
"arn:aws:rds:*:*:db:*" |
], |
"Conditions": |
"StringEquals": |
[ |
{ |
"ConditionKey":"aws:ResourceTag/backup", |
"ConditionValue":"true" |
} |
], |
"StringNotEquals": |
[ |
{ |
"ConditionKey":"aws:ResourceTag/stage", |
"ConditionValue":"test" |
} |
] |
} |
```
### Resource assignment

Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude".

```json
{
    "BackupSelection": {
        "Resources": [],
        "Conditions": {
            "StringLike": [
                {
                    "ConditionKey": "aws:ResourceTag/key1",
                    "ConditionValue": "include*"
                }
            ],
            "StringNotLike": [
                {
                    "ConditionKey": "aws:ResourceTag/key2",
                    "ConditionValue": "*exclude*"
                }
            ]
        }
    }
}
```

You can use the wildcard character at the start, end, and middle of a string. Note the use of the wildcard character (*) in `include*` and `*exclude*` in the example above. You can also use the wildcard character in the middle of a string as shown in the previous example, `arn:aws:rds:*:*:db:*`.

Select all resources tagged with "backup":"true" except FSx file systems and RDS, Aurora, Neptune, and DocumentDB resources.

```json
{
    "BackupSelection": {
        "Resources": [],
        "NotResources": [
            "arn:aws:fsx:*",
            "arn:aws:rds:*"
        ],
        "Conditions": {
            "StringEquals": [
                {
                    "ConditionKey": "aws:ResourceTag/backup",
                    "ConditionValue": "true"
                }
            ]
        }
    }
}
```

Items in `NotResources` are combined using the Boolean OR.
### Resource assignment

<table>
<thead>
<tr>
<th>JSON</th>
</tr>
</thead>
</table>

Select all resources tagged with a tag "backup" and any value

```
{
  "BackupSelection":{
    "Resources":[
      "*
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"*"
        }
      ]
    }
  }
}
```

Select all FSx file systems, the Aurora cluster "my-aurora-cluster", and all resources tagged with "backup":"true", except for those resources tagged with "stage":"test".

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster",
    ],
    "ListOfTags":[
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```
## Assigning resources using AWS CloudFormation

This end-to-end AWS CloudFormation template creates a resource assignment, a backup plan, and a destination backup vault:

- A backup vault named `CloudFormationTestBackupVault`.
- A backup plan named `CloudFormationTestBackupPlan`. This plan will run two contains two backup rules, both of which take backups daily at 12 noon UTC and retain them for 210 days.

### Resource assignment

<table>
<thead>
<tr>
<th>JSON</th>
<th>Resource assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select all resources tagged with tag &quot;backup&quot;: &quot;true&quot; except for EBS volumes tagged with &quot;stage&quot;: &quot;test&quot;.</td>
</tr>
<tr>
<td></td>
<td>Use two CLI commands to create two selections to select this group of resources. The first selection applies to all resources except for EBS volumes. The second selection applies to EBS volumes.</td>
</tr>
</tbody>
</table>

```json
{
  "BackupSelection":{
    "Resources":[
      "*
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        { "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}

{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        { "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        { "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```
- A resource selection named `BackupSelectionName`.
- The resource assignment backs up the following resources:
  - Any resource tagged with the key-value pair `backupplan:dsi-sandbox-daily`.
  - Any resource tagged with the value `prod` or values beginning with `prod/`.
- The resource assignment does not back up the following resources:
  - Any RDS, Aurora, Neptune, or DocumentDB cluster.
  - Any resource tagged with the value `test` or values beginning with `test/`.

```yaml
Description: "Template that creates Backup Selection and its dependencies"
Parameters:
  BackupVaultName:
    Type: String
    Default: "CloudFormationTestBackupVault"
  BackupPlanName:
    Type: String
    Default: "CloudFormationTestBackupPlan"
  BackupSelectionName:
    Type: String
    Default: "CloudFormationTestBackupSelection"
  BackupPlanTagValue:
    Type: String
    Default: "test-value-1"
  RuleName1:
    Type: String
    Default: "TestRule1"
  RuleName2:
    Type: String
    Default: "TestRule2"
  ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
  StartWindowMinutes:
    Type: Number
    Default: 60
  CompletionWindowMinutes:
    Type: Number
    Default: 120
  RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
  MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
  DeleteAfterDays:
    Type: Number
    Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlanName: !Ref BackupPlanName
      BackupPlanRule:
        - RuleName: !Ref RuleName1
          TargetBackupVault: !Ref BackupVaultName
          ScheduleExpression: !Ref ScheduleExpression
          StartWindowMinutes: !Ref StartWindowMinutes
```
CompletionWindowMinutes: !Ref CompletionWindowMinutes
RecoveryPointTags:
  test-recovery-point-key-1: !Ref RecoveryPointTagValue
Lifecycle:
  MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
  DeleteAfterDays: !Ref DeleteAfterDays
- RuleName: !Ref RuleName2
  TargetBackupVault: !Ref BackupVaultName
  ScheduleExpression: !Ref ScheduleExpression
  StartWindowMinutes: !Ref StartWindowMinutes
  CompletionWindowMinutes: !Ref CompletionWindowMinutes
  RecoveryPointTags:
    test-recovery-point-key-1: !Ref RecoveryPointTagValue
  Lifecycle:
    MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
    DeleteAfterDays: !Ref DeleteAfterDays
BackupPlanTags:
  test-key-1: !Ref BackupPlanTagValue
DependsOn: CloudFormationTestBackupVault

TestRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "backup.amazonaws.com"
          Action:
            - "sts:AssumeRole"
          ManagedPolicyArns:
            - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup"

BasicBackupSelection:
  Type: 'AWS::Backup::BackupSelection'
  Properties:
    BackupPlanId: !Ref BasicBackupPlan
    BackupSelection:
      SelectionName: !Ref TestBackupPlanName
      IamRoleArn: !GetAtt TestRole.Arn
      ListOfTags:
        - ConditionType: STRINGEQUALS
          ConditionKey: backupplan
          ConditionValue: dsi-sandbox-daily
      NotResources:
        - 'arn:aws:rds:*:*:cluster:*'
      Conditions:
        StringEquals:
          - ConditionKey: 'aws:ResourceTag/path'
            ConditionValue: prod
        StringNotEquals:
          - ConditionKey: 'aws:ResourceTag/path'
            ConditionValue: test
        StringLike:
          - ConditionKey: 'aws:ResourceTag/path'
            ConditionValue: prod/*
        StringNotLike:
          - ConditionKey: 'aws:ResourceTag/path'
            ConditionValue: test/*
Quotas on resource assignment

The following quotas apply to a single resource assignment:

- 500 Amazon Resource Names (ARNs) without wildcards
- 30 ARNs with wildcard expressions
- 30 conditions
- 30 tags per resource assignment (and an unlimited number of resources per tag)

Deleting a backup plan

You can delete a backup plan only after all associated selections of resources have been deleted. Deleting a backup plan deletes the current version of the plan. The current and previous versions, if any, still exist, but they are no longer listed on the console under Backup plans.

Note
When a backup plan is deleted, existing backups are not deleted. To remove existing backups, delete them from the backup vault using the steps in Deleting backups.

To delete a backup plan using the AWS Backup console

2. In the navigation pane on the left, choose Backup plans.
3. Choose your backup plan in the list.
4. Select any resource assignments that are associated with the backup plan.
5. Choose Delete.

Updating a backup plan

After creating a backup plan, you can edit the plan—for example, you can add tags, or you can add, edit, or delete backup rules. Any changes that you make to a backup plan have no effect on existing backups created by the backup plan. The changes apply only to backups that are created in the future.

For example, when you update the retention period in a backup rule, the retention period of backups created before you made the update remain the same. Any backups that are created by that rule going forward reflect the updated retention period.

To edit a backup plan using the AWS Backup console

2. In the navigation pane, choose Backup plans.
3. Choose a backup rule and choose Edit.
4. In the backup rule, change the settings that you want, and then choose Save.
Backup vaults

**Note**
Starting August 9, 2023, AWS Backup is offering a preview to use a **logically air-gapped vault**. To enroll in this preview, send a request via email to <aws-backup-vault-preview@amazon.com>. Features may change or be adjusted during and after the preview period. When the service becomes Generally Available (GA), the data and configurations provided during the preview will no longer be available. AWS recommends using test data instead of production data with the preview.

In AWS Backup, a **backup vault** is a container that stores and organizes your backups.

When creating a backup vault, you must specify the AWS Key Management Service (AWS KMS) encryption key that encrypts some of the backups placed in this vault. Encryption for other backups is managed by their source AWS services. For more information about encryption, see the chart in Encryption for backups in AWS.

Your account will always have a default backup vault. If you require different encryption keys or access policies for different groups of backups, you can create multiple backup vaults.

This section provides an overview of how to manage your backup vaults in AWS Backup.

**Topics**

- [Logically air-gapped vaults (preview) (p. 54)](#)
- [Create a backup vault (p. 61)](#)
- [Set access policies on backup vaults (p. 62)](#)
- [AWS Backup Vault Lock (p. 65)](#)
- [Delete a backup vault (p. 70)](#)

### Logically air-gapped vaults (preview)

**Note**
Starting August 9, 2023, AWS Backup is offering a preview to use a **logically air-gapped vault**. To enroll in this preview, send a request via email to <aws-backup-vault-preview@amazon.com>. Features may change or be adjusted during and after the preview period. When the service becomes Generally Available (GA), the data and configurations provided during the preview will no longer be available. AWS recommends using test data instead of production data with the preview.

**Overview**

AWS Backup is previewing a secondary type of vault which can store copies of backups in other vaults. A **logically air-gapped vault** is a specialized vault which offers increased security features in addition to those of a backup vault as well as the ability to share vault access to other accounts and organizations so that recovery time (RTO) can be faster and more flexible in case of an incident that requires rapid restoration of resources.

Logically air-gapped vaults come equipped with additional protection features: each of these vaults is encrypted with an AWS owned key, and each vault has a **vault lock** set in compliance mode.

You can choose to share a logically air-gapped vault across organizations and accounts so that the backups stored within can be restored from an account with which the vault is shared, if needed.
Use case

A logically air-gapped vault is a secondary vault that serves as part of a data protection strategy. This vault can help enhance your organizational retention and recovery when you desire a vault for your backups that

- Is automatically set with a vault lock in compliance mode
- Contains backups which can be shared with and restored from a different account than the one that created the backup
- Comes encrypted with an AWS owned key

Resources supported in a logically air-gapped vault include

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon EFS
- Amazon RDS

This preview of logically air-gapped vaults is only available in US East (N. Virginia) Region. Because this feature is currently only in one Region, cross-Region copy is not supported during this preview period.

Compare and contrast with a standard backup vault

A backup vault is the primary and standard type of vault used in AWS Backup. Each backup is stored in a backup vault when the backup is created. You can assign resource-based policies to manage backups stored in the vault, such as the lifecycle of backups stored within the vault.

A logically air-gapped vault is a specialized vault with additional security and flexible sharing for faster recovery time (RTO). This vault stores copies of backups that were initially created and stored within a standard backup vault.

Backup vaults can be encrypted with a key, a security mechanism that limits access to intended users. These keys can be customer managed or AWS managed. Additionally, a backup vault can be even more secured by a vault lock; logically air-gapped vaults come equipped by a vault lock in compliance mode.

If the AWS KMS key was not manually changed or set as a customer managed key (CMK) at the time the initial resource was created, a backup cannot be copied into a logically air-gapped vault.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Backup vault</th>
<th>Logically air-gapped vault (preview)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup creation</td>
<td>When a backup is created, it is stored as a recovery point</td>
<td>Backups are not stored in this vault upon creation</td>
</tr>
<tr>
<td>Backup storage</td>
<td>Can store initial backups of resources and copies of backups</td>
<td>Can store copies of backups from other vaults</td>
</tr>
<tr>
<td>Security</td>
<td>Can optionally be encrypted with a key (customer managed or AWS managed)</td>
<td>Is encrypted with an AWS owned key</td>
</tr>
</tbody>
</table>
Create a logically air-gapped vault from the console

Important
Once the vault is created, the vault name, the vault type, and the minimum and maximum retention periods cannot be changed; additionally, the vault lock cannot be removed.
When the service becomes Generally Available, the data and configurations provided during the preview will no longer be available. AWS recommends using test data instead of production data with the preview.

2. In the navigation pane, select Vaults.
3. Both types of vaults will be displayed. Select Create new vault.
4. Enter a name for your backup vault. You can name your vault to reflect what you will store in it, or to make it easier to search for the backups you need. For example, you could name it FinancialBackups.
5. Select the radio button for logically air-gapped vault.
6. Set the Minimum retention period.
   This value (in days, months, or years) is the shortest amount of time a backup can be retained in this vault. Backups with retention periods shorter than this value cannot be copied to this vault.
7. Set the Maximum retention period.
   This value (in days, months, or years) is the longest amount of time a backup can be retained in this vault. Backups with retention periods greater than this value cannot be copied to this vault.
8. (Optional) Add tags that will help you search for and identify your logically air-gapped vault. For example, you could add a BackupType:Financial tag.
9. Select Create vault.
10. Review the settings. If all settings show as you intended, select Create logically air-gapped vault.
11. The console will take you to the details page of your new vault. Verify the vault details are as expected.

**View logically air-gapped vault details in the console**

2. Select **Vaults** from the left-hand navigation.
3. Below the descriptions of vaults will be two lists, **Vaults owned by this account** and **Vaults shared with this account**. Select the desired tab to view the vaults.
4. Under **Vault name**, click on the name of the vault to open the details page. You can see the summary, the recovery points, the protected resources, account sharing, access policy, and tag details.

**Copy from a standard backup vault to a logically air-gapped vault in the console**

Logically air-gapped vaults can only be a copy job destination target in a backup plan or a target for an on-demand copy job. To initiate a copy job, you must have:

- A backup vault
- A logically air-gapped vault
- A backup containing Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3, or Amazon EFS data
- The permission `kms:CreateGrant` for the role being used to create the copy.
- No backups encrypted with an AWS managed key as part of your copy job to the logically air-gapped vault

Once you confirm the above,

2. Select **Vaults** from the left-hand navigation.
3. In the vault detail page, all recovery points within that vault are displayed. Place a check mark next to the recovery point you wish to copy.
4. Select **Actions**, and then select **Copy** from the drop-down menu.
5. On the next screen, input the details of the destination.
   a. Region must be set to US East (N. Virginia)
   b. Destination backup vault drop-down menu displays eligible destination vaults. Select one with the type logically air-gapped vault
6. Select **Copy** once all details are set to your preferences.

On the **Jobs** page in the console, you can select **Copy** jobs to see current copy jobs.

For more information, see [Copying a backup], [cross-Region backup], and [Cross-account backup].

**Share a logically air-gapped vault from the console**

**Note**

Only accounts with certain IAM privileges can share and manage sharing of accounts.
You can use AWS RAM to share a logically air-gapped vault with other accounts you designate. To share using AWS RAM, ensure you have the following:

- Two or more accounts that can access AWS Backup
- An account that intends to share has necessary RAM permissions. The permission `ram:CreateResourceShare` is necessary for this procedure. The policy `AWSResourceAccessManagerFullAccess` contains all needed RAM-related permissions.
- At least one logically air-gapped vault

To share a logically air-gapped vault,

2. Select Vaults from the left-hand navigation.
3. Below the descriptions of vaults will be two lists, Vaults owned by this account and Vaults shared with this account. Select the desired list to view the vaults.
4. Under Vault name, select the name of the logically air-gapped vault to open the details page.
5. The account sharing pane shows with which accounts the vault is being shared.
6. To begin sharing with another account or to edit accounts already being shared, select Manage sharing.

AWS RAM console opens when Manage sharing is selected. For steps to share a resource using AWS RAM, see Creating a resource share in AWS RAM.

Ensure you have appropriate permissions. Backup Administrator IAM Policy [AWSBackupFullAccess] and Backup Operator IAM Policy [AWSBackupOperatorAccess] contain the required permission to view shared accounts; however, the role you use to share needs Resource Access Manager write permissions to share the account from RAM, such as `ram:CreateResourceShare`.

The account invited to accept an invitation to receive a share has 12 hours to accept the invitation. See Accepting and rejecting resource share invitations in the AWS RAM User Guide.

If the sharing steps are completed and accepted, the vault summary page will show under Account sharing = “Shared - see account sharing table below”.

### Restore a backup from a logically air-gapped vault using the console

You can restore a backup stored in a logically air-gapped vault from either the account that owns the vault or from any accounts with which the vault is shared.

See Restoring a backup for information on how to restore a recovery point.

### Delete a logically air-gapped vault using the console

**Important**

When the service becomes Generally Available, the data and configurations provided during the preview will no longer be available. AWS recommends using test data instead of production data with the preview.

See delete a backup vault to delete a vault. Vaults cannot be deleted if they still contain backups (recovery points). Ensure the vault is empty of backups before you initiate a delete operation.
Logically air-gapped vaults through CLI/API

You can use AWS CLI to programmatically carry out operations for logically air-gapped vaults. Each CLI is specific to the AWS service in which it originates. Commands related to sharing are prepended with `aws ram`; all other commands should be prepended with `aws backup`.

Create

The following sample CLI command `CreateLogicallyAirGappedBackupVault` can be modified to create a logically air-gapped backup vault:

```
aws backup create-logically-air-gapped-backup-vault \\
--region us-east-1 \\
--logically-air-gapped-backup-vault-name sampleName \\
--min-retention-days 1 \\
--max-retention-days 7 \\
--creator-request-id 123456789012-34567-8901 (optional)
```

View details

The following sample CLI command `DescribeBackupVault` can be modified to obtain details about a vault:

```
aws backup describe-backup-vault \\
--region us-east-1 \\
--backup-vault-name testvaultname
```

Share

**Note**

Only accounts with sufficient IAM permissions can share and manage sharing of accounts.

You can share a logically air-gapped vault through [AWS Resource Access Manager](https://aws.amazon.com/ram/) (RAM), a service that helps users share resources.

AWS RAM uses the CLI command `create-resource-share`. The access to this command is only available to admin accounts with sufficient permissions. See [Creating a resource share in AWS RAM](https://docs.aws.amazon.com/ram/latest/userguide/creating-resource-share.html) for CLI steps.

Steps 1 through 4 are conducted with the account that owns the logically air-gapped vault. Steps 5 through 8 are conducted with the account with which the logically air-gapped vault will be shared.

1. Log into the owning account OR request a user at your organization with sufficient credentials for accessing the source account completes these steps.
   - If a resource share was previously created and you wish to add an additional resource to it, use CLI `associate-resource-share` instead with the ARN of the new vault.

2. Fetch credentials of a role with sufficient permissions to share via RAM. [Input these into the CLI](https://docs.aws.amazon.com/ram/latest/userguide/creating-resource-share.html).
   - The permission `ram:CreateResourceShare` is necessary for this procedure. The policy `AWSResourceAccessManagerFullAccess` contains all RAM-related permissions.

3. Use `create-resource-share`.
   - Include the ARN of the logically air-gapped vault.
   - Example input:
aws ram create-resource-share \
 --name MyLogicallyAirGappedVault  \
 --resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1 \
 --principals 123456789012 \
 --region us-east-1

Example output:

```json
{
  "resourceShare":{
    "name":"MyLogicallyAirGappedVault",
    "owningAccountId":"123456789012",
    "allowExternalPrincipals":true,
    "status":"ACTIVE",
    "creationTime":"2021-09-14T20:42:40.266000-07:00",
    "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
  }
}
```

4. Copy the resource share ARN in the output (which is needed for subsequent steps). Give the ARN to the operator of account you are inviting to receive the share.

5. Obtain the resource share ARN
   a. If you did not perform steps 1 through 4, obtain the resourceShareArn from whomever did.

6. In the CLI, assume credentials of the recipient account.


8. Accept the invitation in destination (recovery) account.
   a. Use `accept-resource-share-invitation` (can also `reject-resource-share-invitation`).

**List**

The CLI command `listBackupVaults` can be modified to list all the vaults owned by and present in the account:

```
aws backup list-backup-vaults \
 --region us-east-1
```

To list just the logically air-gapped vaults, add the parameter

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

To list vaults shared with the account, use

```
aws backup list-backup-vaults \
 --region us-east-1 \
 --by-shared
```
Copy

A logically air-gapped vault can only be a target for a copy job of a backup, not the target of an initial backup job. Use `StartCopyJob` to copy an existing backup in a backup vault to a logically air-gapped vault.

The role which is being used to create the copy job to the logically air-gapped vault must contain the permission `kms:CreateGrant`.

Sample CLI input:

```bash
aws backup start-copy-job \
--region us-east-1 \
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567 \
--source-backup-vault-name sourcevaultname \
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-vault:destinationvaultname \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

Restore

Once a backup has been shared from a logically air-gapped vault to your account, you can use `StartRestoreJob` to restore the backup. Sample CLI input:

```bash
aws backup start-restore-job \
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-point:RecoveryPointID \
--metadata {"availabilityzone":"us-east-1d"} \
--idempotency-token TokenNumber \
--resource-type ResourceType \
--iam-role arn:aws:iam::number:role/service-role/servicerole \
--region us-east-1
```

Delete

The following sample CLI command `DeleteBackupVault` can be used to delete a vault. A vault can only be deleted if there are no backups (recovery points) inside the vault.

```bash
aws backup delete-backup-vault \
--region us-east-1 \
--backup-vault-name testvaultname
```

Other programmatic options available include:

- `CreateBackupPlan`
- `UpdateBackupPlan`
- `DescribeRecoveryPoint`
- `ListRecoveryPointByBackupVault`
- `ListProtectedResourcesByBackupVault`

Create a backup vault

You must create at least one vault before creating a backup plan or starting a backup job.

When you first use the AWS Backup console in an AWS Region, the console automatically creates a default vault.
However, if you use AWS Backup through the AWS CLI, AWS SDK, or AWS CloudFormation, a default vault is not created. You must create your own vault.

An AWS account can create up to 100 backup vaults per AWS Region.

**Creating a backup vault (console)**

For step-by-step instructions for creating a backup vault using the AWS Backup console, see [Step 3: Create a backup vault (p. 28)](p. 28) in the Getting Started guide.

**Creating a backup vault (programmatically)**

The following AWS Command Line Interface command creates a backup vault:

```
aws backup create-backup-vault --backup-vault-name test-vault
```

You can also specify the following configurations for a backup vault.

**Backup vault name**

Backup vault names are case sensitive. They must contain from 2 to 50 alphanumeric characters, hyphens, or underscores.

**AWS KMS encryption key**

The AWS KMS encryption key protects your backups in this backup vault. By default, AWS Backup creates a KMS key with the alias `aws/backup` for you. You can choose that key or choose any other key in your account (cross-account KMS keys can be used via CLI).

You can create a new encryption key by following the [Creating Keys](Creating Keys) procedure in the *AWS Key Management Service Developer Guide*.

After you create a backup vault and set the AWS KMS encryption key, you can no longer edit the key for that backup vault.

The encryption key that is specified in an AWS Backup vault applies to the backups of certain resource types. For more information about backup encryption, see [Encryption for backups in AWS Backup (p. 227)](p. 227) in the Security section. Backups of all other resource types are backed up using the key that is used to encrypt the source resource.

**Backup vault tags**

These tags are associated with the backup vault to help you organize and track your backup vaults.

**Set access policies on backup vaults**

With AWS Backup, you can assign policies to backup vaults and the resources they contain. Assigning policies allows you to do things like grant access to users to create backup plans and on-demand backups, but limit their ability to delete recovery points after they're created.

For information about using policies to grant or restrict access to resources, see [Identity-Based Policies and Resource-Based Policies](Identity-Based Policies and Resource-Based Policies) in the *IAM User Guide*. You can also control access using tags.

You can use the following example policies as a guide to limit access to resources when you are working with AWS Backup vaults.
Note
Unlike other IAM-based policies, AWS Backup access policies don't support a wildcard in the Action key.

For a list of Amazon Resource Names (ARNs) that you can use to identify recovery points for different resource types, see AWS Backup resource ARNs (p. 240) for resource-specific recovery point ARNs.

Note
Vault access policies only control user access to AWS Backup APIs. Some backup types, such as Amazon Elastic Block Store (Amazon EBS) and Amazon Relational Database Service (Amazon RDS) snapshots, can also be accessed using the APIs of those services. You can create separate access policies in IAM that control access to those APIs to fully control the access to those backup types.

Regardless of the AWS Backup vault's access policy, AWS Backup will reject any request from an account that is different from the account of the resource that is being referenced.

Topics
- Deny access to a resource type in a backup vault (p. 63)
- Deny access to a backup vault (p. 63)
- Deny access to delete recovery points in a backup vault (p. 64)

Deny access to a resource type in a backup vault

This policy denies access to the specified API operations for all Amazon EBS snapshots in a backup vault.

```json
{
   "Version": "2012-10-17",
   "Statement": [ {
                  "Sid": "statement ID",
                  "Effect": "Deny",
                  "Principal": {
                                 "AWS": "arn:aws:iam::Account ID:role/MyRole"
                  },
                  "Action": [ "backup:UpdateRecoveryPointLifecycle",
                              "backup:DescribeRecoveryPoint",
                              "backup:DeleteRecoveryPoint",
                              "backup:GetRecoveryPointRestoreMetadata",
                              "backup:StartRestoreJob"
                           ],
                  "Resource": [ "arn:aws:ec2:Region::snapshot/*" ]
               }
   ]
}
```

Deny access to a backup vault

This policy denies access to the specified API operations targeting a backup vault.

```json
{
   "Version": "2012-10-17",
   "Statement": [ {
                  "Sid": "statement ID",
                  "Effect": "Deny",
                  "Principal": {
```

63
Deny access to delete recovery points in a backup vault

Access to vaults and the ability to delete recovery points stored in them is determined by the access that you grant your users.

Follow these steps to create a resource-based access policy on a backup vault that prevents the deletion of any backups in the backup vault.

**To create a resource-based access policy on a backup vault**

2. In the navigation pane on the left, choose Backup vaults.
3. Choose a backup vault in the list.
4. In the Access policy section, paste the following JSON example. This policy prevents anyone who is not the principal from deleting a recovery point in the target backup vault. Replace `statement ID`, and `aws:userId (role/MyRole)` with values for your environment.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement ID",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "backup:DeleteRecoveryPoint",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:userId": [
            "AAAAAAAAAAAAAAAAAAAAA:",
            "BBBBBBBBBBBBBBBBBBBBB",
            "1123456789",
            "11233445566"
          ]
        }
      }
    }
  ]
}
```
To allow list IAM identities using their ARN, use the aws:PrincipalArn global condition key in the following example.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement ID",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::112233445566:role/mys3role",
                        "arn:aws:iam::112233445566:user/shaheer",
                        "112233445566"
                    ]
                }
            }
        }
    ]
}
```

For information about getting a unique ID for an IAM entity, see [Getting the unique identifier](#) in the [IAM User Guide](#).

If you want to limit this to specific resource types, instead of "Resource": "*", you can explicitly include the recovery point types to deny. For example, for Amazon EBS snapshots, change the resource type to the following.

```
"Resource": ["arn:aws:ec2:Region::snapshot/*"]
```

5. Choose **Attach policy**.

---

**AWS Backup Vault Lock**

**Note**

AWS Backup Vault Lock has been assessed by Cohasset Associates for use in environments that are subject to SEC 17a-4, CFTC, and FINRA regulations. For more information about how AWS Backup Vault Lock relates to these regulations, see the [Cohasset Associates Compliance Assessment](#).

AWS Backup Vault Lock is an optional feature of a backup vault, which can be helpful in giving you additional security and control over your backup vaults. When a lock is active in Compliance mode and the grace time is over, the vault configuration cannot be altered or deleted by a customer, account/data owner, or AWS. Each vault can have one vault lock in place.

AWS Backup ensures that your backups are available for you until they reach the expiration of their retention periods. If any user (including the root user) attempts to delete a backup or change the lifecycle properties in a locked vault, AWS Backup will deny the operation.

- Vaults locked in **governance mode** can have the lock removed by users with sufficient IAM permissions.
- Vaults locked in **compliance mode cannot be deleted** once the cooling-off period ("grace time") expires. During grace time, you can still remove the vault lock and change the lock configuration.
Vault lock modes

When you create a vault lock, you have a choice of two modes: Governance mode or Compliance mode. Governance mode is intended to allow a vault to be managed only by users with sufficient IAM privileges. Governance mode helps an organization meet governance requirements, ensuring only designated personnel can make changes to a backup vault. Compliance mode is intended for backup vaults in which the vault (and by extension, its contents) is expected to never be deleted or altered until the data retention period is complete. Once a vault in compliance mode is locked, it is immutable, meaning the lock cannot be removed.

A vault locked in Governance mode can be managed or deleted by users who have the appropriate IAM permissions.

A vault lock in Compliance mode cannot be altered or deleted by any user or by AWS. A vault lock in compliance mode has a grace time period you set before it locks and becomes immutable.

Vault lock benefits

AWS Backup Vault Lock provides several benefits, including:

- WORM (write-once, read-many) configuration for all the backups you store and create in a backup vault.
- An additional layer of defense that protects backups (recovery points) in your backup vaults from inadvertent or malicious deletions.
- Enforcement of retention periods, which prevent early deletions by privileged users (including the AWS account root user), and meet your organization’s data protection policies and procedures.

Lock a backup vault using the console

You can add a vault lock to your AWS Backup Vault using the Backup console.

To add a vault lock to your backup vault:

2. In the navigation pane, find Backup vaults. Click the link nested under Backup vaults called Vault locks.
3. Under How vault locks work or Vault locks, click + Create vault lock.
4. In the pane Vault lock details, choose which vault to which you want your lock applied.
5. Under Vault lock mode choose in which mode you want your vault locked. For more information on choosing your modes, see Vault lock modes earlier on this page.
6. For the Retention period, choose the minimum and maximum retention periods (retention periods are optional). Only backup jobs within the retention periods will be successful.
7. If you chose compliance mode, a section called Vault lock start date is shown. If you chose Governance mode, this will not be displayed, and this step can be skipped.

In compliance mode, a vault lock has a cooling-off period from the creation of the vault lock until the vault and its lock becomes immutable and unchangeable. You choose the duration of this period (called grace time), though it must be at least 3 days (72 hours).

Important
Once the grace time is expired, the vault and its lock are immutable. It cannot be changed or deleted by any user or by AWS.
8. When you are satisfied with the configuration choices, click **Create vault lock**.
9. To confirm you wish to create this lock in the chosen mode, type **confirm** in the text box, then check the box acknowledging the configuration is as intended.

If the steps have been completed successfully, a "Success" banner will appear at the top of the console.

## Lock a backup vault programmatically

To configure AWS Backup Vault Lock, use the API **PutBackupVaultLockConfiguration**. The parameters to include will depend on which vault lock mode you intend. If you wish to create a vault lock in governance mode, do not include **ChangeableForDays**. If this parameter is included, the vault lock will be created in compliance mode.

Here is a CLI example of a compliance mode vault lock creation:

```
aws backup put-backup-vault-lock-configuration
  --backup-vault-name my_vault_to_lock
  --changeable-for-days 3
  --min-retention-days 7
  --max-retention-days 30
```

Here is a CLI example of a governance mode vault lock creation:

```
aws backup put-backup-vault-lock-configuration
  --backup-vault-name my_vault_to_lock
  --min-retention-days 7
  --max-retention-days 30
```

You can configure four options.

1. **BackupVaultName**
   
   The name of the vault to lock.

2. **ChangeableForDays** (include only for compliance mode)
   
   This parameter instructs AWS Backup to create the vault lock in compliance mode. Omit this parameter if you intend to create the lock in governance mode.

   This value is expressed in days. It must be a number no less than 3 and no greater than 36,500; otherwise, an error will return.

   From the creation of this vault lock until the expiration of the date specified, the vault lock can be removed from the vault using **DeleteBackupVaultLockConfiguration**. Alternatively, during this time, you can change the configuration using **PutBackupVaultLockConfiguration**.

   On and after the specified date determined by this parameter, the backup vault will be immutable and cannot be changed or deleted.

3. **MaxRetentionPolicyDays** (optional)

   This is a numerical value expressed in days. This is the maximum retention period that the vault retains its recovery points.

   The maximum retention time frame you choose should be in alignment with your organization's policies for retaining data. If your organization instructs data to be retained for a period, this value can be set to that period (in days). For example, financial or banking data may be required to be kept for 7 years (approximately 2,557 days, depending on leap years).
If not specified, AWS Backup Vault Lock will not enforce a maximum retention period. If specified, backup and copy jobs to this vault with lifecycle retention periods longer than the maximum retention period will fail. Recovery points already saved in the vault prior to the vault lock's creation are not affected. The longest maximum retention period you can specify is 36500 days (approximately 100 years).

4. MinRetentionDays (optional; required for CloudFormation)

This is a numerical value expressed in days. This is the minimum retention period that the vault retains its recovery points. This setting should be set to the amount of time your organization is required to maintain data. For example, if regulations or law requires data to be retained for at least seven years, the value in days would be approximately 2,557, depending on leap years.

If not specified, AWS Backup Vault Lock will not enforce a minimum retention period. If specified, backup and copy jobs to this vault with lifecycle retention periods shorter than the minimum retention period will fail. Recovery points already saved in the vault prior to AWS Backup Vault Lock are not affected. The shortest minimum retention period you can specify is 1 day.

Review a backup vault for its AWS Backup Vault Lock configuration

You can review AWS Backup Vault Lock details on a vault anytime by calling DescribeBackupVault or ListBackupVaults APIs.

To determine whether you applied a vault lock to a backup vault, call DescribeBackupVault and check the Locked property. If "Locked": true, like the following example, you have applied AWS Backup Vault Lock to your backup vault.

```json
{
    "BackupVaultName": "my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 1,
    "Locked": true,
    "MinRetentionDays": 7,
    "MaxRetentionDays": 30,
    "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

The preceding output confirms the following options:

1. Locked is a Boolean that indicates whether you have applied AWS Backup Vault Lock to this backup vault. True means that AWS Backup Vault Lock causes delete or update operations to the recovery points stored in the vault to fail (regardless of whether you are still in the cooling-off grace time period).

2. LockDate is the UTC date and time when your cooling-off grace time period ends. After this time, you cannot delete or change your lock on this vault. Use any publicly-available time converters to convert this string to your local time.

If "Locked": false, like the following example, you have not applied a vault lock (or a previous one has been deleted).
Vault lock removal during grace time (Compliance mode)

To delete your vault lock during grace time (the time after locking the vault but before your LockDate) using the AWS Backup console,

2. In the left navigation under My account, click Backup vaults, then click Backup Vault Lock.
3. Click the vault lock you wish to remove, then click Manage vault lock.
4. Click Delete vault lock.
5. A warning box will appear, asking you to confirm your intent to delete the vault lock. Type confirm into the text box, then click confirm.

After the steps have all been completed successfully, a Success banner will appear at the top of the console screen.

To delete your vault lock during grace time using a CLI command, use DeleteBackupVaultLockConfiguration like this CLI example:

```bash
aws backup delete-backup-vault-lock-configuration \
   --backup-vault-name my_vault_to_lock
```

AWS account closure with a locked vault

When you close an AWS account that contains a backup vault, AWS and AWS Backup suspend your account for 90 days with your backups intact. If you do not reopen your account during those 90 days, AWS deletes the contents of your backup vault, even if AWS Backup Vault Lock was in place.

Additional security considerations

AWS Backup Vault Lock adds an additional layer of security to your data protection defense in depth. Vault lock can be combined with these other security features:

- Encryption for your recovery points
- AWS Backup vault and recovery point access policies, which allow you to grant or deny permissions at the vault level,
- AWS Backup security best practices, including its library of customer managed policies that allow you to grant or deny backup and restore permissions by AWS supported service, and
- AWS Backup Audit Manager, which allows you to automate compliance checks for your backups against a list of controls you define.
Note
AWS Backup Vault Lock is not the same feature as S3 Glacier Flexible Retrieval Vault Lock, which is compatible only with Amazon S3.

Delete a backup vault

Note
You cannot delete two backup vaults: the AWS Backup default backup vault and the Amazon EFS automatic backup vault.
When you delete a backup vault, update your backup plans to point to new backup vaults. A backup plan that points to a deleted backup vault will cause the backup creation to fail.

To guard against accidental or malicious mass deletion, you can delete a backup vault in AWS Backup only after you delete (or your backup plan lifecycles) all the recovery points in your backup vault. To delete all your recovery points manually, see that section in Clean up resources.

To delete a backup vault using the AWS Backup console

2. In the navigation pane, choose Backup vaults.
3. Choose the backup vault that you want to delete.
4. Choose and delete any backups that are associated with the backup vault.
5. Delete the backup vault by choosing Delete (in the upper-right corner).
Working with backups

A backup, or recovery point, represents the content of a resource, such as an Amazon Elastic Block Store (Amazon EBS) volume or Amazon DynamoDB table, at a specified time. Recovery point is a term that refers generally to the different backups in AWS services, such as Amazon EBS snapshots and DynamoDB backups. The terms recovery point and backup are used interchangeably.

AWS Backup saves recovery points in backup vaults, which you can organize according to your business needs. For example, you can save a set of resources that contain financial information for fiscal year 2020. When you need to recover a resource, you can use either the AWS Backup console or the AWS Command Line Interface (AWS CLI) to find and recover the resource you need.

Each recovery point has a unique ID. The unique ID is at the end of the recovery point's Amazon Resource Name (ARN). For examples of recovery point ARNs and unique IDs, see the table in Resources and operations (p. 240).

Important
To avoid additional charges, configure your retention policy with a warm storage duration of at least one week. For more information, see Metering, costs, and billing (p. 17).

The following sections provide an overview of the basic backup management tasks in AWS Backup.

Topics
- Creating a backup (p. 71)
- Copy a backup (p. 126)
- Viewing a list of backups (p. 136)
- Editing a backup (p. 137)
- Deleting backups (p. 137)
- Restoring a backup (p. 139)

Creating a backup

With AWS Backup, you can create backups automatically using backup plans or manually by initiating an on-demand backup.

Creating automatic backups

When backups are created automatically by backup plans, they are configured with the lifecycle settings that are defined in the backup plan. They are organized in the backup vault that is specified in the backup plan. They are also assigned the tags that are listed in the backup plan. For more information about backup plans, see Managing backups using backup plans (p. 36).

Creating on-demand backups

When you create an on-demand backup, you can configure these settings for the backup that is being created. When a backup is created either automatically or manually, a backup job is initiated. For how to create an on-demand backup, see Creating an on-demand backup (p. 73).

Note: An on-demand backup begins to back up your resource immediately. You can choose an on-demand backup if you wish to create a backup at a time other than the scheduled time defined in a
backup plan. An on-demand backup can be used, for example, to test backup and functionality at any time.

*On-demand backups* cannot be used with *point-in-time restore (PITR)* since an on-demand backup preserves resources in the state they are in when the backup is taken, whereas PITR uses *continuous backups* which record changes over a period of time.

**Backup job statuses**

Each backup job has a unique ID. For example, D48D8717-0C9D-72DF-1F56-14E703BF2345.

You can view the status of a backup job on the *Jobs* page of the AWS Backup console. Backup job statuses include *pending*, *running*, *aborted*, *completed*, and *failed*.

**How incremental backups work**

Many resources support incremental backup with AWS Backup. A full list is available in the incremental backup section of the *Feature availability by resource (p. 2)* table.

Although each backup after the first one is incremental (meaning it only captures changes from the previous backup), all backups made with AWS Backup retain the necessary reference data to allow a full restore. This is true even if the original (full) backup has reached the end of its lifecycle and been deleted.

For example, if your day 1 (full) backup was deleted due to a 3-day lifecycle policy, you would still be able to perform a full restore with the backups from days 2 and 3. AWS Backup maintains the necessary reference data from day 1 to do so.

**Access to source resources**

AWS Backup needs access to your source resources to back them up. For example:

- To back up an Amazon EC2 instance, the instance can be in the running or stopped state, but not the terminated state. This is because a running or stopped instance can communicate with AWS Backup, but a terminated instance cannot.
- To back up a virtual machine, its hypervisor must have the Backup gateway status ONLINE. For more information, see *Understanding hypervisor status*.
- To back up an Amazon RDS database, Amazon Aurora, or Amazon DocumentDB cluster, those resources must have the status AVAILABLE.
- To back up an Amazon Elastic File System (Amazon EFS), it must have the status AVAILABLE.
- To back up an Amazon FSx file system, it must have the status AVAILABLE. If the status is UPDATING, the backup request is queued until the file system becomes AVAILABLE.

**FSx for ONTAP** doesn't support backing up certain volume types, including DP (data-protection) volumes, LS (load-sharing) volumes, FlexGroup volumes, full volumes, or volumes on file systems that are full. For more information, please see *FSx for ONTAP Working with backups*.

AWS Backup retains previously-created backups consistent with your lifecycle policy, regardless of the health of your source resource.

**Topics**

- [Creating an on-demand backup](p. 73)
- [Restoring to a specified time using Point-In-Time Recovery (PITR)](p. 74)
- [Amazon S3 backups](p. 79)
- [Virtual machine backups](p. 83)
Creating an on-demand backup

On the AWS Backup console, the Protected resources page lists resources that have been backed up by AWS Backup at least once. If you’re using AWS Backup for the first time, there aren’t any resources (such as Amazon EBS volumes or Amazon RDS databases) listed on this page. This is true even if a resource was assigned to a backup plan and that backup plan has not run a scheduled backup job at least once.

Note: An on-demand backup begins to back up your resource immediately. You can choose an on-demand backup if you wish to create a backup at a time other than the scheduled time defined in a backup plan. An on-demand backup can be used, for example, to test backup and functionality at any time.

On-demand backups cannot be used with point-in-time restore (PITR) since an on-demand backup preserves resources in the state they are in when the backup is taken, whereas PITR uses continuous backups which record changes over a period of time.

To create an on-demand backup

2. On the dashboard, choose Create an on-demand backup. Or, in the navigation pane, choose Protected resources and then choose Create an on-demand backup.
3. On the Create on-demand backup page, choose the resource type that you want to back up; for example, choose DynamoDB for Amazon DynamoDB tables.
4. Choose the name or ID of the resource that you want to protect; for example, VideoMetadataTable.
5. Ensure that Create backup now is selected. This initiates a backup immediately and enables you to see your saved resource sooner on the Protected resources page.
6. Only resources which have the feature Transition to cold storage will be able to have an input value; otherwise, this field is marked N/A because the resource type cannot be saved to cold storage. See the Lifecycle to cold storage column in table Feature availability by resource to determine if the resource is eligible.

If you’re using Amazon EFS, choose the desired value to specify when this backup is transitioned to cold storage.
7. Choose an Expire value.
   
   **Note**
   When backups expire and are marked for deletion as part of your lifecycle policy, AWS Backup deletes the backups at a randomly chosen point over the following 8 hours. This window helps ensure consistent performance.

8. Choose an existing Backup vault or create a new one. Choosing Create new Backup vault opens a new page to create a vault and then returns you to the Create on-demand backup page when you are finished.
9. Under IAM role, choose Default role or a role of your choice.

   Note
   If the AWS Backup default role is not present in your account, one will be created for you with the correct permissions.

10. If you want to assign one or more tags to your on-demand backup, enter a Key and optional Value, and then choose Add tag.

   Note
   For Amazon EC2 resources, AWS Backup automatically copies existing group and individual resource tags, in addition to any tags that you add in this step.

11. If the resource you want to back up is running an Amazon EC2 instance, choose Windows VSS in the Advanced settings section. This enables you to take application-consistent Windows Volume Shadow Copy Service (VSS) backups.

   Note
   AWS Backup takes EC2 backups with "no reboot" as the default behavior. AWS Backup currently supports resources running on Amazon EC2, and certain instance types are not supported. For more information, see Creating Windows VSS backups (p. 124).

12. Choose Create on-demand backup. This takes you to the Jobs page, where you can see a list of jobs.

13. Choose the Backup job ID for the resource that you chose to back up. On the job details page, pause on Status to view the details of your job status.

Restoring to a specified time using Point-In-Time Recovery (PITR)

For some resources, AWS Backup supports continuous backups and point-in-time recovery (PITR) in addition to snapshot backups.

With continuous backups, you can restore your AWS Backup-supported resource by rewinding it back to a specific time that you choose, within 1 second of precision (going back a maximum of 35 days). Continuous backup works by first creating a full backup of your resource, and then constantly backing up your resource's transaction logs. PITR restore works by accessing your full backup and replaying the transaction log to the time that you tell AWS Backup to recover.

Alternatively, snapshot backups can be taken as frequently as every hour. Snapshot backups can be stored for up to a maximum of 100 years. Snapshots can by copied for full or incremental backups.

Because continuous and snapshot backups offer different advantages, we recommend that you protect your resources with both continuous and snapshot backup rules.

Note: An on-demand backup begins to back up your resource immediately. You can choose an on-demand backup if you wish to create a backup at a time other than the scheduled time defined in a backup plan. An on-demand backup can be used, for example, to test backup and functionality at any time.

On-demand backups cannot be used with point-in-time restore (PITR) since an on-demand backup preserves resources in the state they are in when the backup is taken, whereas PITR uses continuous backups which record changes over a period of time.

You can opt in to continuous backups for supported resources when you create a backup plan in AWS Backup using the AWS Backup console or the API.

To enable continuous backups using the console

2. In the navigation pane, choose **Backup plans**, and then choose **Create Backup plan**.
3. Under **Backup rules**, choose **Add Backup rule**.
4. In the **Backup rule configuration** section, select **Enable continuous backups for supported resources**.

**Supported services and applications for Point-In-Time Recovery (PITR)**

AWS Backup supports continuous backups and point-in-time recovery for the following services and applications:

- Amazon S3
- Amazon RDS
- SAP HANA databases on Amazon EC2 instances

**Amazon S3**

To turn on PITR for S3 backups, continuous backups need to part of the backup plan. While this original backup of the source bucket can have PITR active, cross-Region or cross-account destination copies will not have PITR, and restoring from these copies will restore to the time they were created (the copies will be snapshot copies) instead of restoring to a specified point in time.

**Amazon RDS**

Amazon RDS calls its continuous backups "automated backups." AWS Backup calls Amazon RDS continuous backups "continuous backups."

If you use AWS Backup for both Amazon RDS snapshots and continuous backups, AWS Backup will intelligently schedule your backup windows, along with the Amazon RDS maintenance window, to prevent conflicts. You no longer have to manually schedule one backup window hours before another. You can't control the Amazon RDS automated backup window. This is because AWS Backup intelligently schedules it for you.

When you change your PITR retention period, AWS Backup calls **ModifyDBInstance** and applies that change immediately. If you have other configuration updates pending the next maintenance window, changing your PITR retention period will also apply those configuration updates immediately. For more information, see **ModifyDBInstance** in the **Amazon Relational Database Service API Reference**.

You can perform a point-in-time recovery using either AWS Backup or Amazon RDS. For AWS Backup console instructions, see **Restoring an Amazon RDS Database**. For Amazon RDS instructions, see **Restoring a DB Instance to a specified time** in the **Amazon RDS User Guide**. RDS takes snapshots once per day regardless if a backup plan has a frequency for snapshot backups other than once per day.

AWS Backup currently does not support Amazon Aurora continuous backups. AWS Backup supports Aurora snapshots.

Incremental snapshot copy jobs process faster than full snapshot copy jobs. Keeping a previous snapshot copy until the new copy job is complete may reduce the copy job duration. If you choose to copy snapshots from RDS database instances, it is important to note that deleting previous copies first will cause full snapshot copies to be made (instead of incremental). For more information on optimizing copying, see **Incremental snapshot copying** in the **Amazon RDS User Guide**

**SAP HANA on Amazon EC2 instances**
You can make continuous backups, which can be used with point-in-time restore (PITR) (note that on-demand backups preserve resources in the state in which they are taken; whereas PITR uses continuous backups which record changes over a period of time).

With continuous backups, you can restore your SAP HANA database on an EC2 instance by rewinding it back to a specific time that you choose, within 1 second of precision (going back a maximum of 35 days). Continuous backup works by first creating a full backup of your resource, and then constantly backing up your resource’s transaction logs. PITR restore works by accessing your full backup and replaying the transaction log to the time that you tell AWS Backup to recover.

You can opt in to continuous backups when you create a backup plan in AWS Backup using the AWS Backup console or the API.

To enable continuous backups using the console

2. In the navigation pane, choose Backup plans, and then choose Create Backup plan.
4. In the Backup rule configuration section, select Enable continuous backups for supported resources.

After you disable PITR (point-in-time restore) for SAP HANA database backups, logs will continue to be sent to AWS Backup until the recovery point expires (status equals EXPIRED). You can change to an alternative log backup location in SAP HANA to stop the transmission of logs to AWS Backup.

A continuous recovery point with a status of STOPPED indicates that a continuous recovery point has been interrupted; that is, the logs transmitted from SAP HANA to AWS Backup that show the incremental changes to a database have a gap. The recovery points that occur within this timeframe gap have a status of STOPPED.

For issues you may encounter during restore jobs of continuous backups (recovery points), see the SAP HANA Restore troubleshooting section of this guide.

Considerations:

Keep in mind the following when performing a point-in-time recovery:

- **Restoring recent activity** — Amazon RDS activity allows restores up until the most recent 5 minutes of activity; Amazon S3 allows restores up until the most recent 15 minutes of activity.
- **Creating copies of Amazon RDS continuous backups** — You can't create copies of Amazon RDS continuous backups because AWS Backup for Amazon RDS does not allow copying transaction logs. Instead, AWS Backup creates a snapshot and copies it with the frequency specified in the backup plan.

For general information about working with Amazon RDS, see the Amazon RDS User Guide.

Managing continuous backup settings

After you apply an AWS Backup continuous backup rule to an Amazon RDS instance, you can't create or modify continuous backup settings to that instance in Amazon RDS. This limitation exists to prevent conflicts.

To view your continuous backup in Amazon RDS, open the Amazon RDS console and choose Automated backups in the left-hand menu.

To transition control of continuous backup for that Amazon RDS instance back to Amazon RDS, you can use the AWS Backup console, AWS CLI, or API.
To transition continuous backup control to Amazon RDS using the AWS Backup console

2. In the navigation pane, choose Backup plans.
3. Delete all the Amazon RDS backup plans with continuous backup protecting that resource.
4. Choose Backup vaults. Delete the continuous backup recovery point from your backup vault. Or, wait for their retention period to elapse, causing AWS Backup to automatically delete the recovery point.

After you complete these steps, AWS Backup will transition continuous backup control of your resource back to Amazon RDS.

To transition continuous backup control to Amazon RDS using the AWS Backup API or CLI

• Call the DisassociateRecoveryPoint API operation.
  To learn more, see DisassociateRecoveryPoint.

IAM permissions required for Amazon RDS continuous backups

• To use AWS Backup to configure continuous backups for your Amazon RDS database, verify that the API permission rds:ModifyDBInstance exists in the IAM role defined by your backup plan configuration. To restore Amazon RDS continuous backups, you must add the permission rds:RestoreDBInstanceToPointInTime to the IAM role that you submitted for the restore job. You can use the AWS Backup default service role to perform backups and restores.
• To describe the range of times available for point-in-time recovery, AWS Backup calls rds:DescribeDBInstanceAutomatedBackups API. In the AWS Backup console, you must have the rds:DescribeDBInstanceAutomatedBackups API permission in your AWS Identity and Access Management (IAM) managed policy. You can use the AWSBackupFullAccess or AWSBackupOperatorAccess managed policies. Both policies have all required permissions. For more information, see Managed Policies.

Working with continuous backups

Finding a continuous backup

You can use the AWS Backup console to find your continuous backup.

To find a continuous backup using the AWS Backup console

2. In the navigation pane, choose Backup vaults, and then choose your backup vault in the list.
3. In the Backups section, in the Backup type column, sort for Continuous recovery points. You can also sort by Recovery point ID for the prefix continuous.

Restoring a continuous backup

To restore a continuous backup using the AWS Backup console

• During the PITR restore process, the AWS Backup console displays a Restore time section. In this section, do one of the following:
  • Choose to restore to the Latest restorable time.
  • Choose Specify date and time to enter your own date and time within your retention period.
To restore a continuous backup using the AWS Backup API

1. For Amazon S3 see Use the AWS Backup API, CLI, or SDK to restore S3 recovery points.
2. For Amazon RDS see Use the AWS Backup API, CLI, or SDK to restore Amazon RDS recovery points.

Stopping continuous backups

If you want to stop continuous backups, you must delete the continuous backup rule from your backup plan. If you wish to stop continuous backups for one or more resources but not for all resources, create a new backup plan with the continuous backup rule for those resources you still want to be continuously backed up. If instead you only delete a continuous backup recovery point from your backup vault, your backup plan will still continue to execute the continuous backup rule, creating a new recovery point.

However, even after you delete your continuous backup rule, AWS Backup remembers the retention period from your now-deleted backup rule. It will automatically delete your continuous backup recovery point from your backup vault based on your specified retention period.

Copying continuous backups

If a continuous backup rule also specifies a cross-account or cross-Region copy, AWS Backup takes a snapshot of the continuous backup and copies that snapshot to the destination vault. To learn more about copying your recovery points across accounts and Regions, see Copying a backup.

Continuous backups will create a periodic backup in accordance with the frequency set in the backup plan rule in the destination account and/or Region.

AWS Backup does not support on-demand copies of continuous backups.

Changing your retention period

You can use AWS Backup to increase or decrease the retention period for your existing continuous backup rule. The minimum retention period is 1 day. The maximum retention period is 35 days.

If you increase your retention period, the effect is immediate. If you decrease your retention period, AWS Backup will wait until enough time passes before applying the change to protect against data loss. For example, if you decrease your retention period from 35 days to 20, AWS Backup will continue to preserve 35 days of continuous backup until 15 days have passed. This design protects your last 15 days of backups at the time you made the change.

Removing the only continuous backup rule from a backup plan

When you create a backup plan with a continuous backup rule and then you remove that rule, AWS Backup remembers the retention period from your now-deleted rule. It will delete the continuous backup from your backup vault when the retention period elapses.

Overlapping continuous backups on the same resource

In general, you should protect each resource with no more than one continuous backup rule. This is because additional continuous backups are redundant. However, as you scale up your backup estate, it is possible for multiple backup plans, rules, and vaults to overlap on a single resource. AWS Backup handles these overlaps as follows.

If you include the same resource in more than one backup plan with a continuous backup rule, AWS Backup will only create a continuous backup for the first backup plan it evaluates. It will create snapshot backups for all of the other backup plans.

If you include multiple continuous backup rules in a single backup plan:

- If your rules point to the same backup vault, AWS Backup only creates a continuous backup for the rule with the longest retention period. It disregards all other rules.
• If your rules point to different backup vaults, AWS Backup rejects the plan as not valid.

Point-in-time recovery considerations

Be aware of the following considerations for point-in-time recovery:

• **Automatic fallback to snapshots** — If AWS Backup is unable to perform a continuous backup, it tries to perform a snapshot backup instead.

• **No support for on-demand continuous backups** — AWS Backup doesn’t support on-demand continuous backup because on-demand backup records a point in time, whereas continuous backup records changes over a period of time.

• **No support for transition to cold storage** — Continuous backups don’t support transition to cold storage because transition to cold requires a minimum transition period of 90 days, whereas continuous backups have a maximum retention period of 35 days.

Amazon S3 backups

**Note**

AWS Backup for S3 is not yet available in China (Beijing) and China (Ningxia) Regions.

AWS Backup supports centralized backup and restore of applications storing data in S3 alone or alongside other AWS services for database, storage, and compute. Many features are available for S3 backups, including Backup Audit Manager.

You can use a single backup policy in AWS Backup to centrally automate the creation of backups of your application data. AWS Backup automatically organizes backups across different AWS services and third-party applications in one centralized, encrypted location (known as a backup vault) so that you can manage backups of your entire application through a centralized experience. For S3, you can create continuous backups and restore your application data stored in S3 and restore the backups to a point-in-time with a single click.

With AWS Backup, you can create the following types of backups of your S3 buckets, including object data, tags, Access Control Lists (ACLs), and user-defined metadata:

• **Continuous backups** allow you to restore to any point in time within the last 35 days. Continuous backups for an S3 bucket should only be configured in one backup plan.

  See [Point-in-Time Recovery](#) for a list of supported services and instructions on how to use AWS Backup to take continuous backups.

• **Periodic backups** use snapshots of your data to allow you to retain data for your specified duration up to 99 years. You can schedule periodic backups in frequencies such as 1 hour, 12 hours, 1 day, 1 week, or 1 month. AWS Backup takes periodic backups during the backup window you define in your backup plan.

  See [Creating a backup plan](#) to understand how AWS Backup applies your backup plan to your resources.

Cross-account and cross-Region copies are available for S3 backups, but copies of continuous backups do not have point-in-time restore capabilities.

Continuous and periodic backups of S3 buckets must both reside in the same backup vault.

For both backup types, the first backup is a full backup, while subsequent backups are incremental at object-level. For example, if there is a 1 kB change in your 1 GB object, the subsequent backup will create a new 1 GB object in the backup vault.
Note
You must enable S3 Versioning on your S3 bucket to use AWS Backup for Amazon S3. We have kept this prerequisite because in AWS we recommend S3 versioning as a best practice for data protection.
We recommend that you set a lifecycle expiration period for your S3 versions. Not setting up a lifecycle expiration period might increase your S3 costs because AWS Backup backs up and stores all unexpired versions of your S3 data. To learn more about setting up S3 lifecycle policies, follow the instructions on this page.

Compare S3 backup types

Your backup strategy for S3 resources can involve just continuous backups, just periodic (snapshot) backups, or a combination of both. The information below can help you choose what works best for your organization:

Continuous backups only:

- After the first full backup of your existing data is complete, changes in your S3 bucket data are tracked as they occur.
- The tracked changes allow you to use PITR (point-in-time restore) for the retention period of the continuous backup. To perform a restore job, you choose the point in time to which you wish to restore.
- The retention period of each continuous backup has a maximum of 35 days.

Periodic (snapshot) backups only, scheduled or on-demand:

- AWS Backup scans the entire S3 bucket, retrieves each object's ACL and tags (if applicable and if feature is turned on), and initiates a Head request for every object that was in the prior snapshot but was not found in the snapshot being created.
- The backup is point-in-time consistent.
- The backup date and time recorded is the time at which AWS Backup completes the traversal of the bucket, not at the time which a backup job was created.
- The first backup of a bucket is a full backup. Each subsequent backup is incremental, representing the change in data since the last snapshot.
- The snapshot made by the periodic backup can have a retention period of up to 99 years.

Continuous backups combined with periodic/snapshot backups:

- After the first full backup of your existing data (each bucket) is complete, changes in your bucket are tracked as they occur.
- You can perform a point-in-time restore from a continuous recovery point.
- Snapshots are point-in-time consistent.
- Snapshots are taken directly from the continuous recovery point, eliminating the need to rescan a bucket to allow for faster processes.
- Snapshots and continuous recovery points share data lineage; storage of data between snapshot and continuous recovery points is not duplicated.

Supported S3 Storage Classes

AWS Backup allows you to backup your S3 data stored in the following S3 Storage Classes:

- S3 Standard
• S3 Standard - Infrequently Access (IA)
• S3 One Zone-IA
• S3 Glacier Instant Retrieval
• S3 Intelligent-Tiering (S3 INT)

With the exception of Glacier Instant Retrieval, archived storage classes (including S3 INT - Glacier, Glacier Flexible Retrieval, and Glacier Deep Archive) are not supported.

Considerations for AWS Backup for Amazon S3

The following points should be considered when you backup S3 resources:

• **Focused object metadata support**: AWS Backup supports the following metadata: tags, access control lists (ACLs), user-defined metadata, original creation date, and version ID. You may also restore all backed-up data and metadata except original creation date, version ID, storage class, and e-tags.

• An S3 object key name can be made up of most UTF-8 encodable strings. The following Unicode characters are allowed: `#x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF`.

Object key names that include characters not in this list may be excluded from backups. For more information, see the [W3C specification for characters](https://www.w3.org/2002/08/unicode/).

• **Cold storage transition**: AWS Backup's lifecycle management policy allows you to define the timeline for backup expiration, but cold storage transition of S3 backups is not currently supported at this time.

• Backups of S3 buckets with many versions of the same object that were created at the same second are not currently supported at this time.

• For periodic backups, AWS Backup makes a best effort to track all changes to your object metadata. However, if you update a tag or ACL multiple times within 1 minute, AWS Backup might not capture all intermediate states.

• AWS Backup does not currently offers support for backups of [SSE-C-encrypted](https://aws.amazon.com/s3/sse-c/) objects. AWS Backup also does not currently support backups of bucket configurations, including bucket policy, settings, name, or access point.

• If you create a backup of an S3 Intelligent Tier (INT) object, then the source object moves to a storage tier that is more expensive than its present storage tier.

• AWS Backup does not currently support backups of S3 on AWS Outposts.

**Important**

In accounts logging data read events, S3 buckets with CloudTrail logs enabled need their access logs saved to a different target bucket; if CloudTrail logs are saved in the same bucket they log, an infinite loop forms. This loop can trigger unexpected and unwanted charges.

For more information, see [Data events](https://docs.aws.amazon.com/AmazonS3/latest/userguide/monitoring-object-operations.html) in the *CloudTrail User Guide*.

### S3 backup completion windows

The table below shows sample buckets of various sizes to help you guide estimates of the completion time of the initial full backup of an S3 bucket. Backup times will vary with the size, content, configuration, and settings of each bucket.

<table>
<thead>
<tr>
<th>Bucket size</th>
<th>Number of objects</th>
<th>Estimated time to complete initial backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>425 GB (gigabytes)</td>
<td>135 million</td>
<td>31 hours</td>
</tr>
</tbody>
</table>
## Permissions and policies for Amazon S3 backup and restore

To backup, copy, and restore S3 resources, you must have the correct policies in your role. To add these policies, go to [AWS managed policies](https://aws.amazon.com/managed-policies/). Add the [AWS Backup For Amazon S3 Backup Policy](https://docs.aws.amazon.com/backup/latest/devguide/s3-backup-policy.html) and the [AWS Backup For Amazon S3 Restore Policy](https://docs.aws.amazon.com/backup/latest/devguide/s3-restore-policy.html) to the roles you intend to use to backup and restore S3 buckets.

If you do not have sufficient permission, please request the manager of your organization's administrative (admin) account to add the policies to the intended roles.

For more information, please see [Get started using permissions with AWS managed policies](https://docs.aws.amazon.com/iam/latest/userguide/managed-policies-permissions.html) in the IAM User Guide.

AWS Backup for S3 relies on receiving S3 events through Amazon EventBridge. If this setting is disabled in S3 bucket notification settings, continuous backups will stop for those buckets with the setting turned off. For more information, see [Using EventBridge](https://docs.aws.amazon.com/AmazonS3/latest/dev/using-events.html).

## Best practices and cost optimization for S3 backups

### Best practices

For buckets with more than 300 million objects:

- For buckets with greater than 300 million objects, the backup rate can reach up to 17,000 objects per second during the initial full backup of the bucket (incremental backups will have a different speed); buckets containing fewer than 300 million objects back up at a rate close to 1,000 objects per second.
- Continuous backups are recommended.
- If backup lifecycle is planned for more than 35 days, you can also enable snapshot backups for the bucket in the same vault in which your continuous backups are stored.

### Cost optimization

- S3 lifecycle policies have an optional feature called [Delete expired object delete markers](https://docs.aws.amazon.com/backup/latest/devguide/s3-backup-lifecycle.html). When this feature is left off, delete markers, sometimes in the millions, expire with no cleanup plan. When buckets without this feature are backed up, two issues impact time and cost:
  - Delete markers are backed up, just like objects. Backup time and restore time can be impacted depending on the ratio of objects to delete markers.
  - Each object and marker that is backed up has a minimum charge. Each delete marker is charged the same as a 128KiB object.
- For accounts which make backups at least daily or more frequently, cost benefits can be realized by using continuous backups if the data within the backups has minimal changes between backups.
- Larger buckets that do not change frequently can benefit from continuous backups, since this can result in lower costs when scans of the whole bucket along with multiple requests per objects don't need to be performed on pre-existing objects (objects that are unchanged from the previous backup).
- Buckets that contain more than 100 million objects and that have a small delete rate compared to the overall backup size might realize cost benefits with a backup plan that contains both a continuous backup with a retention period of 2 days along with snapshots of a longer retention.

---

### Bucket size and estimated time to complete initial backup

<table>
<thead>
<tr>
<th>Bucket size</th>
<th>Number of objects</th>
<th>Estimated time to complete initial backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>800 TB (terabytes)</td>
<td>670 million</td>
<td>38 hours</td>
</tr>
<tr>
<td>6 PB (petabytes)</td>
<td>5 billion</td>
<td>100 hours</td>
</tr>
<tr>
<td>370 TB (terabytes)</td>
<td>7.5 billion</td>
<td>180 hours</td>
</tr>
</tbody>
</table>
Virtual machine backups

AWS Backup supports centralized and automated data protection for on-premises VMware virtual machines (VMs) along with VMs in the VMware Cloud™ (VMC) on AWS and VMware Cloud™ (VMC) on AWS Outposts. You can back up from your on-premises and VMC virtual machines to AWS Backup. Then, you can restore from AWS Backup to on-premises VMs, VMs in the VMC, or the VMC on AWS Outposts.

AWS Backup also provides you with fully-managed, AWS-native VM backup management capabilities, such as VM discovery, backup scheduling, retention management, a low-cost storage tier, cross-Region and cross-account copy, support for AWS Backup Vault Lock and AWS Backup Audit Manager, encryption that is independent from source data, and backup access policies. For a full list of capabilities and details, see the Feature availability by resource (p. 2) table.

You can use AWS Backup to protect your virtual machines on VMware Cloud™ on AWS Outposts. AWS Backup stores your VM backups in the AWS Region to which your VMware Cloud™ on AWS Outposts is
connected. You can use AWS Backup to protect your VMware Cloud™ on AWS Backup VMs when you're using VMware Cloud™ on AWS Outposts to meet your low-latency and local data-processing needs for your application data. Based on your data residency requirements, you may choose AWS Backup to store backups of your application data in the parent AWS Region to which your AWS Outposts is connected.

**Supported VMs**

AWS Backup can back up and restore the following virtual machines: VMware ESXi 6.7, 7.0, and 8.0 VMs running on NFS, VMFS, and VSAN datastores on premises and in VMC on AWS. In addition, AWS Backup supports both SCSI Hot-Add and Network Block Device Secure Sockets Layer (NBDSSL) transport modes for copying data from source VMs to AWS for on-premises VMware. To protect VMs on VMware Cloud on AWS, AWS Backup supports Hot-Add mode.

AWS Backup supports virtual machines managed by a VMware vCenter, including vSphere 8. AWS Backup supports VM virtual disk sizes that are multiples of 1 KiB.

AWS Backup does not support RDM (raw disk mapping) disks or NVMe controllers and their disks.

Note: VMs with independent-persistent and independent-non persistent disk modes are not supported.

**Backup consistency**

AWS Backup, by default, captures application-consistent backups of VMs using the VMware Tools quiescence setting on the VM. Your backups are application consistent if your applications are compatible with VMware Tools. If the quiescence capability is not available, AWS Backup captures crash-consistent backups. Validate that your backups meet your organization’s needs by testing your restores.

**Backup gateway**

Backup gateway is downloadable AWS Backup software that you deploy to your VMware infrastructure to connect your VMware VMs to AWS Backup. The gateway connects to your VM management server to discover VMs, discovers your VMs, encrypts data, and efficiently transfers data to AWS Backup. The following diagram illustrates how Backup gateway connects to your VMs:

To download the Backup gateway software, follow the procedure for [Working with gateways (p. 89)](##).

For information on VPC (Virtual Private Cloud) endpoints, see [AWS Backup and AWS PrivateLink connectivity](##).

Backup gateway comes with its own API which is separately maintained from the AWS Backup API. To view a list of Backup gateway API actions, see [Backup gateway actions](##). To view a list of Backup gateway API data types, see [Backup gateway data types](##).
Endpoints

Existing users who currently use a public endpoint and who wish to switch to a VPC (Virtual Private Cloud) endpoint can create a new gateway with a VPC endpoint using AWS PrivateLink, associate the existing hypervisor to the gateway, and then delete the gateway containing the public endpoint.

Configure your infrastructure to use Backup gateway

Backup gateway requires the following network, firewall, and hardware configurations to back up and restore your virtual machines.

Network configuration

Backup gateway requires certain ports to be allowed for its operation. Allow the following ports:

1. TCP 443 Outbound
   - Source: Backup gateway
   - Destination: AWS
   - Use: Allows Backup gateway to communicate with AWS.

2. TCP 80 Inbound
   - Source: The host you use to connect to the AWS Management Console
   - Destination: Backup gateway
   - Use: By local systems to obtain the Backup gateway activation key. Port 80 is only used during activation of Backup gateway. AWS Backup does not require port 80 to be publicly accessible. The required level of access to port 80 depends on your network configuration. If you activate your gateway from the AWS Management Console, the host from which you connect to the console must have access to your gateway's port 80.

3. UDP 53 Outbound
   - Source: Backup gateway
   - Destination: Domain Name Service (DNS) server
   - Use: Allows Backup gateway to communicate with the DNS.

4. TCP 22 Outbound
   - Source: Backup gateway
   - Destination: AWS Support
   - Use: Allows AWS Support to access your gateway to help you with issues. You don't need to open this port for the normal operation of your gateway, but you must open it for troubleshooting.

5. UDP 123 Outbound
   - Source: NTP client
   - Destination: NTP server
   - Use: Used by local systems to synchronize virtual machine time to the host time.

6. TCP 443 Outbound
   - Source: Backup gateway
   - Destination: VMware vCenter
   - Use: Allows Backup gateway to communicate with VMware vCenter.

7. TCP 443 Outbound
   - Source: Backup gateway
   - Destination: ESXi hosts
   - Use: Allows Backup gateway to communicate with ESXi hosts.

8. TCP 902 Outbound
• Source: Backup gateway
• Destination: VMware ESXi hosts
• Use: Used for data transfer via Backup gateway.

Firewall configuration

Backup gateway requires access to the following service endpoints to communicate with Amazon Web Services. If you use a firewall or router to filter or limit network traffic, you must configure your firewall and router to allow these service endpoints for outbound communication to AWS. Use of an HTTP proxy in between Backup gateway and service points is not supported.

proxy-app.backup-gateway.region.amazonaws.com:443
dp-1.backup-gateway.region.amazonaws.com:443
anon-cp.backup-gateway.region.amazonaws.com:443
client-cp.backup-gateway.region.amazonaws.com:443

Configure your gateway for multiple NICs in VMware

You can maintain separate networks for your internal and external traffic by attaching multiple virtual network interface connections (NICs) to your gateway and then directing internal traffic (gateway to hypervisor) and external traffic (gateway to AWS) separately.

By default, virtual machines connected to AWS Backup gateway have one network adapter (eth0). This network includes the hypervisor, the virtual machines, and network gateway (AWS Backup gateway) which communicates with the broader Internet.

Here is an example of a setup with multiple virtual network interfaces:

<table>
<thead>
<tr>
<th>Network Adapter</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>10.0.3.83</td>
<td>10.0.3.0/24</td>
</tr>
<tr>
<td>eth1</td>
<td>10.0.0.241</td>
<td>10.0.0.0/24</td>
</tr>
</tbody>
</table>

• In this example, the connection is to a hypervisor with IP 10.0.3.123, the gateway will use eth0 as the hypervisor IP is part of the 10.0.3.0/24 block
• To connect to a hypervisor with IP 10.0.0.234, the gateway will use eth1
• To connect to an IP outside of the local networks (ex. 34.193.121.211), the gateway will fall back to the default gateway, 10.0.0.1, which is in the 10.0.0.0/24 block and thus go through eth1

The first sequence to add an additional network adapter occurs in the vSphere client:
1. In the VMware vSphere client, open the context menu (with a right-click) for your gateway virtual machine, and choose Edit Settings.
2. On the Virtual Hardware tab of the Virtual Machine Properties dialog box, open the Add New Device menu, and select Network Adapter to add a new network adapter.
3. a. Expand the New Network details to configure the new adapter.
   b. Ensure that Connect At Power On is selected.
c. For Adapter Type, see Network Adapter Types in the ESXi and vCenter Server Documentation.

4. Click Okay to save the new network adapter settings.

The next sequence of steps to configure an additional adapter occurs in the AWS Backup gateway console (note this is not the same interface as the AWS management console where backups and other services are managed).

Once the new NIC is added to the gateway VM, you need to

- Go to Command Prompt and turn on the new adapters
- Configure static IPs for each new NIC
- Set the preferred NIC as the default

To do these:

1. In the VMware vSphere client, select your gateway virtual machine and Launch Web Console to access the Backup Gateway local console.
   - For more information on accessing a local console, see Accessing the Gateway Local Console with VMware ESXi

2. Exit Command Prompt and go to Network Configuration > Configure Static IP and follow the setup instructions to update the routing table.
   a. Assign a static IP within the network adapter’s subnet.
   b. Set up a network mask.
   c. Enter the IP address of the default gateway. This is the network gateway that connects to all traffic outside of the local network.

3. Select Set Default Adapter to designate the adapter that will be connected to the cloud as the default device.

4. All IP addresses for the gateway can be displayed in both the local console and on the VM summary page in VMware vSphere.

Hardware requirements

You must be able to dedicate the following minimum resources on a virtual machine host for the Backup gateway:

- 4 virtual processors
- 8 GiB of reserved RAM

VMware permissions

This section lists the minimum VMware permissions required to use Backup gateway. These permissions are necessary for Backup gateway to discover, backup, and restore virtual machines.

To use Backup gateway, create a dedicate user with the following permissions. They are listed based on the VMware permissions hierarchy.

Global

- Disable methods
- Enable methods
• Licenses
• Log event
• Manage custom attributes
• Set custom attributes

**vSphere Tagging**
• Assign or Unassign vSphere Tag

**DataStore**
• Allocate space
• Browse datastore
• Configure datastore (for vSAN datastore)
• Low level file operations
• Update virtual machine files

**Host**
• Configuration
  • Advanced settings
  • Storage partition configuration

**Folder**
• Create folder

**Network**
• Assign network

**dvPort Group**
• Create
• Delete

**Resource**
• Assign virtual machine to resource pool

**Virtual Machine**
• Change Configuration
  • Acquire disk lease
  • Add existing disk
  • Add new disk
  • Advanced configuration
  • Change settings
Working with gateways

To back up and restore your virtual machines (VMs) using AWS Backup, you must first install a Backup gateway. A gateway is software in the form of an OVF (Open Virtualization Format) template that connects Amazon Web Services Backup to your hypervisor, allowing it to automatically detect your virtual machines, and enables you to back up and restore them.

A single gateway can run up to 4 backup or restore jobs at once. To run more than 4 jobs at once, create more gateways and associate them with your hypervisor.

Creating a gateway

To create a gateway:
2. In the left navigation pane, under the External resources section, choose Gateways.
3. Choose Create gateway.
4. In the Set up gateway section, follow these instructions to download and deploy the OVF template.

Downloading VMware software

Connecting the hypervisor

Gateways connect AWS Backup to your hypervisor so you can create and store backups of your virtual machines. To set up your gateway on VMware ESXi, download the OVF template. The download may take about 10 minutes.
After it is complete, proceed with the following steps:

1. Connect to your virtual machine hypervisor using VMware vSphere.
2. Right-click a parent object of a virtual machine and select *Deploy OVF Template*.

3. Choose **Local file**, and upload the *aws-appliance-latest.ova* file you downloaded.
4. Follow the deployment wizard steps to deploy it. On the **Select storage** page, select virtual disk format **Thick Provision Lazy Zeroed**.

5. After deploying the OVF, right-click the gateway and choose **Edit Settings**.
a. Under **VM Options**, go to **VM Tools**.
b. Ensure that for **Synchronize Time with Host**, **Synchronize at start up and resume** is selected.
6. Turn on the virtual machine by selecting “Power On” from the Actions menu.
7. Copy the IP address from the VM summary and enter it below.

Once the VMWare software is downloaded, complete the following steps:

1. In the Gateway connection section, type in the IP address of the gateway.
   a. To find this IP address, go to the vSphere Client.
   b. Select your gateway under the Summary tab.
c. Copy the **IP address** and paste it in the AWS Backup console text bar.

2. In the **Gateway settings** section,
   a. Type in a **Gateway name**.
   b. Verify the AWS Region.
   c. Choose whether the endpoint is publicly accessible or hosted with your virtual private cloud (VPC).
   d. Depending on the endpoint chosen, enter the VPC endpoint DNS Name. 

   *For more information, see [Creating a VPC endpoint](#).*

3. **[Optional]** In the **Gateway tags** section, you can assign tags by inputting the **key** and **optional value**. To add more than one tag, click **Add another tag**.

4. To complete the process, click **Create gateway**, which takes you to the gateway detail page.

**Editing or deleting a gateway**

**To edit or delete a gateway:**

1. In the left navigation pane, under the **External resources** section, choose **Gateways**.
2. In the **Gateways** section, choose a gateway by its **Gateway name**.
3. To edit the gateway name, choose **Edit**.
4. To delete the gateway, choose **Delete**, then choose **Delete gateway**.

   You cannot reactivate a deleted gateway. If you want to connect to the hypervisor again, follow the procedure in [Creating a gateway](#) (p. 89).

5. To connect to a hypervisor, in the **Connected hypervisor** section, choose **Connect**.

   Each gateway connects to a single hypervisor. However, you can connect multiple gateways to the same hypervisor to increase the bandwidth between them beyond that of the first gateway.

6. To assign, edit, or manage tags, in the **Tags** section, choose **Manage tags**.

**Backup Gateway Bandwidth Throttling**

**Note**

This feature will be available on new gateways deployed after December 15, 2022. For existing gateways, this new capability will be available through an automatic software update on or before January 30, 2023. To update the gateway to the latest version manually, use AWS CLI command `UpdateGatewaySoftwareNow`.

You can limit the upload throughput from your gateway to AWS Backup to control the amount of network bandwidth the gateway uses. By default, an activated gateway has no rate limits.

You can configure a bandwidth rate-limit schedule using the AWS Backup Console or using API through the AWS CLI ([PutBandwidthRateLimitSchedule](#)). When you use a bandwidth rate limit schedule, you can configure limits to change automatically throughout the day or week.

Bandwidth rate limiting works by balancing the throughput of all data being uploaded, averaged over each second. While it is possible for uploads to cross the bandwidth rate limit briefly for any given micro- or millisecond, this does not typically result in large spikes over longer periods of time.

You can add up to a maximum of 20 intervals. The maximum value for the upload rate is 8,000,000 (million) megabytes per second (Mbps).
View and edit the bandwidth rate-limit schedule for your gateway using the AWS Backup console.

This section describes how to view and edit the bandwidth rate limit schedule for your gateway.

To view and edit the bandwidth rate limit schedule

2. In the left navigation pane, choose Gateways. In the Gateways pane, gateways are displayed by name. Click the radio button adjacent to the gateway name you want to manage.
3. Once you select a radio button, the drop-down menu Action is available to click. Click Actions, then click Edit bandwidth rate limit schedule. The current schedule is displayed. By default, a new or unedited gateway has no defined bandwidth rate limits.

   **Note**
   You can also click Manage schedule in the gateway details page to navigate to the Edit bandwidth page.

4. **(Optional)** Choose Add interval to add a new configurable interval to the schedule. For each interval, input the following information:
   a. **Days of week** — Select the recurring day or days on which you want the interval to apply. When chosen, the days will display below the drop-down menu. You can remove them by clicking the X next to the day.
   b. **Start time** — Enter the start time for the bandwidth interval, using the HH:MM 24-hour format. Time is rendered in Universal Coordinated Time (UTC).

   **Note:** Your bandwidth-rate-limit interval begins at the start of the specified minute.

   c. **End time** — Enter the end time for the bandwidth interval, using the HH:MM 24-hour format. Time is rendered in Universal Coordinated Time (UTC).

      **Important**
      The bandwidth-rate-limit interval ends at the end of the minute specified. To schedule an interval that ends at the end of an hour, enter 59. To schedule consecutive continuous intervals, transitioning at the start of the hour, with no interruption between the intervals, enter 59 for the end minute of the first interval. Enter 00 for the start minute of the succeeding interval.

   d. **Upload rate** — Enter the upload rate limit, in megabits per second (Mbps). The minimum value is 102 megabytes per second (Mbps).

5. **(Optional)** Repeat the previous step as desired until your bandwidth rate-limit schedule is complete. If you need to delete an interval from your schedule, choose Remove.

   **Important**
   Bandwidth rate-limit intervals cannot overlap. The start time of an interval must occur after the end time of a preceding interval and before the start time of a following interval; its end time must occur before the start time of the following interval.

6. When you are finished, click the Save changes button.

View and edit the bandwidth rate-limit schedule for your gateway using AWS CLI.

The GetBandwidthRateLimitSchedule action can be used to view the bandwidth throttle schedule for a specified gateway. If there is no schedule set, the schedule will be an empty list of intervals. Here is an example using the AWS CLI to fetch the bandwidth schedule of a gateway:

```
```
To edit a gateway's bandwidth throttle schedule, you can use the `PutBandwidthRateLimitSchedule` action. Note that you can only update a gateway's schedule as a whole, rather than modifying, adding, or removing individual intervals. Calling this action will overwrite the gateway's previous bandwidth throttle schedule.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

### Working with hypervisors

After you finish Creating a gateway (p. 89), you can connect it to a hypervisor to enable AWS Backup to work with the virtual machines managed by that hypervisor. For example, the hypervisor for VMware VMs is VMware vCenter Server. Ensure your hypervisor is configured with the necessary permissions for AWS Backup.

#### Adding a hypervisor

**To add a hypervisor:**

1. In the left navigation pane, under the External resources section, choose Hypervisors.
2. Choose Add hypervisor.
3. In the Hypervisor settings section, type in a Hypervisor name.
4. For vCenter server host, use the dropdown menu to select either IP address or FQDN (fully-qualified domain name). Type in the corresponding value.
5. To allow AWS Backup to discover the virtual machines on the hypervisor, enter the hypervisor's Username and Password.
6. Encrypt your password. You can specify this encryption by selecting a specific service-managed KMS key or a customer-managed KMS key using the dropdown menu or choose Create KMS key. If you do not select a specific key, AWS Backup will encrypt your password using a service-owned key.
7. In the Connecting gateway section, use the dropdown list to specify which Gateway to connect to your hypervisor.
8. Choose Test gateway connection to verify your previous inputs.
9. Optionally, in the Hypervisor tags section, you can assign tags to the hypervisor by choosing Add new tag.
10. Optional VMware tag mapping: You can add up to 10 VMware tags you currently use on your virtual machines to generate AWS tags.
11. In the Log group setting panel, you may choose to integrate with Amazon CloudWatch Logs to maintain logs of your hypervisor (standard CloudWatch Logs pricing will apply based on usage). Each hypervisor can belong to one log group.
   a. If you have not yet created a log group, select the Create a new log group radio button. The hypervisor you are editing will be associated with this log group.
   b. If you have previously created a log group for a different hypervisor, you can use that log group for this hypervisor. Select Use an existing log group.
   c. If you do not want CloudWatch logging, select Deactivate logging.
12. Choose Add hypervisor, which takes you to its detail page.

**Tip**

You can use Amazon CloudWatch Logs (see step 11 above) to obtain information about your hypervisor, including error monitoring, network connection between the gateway and the hypervisor, and network configuration information. For information about CloudWatch log groups, see Working with Log Groups and Log Streams in the Amazon CloudWatch User Guide.
Viewing virtual machines managed by a hypervisor

To view virtual machines on a hypervisor:

1. In the left navigation pane, under the External resources section, choose Hypervisors.
2. In the Hypervisors section, choose a hypervisor by its Hypervisor name to go to its detail page.
3. In the section under Hypervisor summary, choose the Virtual machines tab.
4. In the Connected virtual machines section, a list of virtual machines populates automatically.

Viewing gateways connected to a hypervisor

To view gateways connected to the hypervisor:

1. Choose the Gateways tab.
2. In the Connected gateways section, a list of gateways populates automatically.

Connecting a hypervisor to additional gateways

Your backup and restore speeds might be limited by the bandwidth of the connection between your gateway and hypervisor. You can increase these speeds by connecting one or more additional gateways to your hypervisor. You can do this in the Connected gateways section as follows:

1. Choose Connect.
2. Select another gateway using the dropdown menu. Alternatively, choose Create gateway to create a new gateway.
3. Choose Connect.

Editing a hypervisor configuration

If you do not use the Test gateway connection feature, you might add a hypervisor with an incorrect username or password. In that case, the hypervisor’s connection status is always Pending. Alternatively, you might rotate the username or password to access your hypervisor. Update this information using the following procedure:

To edit an already-added hypervisor:

1. In the left navigation pane, under the External resources section, choose Hypervisors.
2. In the Hypervisors section, choose a hypervisor by its Hypervisor name to go to its detail page.
3. Choose Edit.
4. The top panel is named Hypervisor settings.
   a. Under vCenter server host, you can also edit the FQDN (Fully-Qualified Domain Name) or the IP address.
   b. Optionally, enter the hypervisor’s Username and Password.
5. In the Log group setting panel, you may choose to integrate with Amazon CloudWatch to maintain logs of your hypervisor (standard CloudWatch pricing will apply based on usage). Each hypervisor can belong to one log group.
   a. If you have not yet created a log group, select the Create a new log group radio button. The hypervisor you are editing will be associated with this log group.
   b. If you have previously created a log group for a different hypervisor, you can use that log group for this hypervisor. Select Use an existing log group.
   c. If you do not want CloudWatch logging, select Deactivate logging.
Tip
You can use Amazon CloudWatch Logs (see step 5 above) to obtain information about your hypervisor, including error monitoring, network connection between the gateway and the hypervisor, and network configuration information. For information about CloudWatch log groups, see Working with Log Groups and Log Streams in the Amazon CloudWatch User Guide.

To update a hypervisor programmatically, use the CLI command update-hypervisor and UpdateHypervisor API call.

Deleting a hypervisor configuration
If you need to remove an already-added hypervisor, remove the hypervisor configuration and add another. This remove operation applies to the configuration to connect to the hypervisor. It does not delete the hypervisor.

To delete the configuration to connect to an already-added hypervisor:
1. In the left navigation pane, under the External resources section, choose Hypervisors.
2. In the Hypervisors section, choose a hypervisor by its Hypervisor name to go to its detail page.
3. Choose Remove, then choose Remove hypervisor.
4. Optional: replace the removed hypervisor configuration using the procedure for Adding a hypervisor (p. 97).

Understanding hypervisor status
The following describes each of the possible hypervisor statuses and, if applicable, remediation steps. The ONLINE status is the normal status of the hypervisor. A hypervisor should have this status all or most of the time it’s in use for backup and recovery of VMs managed by the hypervisor.

Hypervisor statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning and remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONLINE</td>
<td>You added a hypervisor to AWS Backup, associated with it a gateway, and can connect with that gateway over your network to perform backup and recovery of virtual machines managed by the hypervisor. You can perform on-demand and scheduled backups of those virtual machines at any time.</td>
</tr>
<tr>
<td>PENDING</td>
<td>You added a hypervisor to AWS Backup but:</td>
</tr>
<tr>
<td></td>
<td>• It is not associated with any gateway, or</td>
</tr>
<tr>
<td></td>
<td>• It is associated with one or more gateways, but all those gateways were deleted or are otherwise not active.</td>
</tr>
<tr>
<td></td>
<td>To change a hypervisor status from PENDING to ONLINE, create a gateway and connect your hypervisor to that gateway.</td>
</tr>
<tr>
<td>OFFLINE</td>
<td>You added a hypervisor to AWS Backup and associated it with a gateway, but the gateway cannot connect to the hypervisor over your network.</td>
</tr>
</tbody>
</table>
Status | Meaning and remediation
---|---
OFFLINE | To change a hypervisor status from OFFLINE to ONLINE, verify the correctness of your network configuration.
 | If the issue persists, verify that your hypervisor's IP address or fully-qualified domain name is correct. If they are incorrect, add your hypervisor again using the correct information and test your gateway connection.
ERROR | You added a hypervisor to AWS Backup and associated it with a gateway, but the gateway cannot communicate with the hypervisor.
 | To change a hypervisor status from ERROR to ONLINE, verify that hypervisor's username and password are correct. If they are incorrect, edit your hypervisor configuration.

Next steps

To back up virtual machines on your hypervisor, see Backing up virtual machines (p. 100).

Backing up virtual machines

**Note**
AWS Backup support for VMware is not available in Asia Pacific (Jakarta) Region, China (Beijing) Region or China (Ningxia) Region.

After Adding a hypervisor (p. 97), Backup gateway automatically lists your virtual machines. You can view your virtual machines by choosing either Hypervisors or Virtual machines in the left navigation pane.

- Choose Hypervisors to view only the virtual machines managed by a specific hypervisor. With this view, you can work with one virtual machine at a time.
- Choose Virtual machines to view all the virtual machines across all the hypervisors you added to your AWS account. With this view, you can work with some or all your virtual machines across multiple hypervisors.

Regardless of which view you choose, to perform a backup operation on a specific virtual machine, choose its VM name to open its detail page. The VM detail page is the starting point for the following procedures.

Creating an on-demand backup of a virtual machine

An on-demand backup is a one-time, full backup you manually initiate. You can use on-demand backups to test AWS Backup's backup and restore capabilities.

To create an on-demand backup of a virtual machine:

1. Choose Create on-demand backup.
2. Configure your on-demand backup.
3. Choose Create on-demand backup.
4. Check when your backup job has the status Completed. In the left navigation menu, choose Jobs.
5. Choose the Backup Job ID to view backup job information such as the Backup size and time elapsed between the Creation date and Completion date.

**Incremental VM backups**

Newer VMware versions contain a feature called Changed Block Tracking, which keeps track of the storage blocks of virtual machines as they change over time. When you use AWS Backup to back up a virtual machine, AWS Backup attempts to use the CBT data if it is available. AWS Backup uses CBT data to speed up the backup process; without CBT data, backup jobs are often slower and use more hypervisor resources. The backup can still be successfully completed even when the CBT data is not valid or available. For example, the CBT data might not be valid or might be unavailable if the virtual machine or ESXi host experiences a hard shutdown.

On the occasions CBT data is invalid or unavailable, the backup status will read Successful with a message. In these cases, the message will indicate that, in the absence of CBT data, AWS Backup used its own proprietary change detection mechanism to complete the backup instead of VMware’s CBT data. Subsequent backups will reattempt to use CBT data, and in most cases the CBT data will be successfully valid and available. If the issue persists, see VMware Troubleshooting for steps to remedy.

For CBT to function correctly, the following must be true:

- Host needs to be ESXi 4.0 or later
- The VM owning the disks must have hardware version 7 or later
- CBT must be enabled for the virtual machine (it is enabled by default)

To verify if a virtual disk has CBT enabled:

1. Open the vSphere Client and select a powered-off virtual machine.
2. Right-click the virtual machine and navigate to Edit Settings > Options > Advanced/General > Configuration Parameters.
3. The option ctkEnabled needs to equal True.

**Automating virtual machine backup by assigning resources to a backup plan**

A backup plan is a user-defined data protection policy that automates data protection across many AWS services and third-party applications. You first create your backup plan by specifying its backup frequency, retention period, lifecycle policy, and many other options. To create a backup plan, see Getting started tutorial.

After you create your backup plan, you assign AWS Backup-supported resources, including virtual machines, to that backup plan. AWS Backup offers many ways to assign resources, including assigning all the resources in your account, including or excluding single specific resources, or adding resources with certain tags.

In addition to its existing resource assignment features, AWS Backup support for virtual machines introduces several new features to help you quickly assign virtual machines to backup plans. From the Virtual machines page, you can assign tags to multiple virtual machines or use the new Assign resources to plan feature. Use these features to assign your virtual machines already discovered by AWS Backup gateway.

If you anticipate discovering and assigning additional virtual machines in the future, and would like to automate the resource assignment step to include those future virtual machines, use the new Create group assignment feature.
VMware Tags

Tags are key-value pairs you can use to manage, to filter, and to search for your resources.

A VMware tag is composed of a category and a tag name. VMware tags are used to group virtual machines. A tag name is a label assigned to a virtual machine. A category is a collection of tag names.

In AWS tags, you can use characters among UTF-8 letters, numbers, spaces, and special characters + - = . _ /.

If you use tags on your virtual machines, you can add up to 10 matching tags in AWS Backup to help with organization. You can map up to 10 VMware tags to AWS tags. In the AWS Backup console, these can be found in My organization > Virtual Machines > AWS tags or VMware tags.

VMware tag mapping

If you use tags on your virtual machines, you can add up to 10 matching tags in AWS Backup for additional clarity and organization. Mappings apply to any virtual machine on the hypervisor.

2. In the console, go to edit Hypervisor (Click External resources, then Hypervisors, then click the Hypervisor name, then click Manage mappings).
3. The last pane, VMware tag mapping, contains four textbox fields into which you can enter your extant VMware tag information into corresponding AWS tags. The four fields are VMware tag category, VMware tag name, AWS tag key, and AWS tag value (example: Category = OS; Tag name = Windows; AWS tag key = OS-Windows, and AWS tag value = Windows).
4. Once you have entered your preferred values, click Add mapping. If you make an error, you can click Remove to delete entered information.
5. After adding mapping(s), specify the IAM role you intend to use to apply these AWS tags to the VMware virtual machines.

The policy AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync contains needed permissions. You can attach this policy to the role you are using (or have an administrator attached it) or you can create a custom policy for the role being used.

6. Lastly, click Add hypervisor or Save.

The IAM role trust relationship should be modified to add the backup-gateway.amazonaws.com and backup.amazonaws.com services. Without this service, you will likely experience an error when you map tags. To edit the trust relationship for an existing role,

1. Log into the IAM console.
2. In the navigation pane of the console, choose Roles.
3. Choose the name of the role you wish to modify, then select the Trust relationships tab on the details page.
4. Under Policy Document, paste the following:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "backup.amazonaws.com",
               "backup-gateway.amazonaws.com"
            ]
      ]
   ]
}
```
5. Choose **Update Trust Policy**.


### View VMware tag mappings

In the AWS Backup console, click on **External Resources**, then click on **Hypervisors**, then click on the Hypervisor name link to view properties for the selected hypervisor. Under the summary pane, there are four tabs, the last of which is **VMware tag mappings**. Note if you do not yet have mappings, "No VMware tag mappings." will be displayed.

From here, you can sync the metadata of virtual machines discovered by the hypervisor, you can copy mappings to your hypervisor(s), you can add AWS tags mapped to teh VMware tags to the backup selection of a backup plan, or you can manage mappings.

In the console, to see which tags are applied to a selected virtual machine, click **Virtual machines**, then the virtual machine name, then **AWS tags** or **VMware tags**. You can view the tags associated with this virtual machine, and additionally you can manage the tags.

### Assign virtual machines to plan using VMware tag mappings

To assign virtual machines to a backup plan using mapped tags, do the following:

2. In the console go to VMware tag mappings on the hypervisor details page (click **External resources**, then click **Hypervisors** then click on the hypervisor name).
3. Select the checkbox next to multiple mapped tags to assign those tags to the same backup plan.
4. Click **Add to resource assignment**.
5. Choose an existing **Backup plan** from the dropdown list. Alternatively, you can choose **Create backup plan** to create a new backup plan.
6. Click **Confirm**. This opens the **Assign resources** page with **Refine selection using tags** fields with values pre-populated.

### VMware tags using the AWS CLI

AWS Backup uses the API call `PutHypervisorPropertyMappings` to map hypervisor entity properties in on-premise to properties in AWS.

In the AWS CLI, use the operation `put-hypervisor-property-mappings`:

```bash
aws backup-gateway put-hypervisor-property-mappings
  --hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId
  --vmware-to-aws-tag-mappings list of VMware to AWS tag mappings
  --iam-role-arn arn:aws:iam::account:role/roleName
  --region AWSRegion
  --endpoint-url URL
```

Here is an example:
aws backup-gateway put-hypervisor-property-mappings
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345
--vmware-to-aws-tag-mappings VmwareCategory=OS, VmwareTagName=Windows, AwsTagKey=OS-Windows, AwsTagValue=Windows
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole
--region us-east-1

You can also use GetHypervisorPropertyMappings to assist with property mappings information. In the AWS CLI, use the operation get-hypervisor-property-mappings. Here is an example template:

aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion

Here is an example:

aws backup-gateway get-hypervisor-property-mappings
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345
--region us-east-1

Sync metadata of virtual machines discovered by the hypervisor in AWS using API, CLI, or SDK

You can sync the metadata of virtual machines. When you do, the VMware tags present on the virtual machine that are part of the mappings will be synched. Also, AWS tags mapped to the VMware tags present on the virtual machine will be applied to the AWS Virtual Machine resource.

AWS Backup uses the API call StartVirtualMachinesMetadataSync to sync the metadata of the virtual machines discovered by the hypervisor. To sync metadata of virtual machines discovered by the hypervisor using AWS CLI, use the operation start-virtual-machines-metadata-sync.

Example template:

aws backup-gateway start-virtual-machines-metadata-sync
--hypervisor-arn HypervisorARN
--region AWSRegion

Example:

aws backup-gateway start-virtual-machines-metadata-sync
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345
--region us-east-1

You can also use GetHypervisor to assist with hypervisor information, such as host, state, status of latest metadata sync, and also to retrieve the last successful metadata sync time. In the AWS CLI, use the operation get-hypervisor.

Example template:

aws backup-gateway get-hypervisor
--hypervisor-arn HypervisorARN
--region AWSRegion

Example:

aws backup-gateway get-hypervisor
Virtual machine backups

```
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345
--region us-east-1
```

For more information, see API documentation [VmwareTag](#) and [VmwareToAwsTagMapping](#).

This feature will be available on new gateways deployed after December 15, 2022. For existing gateways, this new capability will be available through an automatic software update on or before January 30, 2023. To update the gateway to the latest version manually, use AWS CLI command [UpdateGatewaySoftwareNow](#).

Example:

```
aws backup-gateway update-gateway-software-now
--region us-east-1
```

Assigning virtual machines using tags

You can assign your virtual machines currently discovered by AWS Backup, along with other AWS Backup resources, by assigning them a tag that you have already assigned to one of your existing backup plans. You can also create a new backup plan and a new tag-based resource assignment. Backup plans check for newly-assigned resources each time they run a backup job.

**To tag multiple virtual machines with the same tag:**

1. In the left navigation pane, choose **Virtual machines**.
2. Select the checkbox next to **VM name** to choose all your virtual machines. Alternatively, select the checkbox next to the VM names you want to tag.
3. Choose **Add tags**.
4. Type in a tag **Key**.
5. Recommended: type in a tag **Value**.
6. Choose **Confirm**.

Assigning virtual machines using the Assign resources to plan feature

You can assign virtual machines currently discovered by AWS Backup to an existing or new backup plan using the **Assign resources to plan** feature.

**To assign virtual machines using the Assign resources to plan feature:**

1. In the left navigation pane, choose **Virtual machines**.
2. Select the checkbox next to **VM name** to choose all your virtual machines. Alternatively, select the checkbox next to multiple VM names to assign them to the same backup plan.
3. Choose **Assignments**, then choose **Assign resources to plan**.
4. Type in a **Resource assignment name**.
5. Choose a resource assignment **IAM role** to create backups and manage recovery points. If you do not have a specific IAM role to use, we recommend the **Default role** which has the correct permissions.
6. In the **Backup plan** section, choose an existing **Backup plan** from the dropdown list. Alternatively, choose **Create backup plan** to create a new backup plan.
7. Choose **Assign resources**.
8. Optional: Verify your virtual machines are assigned to a backup plan by choosing **View Backup plan**. Then, in the **Resource assignments** section, choose the resource assignment **Name**.
Assigning virtual machines using the Create group assignment feature

Unlike the preceding two resource assignment features for virtual machines, the Create group assignment feature not only assigns virtual machines currently discovered by AWS Backup, but also virtual machines discovered in the future in a folder or hypervisor you define.

Also, you do not need to select any checkboxes to use the Create group assignment feature.

To assign virtual machines using the Assign resources to plan feature:

1. In the left navigation pane, choose Virtual machines.
2. Choose Assignments, then choose Create group assignment.
3. Type in a Resource assignment name.
4. Choose a resource assignment IAM role to create backups and manage recovery points. If you do not have a specific IAM role to use, we recommend the Default role which has the correct permissions.
5. In the Resource group section, select the Group type dropdown menu. Your options are Folder or Hypervisor.
   a. Choose Folder to assign all the virtual machines in a folder on a hypervisor. Select a folder Group name, such as datacenter/vm, using the dropdown menu. You can also choose to include Subfolders.
      Note
      To make Folder-based assignments, during the discovery process, AWS Backup tags virtual machines with the folder it finds them in during the discovery process. If you later move a virtual machine to a different folder, AWS Backup cannot update the tag for you due to AWS tagging best practices. This assignment method might result in continuing to take backups of virtual machines you moved out of your assigned folder.
   b. Choose Hypervisor to assign all the virtual machines managed by a hypervisor. Select a hypervisor ID Group name using the dropdown menu.
6. In the Backup plan section, choose an existing Backup plan from the dropdown list. Alternatively, choose Create backup plan to create a new backup plan.
7. Choose Create group assignment.
8. Optional: verify your virtual machines are assigned to a backup plan by choosing View Backup plan. In the Resource assignments section, choose the resource assignment Name.

Next steps

To restore a virtual machine, see Restoring a virtual machine (p. 144).

Information about third-party source components for Backup gateway

In this section, you can find information about third party tools and licenses that we depend on to deliver Backup gateway functionality.

The source code for certain third-party source software components that are included with the Backup gateway software is available for download at the following locations:

- For gateways deployed on VMware ESXi, download sources.tgz.

This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit (http://www.openssl.org/).
This product includes software developed by VMware® vSphere Software Development Kit (https://www.vmware.com).

For the relevant licenses for all dependent third-party tools, see Third-Party Licenses.

Open-source components for AWS Appliance

Several third-party tools and licenses are used to deliver functionality for Backup gateway.

Use the following links to download source code for certain open-source software components that are included with AWS Appliance software:

- For gateways deployed on VMware ESXi, download sources.tar

This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit (http://www.openssl.org/). For the relevant licenses for all dependent third-party tools, see Third-Party Licenses.

Troubleshoot VM issues

Incremental Backups / CBT issues and messages

Failure message: "The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."

If this message continues, reset CBT as directed by VMware.

Message notes CBT was not turned on or was unavailable: "VMware Change Block Tracking (CBT) was not available for this virtual machine, but the incremental backup was successfully completed with our proprietary change mechanism."

Check to make sure CBT is turned on. To verify if a virtual disk has CBT enabled:

1. Open the vSphere Client and select a powered-off virtual machine.
2. Right-click the virtual machine and navigate to Edit Settings > Options > Advanced/General > Configuration Parameters.
3. The option ctkEnabled needs to equal True.

If it is turned on, ensure you are using up-to-date VMware features. The host must be ESXi 4.0 or later and the virtual machine owning the disks to be tracked must be hardware version 7 or later.

If CBT is turned on (enabled) and the software and hardware are up to date, turn off the virtual machine and then turn it back on again. Ensure that CBT is turned on. Then, perform the backup again.

Advanced DynamoDB backup

AWS Backup supports additional, advanced features for your Amazon DynamoDB data protection needs. After you enable AWS Backup's advanced features in your AWS Region, you unlock the following features for all new for DynamoDB table backups you create:

- Cost savings and optimization:
  - Tiering backups to cold storage to reduce storage costs
  - Cost allocation tagging for use with Cost Explorer
• Business continuity:
  • Cross-Region copy
  • Cross-account copy
• Security:
  • Store backups in encrypted AWS Backup vaults, which you can secure with AWS Backup Vault Lock, AWS Backup policies, and encryption keys.
  • Backups inherit tags from their source DynamoDB tables, allowing you to use those tags to set permissions and service control policies (SCPs).

New customers onboarding to AWS Backup after November 2021 have advanced DynamoDB backup features enabled by default. Specifically, advanced DynamoDB backup features are enabled by default to customers who have not created a backup vault prior to November 21, 2021.

We recommend all existing AWS Backup customers enable advanced features for DynamoDB. There is no difference in warm backup storage pricing after you enable advanced features. You can save money by tiering backups to cold storage and optimize your costs by using cost allocation tags. You can also start taking advantage of AWS Backup’s business continuity and security features.

**Note**
If you use a custom role or policy instead of AWS Backup’s default service role, you must add or use the following permissions policies (or add their equivalent permissions) to your custom role:

- AWSBackupServiceRolePolicyForBackup to perform advanced DynamoDB backup.
- AWSBackupServiceRolePolicyForRestores to restore advanced DynamoDB backups.

To learn more about AWS-managed policies and view examples of customer-managed policies, see [Managed policies for AWS Backup](p. 246).

**Topics**
- Enabling advanced DynamoDB backup using the console (p. 108)
- Enabling advanced DynamoDB backup programmatically (p. 109)
- Editing an advanced DynamoDB backup (p. 109)
- Restoring an advanced DynamoDB backup (p. 110)
- Deleting an advanced DynamoDB backup (p. 110)
- Other benefits of full AWS Backup management when you enable advanced DynamoDB backup (p. 110)

### Enabling advanced DynamoDB backup using the console

You can enable AWS Backup advanced features for DynamoDB backups using either the AWS Backup or DynamoDB console.

**To enable advanced DynamoDB backup features from the AWS Backup console:**

2. In the left navigation menu, choose **Settings**.
3. Under the **Supported services** section, verify that **DynamoDB** is **Enabled**.
4. If it is not, choose **Opt-in** and enable DynamoDB as an AWS Backup supported service.
5. Under the **Advanced features for DynamoDB backups** section, choose **Enable**.
6. Choose **Enable features**.
For how to enable AWS Backup advanced features using the DynamoDB console, see Enabling AWS Backup features in the Amazon DynamoDB User Guide.

Enabling advanced DynamoDB backup programmatically

You can also enable AWS Backup advanced features for DynamoDB backups using the AWS Command Line Interface (CLI). You enable advanced DynamoDB backups when you set both of the following values to true:

**To programmatically enable AWS Backup advanced features for DynamoDB backups:**

1. Check if you already enabled AWS Backup advanced features for DynamoDB using the following command:

   ```bash
   $ aws backup describe-region-settings
   ```

   If "DynamoDB":true under both "ResourceTypeManagementPreference" and "ResourceTypeOptInPreference", you have already enabled advanced DynamoDB backup.

   If, like the following output, you have at least one instance of "DynamoDB":false, you have not yet enabled advanced DynamoDB backup, proceed to the next step.

   ```json
   {
     "ResourceTypeManagementPreference":{
       "DynamoDB":false,
       "EFS":true
     }
   "ResourceTypeOptInPreference":{
     "Aurora":true,
     "DocumentDB":false,
     "DynamoDB":false,
     "EBS":true,
     "EC2":true,
     "EFS":true,
     "FSx":true,
     "Neptune":false,
     "RDS":true,
     "Storage Gateway":true
   }
   }
   ```

2. Use the following UpdateRegionSettings operation to set both "ResourceTypeManagementPreference" and "ResourceTypeOptInPreference" to "DynamoDB":true:

   ```bash
   aws backup update-region-settings \
   --resource-type-opt-in-preference DynamoDB=true \
   --resource-type-management-preference DynamoDB=true
   ```

Editing an advanced DynamoDB backup

When you create a DynamoDB backup after you enable AWS Backup advanced features, you can use AWS Backup to:

- Copy a backup across Regions
- Copy a backup across accounts
- Change when AWS Backup tiers a backup to cold storage
• Tag the backup

To use those advanced features on an existing backup, see Editing a backup.

If you later disable AWS Backup advanced features for DynamoDB, you can continue to perform those operations to DynamoDB backups that you created during the period of time when you enabled advanced features.

Restoring an advanced DynamoDB backup

You can restore DynamoDB backups taken with AWS Backup advanced features enabled in the same way you restore DynamoDB backups taken prior to enabling AWS Backup advanced features. You can perform a restore using either AWS Backup or DynamoDB.

You can specify how to encrypt your newly-restored table with the following options:

• When you restore in the same Region as your original table, you can optionally specify an encryption key for your restored table. If you do not specify an encryption key, AWS Backup will automatically encrypt your restored table using the same key that encrypted your original table.

• When you restore in a different Region than your original table, you must specify an encryption key.

To restore using AWS Backup, see Restoring an Amazon DynamoDB table (p. 155).

To restore using DynamoDB, see Restoring a DynamoDB table from a backup in the Amazon DynamoDB User Guide.

Deleting an advanced DynamoDB backup

You cannot delete backups created using these advanced features in DynamoDB. You must use AWS Backup to delete backups to maintain global consistency throughout your AWS environment.

To delete a DynamoDB backup, see Deleting backups (p. 137).

Other benefits of full AWS Backup management when you enable advanced DynamoDB backup

When you enable AWS Backup advanced features for DynamoDB, you give full management of your DynamoDB backups to AWS Backup. Doing so gives you the following, additional benefits:

Encryption

AWS Backup automatically encrypts the backups with the KMS key of your destination AWS Backup vault. Previously, they were encrypted using the same encryption method of your source DynamoDB table. This increases the number of defenses you can use to safeguard your data. See Encryption for backups in AWS Backup (p. 227) for more information.

Amazon Resource Name (ARN)

Each backup ARN’s service namespace is awsbackup. Previously, the service namespace was dynamodb. Put another way, the beginning of each ARN will change from arn:aws:dynamodb to arn:aws:backup. See ARN format in the AWS General Reference for more information.

With this change, you or your backup administrator can create access policies for backups using the awsbackup service namespace that now apply to DynamoDB backups created after you enable advanced features. By using the awsbackup service namespace, you can also apply policies to other backups taken by AWS Backup. See Access control (p. 240) for more information.
Location of charges on billing statement

Charges for backups (including storage, data transfers, restores, and early deletion) appear under "Backup" in your AWS bill. Previously, charges appeared under "DynamoDB" in your bill.

This change ensures that you can use AWS Backup billing to centrally monitor your backup costs. See Metering, costs, and billing (p. 17) for more information.

Amazon Timestream backups

Amazon Timestream is a scalable time series database that allows storage and analysis of up to trillions of time series data points daily. Timestream is optimized for cost and time savings by keeping recent data in memory and by storing historical data in a cost-optimized storage tier in accordance with your policies.

A Timestream database has tables. These tables contain records, and each record is a single data point in a time series. A time series is a sequence of records recorded over a time interval, such as a stock price, usage level of memory of an Amazon EC2 instance, or a temperature reading. AWS Backup can centrally backup and restore Timestream tables. You can copy these table backups to other accounts and several other AWS Regions within the same organization.

Timestream does not currently offer native backup and restore services, so using AWS Backup to create secure copies of your Timestream tables can add an extra layer of security and resilience to your resources.

Back up Timestream tables

You can backup Timestream tables either through the AWS Backup console or using the AWS CLI.

There are two ways to use the AWS Backup console to backup a Timestream table: on demand or as part of a backup plan.

Create on-demand Timestream backups

2. Using the navigation pane, choose Protected resources, and then Create on-demand backup.
3. On the Create on-demand backup page, choose Amazon Timestream.
4. Choose Resource type Timestream, and then choose the table name you want to back up.
5. In Backup window, ensure that Create backup now is selected. This initiates a backup immediately and enables you to see your cluster sooner on the Protected resources page.
6. In the drop down menu Transition to cold storage, you can set your transition settings.
7. In Retention Period, you can choose how long to retain your backup.
8. Choose an existing backup vault or create a new backup vault. Choosing Create new backup vault opens a new page to create a vault and then returns you to the Create on-demand backup page when you are finished.
9. Under IAM role, choose Default role (if the AWS Backup default role is not present in your account, it will be created for you with the correct permissions).
10. Optionally, tags can be added to your recovery point. If you want to assign one or more tags to your on-demand backup, enter a key and optional value, and choose Add tag.
11. Choose Create on-demand backup. This takes you to the Jobs page, where you will see a list of jobs.
12. Choose the Backup job ID for the cluster to see the details of that job. It will display a status of Completed, In Progress, or Failed. You can click the refresh button to update the displayed status.
Create scheduled Timestream backups in a backup plan

Your scheduled backups can include Timestream tables if they are a protected resource. To opt into protecting Amazon Timestream tables:

2. Using the navigation pane, choose Protected resources.
3. Toggle Amazon Timestream to On.
4. See Assigning resources to the console to include Timestream tables in an existing or new plan.

Under Manage Backup plans, you can choose to create a backup plan and include Timestream tables, or you can update an existing one to include Timestream tables. When adding the resource type Timestream, you can choose to add All Timestream tables, or check the boxes next to the tables you wish to add under Select specific resource types.

The first backup made of Timestream tables will be a full backup. Subsequent backups will be incremental backups.

Once you've created or modified your backup plan, navigate to Backup plans in the left navigation. The backup plan you specified should display your clusters under Resource Assignments.

Backing up programmatically

You can use the operation name start-backup-job. Include the following parameters:

```bash
aws backup start-backup-job \
--backup-vault-name backup-vault-name \
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-name \
--iam-role-arn arn:aws:iam::account:role/role-name \
--region AWS Region \ 
--endpoint-url URL
```

View Timestream table backups

To view and modify your Timestream table backups within the console:

2. Choose Backup vaults. Then, click on the backup vault name that contains your Timestream tables.
3. The backup vault will display a summary and a list of backups.
   a. You can click on the link in the column Recovery point ID, or
   b. You can check the box to the left of the recovery point ID and click Actions to delete the recovery points that are no longer needed.

Restore a Timestream table

See how to restore a Timestream table

SAP HANA databases on Amazon EC2 instances backup

Note
AWS Backup support for SAP HANA databases on Amazon EC2 instances are not currently supported in these Regions: Asia Pacific (Jakarta), AWS GovCloud (US-West), AWS GovCloud
Overview

In addition to the ability to create backups and to restore databases, AWS Backup integration with Amazon EC2 Systems Manager for SAP allows customers to identify and tag SAP HANA databases.

AWS Backup is integrated with AWS Backint Agent to perform SAP HANA backups and restores. For more information, see AWS Backint.

Prerequisites

Several prerequisites must be completed before backup and restore activities can be performed. Note you will need administrative access to your SAP HANA database and permissions to create new IAM roles and policies in your AWS account to perform these steps.

Complete these prerequisites at Amazon EC2 Systems Manager.

1. Set up required permissions for Amazon EC2 instance running SAP HANA database
2. Register credentials in AWS Secrets Manager
3. Install AWS Backint and AWS Systems Manager for SAP Agents
4. Verify SSM Agent
5. Verify parameters
6. Register SAP HANA database

Backup Operations in the AWS Backup console

Once the prerequisites and SSM for SAP setups are complete, you can back up and restore your SAP HANA on EC2 databases.

Opt in to protect SAP HANA resources

To use AWS Backup to protect your SAP HANA databases, SAP HANA must be toggled on as one of the protected resources. To opt in:

2. In the left navigation pane, choose Settings.
3. Under Service opt-in, select Configure resources.
4. Opt in to SAP HANA on Amazon EC2.
Create a scheduled backup

You can edit an existing backup plan and add SAP HANA resources to it, or you can create a new backup plan just for SAP HANA resources.

If you choose to create a new backup plan, you will have three options:

1. **Option 1: Start with a template**
   1. Choose a backup plan template.
   2. Specify a backup plan name.
   3. Click Create plan.

2. **Option 2: Build a new plan**
   1. Specify a backup plan name.
   2. Optionally specify tags to add to backup plan.
   3. Specify the backup rule configuration.
      a. Specify a backup rule name.
      b. Select an existing vault or create a new backup vault. This is where your backups are stored.
      c. Specify a backup frequency.
      d. Specify a backup window.
      
      *Note transition to cold storage is currently unsupported.*
      e. Specify the retention period.
      
      *Copy to destination is currently unsupported*
      f. *(Optional)* Specify tags to add to recovery points.
   4. Click Create plan.

3. **Option 3: Define a plan using JSON**
   1. Specify the JSON for your backup plan by either modifying the JSON expression of an existing backup plan or creating a new expression.
   2. Specify a backup plan name.
   3. Click Validate JSON.

Once the backup plan is created successfully, you can assign resources to the backup plan in the next step.

Whichever plan you use, ensure you assign resources. You can choose which SAP HANA databases to assign, including system and tenant databases. You also have the option to exclude specific resource IDs.

Create an on-demand backup

You can create a full on-demand backup that runs immediately after creation. Note that on-demand backups of SAP HANA databases on Amazon EC2 instances are full backups; incremental backups are not supported.

Your on-demand backup is now created. It will begin backing up your specified resources. The console will transition you to the Backup jobs page where you can view the job progress. Take note of the
backup job ID from the blue banner at the top of your screen, as you will need it to easily find the status of your backup job. When the backup is completed, the status will progress to Completed. Backups can take up to several hours.

Refresh the Backup jobs list to see the status change. You can also search for and click on your backup job ID to view detailed job status.

Continuous backups of SAP HANA databases

You can make continuous backups, which can be used with point-in-time restore (PITR) (note that on-demand backups preserve resources in the state in which they are taken; whereas PITR uses continuous backups which record changes over a period of time).

With continuous backups, you can restore your SAP HANA database on an EC2 instance by rewinding it back to a specific time that you choose, within 1 second of precision (going back a maximum of 35 days). Continuous backup works by first creating a full backup of your resource, and then constantly backing up your resource's transaction logs. PITR restore works by accessing your full backup and replaying the transaction log to the time that you tell AWS Backup to recover.

You can opt in to continuous backups when you create a backup plan in AWS Backup using the AWS Backup console or the API.

To enable continuous backups using the console

2. In the navigation pane, choose Backup plans, and then choose Create Backup plan.
4. In the Backup rule configuration section, select Enable continuous backups for supported resources.

After you disable PITR (point-in-time restore) for SAP HANA database backups, logs will continue to be sent to AWS Backup until the recovery point expires (status equals EXPIRED). You can change to an alternative log backup location in SAP HANA to stop the transmission of logs to AWS Backup.

A continuous recovery point with a status of STOPPED indicates that a continuous recovery point has been interrupted; that is, the logs transmitted from SAP HANA to AWS Backup that show the incremental changes to a database have a gap. The recovery points that occur within this timeframe gap have a status of STOPPED.

For issues you may encounter during restore jobs of continuous backups (recovery points), see the SAP HANA Restore troubleshooting section of this guide.

View your backup jobs and recovery points

View the status of backup and restore jobs:

2. In the navigation pane, choose Jobs.
3. Choose backup jobs, restore jobs or copy jobs to see the list of your jobs.
4. Search for and click on your job ID to view detailed job statuses.

View all recovery points in a vault:

2. In the navigation pane, choose **Backup vaults**.
3. Search for and click on a backup vault to view all the recovery points within the vault.

**View details of protected resources:**
2. In the navigation pane, choose **Protected resources**.
3. You may also filter by resource type to view all backups of that resource type.

**Backup Operations using API and CLI**

Each action within the Backup console has a corresponding API call.

To programmatically configure and manage AWS Backup and its resources, use the API call **StartBackupJob** to backup an SAP HANA database on an EC2 instance.

Use `start-backup-job` as the CLI command.

**Troubleshooting**

If any of the following errors occur while attempting a backup operation, see the associated resolution.

- **Error:** Encountered an issue with log backups, please check SAP HANA for details.
  - **Resolution:** Check SAP HANA to ensure log backups are being sent to AWS Backup from SAP HANA.

- **Error:** One or more log backup attempts failed for recovery point.
  - **Resolution:** Check SAP HANA for details. Ensure log backups are being sent to AWS Backup from SAP HANA.

- **Error:** Unable to determine the status of log backups for recovery point.
  - **Resolution:** Check SAP HANA for details. Ensure log backups are being sent to AWS Backup from SAP HANA.

- **Error:** Log backups for recovery point %s were interrupted due to a restore operation on the database.
  - **Resolution:** Wait for the restore job to complete. The log backups should resume.

- **Error:** b’\* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time=2022-08-12T11:03:18Z level=info msg=Starting execution. time=2022-08-12T11:03:18Z level=info msg=Configuration file not specified in argument, using default location time=2022-08-12T11:03:18Z level=info msg=Loading configuration file /opt/aws-backint-agent/aws-backint-agent-config.yaml time=2022-08-12T11:03:18Z level=error msg=Failed to read config file open /opt/aws-backint-agent/aws-backint-agent-config.yaml: no such file or directory time=2022-08-12T11:03:18Z level=error msg=Error reading config file open /opt/aws-backint-agent/aws-backint-agent-config.yaml: no such file or directory. time=2022-08-12T11:03:18Z level=fatal msg=Error occurred during configuration. open /opt/aws-backint-agent/aws-backint-agent-config.yaml: no such file or directory. 
  - **Resolution:** Not all data could be written: Expected 4096 but transferred 0 SQLSTATE: HY000

116
Resolution: Most likely the BackInt installation did not complete successfully. Retry the process to install AWS Backint Agent and Amazon EC2 Systems Manager Agent on your SAP application server.

- **Error:** Database cannot be backed up while it is stopped.

 Resolution: Ensure the database to be backed up is active. Database data and logs can be backed up only while the database is online.

- **Error:** Getting backup metadata failed. Check the SSM document execution for more details.

 Resolution: Ensure the database to be backed up is active. Database data and logs can be backed up only while the database is online.

---

**Glossary**

**Data Backup Types:** SAP HANA supports two types of data backups: Full and INC (incremental). AWS Backup optimizes which type is used during each backup operation.

**Catalog Backups:** SAP HANA maintains its own manifest called a *catalog*. AWS Backup interacts with this catalog. Each new backup will create an entry in the catalog.

**Continuous Log Backup (Transaction Logs):** For Point in Time Recovery (PITR) functions, SAP HANA tracks all transactions since the most recent backup.

**System Copy:** A restore job in which the restore target database is different from the source database from which the recovery point was created.

**Destructive Restore:** A destructive restore is a type of restore job during which a restored database deletes or overwrites the source or existing database.

**FULL:** A full backup is a backup of a complete database.

**INC:** An incremental backup is a backup of all changes to an SAP HANA database since the previous backup.

For additional details, see the [AWS glossary](#).

---

**Release notes**

Certain functionalities are not supported at this time:

- Cross-Region and cross-account copying is not currently supported.
- Backup Audit Manager and reporting are not currently supported.
- Only a single instance is supported for SAP HANA cluster configuration. High-availability configurations are not currently supported.
- The following Regions are not supported at this time: Asia Pacific (Jakarta), AWS GovCloud (US-West), AWS GovCloud (US-East), China (Beijing), China (Ningxia), Europe (Spain), Europe (Zurich), Asia Pacific (Hyderabad), and Asia Pacific (Melbourne).

---

**Amazon Redshift backups**

Amazon Redshift is a fully managed, scalable cloud data warehouse that accelerates your time to insights with fast, easy, and secure analytics. You can use AWS Backup to protect your data warehouses with immutable backups, separate access policies, and centralized organizational governance of backup and restore jobs.
An Amazon Redshift data warehouse is a collection of computing resources called nodes, which are organized into a group called a cluster. AWS Backup can backup these clusters.

For information on Amazon Redshift, see the Amazon Redshift Getting Started Guide, the Amazon Redshift Database Developer Guide, and the Amazon Redshift Cluster Management Guide.

**Back up Amazon Redshift provisioned clusters**

You can protect your Amazon Redshift clusters using the AWS Backup console or programmatically using API or CLI. These clusters can be backed up on a regular schedule as part of a backup plan, or they can be backed up as needed via on-demand backup.

You can restore a single table (also known as item-level restore) or an entire cluster. Note that tables cannot be backed up by themselves; tables are backed up as part of a cluster when the cluster is backed up.

Using AWS Backup allows you to view your resources in a centralized way; however, if Amazon Redshift is the only resource you use, you can continue to use the automated snapshot scheduler in Amazon Redshift. Note that you cannot continue to manage manual snapshot settings using Amazon Redshift if you choose to manage these via AWS Backup.

You can backup Amazon Redshift clusters either through the AWS Backup console or using the AWS CLI.

There are two ways to use the AWS Backup console to backup a Amazon Redshift cluster: on demand or as part of a backup plan.

**Create on-demand Amazon Redshift backups**

See [Creating an on-demand backup](#) type page for more information.

To create a manual snapshot, leave the continuous backup checkbox unchecked when you create a backup plan that includes Amazon Redshift resources.

**Create scheduled Amazon Redshift backups in a backup plan**

Your scheduled backups can include Amazon Redshift clusters if they are a protected resource. To opt into protecting Amazon Redshift tables:

2. Using the navigation pane, choose Protected resources.
3. Toggle Amazon Redshift to On.
4. See [Assigning resources to the console](#) to include Amazon Redshift clusters in an existing or new plan.

Under Manage Backup plans, you can choose to create a backup plan and include Amazon Redshift clusters, or you can update an existing one to include Amazon Redshift clusters. When adding the resource type Amazon Redshift, you can choose to add All Amazon Redshift clusters, or check the boxes next to the clusters you

**Back up programmatically**

You can also define your backup plan in a JSON document and provide it using the AWS Backup console or AWS CLI. See [Creating backup plans using a JSON document and the AWS Backup CLI](#) for information on how to create a backup plan programatically.

You can do the following operations using API:

- Start a backup job
• Describe a backup job
• Get recovery point metadata
• List recovery points by resources
• List tags for the recovery point

View Amazon Redshift cluster backups

To view and modify your Amazon Redshift table backups within the console:

2. Choose Backup vaults. Then, click on the backup vault name that contains your Amazon Redshift clusters.
3. The backup vault will display a summary and a list of backups. You can click on the link in the column Recovery point ID.
4. To delete one or more recovery points, check the box(es) you wish to delete. Under the button Actions, you can select Delete.

Restore a Amazon Redshift cluster

See how to Restore a Amazon Redshift cluster for more information.

Amazon RDS Multi-Availability Zone backups

AWS Backup backs up and supports Amazon RDS for MySQL and for PostgreSQL Multi-AZ (Availability Zone) deployment options with one primary and two readable standby database instances.

Multi-Availability Zone backups are available in the following regions: Asia Pacific (Sydney) Region, Asia Pacific (Tokyo) Region, Europe (Ireland) Region, US East (Ohio) Region, US West (Oregon) Region, Europe (Stockholm) Region, Asia Pacific (Singapore) Region, US East (N. Virginia) Region, and Europe (Frankfurt) Region.

The Multi-AZ deployment option optimizes write transactions and is ideal when your workloads require additional read capacity, lower write transaction latency, more resilience from network jitter (which impacts the consistency of write transaction latency), and high availability and durability.

To create a Multi-AZ cluster, you can choose either MySQL or PostgreSQL as the engine type.

In the AWS Backup console, there are three deployment options:

• Multi-AZ DB cluster: Creates a DB cluster with a primary DB instances and two readable standby DB instances, which each DB instance in a different Availability Zone. Provides high availability, data redundancy, and increases capacity to server-ready workloads.
• Multi-AZ DB instance: Creates a primary DB instance and a standby DB instance in a different Availability Zone. This provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
• Single DB instance: Creates a single DB instance with no standby DB instances.

To create a backup for Amazon RDS, see Creating a backup for scheduling a backup as part of your backup plans or creating an on-demand backup.

Note
Point-in-Time Recovery (PITR) can support instances, but not clusters. Copying a Multi-AZ DB cluster snapshot is not supported.
Differences between a multi-AZ cluster and an RDS instance

A backup in a single Availability Zone or in two Availability Zones is an RDS instance; a deployment and backup with three or more instances is a cluster, similar to Amazon Aurora, Amazon Neptune, and Amazon DocumentDB clusters.

The ARN (Amazon Resource Name) is rendered differently depending on if instance or cluster is used:


For more information, consult Multi-AZ DB cluster deployments in the Amazon RDS User Guide.

For more information on Creating a Multi-AZ DB cluster snapshot, see the Amazon RDS User Guide.

AWS CloudFormation stack backups

A CloudFormation stack consists of multiple stateful and stateless resources that you can back up as a single unit. In other words, you can backup and restore an application containing multiple resources by backing up a stack and restoring the resources within it. All the resources in a stack are defined by the stack's AWS CloudFormation template.

When a CloudFormation stack is backed up, recovery points are created for the CloudFormation template and for each additional resource supported by AWS Backup in the stack. These recovery points are grouped together within a overarching recovery point called a composite.

This composite recovery point cannot be restored, but nested recovery points can be restored. You can restore anywhere from one to all nested backups within a composite backup using the console or the AWS CLI.

CloudFormation application stack terminology

- **Composite recovery point**: A recovery point used to group nested recovery points together, as well other metadata.
- **Nested recovery point**: A recovery point of a resource that is part of a CloudFormation stack and is backed up as part of the composite recovery point. Each nested recovery point belongs in the stack of one composite recovery point.
- **Composite job**: A backup, copy, or restore job for a CloudFormation stack which can trigger other backup jobs for individual resources within the stack.
- **Nested job**: A backup, copy, or restore job for a resource within a AWS CloudFormation stack.

CloudFormation stack backup jobs

The process of a backup creation is called a backup job. A CloudFormation stack backup job has a status. When a backup job has finished, it has the status of Completed. This signifies a AWS CloudFormation recovery point (p. 121) (a backup) has been created.

CloudFormation stacks can be backed up using the console or backed up programatically. To backup any resource, including a CloudFormation stack, see Creating a backup elsewhere in this AWS Backup Developer Guide.

CloudFormation stacks can be backed up using the API command StartBackupJob. Note that the documentation and console refer to composite and nested recovery points; the API language uses the terminology "parent and child recovery points" in the same contextual relationship.
CloudFormation stacks contain all AWS resources are indicated by your CloudFormation template. Note that your template may contain resources not yet supported by AWS Backup. If your template contains a combination of AWS supported resources and unsupported resources, AWS Backup will still back up the template into a composite stack, but Backup will only create recovery points of the Backup-supported services. Nested backups supported by AWS Backup can be restored. All resource types contained within the CloudFormation template will be included within a backup, even if you have not opted into to a particular service (toggling a service to “Enabled” in console Settings).

The process of a backup creation is called a backup job. A CloudFormation stack backup job has a status.

**AWS CloudFormation recovery point**

**Recovery point status**

When the backup job of a stack is finished (the job status is Completed), a backup of the stack has been created. This backup is also known as a composite recovery point. A composite recovery point can have one of the following statuses: Completed, Failed, or Partial. Note that a backup job has a status, and a recovery point (also called a backup) also has a separate status.

A completed backup job means your entire stack and the resources within in are protected by AWS Backup. A failed status indicates that the backup job was unsuccessful; you should create the backup again once the issue that caused the failure is corrected.

A Partial status means that not all the resources in the stack were backed up. This may happen if the CloudFormation template contains resources that are not currently supported by AWS Backup, or it may happen if one or more of the backup jobs belonging to resources within the stack (nested resources) have statuses other than Completed. You can manually create an on-demand backup to rerun any resources that resulted in a status other than Completed. If you expected the stack to have the status of Completed but it is marked as Partial instead, check to see which of the conditions above might be true about your stack.

Each nested resource within the composite recovery point has its own individual recovery point, each with its own status (either Completed or Failed). Nested recovery points with a status of Completed can be restored.

**Manage recovery points**

Composite recovery points (backups) can be copied or deleted; nested recovery points can be copied, deleted, disassociated or restored. If you delete the composite recovery point using the AWS Backup console, all nested recovery points associated with the composite stack are deleted. After all nested recovery points have been deleted, you can delete the composite recovery point manually, though it will be automatically deleted if it has no nested recovery points.

**Delete a recovery point**

You can delete a recovery point using the AWS Backup console or using the AWS CLI. Also note when the final nested recovery point within a composite recovery point is deleted or disassociated, and the composite recovery point no longer has any remaining nested recovery points, the empty composite recovery point is automatically deleted.

To delete recovery points using the AWS Backup console,

2. Click on Protected Resources in the left-hand navigation. In the text box, type CloudFormation to display only your CloudFormation stacks.
3. Composite recovery points will be displayed in the Recovery points pane. The plus sign (+) to the left of each recovery point ID can be clicked to expand each composite recovery point, showing all nested
recovery points contained in the composite. You can click the radial circle button to the left of any recovery point to delete it.

**Note**

NOTE: If you choose to delete a composite recovery point, it and all nested recovery points within it will be deleted.

4. Click the **Delete** button. Currently you cannot delete nested recovery points simultaneously. You must select an individual nested recovery point each time you choose to delete.

When you use the console to delete one or more composite recovery points, a warning box will pop up. This warning box requires you to confirm your intention to delete the composite recovery points, including nested recovery points within composite stacks.

To delete recovery points using API, use the `DeleteRecoveryPoint` command.

When you use API with the AWS Command Line Interface you must delete all nested recovery points prior to deleting a composite point. If you send an API request to delete a composite stack backup (recovery point) that still contains nested recovery points within it, the request will return an error.

**Disassociate a nested recovery point from composite recovery point**

You can disassociate a nested recovery point from a composite recovery point (for example, you wish to keep the nested recovery point but delete the composite recovery point). Both recovery points will remain, but they will no longer be connected; that is, actions that occur on the composite recovery point will no longer apply to the nested recovery point once it has been disassociated.

You can disassociate the recovery point using the console, or you can call the API `DisassociateRecoveryPointFromParent`. [Note that the API calls use the term “parent” to refer to composite recovery points.]

**Copy a recovery point**

You can copy a composite recovery point, or you can copy a nested recovery point if the resource supports cross-account and cross-Region copying.

To copy recovery points using the AWS Backup console:

1. Open the AWS Backup console at **https://console.aws.amazon.com/backup**.
2. Click on **Protected Resources** in the left-hand navigation. In the text box, type `CloudFormation` to display only your CloudFormation stacks.
3. Composite recovery points will be displayed in the Recovery points pane. The plus sign (+) to the left of each recovery point ID can be clicked to expand each composite recovery point, showing all nested recovery points contained in the composite. You can click the radial circle button to the left of any recovery point to copy it.
4. Once it is selected, click the **Copy** button in the top-right corner of the pane.

When you copy a composite recovery point, nested recovery points that don’t support copy functionality won’t end up in the copied stack. The composite recovery point will have a status of Partial.

**Frequently Asked Questions**

1. "What all is backed up as part of the application backup?"

As part of each backup of an application defined using CloudFormation, the template, the processed value of each parameter in the template, and the nested resources supported by AWS Backup are
backed up. A nested resource is backed up in the same way as an individual resource not part of a CloudFormation stack is backed up. Note that values of parameters marked as no-echo will not be backed up.

2. “Can I back up my AWS CloudFormation stack that has nested stacks?”

AWS CloudFormation stacks that contain nested stacks can be backed up. Nested stack within these stacks will not be part of the backup.

3. “Does a Partial status mean the creation of my backup failed?”

No. A partial status indicates that some of the recovery points were backed up, while some were not. There are three conditions to check if you were expecting a Completed backup result:

a. Does your CloudFormation stack contain resources currently unsupported by AWS Backup? For a list of supported resources, see Supported AWS resources and third-party applications in our Developer Guide.

b. One or more of the backup jobs belonging to resources within the stack were not successful and the job has to be rerun.

c. A nested recovery point was deleted or disassociated from the composite recovery point.

4. “What types of backups are supported for nested resources?”

Backups of nested resources may be either full or incremental backups, depending on which kind of backup is supported by AWS Backup for these resources. For more information, see How incremental backups work. However, note that PITR (point-in-time restore) is not supported for Amazon S3 and Amazon RDS nested resources.

5. “Are change sets that are part of the CloudFormation stack backed up?”

No. Change sets are not backed up as part of CloudFormation stack backup.

6. “How does the status of the AWS CloudFormation stack impact the backup?”

The status of the CloudFormation stack may impact the backup. A stack with a status that includes COMPLETE can be backed up, such as statuses CREATE_COMPLETE, ROLLBACK_COMPLETE, UPDATE_COMPLETE, UPDATE_ROLLBACK_COMPLETE, IMPORT_COMPLETE, or IMPORT_ROLLBACK_COMPLETE.

In the case where an upload of a new template fails and the stack move to the status of ROLLBACK_COMPLETE, the new template will be backed up but backups of the nested resources will be based on the rolled-back resources.

7. “How do application stack lifecycles differ from other recovery point lifecycles?”

Nested recovery point lifecycles are determined by the backup plan to which they belong. The composite recovery point is determined by the longest lifecycle of all nested recovery points. When the last remaining nested recovery point within a composite recovery point is deleted or disassociated, the composite recovery point will also be deleted.

8. “How are tags of a CloudFormation copied to recovery points?”

Yes. Those tags will be copied to each respective nested recovery point.

**Restore applications within a stack**

See How to restore application stack backups for information on restoring nested recovery points.
Creating Windows VSS backups

With AWS Backup, you can back up and restore VSS (Volume Shadow Copy Service)-enabled Windows applications running on Amazon EC2 instances. If the application has VSS writer registered with Windows VSS, then AWS Backup creates a snapshot that will be consistent for that application.

You can perform consistent restores, while using the same managed backup service that is used to protect other AWS resources. With application-consistent Windows backups on EC2, you get the same consistency settings and application awareness as traditional backup tools.

**Note**
AWS Backup currently only supports application-consistent backups of resources running on Amazon EC2, specifically backup scenarios where application data can be restored by replacing existing an instance with a fresh instance created from the backup. Not all instance types or applications are supported for Windows VSS backups.


To back up and restore VSS-enabled Windows resources running Amazon EC2, follow these steps to complete the required prerequisite tasks. For instructions, see [Before You Begin](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/).  

1. Download, install, and configure the SSM agent in AWS Systems Manager. This step is required. For instructions, see [Update SSM Agent by using Run Command](https://docs.aws.amazon.com/AWSServiceCatalog/latest/APIReference/13058847683357315066/) in the [AWS Systems Manager User Guide](https://docs.aws.amazon.com/AWSSystemManager/latest/USER-GUIDE/).
2. Add an IAM policy to the IAM role and attach the role to the Amazon EC2 instance before you take the Windows VSS (Volume Shadow Copy Service) backup. For instructions, see [Create an IAM Role for VSS-Enabled Snapshots](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/). For an example of the IAM policy, see [Managed policies](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/).  
3. Download and install VSS components to the Windows on Amazon EC2 instance.
4. Enable VSS in AWS Backup:
   2. On the dashboard, choose the type of backup you want to create, either [Create an on-demand backup](https://docs.aws.amazon.com/backup/latest/devguide/backup serviço de backup de VSS). Provide the information needed for your backup type.
   3. When you're assigning resources, choose **EC2**. Windows VSS backup is currently supported for EC2 instances only.
   4. In the [Advanced settings](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/). section, choose **Windows VSS**. This enables you to take application-consistent Windows VSS backups.
   5. Create your backup.

A backup job with a status of Completed does not guarantee that the VSS portion is successful; VSS inclusion is made on a best-effort basis. Proceed with the following steps to determine if a backup is application-consistent, crash-consistent, or failed:

2. Under **My account** in the left navigation, click **Jobs**.
3. A status of Completed indicates a successful job that is application-consistent (VSS).
   
   A status of Completed with issues indicates that the VSS operation has failed, so only a crash-consistent backup has been successful. This status will also have a popover message "Windows VSS Backup Job Error encountered, trying for regular backup".

If the backup was unsuccessful, the status will be Failed.
4. To view additional details of the backup job, click on the individual job. For example, the details may read "Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation."

Unsupported Amazon EC2 instances

The following Amazon EC2 instance types are not supported for VSS-enabled Windows backups because they are small instances and might not take the backup successfully.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Amazon EBS multi-volume, crash-consistent backups

By default, AWS Backup creates crash-consistent backups of Amazon EBS volumes that are attached to an Amazon EC2 instance. Crash consistency means that the snapshots for every Amazon EBS volume attached to the same Amazon EC2 instance are taken at the exact same moment. You no longer have to stop your instances or coordinate between multiple Amazon EBS volumes to ensure crash-consistency of your application state.

Since multi-volume, crash-consistent snapshots are a default AWS Backup functionality, you don't need to do anything different to use this feature. You can back up Amazon EBS volumes using one of the following procedures:

- Create an on-demand backup
- Create a scheduled backup

To restore your Amazon EBS volumes, follow the steps in Restoring an Amazon EBS volume.

Copying tags onto backups

In general, AWS Backup copies tags from the resources it protects to your recovery points. For more information on how to copy tags during a restore, see Copy tags during a restore.

For example, when you back up an Amazon EC2 volume, AWS Backup copies its group and individual resource tags to the resulting snapshot, subject to the following:

- For a list of resource-specific permissions that are required to save metadata tags on backups, see Permissions required to assign tags to backups (p. 243).
- Tags that are originally associated with a resource and tags that are assigned during backup are assigned to recovery points stored in a backup vault, up to a maximum of 50 (this is an AWS limitation). Tags that are assigned during backup have priority, and both sets of tags are copied in alphabetical order.
- DynamoDB does not support assigning tags to backups unless you first enable Advanced DynamoDB backup (p. 107).
- Amazon EBS volumes that are attached to Amazon EC2 instances are nested resources. Tags on the Amazon EBS volumes that are attached to Amazon EC2 instances are nested tags. AWS Backup makes
a best-effort attempt to copy nested tags, but if it is unsuccessful, it creates a backup without them and reports Status Completed.

- When an Amazon EC2 backup creates an image recovery point and a set of snapshots, AWS Backup copies tags to the resulting AMI. AWS Backup also makes a best-effort attempt to copy the tags from the volumes associated with the Amazon EC2 instance to the resulting snapshots.

If you copy your backup to another AWS Region, AWS Backup copies all tags of the original backup to the destination AWS Region.

**Stopping a backup job**

You can stop a backup job in AWS Backup after it has been initiated. When you do this, the backup is not created, and the backup job record is retained with the status of aborted.

**To stop a backup job using the AWS Backup console**

2. In the navigation pane on the left, choose Jobs.
3. Choose the backup job that you want to stop.
4. In the backup job details pane, choose Stop.

**Copy a backup**

You can copy backups to multiple AWS accounts or AWS Regions on demand or automatically as part of a scheduled backup plan for most resource types. This feature is not yet available for Amazon FSx for NetApp ONTAP volumes.

You can also automate a sequence of cross-account and cross-Region copies for most supported resources, except for Amazon RDS and Aurora. For Amazon RDS and Aurora snapshots, AWS Backup only supports automating either cross-account or cross-Region copies due to how those services create their encryption keys (copying a Multi-AZ DB cluster snapshot is not supported).

Copies retain their source configuration, including creation dates and expiration dates, unless you specify otherwise. The expiration date in the source and copy reference the creation date of source, not the date the copy was created.

**NOTE:** The source configuration overrides its copy’s expiration setting, even if the copy is set to never expire; a copy set to never expire will still retain its source’s expiration date.

If you want your backup copies to never expire, either set your source backups to never expire or specify your copy to expire 100 years after its creation.

**Topics**

- [Creating backup copies across AWS Regions](#)
- [Creating backup copies across AWS accounts](#)

**Creating backup copies across AWS Regions**

Using AWS Backup, you can copy backups to multiple AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region replication is particularly valuable if you have business
continuity or compliance requirements to store backups a minimum distance away from your production data. For a video tutorial, see Managing cross-Region copies of backups.

When you copy a backup to a new AWS Region for the first time, AWS Backup copies the backup in full. In general, if a service supports incremental backups, subsequent copies of that backup in the same AWS Region will be incremental. AWS Backup will re-encrypt your copy using the customer managed key of your destination vault.

An exception is Amazon EBS, which states, "changing the encryption status of a snapshot during a copy operation results in a full (not incremental) copy."

Most AWS Backup-supported resources support cross-Region backup. For specifics, see that section of the Feature availability by resource (p. 2) table.

Most AWS Regions support cross-Region backup. For specifics, see that section of the Feature availability by AWS Region (p. 4) table.

Performing on-demand cross-Region backup

To copy an existing backup on-demand

2. Choose Backup vaults.
3. Choose the vault that contains the recovery point you want to copy.
4. In the Backups section, select a recovery point to copy.
5. Using the Actions dropdown button, choose Copy.
6. Enter the following values:

   Copy to destination
   
   Choose the destination AWS Region for the copy. You can add a new copy rule per copy to a new destination.

   Destination Backup vault
   
   Choose the destination backup vault for the copy.

   Transition to cold storage
   
   Choose when to transition the backup copy to cold storage. Backups transitioned to cold storage must be stored there for a minimum of 90 days. This value cannot be changed after a copy has transitioned to cold storage.

   To see the list of resources that you can transition to cold storage, see the "Lifecycle to cold storage" section of the Feature availability by resource (p. 2) table. The cold storage expression is ignored for other resources.

   Retention period
   
   Choose specifies the number of days after creation that the copy is deleted. This value must be greater than 90 days beyond the Transition to cold storage value. The Always retention period retains your copy indefinitely.

   IAM role
   
   Choose the IAM role that AWS Backup will use when creating the copy. The role must also have AWS Backup listed as a trusted entity, which enables AWS Backup to assume the role. If you choose Default and the AWS Backup default role is not present in your account, one will be created for you with the correct permissions.

7. Choose Copy.
Scheduling cross-Region backup

You can use a scheduled backup plan to copy backups across AWS Regions.

To copy a backup using a scheduled backup plan

2. In My account, choose Backup plans, and then choose Create Backup plan.
3. On the Create Backup plan page, choose Build a new plan.
4. For Backup plan name, enter a name for your backup plan.
5. In the Backup rule configuration section, add a backup rule that defines a backup schedule, backup window, and lifecycle rules. You can add more backup rules later.
   a. For Backup rule name, enter a name for your rule.
   b. For Backup vault, choose a vault from the list. Recovery points for this backup will be saved in this vault. You can create a new backup vault.
   c. For Backup frequency, choose how often you want to take backups.
   d. For services that support PITR, if you want this feature, choose Enable continuous backups for point-in-time recovery (PITR). For a list a services that support PITR, see that section of the Feature availability by resource (p. 2) table.
   e. For Backup window, choose Use backup window defaults - recommended. You can customize the backup window.
   f. For Copy to destination, Choose the destination AWS Region for your backup copy. Your backup will be copied to this Region. You can add a new copy rule per copy to a new destination. Then enter the following values:

   **Copy to another account's vault**
   Do not toggle this option. To learn more about cross-account copy, see Creating backup copies across AWS accounts

   **Destination Backup vault**
   Choose the backup vault in the destination Region where AWS Backup will copy your backup.
   If you would like to create a new backup vault for cross-Region copy, choose Create new Backup vault. Enter the information in the wizard. Then choose Create Backup vault.
6. Choose Create plan.

Creating backup copies across AWS accounts

**Note**
Before you manage resources across multiple AWS accounts in AWS Backup, your accounts must belong to the same organization in the AWS Organizations service.

Using AWS Backup, you can back up to multiple AWS accounts on demand or automatically as part of a scheduled backup plan. Use a cross-account backup if you want to securely copy your backups to one or more AWS accounts in your organization for operational or security reasons. If your original backup is inadvertently deleted, you can copy the backup from its destination account to its source account, and then start the restore. Before you can do this, you must have two accounts that belong to the same organization in the AWS Organizations service. For more information, see Tutorial: Creating and configuring an organization in the Organizations User Guide.

In your destination account, you must create a backup vault. Then, you assign a customer managed key to encrypt backups in the destination account, and a resource-based access policy to allow AWS Backup
to access the resources you would like to copy. In the source account, if your resources are encrypted with a customer managed key, you must share this customer managed key with the destination account. You can then create a backup plan and choose a destination account that is part of your organizational unit in AWS Organizations.

Most AWS Backup-supported resources support cross-account backup. For specifics, see that section of the Feature availability by resource (p. 2) table.

Most AWS Regions support cross-account backup. For specifics, see that section of the Feature availability by AWS Region (p. 4) table.

Setting up AWS Region (p. 4)

Setting up cross-account backup

What do you need to create cross-account backups?

- **A source account**
  
  The source account is the account where your production AWS resources and primary backups reside.

  The source account user initiates the cross-account backup operation. The source account user or role must have appropriate API permissions to initiate the operation. Appropriate permissions might be the AWS managed policy AWSBackupFullAccess, which enables full access to AWS Backup operations, or a customer managed policy that allows actions such as ec2:ModifySnapshotAttribute. For more information about policy types, see AWS Backup Managed Policies.

- **A destination account**
  
  The destination account is the account where you would like to keep a copy of your backup. You can choose more than one destination account. The destination account must be in the same organization as the source account in AWS Organizations.

  You must “Allow” the access policy backup:CopyIntoBackupVault for your destination backup vault. The absence of this policy will deny attempts to copy into the destination account.

- **A management account in AWS Organizations**
  
  The management account is the primary account in your organization, as defined by AWS Organizations, that you use to manage cross-account backup across your AWS accounts. To use cross-account backup, you also must enable service trust. After enabling service trust, you can use any account in the organization as a destination account. From your destination account, you can choose which vaults to use for cross-account backup.

- **Enable cross-account backup in the AWS Backup console**

  For information about security, see Security consideration for cross-account backup (p. 135).

  To use cross-account backup, you must enable the cross-account backup feature. Then, you must "Allow" the access policy backup:CopyIntoBackupVault into your destination backup vault.

  **To enable cross-account backup**

  1. Log in to AWS using your AWS Organizations management account credentials. Cross-account backup can only be enabled or disabled using these credentials.
  3. In My account, choose Settings.
  4. For Cross-account backup, choose Enable.
  5. In Backup vaults, choose your destination vault.
  6. In the Access policy section, "Allow" backup:CopyIntoBackupVault. For an example, choose Add permissions and then Allow access to a Backup vault from organization.
7. Now, any account in your organization can share the contents of their backup vault with any other account in your organization. For more information, see Sharing a backup vault with a different AWS account (p. 132). To limit which accounts can receive the contents of other accounts' backup vaults, see Configuring your account as a destination account (p. 134).

Scheduling cross-account backup

You can use a scheduled backup plan to copy backups across AWS accounts.

To copy a backup using a scheduled backup plan

2. In My account, choose Backup plans, and then choose Create Backup plan.
3. On the Create Backup plan page, choose Build a new plan.
4. For Backup plan name, enter a name for your backup plan.
5. In the Backup rule configuration section, add a backup rule that defines a backup schedule, backup window, and lifecycle rules. You can add more backup rules later.

   For Rule name, enter a name for your rule.
6. In the Schedule section under Frequency, choose how often you want the backup to be taken.
7. For Backup window, choose Use backup window defaults (recommended). You can customize the backup window.
8. For Backup vault, choose a vault from the list. Recovery points for this backup will be saved in this vault. You can create a new backup vault.
9. In the Generate copy - optional section, enter the following values:

   Destination Region

   Choose the destination AWS Region for your backup copy. Your backup will be copied to this Region. You can add a new copy rule per copy to a new destination.

   Copy to another account's vault

   Toggle to choose this option. The option turns blue when selected. The External vault ARN option will appear.

   External vault ARN

   Enter the Amazon Resource Name (ARN) of the destination account. The ARN is a string that contains the account ID and its AWS Region. AWS Backup will copy the backup to the destination account's vault. The Destination region list automatically updates to the Region in the external vault ARN.

   For Allow Backup vault access, choose Allow. Then choose Allow in the wizard that opens.

AWS Backup needs permissions to access the external account to copy backup to the specified value. The wizard shows the following example policy that provides this access.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Allow account to copy into backup vault",
         "Effect": "Allow",
         "Action": "backup:CopyIntoBackupVault",
         "Resource": "*",
         "Principal": {
            "AWS": "arn:aws:iam::<account-id>:root"
         }
      }
   ]
}
```
Transition to cold storage

Choose when to transition the backup copy to cold storage and when to expire (delete) the copy. Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. This value cannot be changed after a copy has transitioned to cold storage.

To see the list of resources that you can transition to cold storage, see the "Lifecycle to cold storage" section of the Feature availability by resource (p. 2) table. The cold storage expression is ignored for other resources.

**Expire** specifies the number of days after creation that the copy is deleted. This value must be greater than 90 days beyond the Transition to cold storage value.

**Note**
When backups expire and are marked for deletion as part of your lifecycle policy, AWS Backup deletes the backups at a randomly chosen point over the following 8 hours. This window helps ensure consistent performance.

10. Choose *Tags added to recovery points* to add tags to your recovery points.
11. For **Advanced backup settings**, choose Windows VSS to enable application-aware snapshots for the selected third-party software running on EC2.
12. Choose *Create plan*.

**Performing on-demand cross-account backup**

You can copy a backup to a different AWS account on demand.

**To copy a backup on-demand**

2. For **My account**, choose *Backup vault* to see all your backup vaults listed. You can filter by the backup vault name or tag.
3. Choose the *Recovery point ID* of the backup you want to copy.
4. Choose *Copy*.
5. Expand *Backup details* to see information about the recovery point you are copying.
6. In the *Copy configuration* section, choose an option from the *Destination region* list.
7. Choose *Copy to another account's vault*. The option turns blue when selected.
8. Enter the Amazon Resource Name (ARN) of the destination account. The ARN is a string that contains the account ID and its AWS Region. AWS Backup will copy the backup to the destination account's vault. The *Destination region* list automatically updates to the Region in the external vault ARN.
9. For **Allow Backup vault access**, choose *Allow*. Then choose *Allow* in the wizard that opens.

To create the copy, AWS Backup needs permissions to access the source account. The wizard shows an example policy that provides this access. This policy is shown following.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
```
"Effect": "Allow",
"Action": "backup:CopyIntoBackupVault",
"Resource": "*",
"Principal": {
  "AWS": "arn:aws:iam::account-id:root"
}
}
]
]

10. For **Transition to cold storage**, choose when to transition the backup copy to cold storage and when to expire (delete) the copy. Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. This value cannot be changed after a copy has transitioned to cold storage.

To see the list of resources that you can transition to cold storage, see the "Lifecycle to cold storage" section of the Feature availability by resource (p. 2) table. The cold storage expression is ignored for other resources.

**Expire** specifies the number of days after creation that the copy is deleted. This value must be greater than 90 days beyond the **Transition to cold storage** value.

11. For **IAM role**, specify the IAM role (such as the default role) that has the permissions to make your backup available for copying. The act of copying is performed by your destination account’s service linked role.

12. Choose **Copy**. Depending on the size of the resource you are copying, this process could take several hours to complete. When the copy job completes, you will see the copy in the **Copy jobs** tab in the **Jobs** menu.

### Notes on keys for cross-account backups

Cross-account copy is not supported with AWS managed keys. The key policy of an AWS managed key is immutable, which prevents copying the key across accounts. If your resources are encrypted with AWS managed keys and you want to perform a cross-account copy, you may [change the encryption keys](#) to a customer managed key since this supports cross-account copying. Or, you can follow the instructions in [Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups](#) to continue using AWS managed keys.

### Restoring a backup from one AWS account to another

AWS Backup does not support recovering resources from one AWS account to another. However, you can copy a backup from one account to a different account and then restore it in that account. For example, you can't restore a backup from account A to account B, but you can copy a backup from account A to account B, and then restore it in account B.

Restoring a backup from one account to another is a two-step process.

**To restore a backup from one account to another**

1. Copy the backup from the source AWS account to the account you want to restore to. For instructions, see [Setting up cross-account backup](#).
2. Use the appropriate instructions for your resource to restore the backup.

### Sharing a backup vault with a different AWS account

AWS Backup allows you to share a backup vault with one or multiple accounts, or your entire organization in AWS Organizations. You can share a destination backup vault with a source AWS Account, user, or IAM role.
To share a destination Backup vault

1. Choose AWS Backup, and then choose Backup vaults.
2. Choose the name of the backup vault that you want to share.
3. In the Access policy pane, choose the Add permissions dropdown.
4. Choose Allow account level access to a Backup vault. Or, you can choose to allow organization-level or role-level access.
5. Enter the AccountID of the account you’d like to share with this destination backup vault.
6. Choose Save policy.

You can use IAM policies to share your backup vault.

Share a destination backup vault with an AWS account or IAM role

The following policy shares a backup vault with account number 4444555566666 and the IAM role SomeRole in account number 111122223333.

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
}
```

Share a destination backup vault an organizational unit in AWS Organizations

The following policy shares a backup vault with organizational units using their PrincipalOrgPaths.

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":{
          "PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsdddd/*"
          ]
        }
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsdddd/*"
          ]
        }
      }
    }
  ]
}
```

Share a destination backup vault with an organization in AWS Organizations
The following policy shares a backup vault with the organization with PrincipalOrgID "o-a1b2c3d4e5".

```json
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect":"Allow",
            "Principal":"*",
            "Action":"backup:CopyIntoBackupVault",
            "Resource":"*",
            "Condition":{
                "StringEquals":{
                    "aws:PrincipalOrgID": [
                        "o-a1b2c3d4e5"
                    ]
                }
            }
        }
    ]
}
```

**Configuring your account as a destination account**

When you first enable cross-account backups using your AWS Organizations management account, any user of a member account can configure their account to be a destination account. We recommend setting one or more of the following service control policies (SCPs) in AWS Organizations to limit your destination accounts. To learn more about attaching service control policies to AWS Organizations nodes, see [Attaching and detaching service control policies](#).

**Limit destination accounts using tags**

When attached to an AWS Organizations root, OU, or individual account, this policy limits copies destinations from that root, OU, or account to only those accounts with backup vaults you've tagged DestinationBackupVault. The permission "backup:CopyIntoBackupVault" controls how a backup vault behaves and, in this case, which destination backup vaults are valid. Use this policy, along with the corresponding tag applied to approved destination vaults, to control the destinations of cross-account copies to only approved accounts and backup vaults.

```json
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect":"Deny",
            "Action":"backup:CopyIntoBackupVault",
            "Resource":"*",
            "Condition":{
                "Null":{
                    "aws:ResourceTag/DestinationBackupVault":"true"
                }
            }
        }
    ]
}
```

**Limit destination accounts using account numbers and vault names**

When attached to an AWS Organizations root, OU, or individual account, this policy limits copies originating from that root, OU, or account to only two destination accounts. The permission "backup:CopyFromBackupVault" controls how a recovery point in the backup vault behaves, and,
in this case, the destinations where you can copy that recovery point to. The source vault will only permit copies to the first destination account (112233445566) if one or more destination backup vault names begin with cab-. The source vault will only permit copies to the second destination account (123456789012) if the destination is the single backup vault named fort-knox.

```json
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":"backup:CopyFromBackupVault",
            "Resource":"arn:aws:ec2:*:snapshot/*",
            "Condition":{
                "ForAllValues:ArnNotLike":{
                    "backup:CopyTargets":{
                        "arn:aws:backup:*:112233445566:backup-vault:cab-*",
                    }
                }
            }
        }
    ]
}
```

**Limit destination accounts using organizational units in AWS Organizations**

When attached to an AWS Organizations root or OU that contains your source account, or when attached to your source account, the following policy limits the destination accounts to those accounts within the two specified OUs.

```json
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":"backup:CopyFromBackupVault",
            "Resource":"*",
            "Condition":{
                "ForAllValues:StringNotLike":{
                    "backup:CopyTargetOrgPaths":{
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
                    }
                }
            }
        }
    ]
}
```

**Security consideration for cross-account backup**

Be aware of the following when using performing cross-account backups in AWS Backup:

- The destination vault cannot be the default vault. This is because the default vault is encrypted with a key that cannot be shared with other accounts.
- Cross-account backups might still run for up to 15 minutes after you disable cross-account backup. This is due to eventual consistency, and might result in some cross-account jobs starting or completing even after you disable cross-account backup.
- If the destination account leaves the organization at a later date, that account will retain the backups. To avoid potential data leakage, place a deny permission on the
organizations:LeaveOrganization permission in a service control policy (SCP) attached to the destination account. For detailed information about SCPs, see Removing a member account from your organization in the Organizations User Guide.

- If you delete a copy job role during a cross-account copy, AWS Backup can’t unshare snapshots from the source account when the copy job completes. In this case, the backup job finishes, but the copy job status shows as Failed to unshare snapshot.

**Viewing a list of backups**

You can view a list of your backups using the AWS Backup console or programmatically.

**Topics**

- Listing backups by protected resource in the console (p. 136)
- Listing backups by backup vault in the console (p. 136)
- Listing backups programmatically (p. 136)

**Listing backups by protected resource in the console**

Follow these steps to view a list of backups of a particular resource on the AWS Backup console.

2. In the navigation pane, choose Protected resources.
3. Choose a protected resource in the list to view the list of backups. Only resources that have been backed up by AWS Backup are listed under Protected resources.

You can view the backups for the resource. From this view, you can also choose a backup and restore it.

**Listing backups by backup vault in the console**

Follow these steps to view a list of backups organized in a backup vault.

2. In the navigation pane, choose Backup vaults.
3. In the Backups section, view the list of all the backups organized in this backup vault. In this view, you can sort backups by any of the column headers (including status), as well as select a backup to restore it, edit it, or delete it.

**Listing backups programmatically**

You can list backups programmatically using the ListRecoveryPoint API operations:

- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByResource

For example, the following AWS Command Line Interface (AWS CLI) command lists all your backups with the EXPIRED status:

```bash
aws backup list-recovery-points-by-backup-vault
```
Editing a backup

After you create a backup using AWS Backup, you can change the lifecycle or tags of the backup. The lifecycle defines when a backup is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.

To see the list of resources that you can transition to cold storage, see the "Lifecycle to cold storage" section of the Feature availability by resource (p. 2) table. The cold storage expression is ignored for other resources.

**Note**
Editing the tags of a backup using the AWS Backup console is only supported for backups of Amazon Elastic File System (Amazon EFS) file systems and Advanced Amazon DynamoDB.
Tags that were added to the recovery point on creation for other resources will still appear, but will be greyed out and uneditable. Even though these tags are not editable in the AWS Backup console, you can edit the tags of these other services' backups using the service's console or API.

Backups that are transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the “retention” setting must be 90 days greater than the “transition to cold after days” setting. When you update the “transition to cold after days” setting, the value must be a minimum of the backup’s age plus one day. The “transition to cold after days” setting cannot be changed after a backup has been transitioned to cold.

The following is an example of how to update the lifecycle of a backup.

**To edit the lifecycle of a backup**

2. In the navigation pane, choose Backup vaults.
3. In the **Backups** section, choose a backup.
4. On the backup details page, choose **Edit**.
5. Configure the lifecycle settings, and then choose **Save**.

Deleting backups

We recommend you use AWS Backup to automatically delete the backups that you no longer need by configuring your lifecycle when you created your backup plan. For example, if you set your backup plan’s lifecycle to retain your recovery points for one year, AWS Backup will automatically delete on January 1, 2022 the recovery points it created on or within several hours of January 1, 2021. (AWS Backup randomizes its deletions within 8 hours following recovery point expiration to maintain performance.) To learn more about configuring your lifecycle retention policy, see Creating a backup plan.

However, you might want to manually delete one or more recovery points. For example:

- **You have EXPIRED recovery points.** These are recovery points AWS Backup was unable to delete automatically because you deleted or modified the original IAM policy you used to create your backup plan. When AWS Backup attempted to delete them, it lacked permission to do so.

  **Warning**
  You will continue to store expired recovery points in your account. This might increase your storage costs.
After August 6, 2021, AWS Backup will show the target recovery point as **Expired** in its backup vault. You can hover your mouse over the red **Expired** status for a popover status message that explains why it was unable to delete the backup. You can also choose **Refresh** to receive the most recent information.

- You no longer want a backup plan to operate the way you configured it. Updating the backup plan affects the future recovery points it will create, but does not affect the recovery point it already created. To learn more, see [Updating a backup plan](#).
- You need to clean up after finishing a test or tutorial.

## Deleting backups manually

**To manually delete recovery points**

1. In the AWS Backup console, in the navigation pane, choose **Backup vaults**.

2. On the **Backup vaults** page, choose the backup vault where you stored the backups.

3. Choose a recovery point, choose the **Actions** dropdown, then choose **Delete**.

4. 1. If your list contains a continuous backup, choose one of following options. Each continuous backup has a single recovery point.

   - **Permanently delete my backup data** or **Delete recovery point**. By selecting one of these options, you stop future continuous backups and also delete your existing continuous backup data.

   - **Keep my continuous backup data** or **Disassociate recovery point**. By selecting one of these options, you stop future continuous backups but retain your existing continuous backup data until it expires as defined by your retention period.

2. To delete all the recovery points listed, type delete, and then choose **Delete recovery points**.

3. AWS Backup begins to submit your recovery points for deletion and displays a progress bar. Keep your browser tab open and do not navigate away from this page during the submission process.

4. At the end of the submission process, AWS Backup presents you a status in the banner. The status can be:

   - **Successfully submitted**. You can choose to **View progress** about each recovery point's deletion status.

   - Failed to submit. You can choose to **View progress** about each recovery point's deletion status or **Try again** with your submission.

   - A mixed result where some recovery points were successfully submitted while other recovery points failed to submit.

5. If you choose **View progress**, you can review the **Deletion status** of each backup. If a deletion status is **Failed** or **Expired**, you can click that status to see the reason. You can also choose to **Retry failed deletions**.

## Troubleshooting manual deletions

In rare situations, AWS Backup might not complete your delete request. AWS Backup uses the service-linked role **AWSServiceRoleForBackup** to perform deletions.

If your delete request fails, verify that your IAM role has the permission to create service-linked roles. Specifically, verify your IAM role has the `iam:CreateServiceLinkedRole` action. If it does not, add this permission to your service-linked role using the steps in [Service-linked role permissions](#) in the AWS *Identity and Access Management User Guide*. Adding this permission allows AWS Backup to perform manual deletions.
If, after you confirm that your IAM role has the `iam:CreateServiceLinkedRole` action, your recovery points are still stuck in the DELETING status, we are likely investigating your issue. Complete your manual deletion with the following steps:

1. Set up a reminder to come back in 2-3 days.
2. After 2-3 days, check for recently EXPIRED deletion points that are the result of your first manual deletion operation.
3. Manually delete those EXPIRED recovery points.

## Restoring a backup

### How to restore

For console restore instructions and links to documentation for each AWS Backup-supported resource type, see the links at the bottom of this page.

To restore a backup programmatically, use the `StartRestoreJob` API operation.

The configuration values ("restore metadata") that you need to restore your resource varies depending on the resource that you want to restore. To get the configuration metadata that your backup was created with, you can call `GetRecoveryPointRestoreMetadata`. Restore metadata examples are also available in the links at the bottom of this page.

Restoring from cold storage typically takes 4 hours more than restoring from warm storage.

For each restore, a restore job is created with a unique job ID—for example, 1323657E-2AA4-1D94-2C48-5D7A423E7394.

### Non-destructive restores

When you use AWS Backup to restore a backup, it creates a new resource with the backup that you are restoring. This is to protect your existing resources from being destroyed by your restore activity.

### Copy tags during a restore

**Note**

Restores of Amazon DynamoDB, Amazon S3, SAP HANA on Amazon EC2 instances, virtual machines, and Amazon Timestream resources currently do not have this feature available.

### Introduction

You can copy tags as you restore a resource if the tags belonged to the protected resource at the time of backup. Tags, which are labels containing a key and value pair, can help you identify and search for resources. When you start a restore job, tags that belonged to the original backed-up resources can be added to the resource being restored.

When you choose to include tags during a restore job, this step can replace the overhead and labor of manually applying tags to resources after a restore job is completed. Note this is distinct from adding new tags to restored resources.

When you restore a backup in the console flow, your source tags will be copied by default. In the console, uncheck the box if you wish to opt out of copying tags to a restored resource.

In the API operation `StartRestoreJob`, the parameter `CopySourceTagsToRestoredResource` is set to `false` by default, which will exclude the original source tags from the resource you are restoring. If you wish to `include` tags from the original source, set this to `true`. 
Considerations

- A resource can have up to 50 tags, including restored resources. Please see Tagging your AWS resources for more information about tag limits.
- Ensure the correct permissions are present in the role used for restores to copy tags. The default role for restores contains the necessary permissions. A custom role must include additional permissions to tag resources.
- The following resources are not currently supported for restore tag inclusion: VMware Cloud™ on AWS, VMware Cloud™ on AWS Outposts, on-premises systems, SAP HANA on Amazon EC2 instances, Timestream, DynamoDB, Advanced DynamoDB, and Amazon S3.
- For continuous backups, the tags on the original resource as of the most recent backup will be copied to the restored resource.
- Tags will not be copied for item-level restores.
- Tags that were added to a backup after the backup job was completed but were not present on the original resource prior to the backup will not be copied to the restored resource. Only Backups created after May 22, 2023 are eligible for tag copy on restore.

Tag interaction with specific resources

- When you restore an Amazon EFS resource, it must be copied to a new file system. Restorations to an existing file system cannot have tags copied to it.
- Amazon Redshift clusters, by default, always include tags during a restore job.
- Amazon RDS
  - If the RDS cluster that was backed up is still active, tags from this cluster will be copied.
  - If the original cluster is no longer active, tags from the snapshot of the cluster will be copied instead.
  - Tags which were present on the resource at the time of the backup will be copied during the restore regardless if the Boolean parameter for CopySourceTagsToRestoredResource is set to True or False. However, if the snapshot does not contain tags, then the above Boolean setting will be used.

Copy tags via the console

1. Open the AWS Backup console
2. In the navigation pane, choose Protected resources, and select the Amazon S3 resource ID that you want to restore.
3. On the Resource details page, you will see a list of recovery points for the selected resource ID. To restore a resource:
   a. In the Backup pane, choose the recovery point ID of the resource.
   b. In the upper-right corner of the pane, choose Restore (alternatively, you can go to the backup vault, find the recovery point, and then click Actions then click Restore).
4. On the Restore backup page, locate the panel named Restore with tags. To include all tags from the original resource, retain the check box (note in the console this box is checked by default).
5. Click Restore backup after you have selected all your preferred settings and roles.

To include tags programmatically

Use the API operation StartRestoreJob. Ensure the following Boolean parameter is set to True:

```
CopySourceTagsToRestoredResource = true
```
If the boolean parameter `CopySourceTagsToRestoredResource = True`, the restore job will copy the tags from the original resource(s) to the restored material.

**Important**
The restore job will fail if this parameter is included for an unsupported resource (VMware, AWS Outposts, on-premises systems, SAP HANA on EC2 instances, Timestream, DynamoDB, Advanced DynamoDB, and Amazon S3).

```json
{
    "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
    "Metadata": {
        "InstanceInitiatedShutdownBehavior": "stop",
        "DisableApiTermination": "false",
        "EbsOptimized": "false",
        "InstanceType": "t1.micro",
        "SubnetId": "subnet-123ab456cd7efgh89",
        "SecurityGroupIds": "[sg-0a1bc2d345ef67890]",
        "Placement": "{"GroupName":null,"Tenancy":"default"}",
        "HibernationOptions": "{"Configured":false}",
        "IamInstanceProfileName": "UseBackedUpValue",
        "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
    },
    "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
    "ResourceType": "EC2",
    "IdempotencyToken": "54ab5678-9012-3c4d-5678-efgh01f2314",
    "CopySourceTagsToRestoredResource": true
}
```

**Troubleshoot tag restore issues**

**ERROR:** Insufficient Permissions

**REMEDY:** Ensure you have the necessary permissions in your restore role so you can include tags on your restored resource. The default AWS managed service role policy for restores, `AWSBackupServiceRolePolicyForRestores`, contains the necessary permissions for this task.

If you choose to use a custom role, ensure the following permissions are present:

- elasticfilesystem:TagResource
- storagegateway:AddTagsToResource
- rds:AddTagsToResource
- ec2:CreateTags
- cloudformation:TagResource

For more information, see API permissions.

**Restore job statuses**

You can view the status of a restore job on the Jobs page of the AWS Backup console. Restore job statuses include pending, running, completed, aborted, and failed.

**Topics**

- [Restoring S3 data (p. 142)]
- [Restoring a virtual machine (p. 144)]
- [Restoring an FSX file system (p. 147)]
- [Restoring an Amazon EBS volume (p. 151)]
Restoring S3 data

You can restore the S3 data that you backed up using AWS Backup to the S3 Standard storage class. You can restore all the objects in a bucket or specific objects. You can restore them to an existing or new bucket.

If you restore specific objects, you can restore the current version of an object.

While S3 backups can be copied cross-Region, restore jobs only occur in the same Region in which the original backup or copy is located.

Example

Example: An S3 bucket created in US East (N. Virginia) Region can be copied to Canada (Central) Region. The restore job can be initiated using the original bucket in US East (N. Virginia) Region and restored to that Region, or the restore job can be initiated using the copy in Canada (Central) Region and restored to that Region.

Use the AWS Backup console to restore Amazon S3 recovery points

To restore your Amazon S3 data using the AWS Backup console:

2. In the navigation pane, choose Protected resources, and select the Amazon S3 resource ID that you want to restore.
3. On the Resource details page, you will see a list of recovery points for the selected resource ID. To restore a resource:
   a. In the Backups pane, choose the recovery point ID of the resource.
   b. In the upper-right corner of the pane, choose Restore.
      (Alternatively, you can go to the backup vault, find the recovery point, and then click Actions then click Restore.)
4. If you are restoring a continuous backup, in the Restore time pane, select either option:
   a. Accept the default to restore to the Latest restorable time.
   b. Specify date and time to restore.
5. In the Settings pane, specify whether to Restore entire bucket or perform Item level restore.
a. If you choose **Item level restore**, you restore up to 5 items (S3 objects) per restore job by specifying each item's **S3 URI** that uniquely identifies that object.

(For more information about S3 bucket URIs, see Methods for accessing a bucket in the Amazon Simple Storage Service User Guide.)

b. Choose **Add item** to specify another item to restore.

6. Choose your **Restore destination**. You can either **Restore to source bucket**, **Use existing bucket**, or **Create new bucket**.

   **Note**
   Your restore destination bucket must have versioning turned on. AWS Backup notifies you if the bucket you select does not meet this requirement.

   a. If you choose **Use existing bucket**, select the destination S3 bucket from the dropdown menu which shows all existing buckets within your current AWS Region.

   b. If you choose **Create new bucket**, type in the **new bucket name**. The new bucket defaults to S3 versioning enabled. The **Block Public Access** (BPA) settings will be toggled off by default. You can modify these settings after you create the bucket in S3.

7. You have additional options to choose your **Restored object encryption**. Use **original encryption keys** (default), **Amazon S3 key** (SSE-S3), or **AWS Key Management Service key** (SSE-KMS).

   a. If you choose **Use original encryption keys** (default) but the original object was unencrypted, the restored object will also be unencrypted.

   b. If you choose **Amazon S3 key** (SSE-S3), you do not need to specify any other options.

   c. If you choose **AWS Key Management Service key** (SSE-KMS), you can make the following choices: **AWS managed key** (aws/s3), **Choose from your AWS KMS keys**, or **Enter AWS KMS key ARN**.

      i. If you choose **AWS managed key** (aws/s3), you do not need to specify any other options.

      ii. If you **Choose from your AWS KMS keys**, select a AWS KMS key from the dropdown menu. Alternatively, choose **Create key**.

      iii. If you **Enter AWS KMS key ARN**, type in the ARN into the text box. Alternatively, choose **Create key**.

8. In the **Restore role** pane, choose the IAM role that AWS Backup will assume for this restore.

9. Choose **Restore backup**. The **Restore jobs** pane appears. A message at the top of the page provides information about the restore job.

**Limitations:**
AWS Backup creates a backup of all your S3 versions, but restores only the latest version from the version stack at any point in time.

**Considerations:**
Access Control Lists (ACLs) must be enabled in the destination bucket, or the job will fail otherwise. S3 buckets created through the AWS Backup console have ACLs disabled by default (note that restoring with the **Create new bucket** option will create a bucket with ACLs enabled). To enable ACLs, follow the instructions in Configuring ACLs page.

Restores of objects are skipped if the source bucket has an object with the same name or version ID.

**Use the AWS Backup API, CLI, or SDK to restore Amazon S3 recovery points**

Use **StartRestoreJob**. You can specify the following metadata during Amazon S3 restores:
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.
ItemsToRestore // A list of up to five paths of individual objects to restore. Only required for object-level restore.
NewBucket // Boolean to indicate whether to create a new bucket.
Encryption // Boolean to indicate whether to encrypt the restored data.
CreationToken // An idempotency token.
EncryptionType // The type of encryption to encrypt your restored objects. Options are original (same encryption as the original object), SSE-S3, or SSE-KMS).
RestoreTime // The restore time (only valid for continuous recovery points where it is required, in format 2021-11-27T03:30:27Z).

// Optional metadata:
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.

### Recovery point status

Recovery points will have a status indicating their state.

PARTIAL status indicates AWS Backup could not create the recovery point before the backup window closed. To increase your backup plan window using the API, see [UpdateBackupPlan](#). You can also increase your backup plan window using the Console by choosing and editing your backup plan.

EXPIRED status indicates that the recovery point has exceeded its retention period, but AWS Backup lacks permission or is otherwise unable to delete it. To manually delete these recovery points, see [Step 3: Delete the recovery points](#) in the Clean up resources section of Getting started.

STOPPED status occurs on a continuous backup where a user has taken some action that causes the continuous backup to be disabled. This can be caused by the removal of permissions, turning off versioning, turning off events being sent to Amazon EventBridge, or disabling the EventBridge rules that are put in place by AWS Backup.

To resolve STOPPED status, ensure that all requested permissions are in place and that versioning is enabled on the S3 bucket. Once these conditions are met, the next instance of a backup rule running will result in a new continuous recovery point being created. The recovery points with STOPPED status do not need to be deleted.

### Restoring a virtual machine

#### Use the AWS Backup console to restore virtual machine recovery points

You can restore a virtual machine from multiple locations in the left navigation pane of the AWS Backup console:

- **Choose Hypervisors** to view recovery points for virtual machines managed by a hypervisor that is connected to AWS Backup.
- **Choose Virtual machines** to view recovery points for virtual machines across all your hypervisors that are connected to AWS Backup.
- **Choose Backup vaults** to view recovery points stored in a specific AWS Backup vault.
- **Choose Protected resources** to view recovery points across all your AWS Backup protected resources.

If you need to restore a virtual machine that no longer has a connection with Backup gateway, choose **Backup vaults** or **Protected resources** to locate your recovery point.
AWS Backup restores of virtual machines are non-destructive. This means that AWS Backup does not overwrite existing virtual machines during a restore. Instead, it restores by deploying a new virtual machine.

Your restored virtual machine starts on your infrastructure in shutdown mode.

**To restore a virtual machine to VMware, VMware Cloud on AWS, and VMware Cloud on AWS Outposts:**

1. In the Hypervisors or Virtual machines views, choose the VM name to restore. In the Protected resources view, choose the virtual machine Resource ID to restore.
2. Choose the radial button next to the Recovery point ID to restore.
3. Choose Restore.
4. Choose the Restore type.
   a. Full restore restores all the virtual machine's disks.
   b. Disk-level restore restores a user-defined selection of one or more disks. Use the drop-down menu to select which disks to restore.
5. Choose the Restore location. The options are VMware, VMware Cloud on AWS, and VMware Cloud on AWS Outposts.
6. If you are doing a full restore, skip to the next step. If you are performing a disk-level restore, there will be a drop-down menu under VM disks. Choose one or more bootable volumes to restore.
7. Select a Hypervisor from the dropdown menu to manage the restored virtual machine.
8. For the restored virtual machine, use your organization's virtual machine best practices to specify its:
   a. Name
   b. Path (such as /datacenter/vm)
   c. Compute resource name (such as VMHost or Cluster)
   If a host is part of a cluster then you cannot restore to the host but only to the given cluster.
   d. Datastore
9. For Restore role, select either the Default role (recommended) or Choose an IAM role using the dropdown menu.
10. Choose Restore backup.
11. Optional: Check when your restore job has the status Completed. In the left navigation menu, choose Jobs.

**To restore a virtual machine to Amazon EBS:**

1. In the Hypervisors or Virtual machines views, choose the VM name to restore. In the Protected resources view, choose the virtual machine Resource ID to restore.
2. Choose the radial button next to the Recovery point ID to restore.
3. Choose Restore.
4. Choose the Restore type.
   • Disk restore restores a user-defined selection of one disk. Use the drop-down menu to select which disk to restore.
5. Choose the Restore location as Amazon EBS.
6. Under the VM disk dropdown menu, choose bootable volume to restore.
7. Under EBS Volume type, choose the volume type.
8. Choose your Availability Zone.
9. Encryption (optional). Check the box if you choose to encrypt the EBS volume.
10. Select your KMS key from the dropdown menu.
11. For **Restore role**, select either the **Default role** (recommended) or **Choose an IAM role** using the dropdown menu.
12. Choose **Restore backup**.
13. **Optional**: Check when your restore job has the status Completed. In the left navigation menu, choose **Jobs**.
14. **Optional**: Visit [How do I create an LVM logical volume on an entire Amazon EBS volume?](#) to learn more on how to mount managed volumes and access data on the restored Amazon EBS volume.

### To restore a virtual machine to an Amazon EC2 instance

Restoring (or migrating) a virtual machine to EC2 requires a license. By default, an AWS will include a license (charges apply). For more information, see [Licensing options](#) in the Amazon EC2 VM Import/Export User Guide.

1. In the **Hypervisors** or **Virtual machines** views, choose the **VM name** to restore. In the **Protected resources** view, choose the virtual machine **Resource ID** to restore.
2. Choose the radial button next to the **Recovery point ID** to restore.
3. Choose **Restore**.
4. Choose the **Restore type**.
   - **Full restore** restores the file system completely, including the root-level folder and files.
5. Choose the **Restore location** as **Amazon EC2**.
6. Under the dropdown menu **Instance type**, choose the combination of compute and memory necessary for your new instance.
   - **Note**: Choose an instance that has compute and memory to match or exceed that of your original machine; otherwise performance will be affected.
7. Select the **Virtual Private Cloud (VPC)** that defines the virtual networking environment.
8. Select the **subnet** group. This is a range of IP addresses in your virtual private cloud which can be used to isolate distinct Amazon EC2 instances from each other.
9. Specify the **security groups** you want to use to determine firewall rules for your instance traffic.
10. For **Restore role**, select either the **Default role** (recommended) or **Choose an IAM role** using the dropdown menu.
11. Choose **Restore backup**.

Check when your restore job has the status **Completed**. In the left navigation menu, choose **Jobs**.

### Use the AWS Backup API, CLI, or SDK to restore virtual machines recovery points

Use [StartRestoreJob](#).

You can specify the following metadata during any virtual machine restore:

This example shows how to conduct a full restore to VMware:

```json
"{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-east-1:20987078875:hypervisor/hype-981AB1F1","VMName":"name","VMPath":"/Labster/"}
``
To restore to an Amazon EC2 instance, only "RestoreTo":"EC2Instance" needs to be specified. All other attributes will be defaulted.

**Note**

Restoring (or migrating) a virtual machine to EC2 requires a license. By default, AWS will include a license (charges apply). For more information, see [ Licensing options ] in the Amazon EC2 VM Import/Export User Guide.

## Restoring an FSX file system

The restore options that are available when you use AWS Backup to restore Amazon FSx file systems are the same as using the native Amazon FSx backup. You can use a backup's recovery point to create a new file system and restore a point-in-time snapshot of another file system.

When restoring Amazon FSx file systems, AWS Backup creates a new file system and populates it with the data (Amazon FSx for NetApp ONTAP allows restoring a volume to an existing file system). This is similar to how native Amazon FSx backs up and restores file systems. Restoring a backup to a new file system takes the same amount of time as creating a new file system. The data restored from the backup is lazy-loaded onto the file system. You might therefore experience slightly higher latency during the process.

**Note**

You can't restore to an existing Amazon FSx file system, and you can't restore individual files or folders.

FSx for ONTAP doesn't support backing up certain volume types, including DP (data-protection) volumes, LS (load-sharing) volumes, FlexGroup volumes, full volumes, or volumes on file systems that are full. For more information, please see [FSx for ONTAP Working with backups]. AWS Backup vaults that contain recovery points of Amazon FSx file systems are visible outside of AWS Backup. You can restore the recovery points using Amazon FSx but you can't delete them.

You can see backups created by the built-in Amazon FSx automatic backup functionality from the AWS Backup console. You can also recover these backups using AWS Backup. However, you can't delete these backups or change the automatic backup schedules of your Amazon FSx file systems using AWS Backup.

You can restore backups created by AWS Backup using the AWS Backup console, API, or AWS CLI. This section shows you how to use the AWS Backup console to restore Amazon FSx file systems.

**Use the AWS Backup console to restore Amazon FSx recovery points**

FSx for ONTAP is not available in US West (N. California) Region, Asia Pacific (Jakarta) Region, China (Beijing) Region, China (Ningxia) Region, and Asia Pacific (Osaka) Region.

FSx for OpenZFS is only available in Asia Pacific (Sydney) Region, Asia Pacific (Tokyo) Region, Europe (Ireland) Region, Europe (London) Region, US East (Ohio) Region, US West (Oregon) Region, Asia Pacific (Singapore) Region, Canada (Central) Region, US East (N. Virginia) Region, and Europe (Frankfurt) Region.

**Restoring an FSx for Windows File Server file system**

**To restore an FSx for Windows File Server file system**

2. In the navigation pane, choose Protected resources, and then choose the Amazon FSx resource ID that you want to restore.
3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. Choose the recovery point ID of the resource.

4. In the upper-right corner of the pane, choose **Restore** to open the **Restore backup** page.

5. In the **File system details** section, the ID of your backup is shown under **Backup ID**, and the file system type is shown under **File system type**. You can restore both FSx for Windows File Server and FSx for Lustre file systems.

6. (Optional) Enter a name for your file system.

7. For **Deployment type**, accept the default. You can't change the deployment type of a file system during restore.

8. Choose the **Storage type** to use. If the storage capacity of your file system is less than 2,000 GiB, you can't use the **HDD** storage type.

9. For **Throughput capacity**, choose **Recommended throughput capacity** to use the recommended 16 MB per second (MBps) rate, or choose **Specify throughput capacity** and enter a new rate.

10. In the **Network and security** section, provide the required information.

11. If you are restoring an FSx for Windows File Server file system, provide the **Windows authentication** information used to access the file system, or you can create a new one.

   **Note**

   When restoring a backup, you can't change the type of Active Directory on the file system.


12. (Optional) In the **Backup and maintenance** section, provide the information to set your backup preferences.

13. In the **Restore role** section, choose the IAM role that AWS Backup will use to create and manage your backups on your behalf. We recommend that you choose the **Default role**. If there is no default role, one is created for you with the correct permissions. You can also provide your own IAM role.

14. Verify all your entries, and choose **Restore Backup**.

---

**Restoring an Amazon FSx for Lustre file system**

AWS Backup supports Amazon FSx for Lustre file systems that have persistent storage deployment type and are not linked to a data repository like Amazon S3.

**To restore an Amazon FSx for Lustre file system**


2. In the navigation pane, choose **Protected resources**, and then choose the Amazon FSx resource ID that you want to restore.

3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. Choose the recovery point ID of the resource.

4. In the upper-right corner of the pane, choose **Restore** to open the **Restore backup to new file system** page.

5. In the **Settings** section, the ID of your backup is shown under **Backup ID**, and the file system type is shown under **File system type**. **File system type** should be **Lustre**.

6. (Optional) Enter a name for your file system.

7. Choose a **Deployment type**. AWS Backup only supports the persistent deployment type. You can't change the deployment type of a file system during restore.

   Persistent deployment type is for long-term storage. For detailed information about FSx for Lustre deployment options, see [Using Available Deployment Options for Amazon FSx for Lustre File Systems](https://docs.aws.amazon.com/fsx/latest/LustreFiles/using-available-deployment-options.html) in the *Amazon FSx for Lustre User Guide*.

8. Choose the **Throughput per unit storage** that you want to use.
9. Specify the **Storage capacity** to use. Enter a capacity between 32 GiB and 64,436 GiB.
10. In the **Network and security** section, provide the required information.
11. (Optional) In the **Backup and maintenance** section, provide the information to set your backup preferences.
12. In the **Restore role** section, choose the IAM role that AWS Backup will use to create and manage your backups on your behalf. We recommend that you choose the Default role. If there is no default role, one is created for you with the correct permissions. You can also provide your IAM role.
13. Verify all your entries, and choose **Restore Backup**.

### Restoring Amazon FSx for NetApp ONTAP volumes

**To restore Amazon FSx for NetApp ONTAP volumes:**

2. In the navigation pane, choose **Protected resources**, and then choose the Amazon FSx resource ID that you want to restore.
3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. Choose the recovery point ID of the resource.
4. In the upper-right corner of the pane, choose **Restore** to open the **Restore** page.

   The first section, **File system details**, displays the recovery point ID, the file system ID, and the file system type.
5. Under **Restore options**, there are several selections. First, choose the **File system** from the dropdown menu.
6. Next, choose the preferred **Storage virtual machine** from the dropdown menu.
7. Enter a name for your volume.
8. Specify the **Junction Path**, which is location within your file system where your volume will be mounted.
9. Specify the **Volume size** in megabytes (MB) that you are creating.
10. (Optional) You can choose to **Enable storage efficiency** by checking the box. This will allow deduplication, compression, and compaction.
11. In the **Capacity pool tiering policy** dropdown menu, select the tiering preference.
12. In the **Restore permissions**, choose the IAM role that AWS Backup will use to restore backups.
13. Verify all your entries, and choose **Restore Backup**.

### Restoring an Amazon FSx for OpenZFS file system

**To restore an FSx for OpenZFS file system**

2. In the navigation pane, choose **Protected resources**, and then choose the Amazon FSx resource ID that you want to restore.
3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. Choose the recovery point ID of the resource.
4. In the upper-right corner of the pane, choose **Restore** to open the **Restore backup** page.

   In the **File system details** section, the ID of your backup is shown under **Backup ID**, and the file system type is shown under **File system type**. File system type should be **FSx for OpenZFS**.
5. Under **Restore options**, you may select **Quick restore** or **Standard restore**. Quick restore will use the default settings of the source file system. If you are doing Quick Restore, skip to Step 7.
If you choose Standard restore, specify the additional following configurations:

a. **Provisioned SSD IOPS**: You can choose the **Automatic radio button** or you can choose the **User-provisioned option** if available.

b. **Throughput capacity**: You can choose the **Recommended throughput capacity** of 64 MB/sec or you can choose to **Specify throughput capacity**.

c. **(Optional) VPC security groups**: You can specify VPC security groups to associate with your file system’s network interface.

d. **Encryption key**: Specify the AWS Key Management Service key to protect the restored file system data at rest.

e. **(Optional) Root Volume configuration**: This configuration is collapsed by default. You may expand it by clicking the down-pointing carat (arrow). Creating a file system from a backup will create a new file system; the volumes and snapshots will retain their source configurations.

f. **(Optional) Backup and maintenance**: To set a scheduled backup, click the down-pointing carat (arrow) to expand the section. You may choose the backup window, hour and minute, retention period, and weekly maintenance window.

6. **(Optional)** You may enter a name for your volume.

7. The **SSD Storage capacity** will display the file system’s storage capacity.

8. Choose the **Virtual Private Cloud (VPC)** from which your file system can be accessed.

9. In the **Subnet** dropdown menu, choose the subnet in which your file system’s network interface resides.

10. In the **Restore role** section, choose the IAM role that AWS Backup will use to create and manage your backups on your behalf. We recommend that you choose the **Default role**. If there is no default role, one is created for you with the correct permissions. You can also choose an IAM role.

11. Verify all your entries, and choose **Restore Backup**.

### Use the AWS Backup API, CLI, or SDK to restore Amazon FSx recovery points

To restore Amazon FSx using the API or CLI, use **StartRestoreJob**. You can specify the following metadata during any Amazon FSx restore:

<table>
<thead>
<tr>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileSystemId</td>
</tr>
<tr>
<td>FileSystemType</td>
</tr>
<tr>
<td>StorageCapacity</td>
</tr>
<tr>
<td>StorageType</td>
</tr>
<tr>
<td>VpcId</td>
</tr>
<tr>
<td>KmsKeyId</td>
</tr>
<tr>
<td>SecurityGroupIds</td>
</tr>
<tr>
<td>SubnetIds</td>
</tr>
<tr>
<td>DeploymentType</td>
</tr>
<tr>
<td>WeeklyMaintenanceStartTime</td>
</tr>
<tr>
<td>DailyAutomaticBackupStartTime</td>
</tr>
<tr>
<td>AutomaticBackupRetentionDays</td>
</tr>
<tr>
<td>CopyTagsToBackups</td>
</tr>
<tr>
<td>WindowsConfiguration</td>
</tr>
<tr>
<td>LustreConfiguration</td>
</tr>
<tr>
<td>OntapConfiguration</td>
</tr>
<tr>
<td>OpenZFSConfiguration</td>
</tr>
</tbody>
</table>

### FSx for Windows File Server restore metadata

You can specify the following metadata during an FSx for Windows File Server restore:
Restoring an Amazon EBS volume

When you restore an Amazon Elastic Block Store (Amazon EBS) snapshot, AWS Backup creates a new Amazon EBS volume that you can attach to your Amazon EC2 instance.
You can choose to restore the snapshot as an EBS volume or as an AWS Storage Gateway volume.

**Use the AWS Backup console to restore Amazon EBS recovery points**

**To restore an Amazon EBS volume**

2. In the navigation pane, choose **Protected resources** and then choose the EBS resource ID you want to restore.
3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the **Backups** pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose **Restore**.
4. Specify the restore parameters for your resource. The restore parameters you enter are specific to the resource type that you selected.
   - For **Resource type**, choose the AWS resource to create when restoring this backup.
5. If you choose **EBS volume**, provide the values for **Volume type**, **Size (GiB)**, and choose an **Availability zone**.
   - After **Throughput**, there will be an optional checkbox **Encrypt this volume**. *This option will stay active if the EBS recovery point is encrypted.*
     - You may specify a KMS key or you may create an AWS KMS key.
6. If you choose **Storage Gateway volume**, choose a **Gateway** in a reachable state. Also choose your **iSCSI target name**.
   - For **Volume stored** gateways, choose a **Disk Id**.
   - For **Volume cached** gateways, choose a capacity that is at least as large as your protected resource.
7. For **Restore role**, choose the IAM role that AWS Backup will assume for this restore.
   - **Note**
     - If the AWS Backup default role is not present in your account, a **Default role** is created for you with the correct permissions. You can delete this default role or make it unusable.
8. Choose **Restore backup**.

   The **Restore jobs** pane appears. A message at the top of the page provides information about the restore job.

**Use the AWS Backup API, CLI, or SDK to restore Amazon EBS recovery points**

To restore Amazon EBS using the API or CLI, use **StartRestoreJob**. You can specify the following metadata during any Amazon EBS restore:

```python
availabilityZone
volumeType
volumeSize
iops
throughput
encrypted // if set to true, encryption will be enabled as volume is restored
```
AWS Backup Developer Guide
Restoring an EFS file system

| kmsKeyId // if included, this key will be used to encrypt the restored volume instead of default KMS Key Id |

Example:

"restoreMetadata": {"encrypted":false,"volumeId":"vol-04cc95f3490b5ceea","availabilityZone":null}"

Restoring an Amazon EFS file system

If you are restoring an Amazon Elastic File System (Amazon EFS) instance, you can perform a full restore or an item-level restore.

Full Restore

When you perform a full restore, the entire file system is restored.

AWS Backup does not support destructive restores with Amazon EFS. A destructive restore is when a restored file system deletes or overwrites the source or existing file system. Instead, AWS Backup restores your file system to a recovery directory off of the root directory.

Item-Level Restore

When you perform an item-level restore, AWS Backup restores a specific file or directory. You must specify the relative path related to the mount point. For example, if the file system is mounted to /
user/home/myname/efs and the file path is user/home/myname/efs/file1, you enter /file1. Paths are case sensitive. Wildcard characters and regex strings are not supported.

You can select up to 10 items when you use the console to perform an EFS restore. There is no item limit when you use CLI to restore; however, there is a 200 KB limit on the length of the restore metadata that can be passed.

You can restore those items to either a new or existing file system. Either way, AWS Backup creates a new Amazon EFS directory (aws-backup-restore_datetime) off of the root directory to contain the items. The full hierarchy of the specified items is preserved in the recovery directory. For example, if directory A contains subdirectories B, C, and D, AWS Backup retains the hierarchical structure when A, B, C, and D are recovered. Regardless of whether you perform an Amazon EFS item-level restore to an existing file system or to a new file system, each restore attempt creates a new recovery directory off of the root directory to contain the restored files. If you attempt multiple restores for the same path, several directories containing the restored items might exist.

Note

If you only keep one weekly backup, you can only restore to the state of the file system at the time you took that backup. You can't restore to prior incremental backups.

Use the AWS Backup console to restore an Amazon EFS recovery point

To restore an Amazon EFS file system

2. Your EFS backup vault receives the access policy Deny backup:StartRestoreJob upon creation. If you are restoring your backup vault for the first time, you must change your access policy as follows.
   a. Choose Backup vaults.
   b. Choose the backup vault containing the recovery point you would like to restore.
   c. Scroll down to the vault Access policy

153
d. If present, delete `backup:StartRestoreJob` from the Statement. Do this by choosing Edit, deleting `backup:StartRestoreJob`, then choosing Save policy.

3. In the navigation pane, choose Protected resources and the EFS file system ID you want to restore.

4. On the Resource details page, a list of recovery points for the selected file system ID is shown. To restore a file system, in the Backups pane, choose the radio button next to the recovery point ID of the file system. In the upper-right corner of the pane, choose Restore.

5. Specify the restore parameters for your file system. The restore parameters you enter are specific to the resource type that you selected.

You can perform a Full restore, which restores the entire file system. Or, you can restore specific files and directories using Item-level restore.

- Choose the Full restore option to restore the file system in its entirety including all root level folders and files.
- Choose the Item-level restore option to restore a specific file or directory. You can select and restore up to five items within your Amazon EFS.

To restore a specific file or directory, you must specify the relative path related to the mount point. For example, if the file system is mounted to `/user/home/myname/efs` and the file path is `/user/home/myname/efs/file1`, enter `/file1`. Paths are case sensitive and cannot contain special characters, wildcard characters, and regex strings.

1. In the Item path text box, enter the path for your file or folder.
2. Choose Add item to add additional files or directories. You can select and restore up to five items within your EFS file system.

6. For Restore location

- Choose Restore to directory in source file system if you want to restore to the source file system.
- Choose Restore to a new file system if you want to restore to a different file system.

7. For File system type

- (Recommended) Choose Regional if you want to restore your file system across multiple AWS Availability Zones.
- Choose One Zone if you want to restore your file system to a single Availability Zone. Then, in the Availability Zone dropdown, choose the destination for your restore.

For more information, see Managing Amazon EFS storage classes in the Amazon EFS User Guide.

8. For Performance

- If you chose to perform a Regional restore, choose either (Recommended) General purpose or Max I/O.
- If you chose to perform a One Zone restore, you must choose (Recommended) General purpose. One Zone restores do not support Max I/O.

9. For Enable encryption

- Choose Enable encryption, if you want to encrypt your file system. KMS key IDs and aliases appear in the list after they have been created using the AWS Key Management Service (AWS KMS) console.
- In the KMS key text box, choose the key you want to use from the list.

10. For Restore role, choose the IAM role that AWS Backup will assume for this restore.

   Note
   If the AWS Backup default role is not present in your account, a Default role is created for you with the correct permissions. You can delete this default role or make it unusable.

11. Choose Restore backup.
The Restore jobs pane appears. A message at the top of the page provides information about the restore job.

**Note**
If you only keep one weekly backup, you can only restore to the state of the file system at the time you took that backup. You can't restore to prior incremental backups.

**Use the AWS Backup API, CLI, or SDK to restore Amazon EFS recovery points**

Use [StartRestoreJob](https://docs.aws.amazon.com/backup/latest/devguide/API_StartRestoreJob.html). When restoring an Amazon EFS instance, you can restore an entire file system or specific files or directories. To restore Amazon EFS resources, you need the following information:

- **file-system-id** — The ID of the Amazon EFS file system that is backed up by AWS Backup. Returned in GetRecoveryPointRestoreMetadata.
- **Encrypted** — A Boolean value that, if true, specifies that the file system is encrypted. If KmsKeyId is specified, Encrypted must be set to true.
- **KmsKeyId** — Specifies the AWS KMS key that is used to encrypt the restored file system.
- **PerformanceMode** — Specifies the throughput mode of the file system.
- **CreationToken** — A user-supplied value that ensures the uniqueness (idempotency) of the request.
- **newFileSystem** — A Boolean value that, if true, specifies that the recovery point is restored to a new Amazon EFS file system.
- **ItemsToRestore** — An array of up to five strings where each string is a file path. Use ItemsToRestore to restore specific files or directories rather than the entire file system. This parameter is optional.

For more information about Amazon EFS configuration values, see [create-file-system](https://docs.aws.amazon.com/efs/latest/UG/creating-eFS.html).

**Disabling automatic backups in Amazon EFS**

By default, Amazon EFS creates backups of data automatically. These backups are represented as recovery points in AWS Backup. Attempts to remove the recovery point will result in an error message that notes there are insufficient privileges to perform the action.

It is best practice to keep this auto-backup active. Particularly in the case of accidental data deletion, this backup allows restoration of file system content to the date of the last recovery point created.

In the unlikely event you wish to turn these off, the access policy must be changed from "Effect": "Deny" to "Effect": "Allow". See the Amazon EFS User Guide for more information about turning automatic backups on or off.

**Restoring an Amazon DynamoDB table**

**Use the AWS Backup console to restore DynamoDB recovery points**

To restore a DynamoDB table

2. In the navigation pane, choose Protected resources and the DynamoDB resource ID you want to restore.
3. On the Resource details page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the Backups pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose Restore.

4. For Settings, New table name text field, enter a new table name.

5. For Restore role, choose the IAM role that AWS Backup will assume for this restore.

6. For Encryption settings:
   a. If your backup is managed by DynamoDB (its ARN begins with `arn:aws:dynamodb`), AWS Backup encrypts your restored table using an AWS-owned key.

   To choose a different key to encrypt your restored table, you can either use the AWS Backup StartRestoreJob operation or perform the restore from the DynamoDB console.

   b. If your backup supports full AWS Backup management (its ARN begins with `arn:aws:backup`), you can choose any of the following encryption options to protect your restored table:

   - (Default) DynamoDB-owned KMS key (no additional charge for encryption)
   - DynamoDB-managed KMS key (KMS charges apply)
   - Customer-managed KMS key (KMS charges apply)

"DynamoDB-owned" and "DynamoDB-managed" keys are the same as "AWS-owned" and "AWS-managed" keys, respectively. For clarification, see Encryption at Rest: How It Works in the Amazon DynamoDB Developer Guide.

For more information about full AWS Backup management, see Advanced DynamoDB backup (p. 107).

Note

The following guidance applies only if you restore a copied backup AND want to encrypt the restored table with the same key you used to encrypt your original table. When restoring a cross-Region backup, to encrypt your restored table using the same key you used to encrypt your original table, your key must be a multi-Region key. AWS-owned and AWS-managed keys are not multi-Region keys. To learn more, see Multi-Region keys in the AWS Key Management Service Developer Guide.

When restoring a cross-account backup, to encrypt your restored table using the same key you used to encrypt your original table, you must share the key in your source account with your destination account. AWS-owned and AWS-managed keys cannot be shared between accounts. To learn more, see Allowing users in other accounts to use a KMS key in the AWS Key Management Service Developer Guide.

7. Choose Restore backup.

The Restore jobs pane appears. A message at the top of the page provides information about the restore job.

Use the AWS Backup API, CLI, or SDK to restore DynamoDB recovery points

Use StartRestoreJob. You can specify the following metadata during any DynamoDB restore. The metadata is not case-sensitive.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```
The following is an example of the restoreMetadata argument for a StartRestoreJob operation in the CLI:

```
aws backup start-restore-job \\
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-g3hi-4567-8cjk-012345678901" \\
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \\
--metadata \\
  'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,KMSMasterKeyId=arn:aws:kms:us-east-1:123456789012:key/abcdefg' \\
  --region us-east-1 \\
  --endpoint-url https://cell-1.gamma.us-east-1.controller.cryo.aws.a2z.com
```

The preceding example encrypts the restored table using an AWS-owned key. The part of the restore metadata that specifies encryption using the AWS-owned key is: "encryptionType":"Default",
"kmsMasterKeyId": "Not Applicable".

To encrypt your restored table using an AWS-managed key, specify the following restore metadata: "encryptionType":"KMS",
"keyArn": "Not Applicable".

To encrypt your restored table using an customer-managed key, specify the following restore metadata: "encryptionType":"KMS",
"keyArn": "arn:aws:kms:us-west-2:1112222333:key/1234abcd-12ab-34cd-56ef-1234567890ab".

## Restoring an RDS database

Restoring an Amazon RDS database requires specifying multiple restore options. For more information about these options, see Backing Up and Restoring an Amazon RDS DB Instance in the Amazon RDS User Guide.

### Use the AWS Backup console to restore Amazon RDS recovery points

2. In the navigation pane, choose Protected resources and the Amazon RDS resource ID you want to restore.
3. On the Resource details page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the Backups pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose Restore.
4. In the Instance specifications pane, accept the defaults or specify the options for the DB engine, License Model, DB instance class, Multi AZ, and Storage type settings. For example, if you want a standby database instance, specify Multi AZ.
5. In the Settings pane, specify a name that is unique for all DB instances and clusters owned by your AWS account in the current Region. The DB instance identifier is case insensitive, but it is stored as all lowercase, as in "mydbinstance". This is a required field.
6. In the Network & Security pane, accept the defaults or specify the options for the Virtual Private Cloud (VPN), Subnet group, Public Accessibility (usually Yes), and Availability zone settings.
7. In the Database options pane, accept the defaults or specify the options for Database port, DB parameter group, Option Group, Copy tags to snapshots, and IAM DB Authentication Enabled settings.
8. In the Encryption pane, use the default settings. If the source database instance for the snapshot was encrypted, the restored database instance will also be encrypted. This encryption cannot be removed.
9. In the Log exports pane, choose the log types to publish to Amazon CloudWatch Logs. The IAM role is already defined.
10. In the **Maintenance** pane, accept the default or specify the option for **Auto minor version upgrade**.

11. In the **Restore role** pane, choose the IAM role that AWS Backup will assume for this restore.

12. Once all settings have been specified, choose **Restore backup**.

   The **Restore jobs** pane appears. A message at the top of the page provides information about the restore job.

**Use the AWS Backup API, CLI, or SDK to restore Amazon RDS recovery points**

Use **StartRestoreJob**. You can specify the following metadata during Amazon RDS restores:

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String <code>dBInstanceIdentifier</code></td>
<td>-db instance identifier for Amazon RDS instance to create and attach to restored Aurora cluster.</td>
</tr>
<tr>
<td>String <code>engine</code></td>
<td>database engine (e.g., <code>postgresql</code>)</td>
</tr>
<tr>
<td>String <code>licenseModel</code></td>
<td>licensing model (e.g., <code>postgres-license</code>)</td>
</tr>
<tr>
<td>String <code>dBInstanceClass</code></td>
<td>database instance class (e.g., <code>db.t2.small</code>)</td>
</tr>
<tr>
<td>String <code>availabilityZone</code></td>
<td>availability zone (e.g., <code>us-east-1d</code>)</td>
</tr>
<tr>
<td>Boolean <code>multiAZ</code></td>
<td>flag to indicate if multi-AZ is enabled</td>
</tr>
<tr>
<td>Boolean <code>publiclyAccessible</code></td>
<td>flag to indicate if instance is publicly accessible</td>
</tr>
<tr>
<td>String <code>storageType</code></td>
<td>storage type (e.g., <code>gp2</code>)</td>
</tr>
<tr>
<td>Integer <code>port</code></td>
<td>database port (e.g., 0)</td>
</tr>
<tr>
<td>Integer <code>iops</code></td>
<td>input/output operations per second (IOPS)</td>
</tr>
<tr>
<td>Boolean <code>autoMinorVersionUpgrade</code></td>
<td>flag to indicate if minor version upgrades are allowed</td>
</tr>
<tr>
<td>String <code>dBParameterGroupName</code></td>
<td>name of the database parameter group</td>
</tr>
<tr>
<td>List&lt;String&gt; <code>vpcSecurityGroupIds</code></td>
<td>list of VPC security group IDs for the restored instance</td>
</tr>
<tr>
<td>String <code>dBSubnetGroupName</code></td>
<td>name of the database subnet group for the restored instance</td>
</tr>
<tr>
<td>Boolean <code>enableIAMDatabaseAuthentication</code></td>
<td>flag to enable IAM authentication for database access</td>
</tr>
<tr>
<td>Boolean <code>deletionProtection</code></td>
<td>flag to enable deletion protection for the restored instance</td>
</tr>
<tr>
<td>String <code>dBName</code></td>
<td>database name (e.g., <code>cryo-instance-ec2-user-tlrq1</code>)</td>
</tr>
<tr>
<td>String <code>tdeCredentialArn</code></td>
<td>TDE credential ARN for encrypted databases</td>
</tr>
<tr>
<td>String <code>domain</code></td>
<td>domain for the restored instance</td>
</tr>
<tr>
<td>String <code>domainIAMRoleName</code></td>
<td>IAM role name for the restored instance</td>
</tr>
<tr>
<td>Boolean <code>copyTagsToSnapshot</code></td>
<td>flag to copy tags to snapshot during restore</td>
</tr>
<tr>
<td>List&lt;String&gt; <code>enableCloudwatchLogsExports</code></td>
<td>list of CloudWatch log export names for the restored instance</td>
</tr>
<tr>
<td>List&lt;ProcessorFeature&gt; <code>processorFeatures</code></td>
<td>list of processor features for the restored instance</td>
</tr>
</tbody>
</table>

**Example:**

```json
"restoreMetadata": 
"\"LicenseModel\":\"postgresql-license\",\"StorageType\":\"gp2\",\"dBInstanceClass\":\"db.t2.small\",\"Port\":\"0\",\"AvailabilityZone\":\"us-east-1d\",\"OptionGroupName\":\"default:postgres-12\",\"ProcessorFeatures\":\"\"\",\"AutoMinorVersionUpgrade\":\"true\",\"dBSubnetGroupName\":\"default\",\"DeletionProtection\":\"false\",\"dBInstanceIdentifier\":\"cryo-instance-ec2-user-tlrq1\",\"dBParameterGroupName\":\"default.postgres12\",\"VpcSecurityGroupIds\":\"
\"sg-3ba6747b\"
\",\"EnableIAMDatabaseAuthentication\":\"false\",\"CopyTagsToSnapshot\":\"false\",\"PubliclyAccessible\":\"false\",\"MultiAZ\":\"false\",\"Engine\":\"postgres\",\"EnableCloudwatchLogsExports\":\"\"\""
```

**Restoring an Amazon Aurora cluster**

**Use the AWS Backup console to restore Aurora recovery points**

AWS Backup restores your Aurora cluster; it does not create or attach an Amazon RDS instance to your cluster. In the following steps, you will create and attach an Amazon RDS instance to your restored Aurora cluster using the CLI.
Restoring an Aurora cluster requires that you specify multiple restore options. For information about these options, see Overview of Backing Up and Restoring an Aurora DB Cluster in the Amazon Aurora User Guide.

To restore an Amazon Aurora cluster

2. In the navigation pane, choose Protected resources and the Aurora resource ID that you want to restore.
3. On the Resource details page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the Backups pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose Restore.
4. In the Instance specifications pane, accept the defaults or specify the options for the DB engine, DB engine version, and Capacity type settings.

Note
If Serverless capacity type is selected, a Capacity settings pane appears. Specify the options for the Minimum Aurora capacity unit and Maximum Aurora capacity unit settings, or choose different options from the Additional scaling configuration section.

5. In the Settings pane, specify a name that is unique for all DB cluster instances owned by your AWS account in the current Region. The DB cluster identifier is case insensitive, but it is stored as all lowercase, as in "mydbclusterinstance". This is a required field.
6. In the Network & Security pane, accept the defaults or specify the options for the Virtual Private Cloud (VPC), Subnet group, and Availability zone settings.
7. In the Database options pane, accept the defaults or specify the options for Database port, DB cluster parameter group, and IAM DB Authentication Enabled settings.
8. In the Backup pane, accept the default or specify the option for the Copy tags to snapshots setting.
9. In the Backtrack pane, accept the default or specify the options for the Enable Backtrack or Disable Backtrack settings.
10. In the Encryption pane, accept the default or specify the options for the Enable encryption or Disable encryption settings.
11. In the Log exports pane, choose the log types to publish to Amazon CloudWatch Logs. The IAM role is already defined.
12. In the Restore role pane, choose the IAM role that AWS Backup will assume for this restore.
13. After specifying all your settings, choose Restore backup.

The Restore jobs pane appears. A message at the top of the page provides information about the restore job.

14. After your restore finishes, attach your restored Aurora cluster to an Amazon RDS instance.

Using the AWS CLI:

- For Linux, macOS, or Unix:

  ```bash
  aws rds create-db-instance --db-instance-identifier sample-instance
  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-instance-class db.r4.large
  ```

- For Windows:

  ```bash
  aws rds create-db-instance --db-instance-identifier sample-instance
  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-instance-class db.r4.large
  ```
Use the AWS Backup API, CLI, or SDK to restore Aurora recovery points

Use `StartRestoreJob`. You can specify the following metadata during Aurora restores:

```java
List<String> availabilityZones;  
Long backtrackWindow;  
Boolean copyTagsToSnapshot;  
String databaseName;  
String dbClusterIdentifier;  
String dbClusterParameterGroupName;  
String dbSubnetGroupName;  
List<String> enableCloudwatchLogsExports;  
Boolean enableIAMDatabaseAuthentication;  
String databaseName;  
String dbClusterIdentifier;  
String dbClusterParameterGroupName;  
String dbSubnetGroupName;  
List<String> enableCloudwatchLogsExports;  
Boolean enableIAMDatabaseAuthentication;  
String engine;  
String engineMode;  
String engineVersion;  
String kmsKeyId;  
Integer port;  
String optionGroupName;  
ScalingConfiguration scalingConfiguration;  
List<String> vpcSecurityGroupIds;
```

Example:

```
"restoreMetadata":"{"\"EngineVersion\":\"5.6.10a\",\"KmsKeyId\":\"arn:aws:kms:us-east-1:234567890123:key/45678901-ab23-4567-8cd9-012d456e6f7\",\"EngineMode\":\"serverless \",\"AvailabilityZones\":\"[\"us-east-1b\",\"us-east-1c \",\"us-east-1e\"]\",\"Port\":\"3306\",\"DatabaseName\":\"\",\"DBSubnetGroupName\":\"default-vpc-05a3b70c6f6e193e1g\",\"VpcSecurityGroupIds\":\"[\"sg-012d52c68c6e88f00\"]\",\"ScalingConfiguration\":\"MinCapacity\":2,\"MaxCapacity\":64,\"AutoPause\":true,\"SecondsUntilAutoPause\":300,\"TimeoutAction\":\"RollbackCapacityChange \",\"EnableIAMDatabaseAuthentication\":false,\"DBClusterParameterGroupName\":\"default.aurora5.6\",\"CopyTagsToSnapshot\":true,\"Engine\":\"aurora\",\"EnableCloudwatchLogsExports\":false\}"}
```

Restoring an Amazon EC2 instance

When using the console, you can perform restores with 16 options. If you need to set the other parameters, you must use the CLI or SDK.

**Note**

AWS Backup does not backup and restore user-data that is used while launching an Amazon EC2 instance.

Use the AWS Backup console to restore Amazon EC2 recovery points

This is the recommended option.

**To restore Amazon EC2 resources using the AWS Backup console**

2. In the navigation pane, choose **Protected resources** and the Amazon EC2 resource ID that you want to restore.
3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the **Backups** pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose **Restore**.
4. In the **Network settings** pane, accept the defaults or specify the options for the **Instance type**, **Virtual Private Cloud (VPC)**, **Subnet**, **Security groups**, and **Instance IAM role** settings.

5. In the **Restore role** pane, accept the **Default role** or **Choose an IAM role** to specify the IAM role that AWS Backup will assume for this restore.

6. In the **Advanced settings** pane, accept the defaults or specify the options for the **Shutdown behavior**, **Enable termination protection**, **Placement group**, **T2/T3 Unlimited**, **Tenancy**, and **User data** settings. This section is used to customize shutdown and hibernation behavior, termination protection, placement groups, tenancy, and other advanced settings.

7. After specifying all your settings, choose **Restore backup**.

   The **Restore jobs** pane appears. A message at the top of the page provides information about the restore job.

The AWS Backup console allows you to restore Amazon EC2 recovery points with the following parameters and settings you can customize:

- Instance type
- Amazon VPC
- Subnet
- Security groups
- IAM role
- Shutdown behavior
- Stop–hibernate behavior
- Termination protection
- T2/T3 unlimited
- Placement group name
- EBS-optimized instance
- Tenancy
- RAM disk ID
- Kernel ID
- User data
- Deletion on termination

These parameters are prefilled to match the original backup. You can change them before restoring the instance. AWS Backup identifies parameters with values that might not be valid or that might result in an invalid restore.

**Use the AWS Backup API, CLI, or SDK to restore Amazon EC2 recovery points**

Use **StartRestoreJob**. This option allows you to restore all 38 parameters, including the 22 parameters that are not customizable on the console. The Amazon EC2 API Reference lists all 38 parameters. This is suitable if you require all 38 parameters and are comfortable restoring parameters without validation. The following is an example of the metadata you can pass to restore an Amazon EC2 recovery point.

```
"restoreMetadata":
```
You can also restore an Amazon EC2 instance without including any stored parameters. This option is available on the Protected resource tab on the AWS Backup console.

Note
AWS Backup will use the SSH key pair used at time of backup to automatically perform your restore. AWS Backup doesn't allow you to modify the instance profile. This is to prevent the possibility of privilege escalations. If you need to modify the instance profile, do so from Amazon EC2.

To successfully do a restore with the original instance profile, you must edit the restore policy. If you apply an instance profile during the restore, you have to update the operator role and add PassRole permissions of the underlying instance profile role to Amazon EC2. Otherwise, Amazon EC2 can't authorize the instance launch, and it will fail.

During a restore, all Amazon EC2 quotas and configuration restrictions apply.

### Restoring a Storage Gateway volume

If you are restoring an AWS Storage Gateway volume snapshot, you can choose to restore the snapshot as a Storage Gateway volume or as an Amazon EBS volume. This is because AWS Backup integrates with both services, and any Storage Gateway snapshot can be restored to either an Storage Gateway volume or an Amazon EBS volume.

#### To restore a Storage Gateway volume

2. In the navigation pane, choose Protected resources and then choose the Storage Gateway resource ID you want to restore.
3. On the Resource details page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the Backups pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose Restore.
4. Specify the restore parameters for your resource. The restore parameters you enter are specific to the resource type that you selected.
   - For Resource type, choose the AWS resource to create when restoring this backup.
5. If you choose Storage Gateway volume, choose a Gateway in a reachable state. Also choose your iSCSI target name.
   - 1. For "Volume stored" gateways, choose a Disk ID.
   - 2. For "Volume cached" gateways, choose a capacity that is at least as large as your protected resource.
If you choose **EBS volume**, provide the values for **Volume type**, **Size (GiB)**, and choose an **Availability zone**.

6. For **Restore role**, choose the IAM role that AWS Backup will assume for this restore.

   **Note**
   If the AWS Backup default role is not present in your account, a **Default role** is created for you with the correct permissions. You can delete this default role or make it unusable.

7. Choose **Restore backup**.

   The **Restore jobs** pane appears. A message at the top of the page provides information about the restore job.

**Using the AWS Backup API, CLI, or SDK to restore Storage Gateway recovery points**

Use **StartRestoreJob**.

**Restore an Amazon Timestream table**

When you restore a Amazon Timestream table, there are several options to configure, including the new table name, the destination database, your storage allocation preferences (memory and magnetic storage), and which role you'll use to complete the restore job. You can also choose an Amazon S3 bucket in which to store error logs. Magnetic storage writes are asynchronous, so you may wish you log the errors.

Timestream data storage has two tiers: a memory store and a magnetic store. Memory store is required, but you have the option of transferring your restored table to magnetic storage after the specified memory time is finished. Memory store is optimized for high throughput data writes and fast point-in-time queries. The magnetic store is optimized for lower throughput late-arrival data writes, long-term data storage, and fast analytical queries.

When you restore a Timestream table, you determine how long you want the table to remain in each storage tier. Using the console or API, you can set the storage time for both. Note that the storage is linear and sequential. Timestream will store your restored table in memory storage first, then automatically transition it to magnetic storage when the memory storage time has been reached.

**Note**

The magnetic store retention period must be equal or greater than the original retention period (shown at the top-right of the console), or data will be lost.

*Example:* You set the memory store allocation to hold data for one week and set the magnetic store allocation to hold the same data for one year. When the data in the memory store becomes a week old, it is automatically moved to the magnetic store. It is then retained in the magnetic store for a year. At the end of that time, it is deleted from Timestream and from AWS Backup.

**To restore a Amazon Timestream table using the AWS Backup console**

You can restore Timestream tables in the AWS Backup console that were created by AWS Backup.

2. In the navigation pane, choose **Protected resources** and the Amazon Timestream resource ID that you want to restore.
3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the **Backups** pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose **Restore**.

4. Specify your new table configuration settings, including:
   a. **New table name**, consisting of 2 to 256 characters (letters, numbers, dashes, periods, and underscores).
   b. **Destination database**, chosen from the drop down menu.

5. **Storage allocation**: Set the amount of time the restored table will first reside in **memory storage**, and set the amount of time the restored table will then reside in **magnetic storage**. Memory storage can be set to hours, days, weeks, or months. Magnetic storage can be set to days, weeks, months, or years.

6. *(Optional)* **Enable magnetic storage writes**: You have the option of allowing magnetic storage writes. With this option checked, late-arriving data, which is data with a timestamp outside the memory storage retention period, will be written directly into the magnetic store.

7. *(Optional)* **Amazon S3 error logs location**: You can specify an S3 location in which your error logs will be stored. Browse your S3 files or copy and paste the S3 file path.
   **Note**
   If you choose to specify an S3 error log location, the role you use for this restore must have permission to write to an S3 bucket or it must contain a policy with that permission.

8. Choose the IAM role to be passed to perform restores. You can use the default IAM role or specify a different one.

9. Click **Restore backup**.

Your restore jobs will be visible under protected resources. You can see the current status of your restore job by clicking the refresh button or CTRL-R.

**To restore a Amazon Timestream table using API, CLI, or SDK**

Use **StartRestoreJob** to restore a Timestream table via API.

To restore a Timestream using the AWS CLI, use the operation **start-restore-job**. and specify the following metadata:

```plaintext
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriod: value: number unit: 'hours' | 'days' | 'weeks' | 'months'
MagneticStoreRetentionPeriod: value: number unit: 'days' | 'weeks' | 'months' | 'years'
EnableMagneticStoreWrites?: boolean;
```

Here is an example template:

```
aws backup start-restore-job
  --recovery-point-arn "arn:aws:backup:region:account:snapshot:name"
  --iam-role-arn "arn:aws:iam:account:role/role-name"
  --metadata
  --resource-type Timestream
  --region AWS Region
  --endpoint-url URL
```

You can also use **DescribeRestoreJob** to assist with restore information.

In the AWS CLI, use the operation **describe-restore-job** and use the following metadata:

```plaintext
TableName: string;
```
Restore an Amazon Redshift cluster

You can restore automated and manual snapshots in the AWS Backup console or through CLI.

When you restore a Amazon Redshift cluster, the original cluster settings are input into the console by default. You can specify different settings for the configurations below. When restoring a table, you must specify the source and target databases. For more information on these configurations, see [Restoring a cluster from a snapshot](amazon-redshift-management-guide) in the Amazon Redshift Management Guide.

- **Single table or cluster**: You can choose to restore an entire cluster or a single table. If you choose to restore a single table, the source database, source schema, and source table name are needed, as well as the target cluster, schema, and new table name.
- **Node type**: Each Amazon Redshift cluster consists of a leader node and at least one compute node. When you restore a cluster, you need to specify the node type that meets your requirements for CPU, RAM, storage capacity, and drive type.
- **Number of nodes**: When restoring a cluster, you need to specify the number of nodes needed.
- **Configuration summary**
- **Cluster Permissions**

To restore an Amazon Redshift cluster or table using the AWS Backup console

2. In the navigation pane, choose **Settings** and the Amazon Redshift resource ID that you want to restore.
3. On the **Resource details** page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the **Recovery Points** pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose **Restore**.
4. **Restore Options**
   a. Restore cluster from snapshot, or
   b. Restore single table within a snapshot to new cluster. If you choose this options, then you must configure the following:
      i. Toggle on or off case-sensitive names.
      ii. Input the source table values, including the database, the schema, and the table. The source table information can be found in the [Amazon Redshift console](https://console.aws.amazon.com/redshift/).
      iii. Input the target table values, including the database, the schema, and the new table name.
5. **Specify your new cluster configuration settings.**
   a. For cluster restore: choose Cluster identifier, Node type, and number of nodes.
b. Specify availability zone and maintenance windows.
c. You can associate additional roles by clicking **Associate IAM roles**.

6. **Optional:** Additional configurations:
   a. **Use defaults** is toggled on by default.
   b. Use the dropdown menus to select settings for Networking and security, VPC security groups, Cluster subnet group, and Availability zone.
   c. Toggle **Enhanced VPC routing** on or off.
   d. Determine if you want to make your cluster endpoint **publicly accessible**. If it is, instances and devices outside the VPC can connect to your database through the cluster endpoint. If this is toggled on, input the elastic IP address.

7. **Optional:** Database configuration. You may choose to input
   a. Database port (by typing into the text field)
   b. Parameter groups

8. Maintenance: You can choose the
   a. Maintenance window
   b. Maintenance track, from among current, trailing, or preview. This controls which cluster version is applied during a maintenance window.

9. Automated snapshot is set to default.
   a. Automated snapshot retention period. Retention period must be 0 to 35 days. Choose 0 to not create automated snapshots.
   b. The manual snapshot retention period is 1 to 3653 days.
   c. There is an optional checkbox for cluster relocation. If this is checked, it permits the ability to relocate your cluster in another Availability Zone. After you enable relocation, you can use the VPC endpoint.

10. Monitoring: After a cluster is restored, you can set up monitoring through CloudWatch or Amazon Redshift.
11. Choose IAM role to be passed to perform restores. You can use the default role, or you can specify a different one.

Your restore jobs will be visible under **Jobs**. You can see the current status of your restore job by clicking the refresh button or CTRL-R.

**To restore a Amazon Redshift cluster using API, CLI, or SDK**

Use **StartRestoreJob** to restore a Amazon Redshift cluster.

To restore a Amazon Redshift using the AWS CLI, use the operation **start-restore-job**. and specify the following metadata:

| RestoreType \ ClusterIdentifier \ Encrypted \ KmsKeyId |
|----------------|----------------|----------------|
| CLUSTER_RESTORE \ TABLE_RESTORE \ TRUE \ Optional |

Here is an example template:

```
aws backup start-restore-job \
  --recovery-point-arn "arn:aws:backup:region:account:snapshot:name" \
  --iam-role-arn "arn:aws:iam:account:role/role-name"
```
AWS Backup Developer Guide

Restore an SAP HANA database on an Amazon EC2 instance

Here is an example:

```bash
aws backup start-restore-job \
  --iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
  --metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
  --resource-type Redshift \
  --region us-west-2 \
```

You can also use `DescribeRestoreJob` to assist with restore information.

In the AWS CLI, use the operation `describe-restore-job` and use the following metadata:

```bash
aws backup describe-restore-job --restore-job-id restore job ID \
  --region AWS Region
```

Here is an example:

```bash
aws backup describe-restore-job --restore-job-id BEA3B353-S76C-22C0-9E99-09632F262620 \
  --region us-west-2 \
```

**Restore an SAP HANA database on an Amazon EC2 instance**

SAP HANA databases on EC2 instances can be restored using the AWS Backup console, using API, or using AWS CLI.

**Topics**
- [Restore an SAP HANA on Amazon EC2 instance database using the AWS Backup console](p. 167)
- [StartRestoreJob API for SAP HANA on EC2](p. 168)
- [CLI for SAP HANA on EC2](p. 170)
- [Troubleshooting](p. 171)

**Restore an SAP HANA on Amazon EC2 instance database using the AWS Backup console**

Note that backup jobs and restore jobs involving the same database cannot occur concurrently. When an SAP HANA database restore job is occurring, attempts to back up the same database will likely result in an error: “Database cannot be backed up while it is stopped.”

1. Access the AWS Backup console using the credentials from prerequisites.
2. Under the **Target restore location** dropdown menu, choose a database to overwrite with the recovery point you are using to restore (note that the instance hosting the restore target database must also have the permissions from the prerequisites).

   **Important**
   SAP HANA database restores are destructive. Restoring a database will overwrite the database at the specified target restore location.

3. Complete this step only if you are performing a system copy restore; otherwise, skip to step 4.

   System copy restores are restore jobs which restore to a target database different from the source database which generated the recovery point. For system copy restores, notice the `aws ssm-sap put-resource-permission` command provided for you on the console. This command must be copied, pasted, and executed on the machine that completed the prerequisites. When running the command, use the credentials from the role in the prerequisite where you set up the required permissions for registering applications.

   ```bash
   // Example command
   aws ssm-sap put-resource-permission \
   --region us-east-1 \
   --action-type RESTORE \
   --source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
   ```

4. Once you choose the restore location, you can see the target database's **Resource ID, Application name, Database type**, and the **EC2 instance**.

5. Optionally, you may open **Advanced restore settings** to change your catalog restore option. The default selection is to restore the latest catalog from AWS Backup.

6. Click **Restore backup**.

7. The target location will be overwritten during restore ("destructive restore"), so you must provide confirmation that you permit this in the next pop-up dialog box.

   a. To proceed, you must understand that the existing database will be overwritten by the one you are restoring.

   b. Once this is understood, you must acknowledge the existing data will be overwritten. To acknowledge this and to proceed, type **overwrite** into the text input field.

8. Click **Restore backup**.

If the procedure was successful, a blue banner will appear at the top of the console. This signifies that the restore job is in progress. You will be automatically redirected to the Jobs page where your restore job will appear in the list of restore jobs. This most recent job will have a status of **Pending**. You can search for and then click on the restore job ID too see details of each restore job. You can refresh the restore jobs list by clicking the refresh button to view changes to the restore job status.

**StartRestoreJob API for SAP HANA on EC2**

This action recovers the saved resource identified by an Amazon Resource Name (ARN).

**Request Syntax**

```plaintext
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
  "IdempotencyToken": "string",
  "Metadata": {
    "string": "string"
  },
  "RecoveryPointArn": "string",
}
ResourceType: "string"

URI Request Parameters: The request does not use any URI parameters.

Request Body: The request accepts the following data in JSON format:

IdempotencyToken A customer-chosen string that you can use to distinguish between otherwise identical calls to StartRestoreJob. Retryng a successful request with the same idempotency token results in a success message with no action taken.

Type: String
Required: No

Metadata
A set of metadata key-value pairs. Contains information, such as a resource name, required to restore a recovery point. You can get configuration metadata about a resource at the time it was backed up by calling GetRecoveryPointRestoreMetadata. However, values in addition to those provided by GetRecoveryPointRestoreMetadata might be required to restore a resource. For example, you might need to provide a new resource name if the original already exists.

You need to include specific metadata to restore an SAP HANA on Amazon EC2 instance. See StartRestoreJob metadata for SAP HANA-specific items.

To retrieve the relevant metadata, you can use the call GetRecoveryPointRestoreMetadata.

Example of a standard SAP HANA database recovery point:

"RestoreMetadata": {
  "BackupSize": "1660948480",
  "DatabaseName": "DATABASENAME",
  "DatabaseType": "SYSTEM",
  "HanaBackupEndTime": "1674838362",
  "HanaBackupId": "1234567890123",
  "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
  "HanaBackupStartTime": "1674838349",
  "HanaVersion": "2.00.040.00.1553674765",
  "IsCompressedBySap": "FALSE",
  "IsEncryptedBySap": "FALSE",
  "SystemDatabaseSid": "HDB",
  "aws:backup:request-id": "46bbtt4q-7unjz-2897-m486-yn378k2mzw9c"
}

Example of a continuous SAP HANA database recovery point:

"RestoreMetadata": {
  "AvailableRestoreBases": "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
  "BackupSize": "1711284224",
  "DatabaseName": "DATABASENAME",
  "DatabaseType": "TENANT",
  "EarliestRestorablePitrTimestamp": "1674764799789",
  "HanaBackupEndTime": "1668032687",
  "HanaBackupId": "1234567890123",
  "HanaBackupPrefix": "1234567890123_HDB_FULL",
  "HanaBackupStartTime": "1668032667",
  "HanaVersion": "2.00.040.00.1553674765",
  "IsCompressedBySap": "FALSE",
  "IsEncryptedBySap": "FALSE",
  "SystemDatabaseSid": "HDB",
  "aws:backup:request-id": "46bbtt4q-7unjz-2897-m486-yn378k2mzw9c"  
}
"IsEncryptedBySap": "FALSE",
"LatestRestorablePitrTimestamp": "1674850299789",
"SystemDatabaseSid": "HDB",
"aws:backup:request-id": "46bbt4q-7unr-2897-m486-yn378k2mzw9d"
}

**CLI for SAP HANA on EC2**

The command `start-restore-job` recovers the saved resource identified by an Amazon Resource Name (ARN). CLI will follow the API guideline above.

**Synopsis:**

```
start-restore-job
   --recovery-point-arn value
   --metadata value
      [--idempotency-token value]
      [--resource-type value]
      [--cli-input-json value]
      [--generate-cli-skeleton value]
      [--debug]
      [--endpoint-url value]
      [--no-verify-ssl]
      [--no-paginate]
      [--output value]
      [--query value]
      [--profile value]
      [--region value]
      [--version value]
      [--color value]
      [--no-sign-request]
      [--ca-bundle value]
      [--cli-read-timeout value]
      [--cli-connect-timeout value]
```

**Options**

`--recovery-point-arn` (string) is a string in the form of an Amazon Resource Number (ARN) that uniquely identifies a recovery point; for example

```
arn:aws:backup:region:123456789012:recovery-point:46bbt4q-7unr-2897-m486-yn378k2mzw9d
```

`--metadata` (map): A set of metadata key-value pairs. Contains information, such as a resource name, required to restore a recovery point. You can get configuration metadata about a resource at the time it was backed up by calling `GetRecoveryPointRestoreMetadata`. However, values in addition to those provided by `GetRecoveryPointRestoreMetadata` might be required to restore a resource. You need to specify specific metadata to restore an SAP HANA on Amazon EC2 instance:

- `aws:backup:request-id`: This is any UUID string used for idempotency. It does not alter your restore experience in any way.
- `aws:backup:TargetDatabaseArn`: Specify the database to which you want to restore. This is the SAP HANA on Amazon EC2 database ARN.
- `CatalogRestoreOption`: Specify where to restore your catalog from. One of `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP`, `CATALOG_FROM_LOCAL_PATH`
- `LocalCatalogPath`: If `CatalogRestoreOption` metadata value is `CATALOG_FROM_LOCAL_PATH`, then specify the path to local catalog on your EC2 instance. This should be a valid file path in your EC2 instance.
• **RecoveryType**: Currently, **FULL_DATA_BACKUP_RECOVERY**, **POINT_IN_TIME_RECOVERY**, and **MOST_RECENT_TIME_RECOVERY** recovery types are supported.

key = (string); value = (string). Shorthand syntax:

```
KeyName1=string,KeyName2=string
```

JSON syntax:

```
{"string": "string"
...
}
```

`--idempotency-token` is a user-chosen string that you can use to distinguish between otherwise identical calls to `StartRestoreJob`. Retrying a successful request with the same idempotency token results in a success message with no action taken.

`--resource-type` is a string that starts a job to restore a recovery point for one of the following resources: SAP HANA on Amazon EC2 for SAP HANA on Amazon EC2. Optionally, SAP HANA resources can be tagged using the command `aws ssm-sap tag-resource`.

**Output**: `RestoreJobId` is a string that uniquely identifies the job that restores a recovery point.

**Troubleshooting**

If any of the following errors occur while attempting a backup operation, see the associated resolution.

- **Error**: Continuous backup log error

  To maintain recovery points for continuous backups, logs are created by SAP HANA for all changes. When the logs are unavailable, the status of each of these continuous recovery points is STOPPED. The last certain viable recovery point that can be used to restore is one that has the status of AVAILABLE. If the log data is missing for the time between recovery points with a STOPPED status and points with AVAILABLE, these times cannot be guaranteed to have a successful restore. If you input a date and time within this range, AWS Backup will attempt the backup, but will use the closest available restorable time. This error will be shown by the message “Encountered an issue with log backups. Please check SAP HANA for details.”

  **Resolution**: In the console, the most recent restorable time, based on the logs, is displayed. You can input a time more recent than the time shown. However, if the data for this time is unavailable from the logs, AWS Backup will use the most recent restorable time.

- **Error**: Internal error

  **Resolution**: Create a support case from your console or contact AWS Support with the details of your restore such as the restore job ID.

- **Error**: The provided role `arn:aws:iam::ACCOUNT_ID:role/ServiceLinkedRole` cannot be assumed by AWS Backup

  **Resolution**: Ensure that the role assumed when calling the restore has the required permissions to create service linked roles.


  **Resolution**: Ensure that the role assumed when calling the restore permissions outlined in the prerequisites is entered correctly.
Restoring a DocumentDB cluster

Use the AWS Backup console to restore Amazon DocumentDB recovery points

Restoring a Amazon DocumentDB cluster requires that you specify multiple restore options. For information about these options, see Restoring from a Cluster Snapshot in the Amazon DocumentDB Developer Guide.

To restore a Amazon DocumentDB cluster

2. In the navigation pane, choose Protected resources and the Amazon DocumentDB resource ID that you want to restore.
3. On the Resource details page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the Backups pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose Restore.
4. In the Configuration pane, accept the defaults or specify the options for the Cluster identifier, Engine version, Instance class, and Number of instances.
   - NOTE: If the default VPC does not exist when restoring, you must specify a subnet in another VPC.
5. In the Network & Security pane, "No Preferences" will be displayed.
6. In the Encryption-at-rest pane, accept the default or specify the options for the Enable encryption or Disable encryption settings.
7. In the Cluster options pane, type in the Port and choose the Cluster parameter group.
8. In the Backup pane, choose continuous backup for point-in-time recovery (PITR), scheduled snapshot backups, or both.
9. In the Log exports pane, choose the log types to publish to Amazon CloudWatch Logs. The IAM role is already defined.
10. In the Maintenance pane, specify a maintenance window or choose No preference.
11. In the Tags pane, you can choose Add tag.
12. In the Deletion protection pane, you can choose Enable deletion protection.
13. After specifying all your settings, choose Restore backup.

The Restore jobs pane appears. A message at the top of the page provides information about the restore job.

14. After your restore finishes, attach your restored Amazon DocumentDB cluster to an Amazon RDS instance.

Using the AWS CLI:

- For Linux, macOS, or Unix:

  ```bash
  aws docdb create-db-instance --db-instance-identifier sample-instance /
  --db-cluster-identifier sample-cluster --engine docdb --db-instance-class db.r5.large
  ```

- For Windows:

  ```powershell
  aws docdb create-db-instance --db-instance-identifier sample-instance ^
  --db-cluster-identifier sample-cluster --engine docdb --db-instance-class db.r5.large
  ```

Restoring a Neptune cluster

Use the AWS Backup console to restore Amazon Neptune recovery points

Restoring an Amazon Neptune database requires that you specify multiple restore options. For information about these options, see Restoring from a DB Cluster Snapshot in the Neptune User Guide.

To restore an Neptune database

2. In the navigation pane, choose Protected resources and the Neptune resource ID that you want to restore.
3. On the Resource details page, a list of recovery points for the selected resource ID is shown. To restore a resource, in the Backups pane, choose the radio button next to the recovery point ID of the resource. In the upper-right corner of the pane, choose Restore.
4. In the Instance specifications pane, accept the defaults or specify the DB engine and Version.
5. In the Settings pane, specify a name that is unique for all DB cluster instances owned by your AWS account in the current Region. The DB cluster identifier is case insensitive, but it is stored as all lowercase, as in "mydbclusterinstance". This is a required field.
6. In the Database options pane, accept the defaults or specify the options for Database port and DB cluster parameter group.
7. In the Encryption pane, accept the default or specify the options for the Enable encryption or Disable encryption settings.
8. In the Log exports pane, choose the log types to publish to Amazon CloudWatch Logs. The IAM role is already defined.
9. In the Restore role pane, choose the IAM role that AWS Backup will assume for this restore.
10. After specifying all your settings, choose Restore backup.
The **Restore jobs** pane appears. A message at the top of the page provides information about the restore job.

11. After your restore finishes, attach your restored Neptune cluster to an Amazon RDS instance.

Using the AWS CLI:

- For Linux, macOS, or Unix:
  ```bash
  aws neptune create-db-instance --db-instance-identifier sample-instance \
  --db-instance-class db.r5.large --engine neptune --engine-version 1.0.5.0 \
  --db-cluster-identifier sample-cluster --region us-east-1
  ```

- For Windows:
  ```bash
  aws neptune create-db-instance --db-instance-identifier sample-instance ^ \
  --db-instance-class db.r5.large --engine neptune --engine-version 1.0.5.0 \
  --db-cluster-identifier sample-cluster --region us-east-1
  ```

### Restore CloudFormation stack backups

A CloudFormation composite backup is a combination of a CloudFormation template and all associated nested recovery points. Any number of nested recovery points can be restored, but the composite recovery point (which is the top-level recovery point) cannot be restored.

When you restore a CloudFormation template recovery point, you create a new stack with a change set to represent the backup. From the [CloudFormation console](https://console.aws.amazon.com/cloudformation/home) you can see the new stack and change set. To learn more about change sets, see [Updating stacks using change sets](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-changesets-update.html) in the [AWS CloudFormation User Guide](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/).

Determine which nested recovery points you want to restore from with your CloudFormation stack, and then restore them using the AWS Backup console.

2. Go to **Backup vaults**, select the backup vault containing your desired recovery point, then click on **Recovery points**.
3. Restore the AWS CloudFormation template recovery point.
   a. Click the composite recovery point containing the nested recovery points you want to restore to bring up the Details page for the composite recovery point.
   b. Under **Nested recovery points**, the nested recovery points will be displayed. Each recovery point will have a recovery point ID, a status, a resource ID, a resource type, a backup type, and the time that recovery point was created. Click the radio button next to the AWS CloudFormation recovery point, then click **Restore**. Ensure that you are selecting the recovery point that has resource type: **AWS CloudFormation** and backup type: **backup**.
4. Once the restore job for the CloudFormation template is completed, your restored AWS CloudFormation template will be visible in the [AWS CloudFormation console](https://console.aws.amazon.com/cloudformation/home) under **Stacks**.
5. Under **Stack names** you should find the restored template with the status of **REVIEW_IN_PROGRESS**.
6. Click on the name of the stack to see the stack's details.
7. There are tabs under the stack name. Click on **Change sets**.
8. Execute the change set.
9. After this processes, the resources in the original stack will be recreated in the new stack. The stateful resources will be recreated empty. To recover the stateful resources, go back to the list
of recovery points in the AWS Backup console, select the recovery point you need, and initiate a restore.
Audit backups and create reports with AWS Backup Audit Manager

**Note**
AWS Backup Audit Manager is not yet available in Asia Pacific (Jakarta), China (Beijing), China (Ningxia), Asia Pacific (Osaka), Middle East (UAE), Europe (Spain), Europe (Zurich), Asia Pacific (Hyderabad), and Asia Pacific (Melbourne) Regions.

You can use AWS Backup Audit Manager to audit the compliance of your AWS Backup policies against controls that you define. A control is a procedure designed to audit the compliance of a backup requirement, such as the backup frequency or the backup retention period.

AWS Backup Audit Manager helps you answer questions such as:

- "Am I backing up all my resources?"
- "Are all of my backups encrypted?"
- "Are my backups taking place daily?"

You can use AWS Backup Audit Manager to find backup activity and resources that are not yet compliant with the controls that you defined. Note that only active resources will be included when controls evaluate resources for compliance. For example, an Amazon EC2 instance in a running state will be evaluated. An EC2 instance in a stopped state will not be included in the compliance evaluation.

You can also use it to automatically generate an audit trail of daily and on-demand reports for your backup governance purposes.

The following steps provide an overview of how to use AWS Backup Audit Manager. For detailed walkthroughs, choose one of the topics at the end of this page.

1. Create frameworks that contain one or more governance control templates. The preceding questions are examples of three governance control templates. You can customize the parameters of some governance control templates. For example, you can customize the last control to ask, "Are my backups taking place weekly?" instead of daily.

2. View your framework to see how many of your resources are compliant (or non-compliant) with the controls you defined in that framework.

3. Create reports of your backup and compliance status. Store these reports as demonstrable evidence of your compliance practices, or to identify individual backup activities and resources that are not yet in compliance.

AWS Backup Audit Manager automatically generates a new report for you every 24 hours and publishes it to Amazon S3. You can also generate on-demand reports.

**Note**
Before you create your first compliance-related framework, you must turn on resource tracking. Doing so allows AWS Config to track your AWS Backup resources. For technical documentation about how to manage resource tracking, see Setting up AWS Config with the console in the AWS Config Developer Guide.

Charges apply when you turn on resource tracking. For information about resource tracking pricing and billing for AWS Backup Audit Manager, see Metering, costs, and billing.

**Topics**
- Working with audit frameworks (p. 177)
Working with audit frameworks

A framework is a collection of controls that helps you to evaluate your backup practices. You can use pre-built, customizable controls to define your policies and evaluate whether your backup practices comply with your policies. You can also set up automatic daily reports to gain insights into the compliance status of your frameworks.

Each framework applies to a single account and AWS Region. You can deploy a maximum of 10 frameworks per account per Region. You cannot deploy duplicate frameworks (frameworks that contain the same controls and parameters).

There are two different types of frameworks:

- The AWS Backup framework (recommended) – Use the AWS Backup framework to deploy all available controls to monitor your backup activity, coverage, and resources against the best practices that we recommend.
- A custom framework that you define – Use a custom framework to choose one or more specific controls and to customize control parameters.

Choosing your controls

The following table lists the AWS Backup Audit Manager controls, their customizable parameters, and their AWS Config recording resource types. Every control requires the recording resource type AWS Config: resource compliance because this type records your compliance status.

### Available controls

<table>
<thead>
<tr>
<th>Control name</th>
<th>Control description</th>
<th>Customizable parameters</th>
<th>AWS Config recording resource type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup resources are protected by a backup plan</td>
<td>Evaluates if resources are protected by a backup plan.</td>
<td>None</td>
<td>AWS Backup: backup selection</td>
</tr>
<tr>
<td>Backup plan has minimum frequency and minimum retention</td>
<td>Evaluates if backup frequency is at least [1 day] and retention</td>
<td>Backup frequency; retention period</td>
<td>AWS Backup: backup plans</td>
</tr>
</tbody>
</table>

177
## Choosing your controls

<table>
<thead>
<tr>
<th>Control name</th>
<th>Control description</th>
<th>Customizable parameters</th>
<th>AWS Config recording resource type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vaults prevent manual deletion of recovery points</td>
<td>Evaluates if backup vaults do not allow manual deletion of recovery points except by certain AWS Identity and Access Management (IAM) roles. By default, there are no IAM role exceptions. There are also no IAM role exceptions when you deploy this control with the AWS Backup framework.</td>
<td>Up to 5 IAM roles that allow manual deletion of recovery points</td>
<td>AWS Backup: backup vaults</td>
</tr>
<tr>
<td>Recovery points are encrypted</td>
<td>Evaluates if the recovery points are encrypted.</td>
<td>None</td>
<td>AWS Backup: recovery points</td>
</tr>
<tr>
<td>Minimum retention established for recovery point</td>
<td>Evaluates if the recovery point retention period is at least [35 days].</td>
<td>Recovery point retention period</td>
<td>AWS Backup: recovery points</td>
</tr>
<tr>
<td>Cross-Region backup copy is scheduled</td>
<td>Evaluates if a resource is configured to create copies of its backups to another AWS Region.</td>
<td>AWS Region</td>
<td>AWS Backup: backup selection</td>
</tr>
<tr>
<td>Cross-account backup copy is scheduled</td>
<td>Evaluates if a resource has a cross-account backup copy configured.</td>
<td>AWS account ID</td>
<td>AWS Backup: backup selection</td>
</tr>
<tr>
<td>Backups are protected by AWS Backup Vault Lock</td>
<td>Evaluates if a resource is configured to have backups in locked backup vault.</td>
<td>Min Retention Days; Max Retention Days</td>
<td>AWS Backup: backup selection</td>
</tr>
<tr>
<td>Last recovery point was created</td>
<td>Evaluates if a recovery point was created within specified time frame.</td>
<td>Value in hours [1 to 744] or days [1 to 31].</td>
<td>AWS Backup recovery points</td>
</tr>
</tbody>
</table>

For detailed information about these controls, see [AWS Backup Audit Manager controls and remediation (p. 210)](#).

For a list of AWS Backup-supported resources that don't support all controls, see the AWS Backup Audit Manager section of the [Feature availability by resource (p. 2)](#) table.
Note
If you don’t want to use any of the preceding controls, you can still use AWS Backup Audit Manager to create daily reports of your backup, copy, and restore jobs. See Working with audit reports.

Turning on resource tracking

Before you create your first compliance-related framework, you must turn on resource tracking. Doing so allows AWS Config to track your AWS Backup resources. For technical documentation about how to manage resource tracking, see Setting up AWS Config with the console in the AWS Config Developer Guide.

Charges apply when you turn on resource tracking. For information about resource tracking pricing and billing for AWS Backup Audit Manager, see Metering, costs, and billing.

Topics
• Turning on resource tracking using the console (p. 179)
• Turning on resource tracking using the AWS Command Line Interface (AWS CLI) (p. 180)
• Turning on resource tracking using a AWS CloudFormation template (p. 183)

Turning on resource tracking using the console

To turn on resource tracking using the console:

2. In the left navigation pane, under Audit Manager, choose Frameworks.
3. Turn on resource tracking by choosing Manage resource tracking.
4. Choose Go to AWS Config Settings.
5. Choose Enable or disable recording.
6. Choose Enable recording for all of the following resource types, or choose to enable recording for some resource types. Refer to AWS Backup Audit Manager controls and remediation for which resource types are required for your controls.
   • AWS Backup: backup plans
   • AWS Backup: backup vaults
   • AWS Backup: recovery points
   • AWS Backup: backup selection

   Note
   AWS Backup Audit Manager requires AWS Config: resource compliance for every control.
7. Choose Close.
8. Wait for the blue banner with the text Turning on resource tracking to transition to the green banner with the text Resource tracking is on.

You can check whether you have turned on resource tracking and, if so, which resource types you are recording, in two places in the AWS Backup console. In the left navigation pane, either:

• Choose Frameworks, then choose the text under AWS Config recorder status.
• Choose Settings, then choose the text under AWS Config recorder status.
Turning on resource tracking using the AWS Command Line Interface (AWS CLI)

If you have not yet onboarded to AWS Config, it might be faster to onboard using the AWS CLI.

To turn on resource tracking using the AWS CLI:

1. Type the following command to determine if you already enabled your AWS Config recorder.

   ```
   $ aws configservice describe-configuration-recorders
   ```

   a. If your `ConfigurationRecorders` list is empty like this:

   ```
   {  
     "ConfigurationRecorders": []
   }
   ```

   Your recorder is not enabled. Continue to step 2 to create your recorder.
   
   b. If you already enabled recording for all resources, your `ConfigurationRecorders` output will look like this:

   ```
   {  
     "ConfigurationRecorders": [  
       {  
         "recordingGroup": {  
           "allSupported": true,  
           "resourceTypes": [  
             ],  
           "includeGlobalResourceTypes": true  
         },  
         "roleARN": "arn:aws:iam::[account]:role/[roleName]",  
         "name": "default"  
       }  
     ]
   }
   ```

   Since you enabled all resources you already turned on resource tracking. You do not need to complete the rest of this procedure to use AWS Backup Audit Manager.
   
   c. If your `ConfigurationRecorders` is not empty, but you have not enabled recording for all resources, add backup resources to your existing recorder using the following command. Then skip to step 3.

   ```
   $ aws configservice describe-configuration-recorders
   ```

   ```
   {  
     "ConfigurationRecorders": [  
       {  
         "name": "default",  
         "roleARN": "arn:aws:iam::account:role/aws-service-role/config.amazonaws.com/AWSServiceRoleForConfig",  
         "recordingGroup": {  
           "allSupported": false,  
           "includeGlobalResourceTypes": false,  
           "resourceTypes": [  
             "AWS::Backup::BackupPlan",  
             "AWS::Backup::BackupSelection",  
             "AWS::Backup::BackupVault",  
             "AWS::Backup::RecoveryPoint",
]```
2. Create a AWS Config recorder with the AWS Backup Audit Manager resource types

```bash
$ aws configservice put-configuration-recorder --configuration-recorder name=default, \
roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/AWSServiceRoleForConfig \ 
--recording-group resourceTypes=['AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint','AWS::Config::ResourceCompliance']
```

3. Describe your AWS Config recorder.

```bash
$ aws configservice describe-configuration-recorders
```

Verify that it has the AWS Backup Audit Manager resource types by comparing your output with the following expected output.

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

4. Create an Amazon S3 bucket as the destination to store the AWS Config configuration files.

```bash
$ aws s3api create-bucket --bucket my-bucket --region us-east-1
```

5. Use `policy.json` to grant AWS Config permission to access your bucket. See the following sample `policy.json`.

```bash
$ aws s3api put-bucket-policy --bucket MyBucket --policy file://policy.json
```

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      }
    }
  ]
}
```
6. Configure your bucket as an AWS Config delivery channel

```bash
$ aws configservice put-delivery-channel --delivery-channel name=default,s3BucketName=my-bucket
```

7. Enable AWS Config recording

```bash
$ aws configservice start-configuration-recorder --configuration-recorder-name default
```

8. Verify that "FrameworkStatus": "ACTIVE" in the last line of your DescribeFramework output as follows.

```bash
$ aws backup describe-framework --framework-name test --region us-east-1
```

```json
{
   "FrameworkName": "test",
   "FrameworkArn": "arn:aws:backup:us-east-1:accountId:framework:test-f0001b0a-0000-1111-ad3d-4444f5cc6666",
   "FrameworkDescription": "",
   "FrameworkControls": [
      {
         "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
         "ControlInputParameters": [
            {
               "ParameterName": "requiredRetentionDays",
               "ParameterValue": "1"
            }
         ],
         "ControlScope": {
          "ScopeType": "ACCOUNT",
          "ScopeValue": ",",
          "SupportedScopeValues": []
        }
      },
      {
         "ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
         "ControlInputParameters": [
            {
               "ParameterName": "requiredFrequencyUnit",
               "ParameterValue": "1"
            }
         ],
         "ControlScope": {
          "ScopeType": "ACCOUNT",
          "ScopeValue": ",",
          "SupportedScopeValues": []
        }
      }
   ]
}
```
Turning on resource tracking using a AWS CloudFormation template

For a AWS CloudFormation template that turns on resource tracking, see [Using AWS Backup Audit Manager with AWS CloudFormation](#).

Creating frameworks using the AWS Backup console

After turning on resource tracking, create a framework using the following steps.

2. In the left navigation pane, choose **Frameworks**.
3. Choose **Create Framework**.
4. For **Framework name**, enter a unique name. The framework name must be between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).
5. (Optional) Enter a **Framework description**.
6. In **Controls**, your active controls will be displayed. By default, all controls eligible for a resource are listed.

   To change which controls are active, click **Edit controls**.
   
   - The first check box indicates if the control is turned on. To turn off a control, uncheck the box.
   - Under **Choose resources to evaluate**, you can select how to choose resources, either by type, by tags, or by a single resource.

   The list of **AWS Backup Audit Manager controls** describes the customization options for each control.
7. (Optional) Tag your framework by choosing **Add new tag**. You can use tags to search and filter your frameworks or track your costs.
8. Choose **Create framework**.

AWS Backup Audit Manager might take several minutes to create the framework.

If the error **AlreadyExists** occurs, a framework with the same controls and parameters already exists. To successfully create a new framework, at least one control or parameter must be different from existing frameworks.

## Creating frameworks using the AWS Backup API

The following table contains sample API requests to **CreateFramework** (p. 402) for each control, along with sample API responses to the corresponding **DescribeFramework** (p. 448) requests. To work with AWS Backup Audit Manager programmatically, you can refer to these code snippets.

<table>
<thead>
<tr>
<th>Control</th>
<th>CreateFramework request</th>
<th>DescribeFramework response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup resources are protected by a backup plan</td>
<td>{&quot;FrameworkName&quot;: &quot;Control1&quot;, &quot;FrameworkDescription&quot;: &quot;This is a test framework&quot;, &quot;FrameworkControls&quot;: [ {&quot;ControlName&quot;: &quot;BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN&quot;, &quot;ControlInputParameters&quot;: [], &quot;ControlScope&quot;: {&quot;ComplianceResourceTypes&quot;: [&quot;RDS&quot;] // Evaluate only RDS instances } }, ], &quot;IdempotencyToken&quot;: &quot;Control1&quot;, &quot;FrameworkTags&quot;: {&quot;key1&quot;: &quot;foo&quot;} }</td>
<td>{&quot;FrameworkName&quot;: &quot;Control1&quot;, &quot;FrameworkArn&quot;: &quot;arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f45dc19642&quot;, &quot;FrameworkDescription&quot;: &quot;This is a test framework&quot;, &quot;FrameworkControls&quot;: [ {&quot;ControlName&quot;: &quot;BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN&quot;, &quot;ControlInputParameters&quot;: [], &quot;ControlScope&quot;: {&quot;ComplianceResourceTypes&quot;: [&quot;RDS&quot;] // Evaluate only RDS instances } }, ], &quot;IdempotencyToken&quot;: &quot;Control1&quot;, &quot;FrameworkTags&quot;: {&quot;key1&quot;: &quot;foo&quot;} }</td>
</tr>
</tbody>
</table>
Control | CreateFramework request | DescribeFramework response
--- | --- | ---
CreateFramework request | {} | "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"}
Backup plan minimum frequency and minimum retention | {"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [ {"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"} ], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }, "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} } | {"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a8-4f43d0c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [ {"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"} ], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }, "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }
### Control

Vaults prevent manual deletion of recovery points

#### CreateFramework request

```json
{
  "FrameworkName": "Control3",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls": [
    {
      "ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
      "ControlInputParameters": [
        {
          "ParameterName": "principalArnList",
          "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess,
          arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer,
          arn:aws:iam::123456789012:role/service-role/QuickSightAction"
        }
      ],
      "ControlScope": {
        "ComplianceResourceIds": ["default"],
        "ComplianceResourceTypes": ["AWS::Backup::BackupVault"]
      }
    }
  ],
  "IdempotencyToken": "Control3",
  "FrameworkTags": {
    "key1": "foo"
  }
}
```

#### DescribeFramework response

```json
{
  "FrameworkName": "Control3",
  "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls": [
    {
      "ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
      "ControlInputParameters": [
        {
          "ParameterName": "principalArnList",
          "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess,
          arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer,
          arn:aws:iam::123456789012:role/service-role/QuickSightAction"
        }
      ],
      "ControlScope": {
        "ComplianceResourceIds": ["default"],
        "ComplianceResourceTypes": ["AWS::Backup::BackupVault"]
      }
    }
  ],
  "CreationTime": 1516925490,
  "DeploymentStatus": "Active",
  "FrameworkStatus": "Completed",
  "IdempotencyToken": "Control3",
  "FrameworkTags": {
    "key1": "foo"
  }
}
```
<table>
<thead>
<tr>
<th>Control</th>
<th>CreateFramework request</th>
<th>DescribeFramework response</th>
</tr>
</thead>
</table>
| Minimum retention established for recovery point | ```json
{"FrameworkName": "Control4",
"FrameworkDescription": "This is a test framework",
"FrameworkControls": [
  {
    "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
    "ControlInputParameters": [
      {
        "ParameterName": "requiredRetentionDays",
        "ParameterValue": "35"
      }
    ],
    "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points.
  }
],
"IdempotencyToken": "Control4",
"FrameworkTags": {
  "key1": "foo"
}
}`` | ```json
{"FrameworkName": "Control4",
"FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642",
"FrameworkDescription": "This is a test framework",
"FrameworkControls": [
  {
    "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
    "ControlInputParameters": [
      {
        "ParameterName": "requiredRetentionDays",
        "ParameterValue": "35"
      }
    ],
    "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points.
  }
],
"CreationTime": 1516925490,
"DeploymentStatus": "Active",
"FrameworkStatus": "Completed",
"IdempotencyToken": "Control4",
"FrameworkTags": {
  "key1": "foo"
}
}`` |
<table>
<thead>
<tr>
<th>Control</th>
<th>CreateFramework request</th>
<th>DescribeFramework response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup recovery points are encrypted</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
{
"FrameworkName": "Control5",
"FrameworkDescription": "This is a test framework",
"FrameworkControls": [
{
"ControlName": "BACKUP_RECOVERY_POINT_ENCRYPTED",
"ControlInputParameters": [],
"ControlScope": {} // Default scope (no scope input) is all recovery points
},
"IdempotencyToken": "Control5",
"FrameworkTags": {
"key1": "foo"
}
] | 
{
"FrameworkName": "Control5",
"FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-7e7655ae-1e31-45cb-96a0-4f43d8c19642",
"FrameworkDescription": "This is a test framework",
"FrameworkControls": [
{
"ControlName": "BACKUP_RECOVERY_POINT_ENCRYPTED",
"ControlInputParameters": [],
"ControlScope": {} // Default scope (no scope input) is all recovery points
},
"IdempotencyToken": "Control5",
"FrameworkTags": {
"key1": "foo"
}
] |
### CreateFramework request

```json
{"FrameworkName": "Control6",  
"FrameworkDescription": "This is a test framework",  
"FrameworkControls": [  
  {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION",  
   "ControlInputParameters": [],  
   "ControlScope": {  
     "ComplianceResourceTypes": ["EC2"]  
   },  
   "IdempotencyToken": "Control6",  
   "FrameworkTags": {"key1": "foo"}
  }
],  
"IdempotencyToken": "Control6",  
"FrameworkTags": {"key1": "foo"}
}
```

### DescribeFramework response

```json
{"FrameworkName": "Control6",  
"FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642",  
"FrameworkDescription": "This is a test framework",  
"FrameworkControls": [  
  {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION",  
   "ControlInputParameters": [],  
   "ControlScope": {  
     "ComplianceResourceTypes": ["EC2"]  
   },  
   "IdempotencyToken": "Control6",  
   "FrameworkTags": {"key1": "foo"}
  }
],  
"CreationTime": 1516925490,  
"DeploymentStatus": "Active",  
"FrameworkStatus": "Completed",  
"IdempotencyToken": "Control6",  
"FrameworkTags": {"key1": "foo"}
}
```
<table>
<thead>
<tr>
<th>Control</th>
<th>CreateFramework request</th>
<th>DescribeFramework response</th>
</tr>
</thead>
</table>
| Cross-account backup copy is scheduled | ```json
    
    
    "FrameworkName": "Control7",
    "FrameworkDescription": "This is a test framework",
    "FrameworkControls": [
      {
        "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT",
        "ControlInputParameters": [],
        "ControlScope": {
          "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances
        }
      }
    ],
    "IdempotencyToken": "Control7",
    "FrameworkTags": {
      "key1": "foo"
    }
  ``` | ```json
    
    ```
    "FrameworkName": "Control7",
    "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8e19642",
    "FrameworkDescription": "This is a test framework",
    "FrameworkControls": [
      {
        "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT",
        "ControlInputParameters": [],
        "ControlScope": {
          "ComplianceResourceTypes": ["EC2"]
        }
      }
    ],
    "CreationTime": 1516925490,
    "DeploymentStatus": "Active",
    "FrameworkStatus": "Completed",
    "IdempotencyToken": "Control7",
    "FrameworkTags": {
      "key1": "foo"
    }
  ``` |
### Control

Backups are protected by AWS Backup Vault Lock

<table>
<thead>
<tr>
<th>CreateFramework request</th>
<th>DescribeFramework response</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{&quot;FrameworkName&quot;: &quot;Control8&quot;, &quot;FrameworkDescription&quot;: &quot;This is a test framework&quot;, &quot;FrameworkControls&quot;: [ {&quot;ControlName&quot;: &quot;BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK&quot;, &quot;ControlInputParameters&quot;: [], &quot;ControlScope&quot;: {&quot;ComplianceResourceTypes&quot;: [&quot;EC2&quot;] // Evaluate only EC2 instances } }], &quot;IdempotencyToken&quot;: &quot;Control8&quot;, &quot;FrameworkTags&quot;: {&quot;key1&quot;: &quot;foo&quot;}}</code></td>
<td><code>{&quot;FrameworkName&quot;: &quot;Control8&quot;, &quot;FrameworkArn&quot;: &quot;arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642&quot;, &quot;FrameworkDescription&quot;: &quot;This is a test framework&quot;, &quot;FrameworkControls&quot;: [ {&quot;ControlName&quot;: &quot;BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK&quot;, &quot;ControlInputParameters&quot;: [], &quot;ControlScope&quot;: {&quot;ComplianceResourceTypes&quot;: [&quot;EC2&quot;] // Evaluate only EC2 instances } }], &quot;IdempotencyToken&quot;: &quot;Control8&quot;, &quot;FrameworkTags&quot;: {&quot;key1&quot;: &quot;foo&quot;}}</code></td>
</tr>
</tbody>
</table>
### Viewing framework compliance status

Once you create an audit framework, it appears in your Frameworks table. You can view this table by choosing Frameworks in the left navigation pane of the AWS Backup console. To view the audit results for your framework, choose its Framework name. Doing so takes you to the Framework detail page, which has two sections: Summary and Controls.

The Summary section lists the following statuses from left to right:

- **Compliance status** is your audit framework's overall compliance status as determined by the compliance status of each of its controls. Each control's compliance status is determined by the compliance status of each resource it evaluates.

Framework compliance status is Compliant only if all resources in the scope of your control evaluations have passed those evaluations. If one or more resources failed a control evaluation, the compliance status will be Non-Compliant. For information on how to find your non-compliant resources, see Finding non-compliant resources. For information on how to bring your resources into compliance, see the remediation section of AWS Backup Audit Manager controls and remediation.

- **Framework status** refers to whether you have turned on resource tracking for all of your resources. The possible statuses are:
  - **Active** when recording is turned on for all resources the framework evaluates.
• Partially active when recording is turned off for at least one resource the framework evaluates.
• Inactive when recording is turned off for all resources that the framework evaluates.
• Unavailable when AWS Backup Audit Manager is unable to validate recording status at this time.

To correct a Partially active or Inactive status

1. Choose Frameworks from the left navigation pane.
2. Choose Manage resource tracking.
3. Follow the instructions in the pop-up to enable recording that were previously not enabled for your resource types.

For more information about which resource types require resource tracking based on the controls you included in your frameworks, see the resource component of AWS Backup Audit Manager controls and remediation.

• Deployment status refers to your framework’s deployment status. This status should most often be Completed, but can also be Create in progress, Update in progress, Delete in progress, and Failed.
  • A status of Failed means the framework didn't deploy correctly. Delete the framework, then recreate the framework through the AWS Backup console or through AWS Backup API.
• Compliant controls show a count of framework controls with all evaluations passing.
• Non-compliant controls show a count of framework controls with at least one evaluation not passing.

The Controls section shows you the following information:

• Control status refers to each control's compliance status. A control can be Compliant, meaning all resources pass that evaluation; Non-compliant, meaning that at least one resource did not pass that evaluation, or Insufficient data, meaning the control found no resources within the evaluation scope to evaluate.
• Evaluation scope might limit each control to one or more Resource types, one Resource ID, or one Tag key and Tag value, based on how you customized your control when creating your audit framework. If all fields are empty (as shown by a dash, "-"), then the control evaluates all applicable resources.

Finding non-compliant resources

AWS Backup Audit Manager helps you find which resources are non-compliant in two ways.

• When Viewing framework compliance status, choose the control name in the Details section. Doing so takes you to the AWS Config console, where you can view a list of your of your Non-Compliant resources.
• After you Create a report plan with the resource compliance template that includes your framework, you can View your report to identify all your Non-Compliant resources across all your controls.

Furthermore, your Resource compliance report shows the last time AWS Backup Audit Manager last evaluated each of your controls.

Updating audit frameworks

You can update the description, controls, and parameters of an existing audit framework.
To update an existing framework

1. In the AWS Backup console left navigation pane, choose **Frameworks**.
2. Choose the framework you want to edit by its **Framework name**.
3. Choose **Edit**.

Deleting audit frameworks

To delete an existing framework

1. In the AWS Backup console left navigation pane, choose **Frameworks**.
2. Choose the framework you want to delete by its **Framework name**.
3. Choose **Delete**.
4. Type the name of your framework and choose **Delete framework**.

Working with audit reports

AWS Backup Audit Manager reports are automatically generated evidence of your AWS Backup activity, such as:

- Which backup jobs finished and when
- Which resources you backed up

There are two types of reports. One type is a **jobs report**, which shows jobs finished in the last 24 hours and all active jobs. The second type of report is a **compliance report**. Compliance reports can monitor resource levels or the different controls that are in effect. When you create a report, you choose which type of report to create.

AWS Backup Audit Manager delivers a daily report in to your Amazon S3 bucket. If the report is for the current region and current account, you can choose to receive the report in either CSV or JSON format. Otherwise, the report is available in CSV format. The timing of the daily report might fluctuate over several hours because AWS Backup Audit Manager performs randomization to maintain its performance. You can also run an on-demand report anytime.

All account holders can create cross-Region reports; management account holders can also create cross-account reports.

You can have a maximum of 20 report plans per AWS account.

NOTE: Delegated Administrator accounts are unable to access AWS Backup Audit Manager report generation. Contact your account's administrator to generate or edit reports.

**Note**

Resources such as RDS that do not have the capability to show incremental bytes of data of a specific backup will display the value backupSizeInBytes as 0.

To allow AWS Backup Audit Manager to create daily or on-demand reports, you must first create a **report plan from a report template**.

**Topics**

- Choosing your report template (p. 195)
- Creating report plans using the AWS Backup console (p. 199)
- Creating report plans using the AWS Backup API (p. 201)
- Creating on-demand reports (p. 203)
Choosing your report template

A report template defines the information that your report plan includes in your report. When you automate your reports using a report plan, AWS Backup Audit Manager provides you reports for the previous 24 hours. AWS Backup Audit Manager creates these reports between the hours of 1 and 5 AM UTC. It offers the following report templates.

Backup report templates

**Backup report templates.** These templates give you daily updates on your backup, restore, or copy jobs. You can use these reports to monitor your operational posture and identify any failures that might need further action. The following table lists each backup report template name and its sample output.

<table>
<thead>
<tr>
<th>Backup report template</th>
<th>Sample report in JSON format</th>
</tr>
</thead>
</table>
| BACKUP_JOB_REPORT      | {
|                        |   "reportItems": [
|                        |     {
|                        |       "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
|                        |       "accountId": "112233445566",
|                        |       "region": "us-west-2",
|                        |       "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC656AC",
|                        |       "jobStatus": "COMPLETED",
|                        |       "resourceType": "EC2",
|                        |       "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
|                        |       "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e15d5e65dcfb",
|                        |       "creationDate": "2021-07-14T23:53:47.229Z",
|                        |       "completionDate": "2021-07-15T00:16:07.282Z",
|                        |       "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5a6dcfd",
|                        |     }
|                        |   ]
| COPY_JOB_REPORT        | {
|                        | }}
### Choosing your report template

<table>
<thead>
<tr>
<th>Backup report template</th>
<th>Sample report in JSON format</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;reportItems&quot;: [</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;reportTimePeriod&quot;:</td>
</tr>
<tr>
<td></td>
<td>&quot;accountId&quot;: &quot;112233445566&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;region&quot;: &quot;us-west-2&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;copyJobId&quot;: &quot;E0AD48A9-0560-B668-3EF0-941FD0A6681&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;jobStatus&quot;: &quot;RUNNING&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;resourceType&quot;: &quot;EC2&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;resourceArn&quot;: &quot;arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877ae7782ba75&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupRuleId&quot;: &quot;ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcbf&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;creationDate&quot;: &quot;2021-07-15T15:42:04.771Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupSizeInBytes&quot;: 8589934592,</td>
</tr>
<tr>
<td></td>
<td>&quot;sourceRecoveryPointArn&quot;: &quot;arn:aws:ec2:us-west-2:image/ami-007b3819f25697299&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;destinationRecoveryPointArn&quot;: &quot;arn:aws:ec2:us-east-2:image/ami-0eba2199a0beece3c&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;iamRoleArn&quot;: &quot;arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>]</td>
</tr>
</tbody>
</table>
Choosing your report template

Backup report template

RESTORE_JOB_REPORT

Sample report in JSON format

```json
{
    "reportItems": [
        {
            "accountId": "112233445566",
            "region": "us-west-2",
            "restoreJobId": "4CACA67D-4E12-DC05-6C2B-0E97D01FA41E",
            "jobStatus": "RUNNING",
            "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-00201ecb57a5271ae",
            "creationDate": "2021-07-15T15:52:49.797Z",
            "backupSizeInBytes": 8589934592,
            "percentDone": "0.00%",
            "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
        }
    ]
}
```

Compliance report templates

**Compliance report templates** give you daily reports on the compliance of your backup activity and resources against the controls you defined in one or more frameworks. If the compliance status of one of your frameworks is Non-compliant, review a compliance report to identify the non-compliant resources.

**Types of compliance report templates**

- **Control compliance report** helps you track the compliance status of the controls you have defined in your frameworks.
- **Resource compliance report** helps you track the compliance status of your resources against the controls you defined in your frameworks. These reports include detailed evaluation results, including identifying information on non-compliant resources that you can use to identify and correct those resources.

The following table shows sample output from a compliance report.

<table>
<thead>
<tr>
<th>Compliance report template</th>
<th>Sample report in JSON format</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL_COMPLIANCE_REPORT</td>
<td>`{ &quot;reportItems&quot;: [</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;accountId&quot;: &quot;112233445566&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;region&quot;: &quot;me-south-1&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;frameworkName&quot;: &quot;TestFramework7&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;frameworkDescription&quot;: &quot;A test framework&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;controlName&quot;: &quot;BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Choosing your report template

<table>
<thead>
<tr>
<th>Compliance report template</th>
<th>Sample report in JSON format</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;controlComplianceStatus&quot;: &quot;NON_COMPLIANT&quot;, &quot;lastEvaluationTime&quot;: &quot;2021-08-17T03:56:002Z&quot;, &quot;numResourcesCompliant&quot;: 91, &quot;numResourcesNonCompliant&quot;: 205, &quot;controlFrequency&quot;: &quot;Twelve_Hours&quot;, &quot;controlScope&quot;: &quot;&quot;, &quot;controlParameters&quot;: &quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>[</td>
</tr>
<tr>
<td></td>
<td>&quot;accountId&quot;: &quot;112233445566&quot;, &quot;region&quot;: &quot;me-south-1&quot;, &quot;frameworkName&quot;: &quot;TestFramework7&quot;, &quot;frameworkDescription&quot;: &quot;A test framework&quot;, &quot;controlName&quot;: &quot;BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK&quot;, &quot;controlComplianceStatus&quot;: &quot;NON_COMPLIANT&quot;, &quot;lastEvaluationTime&quot;: &quot;2021-08-17T03:19.995Z&quot;, &quot;numResourcesCompliant&quot;: 0, &quot;numResourcesNonCompliant&quot;: 25, &quot;controlScope&quot;: &quot;{ComplianceResourceTypes: [],}&quot;</td>
</tr>
</tbody>
</table>
|                           |   "controlParameters": "{"requiredFrequencyValue": "1", "requiredRetentionDays": "35", "requiredFrequencyUnit": "hours"}"
|                           | ] |
|                           | ] |
## Compliance report template

**RESOURCE_COMPLIANCE_REPORT**

```

```

## Sample report in JSON format

```

```

## Creating report plans using the AWS Backup console

There are two types of reports. One type is a **jobs report**, which shows jobs finished in the last 24 hours and all active jobs. The second type of report is a **compliance report**. Compliance reports can monitor resource levels or the different controls that are in effect. When you create a report, you choose which type of report to create.

**NOTE:** Depending on your type of account, the console display may vary. Only management accounts will see multi-account functionality.

Similar to a **backup plan**, you create a **report plan** to automate the creation of your reports and define their destination Amazon S3 bucket. A report plan requires that you have an S3 bucket to receive your reports. For instructions on setting up a new S3 bucket, see [Step 1: Create your first S3 bucket](#) in the Amazon Simple Storage Service User Guide.

**To create your report plan in the AWS Backup console**

2. In the left navigation pane, choose **Reports**.
3. Choose **Create report plan**.
4. Choose one of the report templates from the dropdown list.
5. Enter a unique **Report plan name**. The name must be between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).
6. (Optional) Enter a **Report plan description**.
7. **Compliance report templates for one account only**. Choose one or more frameworks on which to report. You can add a maximum 1,000 frameworks to a report plan.
   1. Choose your AWS Region using the dropdown.
   2. Choose a framework from that Region using the dropdown.
   3. Choose **Add framework**.
8. (Optional) To add tags to your report plan, choose **Add tags to the report plan**.
9. If you are using a management account, you can specify which accounts you want to include in this report plan. You can select **Only my account**, which will generate reports on just the account to which you’re currently logged in. Or, you can select **One or more accounts in my organization** (only available to management accounts).
10. (If you are creating a compliance report for one Region only, skip this step). You can select which Regions to include in your report. Click the drop down menu to show Regions available to you. Select **All available Regions** or the Regions you prefer.
   - The **Include new Regions when they are incorporated into Backup Audit Manager** check box will trigger new Regions to be included in your reports when they become available.
11. Choose the **File format** of your report. All reports can be exported in CSV format. Additionally, reports for a single region and a single Region can be exported in JSON format.
12. Choose your **S3 bucket name** using the dropdown list.
13. (Optional) Enter a bucket prefix.
   - AWS Backup delivers your **current account, current Region** reports to  s3://your-bucket-name/prefix/Backup/accountID/Region/year/month/day/report-name.
   - AWS Backup delivers your **cross-account** reports to s3://your-bucket-name/prefix/Backup/crossaccount/Region/year/month/day/report-name
   - AWS Backup delivers your **cross-Region** reports to s3://your-bucket-name/prefix/Backup/accountID/crossregion/year/month/day/report-name
14. Choose **Create report plan**.

Next, you must allow your S3 bucket to receive reports from AWS Backup. After you create a report plan, AWS Backup Audit Manager automatically generates an S3 bucket access policy for you to apply. If you encrypt your bucket using a custom KMS key, ensure that key has AWS Backup as a user.

**To view and apply this access policy to your S3 bucket**
2. In the left navigation pane, choose **Reports**.
4. Choose **Edit**.
5. Choose **View access policy for S3 bucket**. You can also use the policy at the end of this procedure.
6. Choose **Copy permissions**.
7. Choose **Edit bucket policy**.
8. Copy the permissions to the **Policy**.
Sample bucket policy

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::1111111111:role/aws-service-role/reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
         },
         "Action": "s3:PutObject",
         "Resource": ["arn:aws:s3:::BucketName/*"]
      },
      "Condition": {
         "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
         }
      }
   }
}
```

Creating report plans using the AWS Backup API

You can also work with report plans programmatically.

There are two types of reports. One type is a **jobs report**, which shows jobs finished in the last 24 hours and all active jobs. The second type of report is a **compliance report**. Compliance reports can monitor resource levels or the different controls that are in effect. When you create a report, you choose which type of report to create.

For single-account, single-Region reports, use the following syntax to call `CreateReportPlan` *(p. 414)*.

```json
{
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   "ReportSetting": {
      "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
      CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT. Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
      "ReportDeliveryChannel": {
         "S3BucketName": "string",
         "S3KeyPrefix": "string",
         "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is CSV if left blank.
      },
      "ReportPlanTags": {
         "string": "string" // Optional.
      },
      "IdempotencyToken": "string"
   }
}
```

When you call `DescribeReportPlan` *(p. 465)* with the unique name of a report plan, the AWS Backup API responds with the following information.

```json
{
   "ReportPlanArn": "string",
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   201
}
```
"ReportSetting": {
    "ReportTemplate": enum,
},
"ReportDeliveryChannel": {
    "S3BucketName": "string",
    "S3KeyPrefix": "string",
    "Formats": [ enum ]
},
"DeploymentStatus": enum
"CreationTime": timestamp,
"LastAttemptExecutionTime": timestamp,
"LastSuccessfulExecutionTime": timestamp
}

For multi-account, multi-Region reports, use the following syntax to call CreateReportPlan (p. 414).

```json
{
    "IdempotencyToken": "string",
    "ReportDeliveryChannel": {
        "Formats": [ "string" ],  //Organization report only support CSV file
        "S3BucketName": "string",
        "S3KeyPrefix": "string"
    },
    "ReportPlanDescription": "string",
    "ReportPlanName": "string",
    "ReportPlanTags": {
        "string": "string"
    },
    "ReportSetting": {
        "Accounts": [ "string" ],
        "OrganizationUnits": [ "string" ],
        "Regions": [ "string" ],
        "FrameworkArns": [ "string" ],
        "NumberOfFrameworks": number,
        "ReportTemplate": "string"
    }
}
```

When you call DescribeReportPlan (p. 465) with the unique name of a report plan, the AWS Backup API responds with the following information for multi-account, multi-Region plans:

```json
{
    "ReportPlan": {
        "CreationTime": number,
        "DeploymentStatus": "string",
        "LastAttemptedExecutionTime": number,
        "LastSuccessfulExecutionTime": number,
        "ReportDeliveryChannel": {
            "Formats": [ "string" ],
            "S3BucketName": "string",
            "S3KeyPrefix": "string"
        },
        "ReportPlanArn": "string",
        "ReportPlanDescription": "string",
        "ReportPlanName": "string",
        "ReportSetting": {
            "Accounts": [ "string" ],
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "ReportTemplate": "string"
        }
    }
}
```
Creating on-demand reports

You can generate new reports at your convenience by creating an on-demand report with the following steps. AWS Backup Audit Manager delivers your on-demand report to the Amazon S3 bucket that you specified in your report plan.

2. In the left navigation pane, choose Reports.
3. Under Report plan name, select a report plan by choosing its name.
4. Choose Create on-demand report.

You can generate an on-demand report for an existing report plan.

2. In the left navigation pane, choose Reports.
3. Under Report plans, select a report plan by clicking on the radio button next to the report plan name.
4. Click Actions, then click Create on-demand report.

You can do this for multiple reports, even while reports are being generated.

Viewing audit reports

You can open, view, and analyze AWS Backup Audit Manager reports using the programs that you ordinarily use to work with CSV or JSON files. Note that reports for multiple regions or multiple accounts are only available in CSV format.

Large files are broken up into multiple reports if the total file size exceeds 50 MB. If the resulting files are over 50 MB, AWS Backup Audit Manager will create additional CSV files with the remainder of the report.

To view a report

2. In the left navigation pane, choose Reports.
3. Under Report plan name, select a report plan by choosing its name.
4. Under Report jobs, click on the report link to view the report.
5. If your report’s Report status has a dotted underline, choose it for information about your report.
6. Choose which report to view by its Completion time.
7. Choose the S3 link. This opens your destination S3 bucket.
8. Under Name, choose the name of the report that you want to view.
9. To save the report to your computer, choose Download.

Updating report plans

You can update an existing report plan’s description, its delivery destination, and format. If applicable, you can also add or remove frameworks from the report plan.
To update an existing report plan

2. In the left navigation pane, choose Reports.
3. Under Report plan name, select a report plan by choosing its name.
4. Choose Edit.
5. You can edit the report plan details, including the report name and description, as well as which accounts and Regions are included in the report.

Deleting report plans

You can delete an existing report plan. When you delete a report plan, any reports already created by that report plan will remain in their destination Amazon S3 bucket.

To delete an existing report plan

2. In the left navigation pane, choose Reports.
3. Under Report plan name, select a report plan by choosing its name.
4. Choose Delete.
5. Enter the name of your report plan, and then choose Delete report plan.

Using AWS Backup Audit Manager with AWS CloudFormation

We provide the following sample AWS CloudFormation templates for your reference:

Topics
- Turn on resource tracking (p. 183)
- Deploy default controls (p. 208)
- Exempt IAM roles from control evaluation (p. 209)
- Create a report plan (p. 209)

Turn on resource tracking

The following template turns on resource tracking as described in Turning on resource tracking.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label: default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceType
            - Label:
```

204
Turn on resource tracking

default: Delivery Channel Configuration
Parameters:
- DeliveryChannelName
- Frequency
- Label:
  default: Delivery Notifications
Parameters:
- TopicArn
- NotificationEmail
ParameterLabels:
  AllSupported:
  default: Support all resource types
IncludeGlobalResourceTypes:
  default: Include global resource types
ResourceTypes:
  default: List of resource types if not all supported
DeliveryChannelName:
  default: Configuration delivery channel name
Frequency:
  default: Snapshot delivery frequency
TopicArn:
  default: SNS topic name
NotificationEmail:
  default: Notification Email (optional)

Parameters:
AllSupported:
Type: String
Default: True
Description: Indicates whether to record all supported resource types.
AllowedValues:
- True
- False

IncludeGlobalResourceTypes:
Type: String
Default: True
Description: Indicates whether AWS Config records all supported global resource types.
AllowedValues:
- True
- False

ResourceTypes:
Type: List<String>
Description: A list of valid AWS resource types to include in this recording group, such as AWS::EC2::Instance or AWS::CloudTrail::Trail.
Default: <All>

DeliveryChannelName:
Type: String
Default: <Generated>
Description: The name of the delivery channel.

Frequency:
Type: String
Default: 24hours
Description: The frequency with which AWS Config delivers configuration snapshots.
AllowedValues:
- 1hour
- 3hours
- 6hours
- 12hours
- 24hours

TopicArn:
Type: String
Default: <New Topic>
Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification Service (Amazon SNS) topic that AWS Config delivers notifications to.

NotificationEmail:
Type: String
Default: <None>
Description: Email address for AWS Config notifications (for new topics).

Conditions:
IsAllSupported: !Equals
- !Ref AllSupported
- True
IsGeneratedDeliveryChannelName: !Equals
- !Ref DeliveryChannelName
- <Generated>
CreateTopic: !Equals
- !Ref TopicArn
- <New Topic>
CreateSubscription: !And
- !Condition CreateTopic
- !Not
  - !Equals
    - !Ref NotificationEmail
    - <None>

Mappings:
Settings:
  FrequencyMap:
  1hour    : One_Hour
  3hours   : Three_Hours
  6hours   : Six_Hours
  12hours  : Twelve_Hours
  24hours  : TwentyFour_Hours

Resources:
ConfigBucket:
  DeletionPolicy: Retain
  Type: AWS::S3::Bucket
  Properties:
    BucketEncryption:
      ServerSideEncryptionConfiguration:
        - ServerSideEncryptionByDefault:
          SSEAlgorithm: AES256
  ConfigBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
AWS Backup Developer Guide

Turn on resource tracking

```yaml
Action: s3:PutObject
Resource:
  - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/${AWS::AccountId}/*

  - Sid: AWSConfigBucketSecureTransport
    Action:
      - s3:*
    Effect: Deny
    Resource:
      - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
      - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/**"
    Principal: "*
    Condition:
      Bool:
        aws:SecureTransport:
        false

ConfigTopic:
  Condition: CreateTopic
  Type: AWS::SNS::Topic
  Properties:
    TopicName: !Sub "config-topic-${AWS::AccountId}"
    DisplayName: AWS Config Notification Topic
    KmsMasterKeyId: "alias/aws/sns"

ConfigTopicPolicy:
  Condition: CreateTopic
  Type: AWS::SNS::TopicPolicy
  Properties:
    Topics:
      - !Ref ConfigTopic
    PolicyDocument:
      Statement:
        - Sid: AWSConfigSNSPolicy
          Action:
            - sns:Publish
          Effect: Allow
          Resource: !Ref ConfigTopic
        Principal:
          Service:
            - config.amazonaws.com

EmailNotification:
  Condition: CreateSubscription
  Type: AWS::SNS::Subscription
  Properties:
    Endpoint: !Ref NotificationEmail
    Protocol: email
    TopicArn: !Ref ConfigTopic

ConfigRecorderServiceRole:
  Type: AWS::IAM::ServiceLinkedRole
  Properties:
    AWSServiceName: config.amazonaws.com
    Description: Service Role for AWS Config

ConfigRecorder:
  Type: AWS::Config::ConfigurationRecorder
  DependsOn:
    - ConfigBucketPolicy
    - ConfigRecorderServiceRole
  Properties:
    RoleARN: !Sub arn:${AWS::Partition}:iam:${AWS::AccountId}:role/aws-service-role/config.amazonaws.com/AWSServiceRoleForConfig
    RecordingGroup:
      AllSupported: !Ref AllSupported
```
Deploy default controls

The following template creates a framework with the default controls described in AWS Backup Audit Manager controls and remediation.

```yaml
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
        ControlScope:
          Tags:
            - Key: customizedKey
              Value: customizedValue
            - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
            - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
            - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
            - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
      Outputs:
        FrameworkArn:
```
Exempt IAM roles from control evaluation

The control `BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED` allows you to exempt up to five IAM roles that can still manually delete recovery points. The following template deploys this control and also exempts two IAM roles.

```yaml
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
          ControlInputParameters:
            - ParameterName: "principalArnList"
              ParameterValue: !Sub "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/ConfigRole"
  Outputs:
    FrameworkArn:
      Value: !GetAtt TestFramework.FrameworkArn
```

Create a report plan

The following template creates a report plan.

```yaml
Description: "Basic AWS::Backup::ReportPlan template"
Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"
Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
        S3BucketName: !Ref S3BucketName
        S3KeyPrefix: !Ref S3KeyPrefix
      ReportSetting:
        ReportTemplate: !Ref ReportTemplate
        Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
        Accounts: ['123456789098']
        OrganizationUnits: ['ou-abcd-1234wxyz']
      ReportPlanTags:
```
Using AWS Backup Audit Manager with AWS Audit Manager

AWS Backup Audit Manager controls map to prebuilt, standard controls in AWS Audit Manager, allowing you to import your AWS Backup Audit Manager compliance findings to your AWS Audit Manager reports. You might want to do so to help a compliance officer, audit manager, or other colleague who reports on backup activity as part of your organization's overall compliance posture.

You can import the compliance results of your AWS Backup Audit Manager controls to your AWS Audit Manager frameworks. To enable AWS Audit Manager to automatically collect data from your AWS Backup Audit Manager controls, create a custom control in AWS Audit Manager using the instructions for Customizing an existing control in the AWS Audit Manager User Guide. As you follow those instructions, note that the Data source for AWS Backup controls is AWS Config.

For a list of AWS Backup controls, see Choosing your controls.

AWS Backup Audit Manager controls and remediation

This page lists the available controls for AWS Backup Audit Manager. You can choose the right info pane to see a list of controls and jump to a specific control. To quickly compare controls, see the table in Choosing your controls. To programatically define controls, see the code snippets in Creating frameworks using the AWS Backup API.

You can use up to 50 controls per account per Region. Using the same control in two different frameworks counts as using two controls of the 50 control limit.

This page lists each control with the following information:

- Description. Values in brackets ("["]) are the default parameter values.
- The resources the control evaluates.
- The parameters of the control.
- The scope of the control, as follows:
  - You can specify Resources by type by choosing one or more AWS Backup-supported services.
  - You specify a Tagged resources scope with a single tag key and optional value.
  - You can specify a single resource using the Single resource dropdown list.
- Remediation steps to bring applicable resources into compliance.

Note that only active resources will be included when controls evaluate resources for compliance. For example, an Amazon EC2 instance in a running state will be evaluated by the control Last recovery point was created. An EC2 instance in a stopped state will not be included in the compliance evaluation.
Backup resources are protected by a backup plan

**Description:** Evaluates if resources are protected by a backup plan.

**Resource:** AWS Backup: backup selection

**Parameters:** None

**Scope:**
- Tagged resources
- Resources by type (default)
- Single resource

**Remediation:** Assign the resources to a backup plan. AWS Backup automatically protects your resources after you assign them to a backup plan. For more information, see [Assigning resources to a backup plan](#).

Backup plan minimum frequency and minimum retention

**Description:** Evaluates if backup plans contain at least one backup rule for which the backup frequency is at least [1 day] and retention period is at least [35 days].

**Resource:** AWS Backup: backup plans

**Parameters:**
- Required backup frequency in number of hours or days.
- Required retention period in number of days, weeks, months, or years. We recommend a warm storage retention of period of at least one week to enable AWS Backup to take incremental backups when possible, avoiding additional charges.

**Scope:**
- Tagged resources
- Single resource

**Remediation:** [Update a backup plan](#) to change either its backup frequency, retention period, or both. Updating your backup plan changes the retention period for recovery points the plan creates after your update.

Vaults prevent manual deletion of recovery points

**Description:** Evaluates if backup vaults do not allow manual deletion of recovery points except by certain IAM roles.

**Resource:** AWS Backup: backup vaults

**Parameters:** The Amazon Resource Names (ARNs) of up to five IAM roles allowed to manually delete recovery points.

**Scope:**
- Tagged resources
- Single resource

**Remediation:** Create or modify a resource-based access policy on a backup vault. For an example policy and instructions on how to set a backup vault access policy, see [Deny access to delete recovery points in a backup vault](#).

**Recovery points are encrypted**

**Description:** Evaluates if recovery points are encrypted.

**Resource:** AWS Backup: recovery points

**Parameters:** None

**Scope:**
- Tagged resources

**Remediation:** Configure encryption for the recovery points. The way you configure encryption for AWS Backup recovery points differs depending on the resource type.

You can configure encryption for resource types that support full AWS Backup management in using AWS Backup. If the resource type does not support full AWS Backup management, you must configure its backup encryption by following that service's instructions, such as [Amazon EBS encryption](#) in the *Amazon Elastic Compute Cloud User Guide*. To see the list of resource types that support full AWS Backup management, see the "Full AWS Backup management" section of the [Feature availability by resource (p. 2)](#) table.

**Minimum retention established for recovery point**

**Description:** Evaluates if recovery point retention period is at least [35 days].

**Resource:** AWS Backup: recovery points

**Parameters:** Required recovery point retention period in number of days, weeks, months, or years. We recommend a warm storage retention of period of at least one week to enable AWS Backup to take incremental backups when possible, avoiding additional charges.

**Scope:**
- Tagged resources

**Remediation:** Change the retention periods of your recovery points. For more information, see [Editing a backup](#).

**Cross-Region backup copy is scheduled**

**Description:** Evaluates if a resource is configured to create copies of its backups to another AWS Region.

**Resource:** AWS Backup: backup plans

**Parameters:**
- Select the AWS Region(s) where the backup copy should exist (Optional)
- Region
Scope:

- Tagged resources
- Resources by type
- Single resource

Remediation: Update a backup plan to change the AWS Region where backup copy should exist.

Cross-account backup copy is scheduled

Description: Evaluates if a resource is configured to create copies of its backups to another account. You can add up to 5 accounts for the control to evaluate. The destination account must be in the same organization as the source account in AWS Organizations.

Resource: AWS Backup: backup plans

Parameters:

- Select the AWS account ID(s) where the backup copy should exist (Optional)
- Account ID

Scope:

- Tagged resources
- Resources by type
- Single resource

Remediation: Update a backup plan to change or add the AWS account ID(s) where the copy should exist.

Backups are protected by AWS Backup Vault Lock

Description: Evaluates if a resource has immutable backups stored in a locked backup vault.

Resource: AWS Backup: backup vaults

Parameters:

- Input the minimum and maximum retention days for AWS Backup Vault Lock (optional)
- Minimum retention days
- Maximum retention days

Scope:

- Tagged resources
- Resources by type
- Single resource

Remediation: Lock a backup vault to set its name, change either its minimum retention days, maximum retention days, or both. Can also include ChangeableForDays for a vault lock in compliance mode.
Last recovery point was created

**Description:** This control evaluates if a recovery point has been created within the specified time frame (in days or hours).

The control is compliant if the resource has had a recovery point created within the time frame specified. The control is non-compliant if a recovery point was not created within the number of days or hours specified.

This control runs automatically every 24 hours.

**Resource:** AWS Backup: recovery points

**Parameters:**

- Input the specified time frame in whole numbers, either in hours or days.
- Values of hours can range from 1 to 744.
- Value of days can range from 1 to 31.

**Scope:**

- Tagged resources
- Resources by type
- Single resource

**Remediation:**

- [Update a backup plan](#) to change the specified time frame of recovery point creation.
- Additionally, you can create an on-demand backup.
Managing AWS Backup resources across multiple AWS accounts

**Note**
Before you manage resources across multiple AWS accounts in AWS Backup, your accounts must belong to the same organization in the AWS Organizations service.

You can use the cross-account management feature in AWS Backup to manage and monitor your backup, restore, and copy jobs across AWS accounts that you configure with AWS Organizations. AWS Organizations is a service that offers policy-based management for multiple AWS accounts from a single management account. It enables you to standardize the way you implement backup policies, minimizing manual errors and effort simultaneously. From a central view, you can easily identify resources in all accounts that meet the criteria that you are interested in.

If you set up AWS Organizations, you can configure AWS Backup to monitor activities in all of your accounts in one place. You can also create a backup policy and apply it to selected accounts that are part of your organization and view the aggregate backup job activities directly from the AWS Backup console. This functionality enables backup administrators to effectively monitor backup job status in hundreds of accounts across their entire enterprise from a single management account.

For example, you define a backup policy A that takes daily backups of specific resources and keeps them for 7 days. You choose to apply backup policy A to the whole organization. (This means that each account in the organization gets that backup policy, which creates a corresponding backup plan that is visible in that account.) Then, you create an OU named Finance, and you decide to keep its backups for only 30 days. In this case, you define a backup policy B, which overrides the lifecycle value, and attach it to that Finance OU. This means that all the accounts under the Finance OU get a new effective backup plan that takes daily backups of all specified resources and keeps them for 30 days.

In this example, backup policy A and backup policy B were merged into a single backup policy, which defines the protection strategy for all accounts under the OU named Finance. All the other accounts in the organization remain protected by backup policy A. Merging is done only for backup policies that share the same backup plan name. You can also have policy A and policy B coexist in that account without any merging. You can use advanced merging operators in the JSON view of the console only. For details about merging policies, see Defining policies, policy syntax, and policy inheritance (p. 223) in the AWS Organizations User Guide. For additional references and use cases, see the blog Managing backups at scale in your AWS Organizations using AWS Backup and the video tutorial Managing backups at scale in your AWS Organizations using AWS Backup.

Please see Feature availability by AWS Region to see where the cross-account management feature is available.

To use cross-account management, you must follow these steps:

1. Create a management account in AWS Organizations and add accounts under the management account.
2. Enable the cross-account management feature in AWS Backup.
3. Create a backup policy to apply to all AWS accounts under your management account.

**Note**
For backup plans that are managed by Organizations, the resource opt-in settings in the management account override the settings in a member account.

4. Manage backup, restore, and copy jobs in all your AWS accounts.
Creating a management account in Organizations

First, you must create your organization and configure it with AWS member accounts in AWS Organizations.

To create a management account in AWS Organizations and add accounts

- For instructions, see Tutorial: Creating and configuring an organization in the AWS Organizations User Guide.

Enabling cross-account management

Before you can use cross-account management in AWS Backup, you have to enable the feature (that is, opt in to it). After the feature is enabled, you can create backup policies that allow you to automate simultaneous management of multiple accounts.

To enable cross-account management


   You can do this step only from the management account.

2. In the left navigation pane, choose Settings to open the cross-account management page.

3. In the Backup policies section, choose Enable.

   This gives you access to all the accounts and allows you to create policies that automate management of multiple accounts in your organization simultaneously.

4. In the Cross-account monitoring section, choose Enable.

   This enables you to monitor the backup, copy, and restore activities of all accounts in your organization from your management account.

Delegated administrator

Delegated administration provides a convenient way for assigned users in a registered member account to perform most AWS Backup administrative tasks. You can choose to delegate administration of AWS Backup to a member account in AWS Organizations, thereby extending the ability to manage AWS Backup from outside the management account and across the entire organization.
A management account, by default, is the account used to edit and manage policies. Using the delegated administrator feature, you can delegate these management functions to member accounts you designate. In turn, those accounts can manage policies, in addition to the management account.

After a member account has been successfully registered for delegated administration, it is a delegated administrator account. Note that accounts, not users, are designated as delegated administrators.

Enabling delegated administrator accounts allows the option of managing backup policies, it minimizes the number of users with access to the management account, and it permits cross-account monitoring of jobs.

Below is a table showing the functions of the management account, accounts delegated as Backup administrators, and accounts that are members within the AWS Organization.

<table>
<thead>
<tr>
<th>PRIVILEGES</th>
<th>MANAGEMENT ACCOUNT</th>
<th>DELEGATED ADMINISTRATOR</th>
<th>MEMBER ACCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register/deregister delegated administrator accounts</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Manage backup policies across accounts in AWS Organizations</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Monitor cross-account jobs</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Prerequisites**

Before you can delegate backup administration, you must first register at least one member account in your AWS organization as a delegated administrator. Before you can register an account as a delegated administrator, you must first configure the following:

- **AWS Organizations must be enabled and configured** with at least one member account in addition to your default management account.

- In the AWS Backup console, ensure backup policies, cross-account monitoring, and cross-account backup features are turned on. These are below the Delegated administrators pane in the AWS Backup console.

- Cross-account monitoring allows you to monitor backup activity across all the accounts in your organization from the management account, as well as from delegated administrator accounts.

- Optional: Cross-account backup, which allows accounts in your organization to copy backups to other accounts (for Backup-supported cross-account resources).

- Enable service access with AWS Backup.

There are two steps involved in setting up delegated administration. The first step is to delegate cross-account jobs monitoring. The second step is to delegate backup policy management.
Register a member account as a delegated administrator account

This is the first section: Using the AWS Backup console to register a delegated administrator account to monitor cross-account jobs. To delegate AWS Backup policies, you will use the Organizations console in the next section.

To register a member account using the AWS Backup Console:

1. Sign in to the AWS Backup console using the credentials of your management account in AWS Organizations.
2. Under My Account in the left-hand navigation of the console, choose Settings.
3. In the Delegated administrator pane, click Register delegated administrator or Add delegated administrator.
4. On the Register delegated administrator page, select the account you want to register, and then choose Register account.

This designated account will now be registered as a delegated administrator, with administrative privileges to monitor jobs across accounts within the organization and can view and edit policies (policy delegation). This member account cannot register or deregister other delegated administrator accounts. You can use the console to register up to 5 accounts as delegated administrators.

To register a member account using programmatically:

Use the CLI command register-delegated-administrator. You can specify the following parameters in your CLI request:

- service-principal
- account-id

Below is an example of a CLI request to register a member account programmatically:

```
aws organizations register-delegated-administrator \  
--account-id 012345678912 \  
--service-principal "backup.amazonaws.com"
```

Deregister a member account

Use the following procedure to remove administrative access from AWS Backup by deregistering a member account in your AWS organization that had previously been designated as a delegated administrator.

To deregister a member account using the Console

1. Sign in to the AWS Backup console using the credentials of your management account in AWS Organizations.
2. Under My Account in the left-hand navigation of the console, choose Settings.
3. In the Delegated administrator section, click Deregister account.
4. Choose the account(s) you want to deregister.
5. In the Deregister account dialog box, review the security implications, and then type confirm to complete the deregistration.
Delegate AWS Backup policies through AWS Organizations

Within the AWS Organizations console, you can delegate administration of multiple policies, including Backup policies.

From the management account logged into the AWS Organizations console, you can create, view, or delete a resource-based delegation policy for your organization. For steps to delegate policies, see Create a resource-based delegation policy in the AWS Organizations User Guide.

Creating a backup policy

After you enable cross-account management, create a cross-account backup policy from your management account.

To create a backup policy

1. In the left navigation pane, choose Backup policies. On the Backup policies page, choose Create backup policies.
2. In the Details section, enter a backup policy name and provide a description.
3. In the Backup plans details section, choose the visual editor tab and do the following:
   a. For Backup plan name, enter a name.
   b. For Regions, choose a Region from the list.
4. In the Backup rule configuration section, choose Add backup rule.
   a. For Rule name, enter a name for the rule. The rule name is case sensitive and can contain only alphanumeric characters or hyphens.
   b. For Schedule, choose a backup frequency in the Frequency list, and choose one of the Backup window options. We recommend that you choose Use backup window defaults—recommended.
5. For Lifecycle, choose the lifecycle settings you want.
6. For Backup vault name, enter a name. This is the backup vault where recovery points created by your backups will be stored.
Make sure that the backup vault exists in all your accounts. AWS Backup doesn't check for this.

7. (optional) Choose a destination Region from the list if you want your backups to be copied to another AWS Region, and add tags. You can choose tags for the recovery points that are created, regardless of the cross-Region copy settings. You can also add more rules.

8. In the Resource assignment section, provide the name of the AWS Identity and Access Management (IAM) role. To use the AWS Backup service-linked role, provide service-role/AWSBackupDefaultServiceRole.

AWS Backup assumes this role in each account to gain the permissions to perform backup and copy jobs, including encryption key permissions when applicable. AWS Backup also uses this role to perform lifecycle deletions.

   **Note**
   AWS Backup doesn't validate that the role exists or if the role can be assumed.
   For backup plans created by cross-account management, AWS Backup will use the opt-in settings from the management account and overrides the settings specific accounts.
   For each account that you want to add backup policies to, you must create the vaults and IAM roles yourself.

9. Add tags to the backup plan, if desired. The maximum number of tags allowed is 20.

10. In the Advanced settings section, choose Windows VSS if the resource you’re backing up is running Microsoft Windows on an Amazon EC2 instance. This enables you to take application-consistent Windows VSS backups.

   **Note**
   AWS Backup currently supports application-consistent backups of resources running on Amazon EC2 only. Not all instance types or applications are supported for Windows VSS backups. For more information, see Creating Windows VSS backups (p. 124).

   **Note**
   AWS Organizations policy allows specifying 20 tags maximum if a backup plan is created via Organizations policy. Additional tags can be included by utilizing multiple resource assignments or engaging multiple backups plans through JSON.

11. Choose Add backup plan to add it to the policy, and then choose Create backup policy.

Creating a backup policy doesn't protect your resources until you attach it to the accounts. You can choose your policy name and see the details.

The following is an example AWS Organizations policy that creates a backup plan. If you enable Windows VSS backup, you must add permissions that allow you to take application-consistent backups as shown in the advanced_backup_settings section of the policy.

```json
{
   "plans": {
      "PiiBackupPlan": {
         "regions": {
            "@@append": [
               "us-east-1",
               "eu-north-1"
            ]
         },
         "rules": {
            "Hourly": {
               "schedule_expression": {
                  "@@assign": "cron(0 0/1 ? * *)"
               },
               "start_backup_window_minutes": {
                  "@@assign": "60"
               },
               "complete_backup_window_minutes": {
                  "@@assign": "220"
               }
            }
         }
      }
   }
}
```
Creating a backup policy

```json
"@@assign": "604800",
"target_backup_vault_name": {
  "@@assign": "FortKnox"
},
"recovery_point_tags": {
  "owner": {
    "tag_key": {
      "@@assign": "Owner"
    },
    "tag_value": {
      "@@assign": "Backup"
    }
  }
},
"lifecycle": {
  "delete_after_days": {
    "@@assign": "365"
  },
  "move_to_cold_storage_after_days": {
    "@@assign": "180"
  }
},
"copy_actions": {
  "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault": {
    "target_backup_vault_arn": {
      "@@assign": "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault"
    },
    "lifecycle": {
      "delete_after_days": {
        "@@assign": "365"
      },
      "move_to_cold_storage_after_days": {
        "@@assign": "180"
      }
    }
  }
},
"selections": {
  "tags": {
    "SelectionDataType": {
      "iam_role_arn": {
        "@@assign": "arn:aws:iam::$account:role/MyIamRole"
      },
      "tag_key": {
        "@@assign": "dataType"
      },
      "tag_value": {
        "@@assign": [
          "PII",
          "RED"
        ]
      }
    }
  }
},
"backup_plan_tags": {
  "stage": {
    "tag_key": {
      "@@assign": "Stage"
    },
    "tag_value": {
      "@@assign": "Beta"
    }
  }
}
```
12. In the Targets section, choose the organizational unit or account that you want to attach the policy to, and choose Attach. The policy can also be added to individual organizational units or accounts.

**Note**

Make sure to validate your policy and that you include all required fields in the policy. If parts of the policy are not valid, AWS Backup ignores those parts, but the valid parts of the policy will work as expected. Currently, AWS Backup does not validate AWS Organizations policies for correctness.

If you apply one policy to the management account and a different policy to a member account, and they conflict (for example, having different backup retention periods), both policies will run without issues (that is, the policies will independently run for each account). For example, if the management account policy backs up an Amazon EBS volume once a day, and the local policy backs up an EBS volume once a week, both policies will run. If required fields are missing in the effective policy that will be applied to an account (probably due to merging between different policies), AWS Backup doesn’t apply the policy to the account at all. If some settings are not valid, AWS Backup adjusts them.

Regardless of the opt-in settings in a member account in a backup plan that is created from a backup policy, AWS Backup will use the opt-in settings specified in the management account of the organization.

When you attach a policy to an organizational unit, every account that joins this organizational unit gets this policy automatically, and every account that is removed from the organizational unit loses this policy. The corresponding backup plans are deleted automatically from that account.

---

**Monitoring activities in multiple AWS accounts**

To monitor backup, copy, and restore jobs across accounts, you must enable cross-account monitoring. This lets you monitor backup activities in all accounts from your organizations management account. After you opt in, all the jobs across your organization that were created after the opt-in are visible. When you opt out, AWS Backup keeps the jobs in the aggregated view for 30 days (from reaching a terminus state). Created jobs after the opt-out are not visible and do not show any newly created backup jobs. For opt-in instructions, see [Enabling cross-account management](p. 216).

**To monitor multiple accounts**


   You can only do this from the management account.

2. In the left navigation pane, choose **Settings** to open the cross-account management page.

3. In the **Cross-account monitoring** section, choose **Enable**.

   This enables you to monitor the backup and restore activities of all accounts in your organization from your management account.

4. In the left navigation pane, choose **Cross-account monitoring**.

5. On the **Cross-account monitoring** page, choose the **Backup jobs**, **Restore jobs**, or **Copy jobs** tab to see all the jobs created in all your accounts. You can see each of these jobs by AWS account ID, and you can see all the jobs in a particular account.
6. In the search box, you can filter the jobs by **Account ID**, **Status**, or **Job ID**.

For example, you can choose the **Backup jobs** tab and see all backup jobs created in all your accounts. You can filter the list by **Account ID** and see all the backup jobs created in that account.

**Resource opt-in rules**

If a member account's backup plan was created by an Organizations-level backup policy (with an ID starting `orgs-`), the AWS Backup opt-in settings for the Organizations management account will override the opt-in settings in that member account, but only for that backup plan.

If the member account also has local-level backup plans created by users, those backup plans will follow the opt-in settings in the member account, without reference to the Organizations management account's opt-in settings.

**Defining policies, policy syntax, and policy inheritance**

The following topics are documented in the *AWS Organizations User Guide*.

- **Backup policies** – See [Backup policies](#).
- **Policy syntax** – See [Backup policy syntax and examples](#).
- **Inheritance for management policy types** – See [Inheritance for management policy types](#).
AWS Backup and AWS CloudFormation

In general

With AWS CloudFormation, you can provision and manage your AWS resources in a safe, repeatable manner using templates that you create. You can use AWS CloudFormation templates and StackSets to manage your backup plans, backup resource selections, and backup vaults. For information about using AWS CloudFormation, see How Does AWS CloudFormation Work? in the AWS CloudFormation User Guide.

Before you create your AWS CloudFormation template or StackSet, consider the following:

- Create separate templates for your backup plans and your backup vaults. You can only delete backup vaults that are empty. You can't delete a stack that includes backup vaults if they contain recovery points.
- Verify you have a service role available before you create your stack. The AWS Backup default service role is created for you the first time you assign resources to a backup plan. If you haven't assigned resources to your backup plan, do so before creating your stack. You can also specify a custom role that you create. For more information about roles, see IAM service roles (p. 244).

Deploying a backup vault, backup plan, and resource assignment using AWS CloudFormation

For sample AWS CloudFormation templates that deploys a backup vault, backup plans, and resource assignment, see Assigning resources using AWS CloudFormation (p. 50).

Deploying backup plans using AWS CloudFormation

For sample AWS CloudFormation templates that deploy backup plans, see AWS CloudFormation templates for backup plans.

Deploying AWS Backup Audit Manager frameworks and report plans using AWS CloudFormation

For sample AWS CloudFormation templates that deploy AWS Backup Audit Manager frameworks and report plans, see AWS CloudFormation templates for backup plans.
Deploying backup plans across accounts using AWS CloudFormation

You can use AWS CloudFormation StackSets across multiple accounts in an AWS Organization. Sample templates are available in the AWS CloudFormation User Guide.

An excellent starting point and reference is the publication Automate centralized backup at scale across AWS services using AWS Backup. With Ibukun Oyewumi and Sabith Venkitachalapathy (Jul. 2021).

Learning more about AWS CloudFormation

For information about using AWS CloudFormation with AWS Backup, see AWS Backup Resource Type Reference in the AWS CloudFormation User Guide.

For information about controlling access to AWS service resources when using AWS CloudFormation, see Controlling Access with AWS Identity and Access Management in the AWS CloudFormation User Guide.
Security in AWS Backup

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to AWS Backup, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility for AWS Backup includes, but is not limited to, the following. You are also responsible for other factors including the sensitivity of your data, your organization's requirements, and applicable laws and regulations.
  - Responding to communications you receive from AWS.
  - Managing the credentials you and your team use. For more information, see Identity and access management in AWS Backup.
  - Configuring your backup plans and resource assignments to reflect your organization's data protection policies. For more information, see Managing backup plans.
  - Regularly testing your ability to find certain recovery points and restore them. For more information, see Working with backups.
  - Incorporating AWS Backup procedures in your organization's disaster recovery and business continuity written procedures. For a start point, see Getting started with AWS Backup.
  - Ensuring that your employees are familiar with and have practiced using AWS Backup along with your organizational procedures in the event of an emergency. For more information, see the AWS Well-Architected Framework.

This documentation helps you understand how to apply the shared responsibility model when using AWS Backup. The following topics show you how to configure AWS Backup to meet your security and compliance objectives. You also learn how to use other AWS services that help you monitor and secure your AWS Backup resources.

**Topics**
- Data protection in AWS Backup (p. 226)
- Legal hold (p. 233)
- Identity and access management in AWS Backup (p. 238)
- Compliance validation for AWS Backup (p. 337)
- Resilience in AWS Backup (p. 337)
- Infrastructure security in AWS Backup (p. 338)
- AWS PrivateLink (p. 338)

Data protection in AWS Backup

AWS Backup conforms to the AWS shared responsibility model, which includes regulations and guidelines for data protection. AWS is responsible for protecting the global infrastructure that runs all the AWS services. AWS maintains control over data hosted on this infrastructure, including the security configuration controls for handling customer content and personal data. AWS customers and AWS
Partner Network (APN) partners, acting either as data controllers or data processors, are responsible for any personal data that they put in the AWS Cloud.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). This helps ensure that each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to communicate with AWS resources.
- Use AWS encryption solutions, along with all default security controls within AWS services.

We strongly recommend that you never put sensitive identifying information, such as your customers’ account numbers, into free-form fields such as a Name field. This includes when you work with AWS Backup or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into AWS Backup or other services might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

For more information about data protection, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

Encryption for backups in AWS Backup

**Note**
AWS Backup Audit Manager helps you automatically detect unencrypted backups.

You can configure encryption for resource types that support full AWS Backup management in using AWS Backup. If the resource type does not support full AWS Backup management, you must configure its backup encryption by following that service’s instructions, such as Amazon EBS encryption in the Amazon Elastic Compute Cloud User Guide. To see the list of resource types that support full AWS Backup management, see the “Full AWS Backup management” section of the Feature availability by resource (p. 2) table.

The following table lists each supported resource type, how encryption is configured for backups, and whether independent encryption for backups is supported. When AWS Backup independently encrypts a backup, it uses the industry-standard AES-256 encryption algorithm.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>How to configure encryption</th>
<th>Independent AWS Backup encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td>Amazon S3 backups are encrypted using a AWS KMS (AWS Key Management Service) key associated with the backup vault. The AWS KMS key can either be a customer-managed CMK or an AWS-managed CMK associated with the AWS Backup service. AWS Backup encrypts all backups even if the source Amazon S3 buckets are not encrypted.</td>
<td>Supported</td>
</tr>
<tr>
<td>Virtual machines</td>
<td>Virtual machine backups are always encrypted. The AWS KMS encryption key for virtual</td>
<td>Supported</td>
</tr>
<tr>
<td>Resource type</td>
<td>How to configure encryption</td>
<td>Independent AWS Backup encryption</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Machine backups</td>
<td>machine backups is configured in the AWS Backup vault that the virtual machine backups are stored in.</td>
<td></td>
</tr>
<tr>
<td>Amazon DynamoDB after enabling <strong>Advanced DynamoDB backup</strong> (p. 107)</td>
<td>DynamoDB backups are always encrypted. The AWS KMS encryption key for DynamoDB backups is configured in the AWS Backup vault that the DynamoDB backups are stored in.</td>
<td>Supported</td>
</tr>
<tr>
<td>Amazon DynamoDB without enabling <strong>Advanced DynamoDB backup</strong> (p. 107)</td>
<td>DynamoDB backups are automatically encrypted with the same encryption key that was used to encrypt the source DynamoDB table. Snapshots of unencrypted DynamoDB tables are also unencrypted. <strong>Note</strong> In order for AWS Backup to create a backup of an encrypted DynamoDB table, you must add the permissions kms:Decrypt and kms:GenerateDataKey to the IAM role used for backup. Alternately, you can use the AWS Backup default service role.</td>
<td>Not supported</td>
</tr>
<tr>
<td>Amazon Elastic File System (Amazon EFS)</td>
<td>Amazon EFS backups are always encrypted. The AWS KMS encryption key for Amazon EFS backups is configured in the AWS Backup vault that the Amazon EFS backups are stored in.</td>
<td>Supported</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (Amazon EBS)</td>
<td>By default, Amazon EBS backups are either encrypted using the key that was used to encrypt the source volume, or they are unencrypted. During restore, you can choose to override the default encryption method by specifying a KMS key.</td>
<td>Not supported</td>
</tr>
<tr>
<td>Resource type</td>
<td>How to configure encryption</td>
<td>Independent AWS Backup encryption</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2) AMIs</td>
<td>Amazon EC2 AMIs backed by Amazon EBS snapshots can take advantage of Amazon EBS encryption. Snapshots of both data and root volumes can be encrypted and attached to an AMI. Snapshots of unencrypted AMIs are also unencrypted.</td>
<td>Not supported</td>
</tr>
<tr>
<td>Amazon Relational Database Service (Amazon RDS)</td>
<td>Amazon RDS snapshots are automatically encrypted with the same encryption key that was used to encrypt the source Amazon RDS database. Snapshots of unencrypted Amazon RDS databases are also unencrypted.</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>&lt;br&gt;AWS Backup currently supports all Amazon RDS database engines, including Amazon Aurora.</td>
<td></td>
</tr>
<tr>
<td>Amazon Aurora</td>
<td>Aurora cluster snapshots are automatically encrypted with the same encryption key that was used to encrypt the source Amazon Aurora cluster. Snapshots of unencrypted Aurora clusters are also unencrypted.</td>
<td>Not supported</td>
</tr>
<tr>
<td>Resource type</td>
<td>How to configure encryption</td>
<td>Independent AWS Backup encryption</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>Storage Gateway snapshots are automatically encrypted with the same encryption key that was used to encrypt the source Storage Gateway volume. Snapshots of unencrypted Storage Gateway volumes are also unencrypted.</td>
<td>Not supported</td>
</tr>
<tr>
<td>Note</td>
<td>You don’t need to use a customer managed key across all services to enable Storage Gateway. You only need to copy the Storage Gateway backup to a vault that configured a KMS key. This is because Storage Gateway does not have a service-specific AWS KMS managed key.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon FSx</td>
<td>Encryption features for Amazon FSx file systems differ based on the underlying file system. To learn more about your particular Amazon FSx file system, see the appropriate FSx User Guide.</td>
<td>Not supported</td>
</tr>
<tr>
<td>Amazon DocumentDB</td>
<td>Amazon DocumentDB cluster snapshots are automatically encrypted with the same encryption key that was used to encrypt the source Amazon DocumentDB cluster. Snapshots of unencrypted Amazon DocumentDB clusters are also unencrypted.</td>
<td>Not supported</td>
</tr>
<tr>
<td>Amazon Neptune</td>
<td>Neptune cluster snapshots are automatically encrypted with the same encryption key that was used to encrypt the source Neptune cluster. Snapshots of unencrypted Neptune clusters are also unencrypted.</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
Virtual machine hypervisor credential encryption

Virtual machines managed by a hypervisor use AWS Backup Gateway to connect on-premises systems to AWS Backup. It is important that hypervisors have the same robust and reliable security. This security can be achieved by encrypting the hypervisor, either by AWS owned keys or by customer managed keys.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>How to configure encryption</th>
<th>Independent AWS Backup encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Timestream</td>
<td>Timestream table snapshot backups are always encrypted. The AWS KMS encryption key for Timestream backups is configured in the backup vault in which the Timestream backups are stored.</td>
<td>Supported</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>Amazon Redshift clusters are automatically encrypted with the same encryption key that was used to encrypt the source Amazon Redshift cluster. Snapshots of unencrypted Amazon Redshift clusters are also unencrypted.</td>
<td>Not supported</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>CloudFormation backups are always encrypted. The CloudFormation encryption key for CloudFormation backups is configured in the CloudFormation vault in which the CloudFormation backups are stored.</td>
<td>Supported</td>
</tr>
<tr>
<td>SAP HANA databases on Amazon EC2 instances</td>
<td>SAP HANA database backups are always encrypted. The AWS KMS encryption key for SAP HANA database backups is configured in the AWS Backup vault in which the database backups are stored.</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Encryption for backup copies

When you use AWS Backup to copy your backups across accounts or Regions, AWS Backup automatically encrypts those copies, even if the original backup is unencrypted. AWS Backup encrypts your copy using the target vault’s KMS key.

**Note**

**Note:** Snapshots of unencrypted Aurora, Amazon DocumentDB, and Neptune clusters are also unencrypted.

**Note**

AWS managed keys are not supported for cross-account copies. For more information, see Cross-account backup.
AWS owned and customer managed keys

AWS Backup provides encryption for hypervisor credentials to protect sensitive customer login information using **AWS owned encryption** keys. You have the option of using **customer managed keys** instead.

By default, the keys used to encrypt credentials in your hypervisor are **AWS owned keys**. AWS Backup uses these keys to automatically encrypt hypervisor credentials. You can neither view, manage, or use AWS owned keys, nor can you audit their use. However, you don't have to take any action or change any programs to protect the keys that encrypt your data. For more information, see AWS owned keys in the [AWS KMS Developer Guide](https://docs.aws.amazon.com/kms/latest/developerguide/)

Alternatively, credentials can be encrypted using **Customer managed keys**. AWS Backup supports the use of symmetric customer-managed keys that you create, own, and manage to perform your encryption. Because you have full control of this encryption, you can perform tasks such as:

- Establishing and maintaining key policies
- Establishing and maintaining IAM policies and grants
- Enabling and disabling key policies
- Rotating key cryptographic material
- Adding tags
- Creating key aliases
- Scheduling keys for deletion

When you use a customer managed key, AWS Backup validates whether your role has permission to decrypt using this key (prior to a backup or restore job being run). You must add the `kms:Decrypt` action to the role used to start a backup or restore job.

Because the `kms:Decrypt` action cannot be added to the default backup role, you must use a role other than the default backup role to use customer managed keys.

For more information, see [customer managed keys](https://docs.aws.amazon.com/kms/latest/developerguide/) in the [AWS Key Management Service Developer Guide](https://docs.aws.amazon.com/kms/latest/developerguide/).

Grant required when using customer managed keys

AWS KMS requires a [grant](https://docs.aws.amazon.com/kms/latest/developerguide/) to use your customer managed key. When you import a [hypervisor configuration](https://docs.aws.amazon.com/kms/latest/developerguide/) encrypted with a customer managed key, AWS Backup creates a grant on your behalf by sending a `CreateGrant` request to AWS KMS. AWS Backup uses grants to access a KMS key in a customer account.

You can revoke access to the grant, or remove AWS Backup's access to the customer managed key at any time. If you do, all your gateways associated with your hypervisor can no longer access the hypervisor's username and password encrypted by the customer managed key, which will affect your backup and restore jobs. Specifically, backup and restore jobs you perform on the virtual machines in this hypervisor will fail.

Backup gateway uses the `RetireGrant` operation to remove a grant when you delete a hypervisor.

Monitoring encryption keys

When you use an AWS KMS customer managed key with your AWS Backup resources, you can use [AWS CloudTrail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/) or [Amazon CloudWatch Logs](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/) to track requests that AWS Backup sends to AWS KMS.

Look for AWS CloudTrail events with the following "eventName" fields to for monitor AWS KMS operations called by AWS Backup to access data encrypted by your customer managed key:
Legal hold

A legal hold is an administrative tool that helps prevent backups from being deleted while under a hold. While the hold is in place, backups under a hold cannot be deleted and lifecycle policies that would alter the backup status (such as transition to a Deleted state) are delayed until the legal hold is removed. A backup can have more than one legal hold.

Legal holds can be applied to one or more backups (also known as recovery points) created by AWS Backup. When a legal hold is created, it can take into account specific filtering criteria, such as resource types and resource IDs. Additionally, you can define the creation date range of backups you wish to include in a legal hold. Legal holds and backups have a many:many relationship, meaning a backup can have more than one legal hold and a legal hold can include more than one backup. Each account can have a maximum of 50 legal holds active at one time.

Legal holds apply only to the original backup on which they are placed. When a backup is copied across Regions or accounts (if the resource supports it), it does not retain or carry its legal hold with it. A legal hold, like other resources, has a unique ARN (Amazon Resource Name) associated with it. Only recovery points created by AWS Backup can be part of a legal hold.

Note that while AWS Backup Vault Lock provides additional protections and immutability to a vault, a legal hold provides additional protection against deletion individual backups (recovery points). The legal hold does not expire and will retain the data within the backup indefinitely. The hold remains active until the hold is released by a user with sufficient IAM permissions.

Create a legal hold

Legal holds can be added and released only by users who have specific IAM permissions. To check your permissions or to grant permissions, log into the AWS Identity and Access Management console.

When a legal hold is created, it contains only recovery points that have already been created. Backups (recovery points) with a status of EXPIRED or DELETING will not be included in the legal hold. Recovery points (backups) with the status of CREATING may not be included in the legal hold, depending on the time of completion.

Legal holds can be added to existing backups using the AWS Backup console or programmatically.

Create a legal hold using the console

As you create a legal hold via the console, you will need to configure several elements, including its title, its description, its scope, and (optionally) any tags you wish to include to help with organization and filtering.

Create a legal hold using the AWS Backup console

2. In the dashboard in the left of the console, find My Account. Click Legal holds.
3. Click Add legal hold.
4. There will be three panels shown: Legal hold details, Legal hold scope, and Legal hold tags.
a. Under **Legal hold details**, enter a legal hold title and a description for the hold in the text boxes provided.

b. In the panel **Legal hold scope**, choose how you wish to select the resource to include in the hold. When you create a hold, you choose which method you want to select the resources that will be within the legal hold. You can choose to include one of the following:

- Specific resource types and IDs;
- Select backup vaults;
- Include all resources types or all backup vaults within your account

c. Specify the date range of your legal hold. Enter the dates in the YYYY:MM:DD format (dates are inclusive).

d. *Optionally*, you can add tags for the hold you are creating. Tags can help categorize the hold for future reference and organization. You can add up to 50 tags total.

5. When you are satisfied with the configuration of your new legal hold, click the button **Add new hold**.

### Create a legal hold using the AWS CLI

You can specify the following metadata:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>VaultArns</th>
<th>Resources</th>
<th>FromDate</th>
<th>ToDate</th>
<th>DateRange</th>
<th>LegalHoldTags</th>
</tr>
</thead>
</table>

1. Copy the following JSON template and input it into the CLI.

```
{
    "Title": "Your name for the legal hold",
    "Description": "Your description of the legal hold",
    "ResourceSelection": {
        "VaultArns": [], // only one of vaultArns or resourceIds is allowed; error will return if both are included
        "Resources": []
    },
    "ResourceFilters": {
        "DateRange": {
            "FromDate": DateTime,
            "ToDate": DateTime
        } // both required: future DateTime values will not be allowed
    },
    "LegalHoldTags": { // optional, up to 50 tags
        "name": "value",
    }
}
```

2. Review this example for reference.

```
{
    "Title": "a legal hold",
    "Description": "some description",
    "ResourceSelection": {
        "VaultArns": [
```
View legal holds

You can see legal hold details in the AWS Backup console or programmatically.

View legal holds in the console

To view all legal holds within an account using the Backup console,

2. Using the left part of the dashboard, under My account, click Legal holds.
3. The legal hold table displays the title, status, description, ID, and creation date of existing holds. Click on the carat (down arrow) next to the table header to filter the table by the selected column.

View legal holds programatically

To view all legal holds programmatically, you can use the following API calls:

GetLegalHold: This action returns details for a specified legal hold. The details are the body of a legal hold in JSON format, in addition to metadata.
ListRecoveryPointsByLegalHold: This action returns recovery point ARNs (Amazon Resource Name) about the recovery points included in the specified legal hold. You need to include the parameters: nextToken and maxResults in your request.

The following JSON template can be used for GetLegalHold. You can copy it and input it into the CLI.

```json
GET /legal-holds/{legalHoldId} HTTP/1.1

Request
empty body

Response
{
  Title: string,
  Status: LegalHoldStatus,
  Description: string, // 280 chars max
  CancelDescription: string, // this is provided during cancel // 280 chars max
  LegalHoldId: string,
  LegalHoldArn: string,
  CreatedTime: number,
  CanceledTime: number,
  ResourceSelection: {
    VaultArns: [ string ],
    Resources: [ string ]
  },
  ResourceFilters: {
    DateRange: {
      FromDate: number,
     ToDate: number
    }
  }
}
```

The following JSON template can be used for ListLegalHolds. You can copy it and input it into the CLI.

```json
GET /legal-holds/ 
      &maxResults=MaxResults 
      &nextToken=NextToken
Request
empty body
url params:
  MaxResults: number // optional,
  NextToken: string // optional
status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING
maxResults: 1-1000

Response
{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
  ]
}
```
Release a legal hold

Legal holds will remain with one or more backups (recovery points) until they are removed by a user with sufficient IAM permissions. Removing a legal hold is also known as cancelling, deleting, or releasing a legal hold. The console uses the term release while the API uses the command cancelLegalHold. Removing a legal hold eliminates it from all backups to which it was attached.

Release a legal hold using the AWS Backup console

To release a hold using the console,

2. Enter the description you would like associated with the release.
3. Review the details, then click Release hold.
4. When the Release hold dialogue box appears, confirm your intent to release the hold by typing confirm into the text box.
   - Check the box that acknowledges you are cancelling the hold.

On the Legal holds page you can see all your holds. If the release was successful, the status of that hold will be shown as Released.

Release a legal hold using API and AWS CLI

To remove a hold programmatically, use the API call CancelLegalHold. You can specify the following metadata:

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CancelDescription: String</td>
<td>Legal hold is fully released and no longer has any effect. Recovery points can be deleted.</td>
</tr>
</tbody>
</table>

For details on the returned information, see GetLegalHold and ListLegalHolds in our API guide.
DeleteAfterDays: number // Optional. Default equals 30 days. This specifies number (in days to keep legal hold record after cancellation. This applies to the actual legal hold record only. Recovery points are unlocked as soon as cancelation processes and are not subject to this date.

1. Copy the following JSON template and input it into the CLI.

   ```json
   POST /legal-holds/{legalHoldId}
   
   Request
   {
   CancelDescription: String
   DeleteAfterDays: number // optional
   }
   
   DeleteAfterDays: optional.
   Defaults to 180 days. How long to keep legal hold record after canceled.
   This applies to the actual legal hold record only.
   Recovery points are unlocked as soon as cancelation processes and are not subject to this date.
   
   Response
   Empty body
   200 if successful
   other standard codes
   
   2. Review the response, which may contain elements of the following:

   ```
   POST /legal-holds/abc1-4d0-989f-19af HTTP/1.1
   
   Request
   {
   CancelDescription: "Canceling because case is closed 4/21"
   }
   ```

   For more information, see [CancelLegalHold](#).

### Identity and access management in AWS Backup

Access to AWS Backup requires credentials. Those credentials must have permissions to access AWS resources, such as an Amazon DynamoDB database or an Amazon EFS file system. Moreover, recovery points created by AWS Backup for some AWS Backup-supported services cannot be deleted using the source service (such as Amazon EFS). You can delete those recovery points using AWS Backup.

The following sections provide details on how you can use [AWS Identity and Access Management (IAM)](#) and AWS Backup to help secure access to your resources.

**Warning**
AWS Backup uses the same IAM role that you chose when assigning resources to manage your recovery point lifecycle. If you delete or modify that role, AWS Backup cannot manage your recovery point lifecycle. When this occurs, it will attempt to use a service-linked role to manage your lifecycle. In a small percentage of cases, this might also not work, leaving EXPIRED...
recovery points on your storage, which might create unwanted costs. To delete EXPIRED recovery points, manually delete them using the procedure in Deleting backups.

Topics

• Authentication (p. 239)
• Access control (p. 240)
• IAM service roles (p. 244)
• Managed policies for AWS Backup (p. 246)
• Using service-linked roles for AWS Backup (p. 333)

Authentication

Access to AWS Backup or the AWS services that you are backing up requires credentials that AWS can use to authenticate your requests. You can access AWS as any of the following types of identities:

• AWS account root user – When you sign up for AWS, you provide an email address and password that is associated with your AWS account. This is your AWS account root user. Its credentials provide complete access to all of your AWS resources.

  Important
  For security reasons, we recommend that you use the root user only to create an administrator. The administrator is an IAM user with full permissions to your AWS account. You can then use this admin user to create other IAM users and roles with limited permissions. For more information, see IAM Best Practices and Creating Your First IAM Admin User and Group in the IAM User Guide.

• IAM user – An IAM user is an identity within your AWS account that has specific custom permissions (for example, permissions to create a backup vault to store your backups in). You can use an IAM user name and password to sign in to secure AWS webpages like the AWS Management Console, AWS Discussion Forums, or the AWS Support Center.

  In addition to a user name and password, you can also generate access keys for each user. You can use these keys when you access AWS services programmatically, either through one of the several SDKs or by using the AWS Command Line Interface (AWS CLI). The SDK and AWS CLI tools use the access keys to cryptographically sign your request. If you don’t use the AWS tools, you must sign the request yourself. For more information about authenticating requests, see Signature Version 4 Signing Process in the AWS General Reference.

• IAM role – An IAM role is another IAM identity that you can create in your account that has specific permissions. It is similar to an IAM user, but it is not associated with a specific person. An IAM role enables you to obtain temporary access keys that can be used to access AWS services and resources. IAM roles with temporary credentials are useful in the following situations:

  • Federated user access – Instead of creating an IAM user, you can use pre-existing user identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated Users and Roles in the IAM User Guide.

  • Cross-account administration – You can use an IAM role in your account to grant another AWS account permissions to administer your account’s resources. For an example, see Tutorial: Delegate Access Across AWS accounts Using IAM Roles in the IAM User Guide.

  • AWS service access – You can use an IAM role in your account to grant an AWS service permissions to access your account’s resources. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the IAM User Guide.

  • Applications running on Amazon Elastic Compute Cloud (Amazon EC2) – You can use an IAM role to manage temporary credentials for applications running on an Amazon EC2 instance and making AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS
role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs running on the EC2 instance to get temporary credentials. For more information, see Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances in the IAM User Guide.

Access control

You can have valid credentials to authenticate your requests, but unless you have the appropriate permissions, you can't access AWS Backup resources such as backup vaults. You also can't back up AWS resources such as Amazon Elastic Block Store (Amazon EBS) volumes.

Every AWS resource is owned by an AWS account, and permissions to create or access a resource are governed by permissions policies. An account administrator can attach permissions policies to AWS Identity and Access Management (IAM) identities (that is, users, groups, and roles). And some services also support attaching permissions policies to resources.

Note
An account administrator (or administrator user) is a user with administrator permissions. For more information, see IAM Best Practices in the IAM User Guide.

When granting permissions, you decide who is getting the permissions, the resources they get permissions for, and the specific actions that you want to allow on those resources.

The following sections cover how access policies work and how you use them to protect your backups.

Topics
- Resources and operations (p. 240)
- Resource ownership (p. 241)
- Specifying policy elements: actions, effects, and principals (p. 242)
- Specifying conditions in a policy (p. 242)
- API permissions: actions, resources, and conditions reference (p. 243)
- Copy tags permissions (p. 243)
- Access policies (p. 244)

Resources and operations

A resource is an object that exists within a service. AWS Backup resources include backup plans, backup vaults, and backups. Backup is a general term that refers to the various types of backup resources that exist in AWS. For example, Amazon EBS snapshots, Amazon Relational Database Service (Amazon RDS) snapshots, and Amazon DynamoDB backups are all types of backup resources.

In AWS Backup, backups are also referred to as recovery points. When using AWS Backup, you also work with the resources from other AWS services that you are trying to protect, such as Amazon EBS volumes or DynamoDB tables. These resources have unique Amazon Resource Names (ARNs) associated with them. ARNs uniquely identify AWS resources. You must have an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies or API calls.

The following table lists resources, subresources, ARN format, and an example unique ID.

AWS Backup resource ARNs

<table>
<thead>
<tr>
<th>Resource type</th>
<th>ARN format</th>
<th>Example unique ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource type</td>
<td>ARN format</td>
<td>Example unique ID</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup vault</td>
<td>arn:aws:backup:region:account-id:backup-vault:*</td>
<td>snap-05f426fd8kdjbj4224</td>
</tr>
<tr>
<td>Recovery point for Amazon EBS</td>
<td>arn:aws:ec2:region: snapshot:*</td>
<td>snap-05f426fd8kdjbj4224</td>
</tr>
<tr>
<td>Recovery point for Amazon EC2 images</td>
<td>arn:aws:ec2:region: image/ami-*</td>
<td>ami-1a2b3e4f5e6f7g890</td>
</tr>
<tr>
<td>Recovery point for Storage Gateway</td>
<td>arn:aws:ec2:region: snapshot:*</td>
<td>snapshot/snap-04d0e49137e31d9e0</td>
</tr>
<tr>
<td>Recovery point for DynamoDB without Advanced DynamoDB backup</td>
<td>arn:aws:dynamodb:region:account-id:table/<em>/backup/</em></td>
<td>table/MyDynamoDBTable/backup/01547087347000-c8b6dkd3</td>
</tr>
<tr>
<td>Recovery point for DynamoDB with Advanced DynamoDB backup (p. 107) enabled</td>
<td>arn:aws:backup:region:account-id:recovery-point:*</td>
<td>12ba35a6-7bb8-901c-cdcd-4567d8e9ef01</td>
</tr>
<tr>
<td>Recovery point for Amazon EFS</td>
<td>arn:aws:backup:region:account-id:recovery-point:*</td>
<td>169699e7-e183-477e-bfcd-cb1c6e5455e</td>
</tr>
<tr>
<td>Recovery point for Amazon FSx</td>
<td>arn:aws:fsx:region:account-id:backup/backup-*</td>
<td>backup/backup-1a20e49137e31d9e0</td>
</tr>
<tr>
<td>Recovery point for virtual machine</td>
<td>arn:aws:backup:region:account-id:recovery-point:*</td>
<td>1681234a-5b6b-7dc8-8032-836f7fffc623b</td>
</tr>
<tr>
<td>Recovery point for Amazon S3 continuous backup</td>
<td>arn:aws:backup:region:account-bucket:5ec207d0</td>
<td>5ec207d0</td>
</tr>
<tr>
<td>Recovery point for S3 periodic backup</td>
<td>arn:aws:backup:region:account-bucket:20211231900000-5ec207d0</td>
<td>20211231900000-5ec207d0</td>
</tr>
</tbody>
</table>

Resources that support full AWS Backup management all have recovery points in the format arn:aws:backup:region:account-id:recovery-point:*, making it easier for you to apply permissions policies to protect those recovery points. To see which resources support full AWS Backup management, see that section of the Feature availability by resource (p. 2) table.

AWS Backup provides a set of operations to work with AWS Backup resources. For a list of available operations, see AWS Backup Actions (p. 385).

**Resource ownership**

The AWS account owns the resources that are created in the account, regardless of who created the resources. Specifically, the resource owner is the AWS account of the principal entity (that is, the AWS account that created the resource).
account root user, an IAM user, or an IAM role) that authenticates the resource creation request. The following examples illustrate how this works:

- If you use the AWS account root user credentials of your AWS account to create a backup vault, your AWS account is the owner of the vault.
- If you create an IAM user in your AWS account and grant permissions to create a backup vault to that user, the user can create a backup vault. However, your AWS account, to which the user belongs, owns the backup vault resource.
- If you create an IAM role in your AWS account with permissions to create a backup vault, anyone who can assume the role can create a vault. Your AWS account, to which the role belongs, owns the backup vault resource.

Specifying policy elements: actions, effects, and principals

For each AWS Backup resource (see Resources and operations (p. 240)), the service defines a set of API operations (see Actions (p. 385)). To grant permissions for these API operations, AWS Backup defines a set of actions that you can specify in a policy. Performing an API operation can require permissions for more than one action.

The following are the most basic policy elements:

- Resource – In a policy, you use an Amazon Resource Name (ARN) to identify the resource to which the policy applies. For more information, see Resources and operations (p. 240).
- Action – You use action keywords to identify resource operations that you want to allow or deny.
- Effect – You specify the effect when the user requests the specific action—this can be either allow or deny. If you don't explicitly grant access to (allow) a resource, access is implicitly denied. You can also explicitly deny access to a resource, which you might do to make sure that a user cannot access it, even if a different policy grants access.
- Principal – In identity-based policies (IAM policies), the user that the policy is attached to is the implicit principal. For resource-based policies, you specify the user, account, service, or other entity that you want to receive permissions (applies to resource-based policies only).

To learn more about IAM policy syntax and descriptions, see IAM JSON Policy Reference in the IAM User Guide.

For a table showing all of the AWS Backup API actions, see API permissions: actions, resources, and conditions reference (p. 243).

Specifying conditions in a policy

When you grant permissions, you can use the IAM policy language to specify the conditions when a policy should take effect. For example, you might want a policy to be applied only after a specific date. For more information about specifying conditions in a policy language, see Condition in the IAM User Guide.

To express conditions, you use predefined condition keys. There are no condition keys specific to AWS Backup. However, there are AWS-wide condition keys that you can use as appropriate. For a complete list of AWS-wide keys, see AWS Global Condition Context Keys in the IAM User Guide.

Note

AWS Backup does not support tag or context key conditions in access policies for any of its actions.
API permissions: actions, resources, and conditions reference

When you are setting up Access control (p. 240) and writing a permissions policy that you can attach to an IAM identity (identity-based policies), you can use the following list as a reference. The list includes each AWS Backup API operation, the corresponding actions for which you can grant permissions to perform the action, and the AWS resource for which you can grant the permissions. You specify the actions in the policy's Action field, and you specify the resource value in the policy's Resource field. If Resource field is blank, you can use the wildcard (*) to include all resources.

You can use AWS-wide condition keys in your AWS Backup policies to express conditions. For a complete list of AWS-wide keys, see Available Keys in the IAM User Guide.

Copy tags permissions

When AWS Backup performs a backup or copy job, it attempts to copy the tags from your source resource (or recovery point in the case of copy) to your recovery point.

Note
AWS Backup does not natively copy tags during restore jobs. For an event-driven architecture that will copy tags during restore jobs, see How to retain resource tags in AWS Backup restore jobs.

During a backup or copy job, AWS Backup aggregates the tags you specify in your backup plan (or copy plan, or on-demand backup) with the tags from your source resource. However, AWS enforces a limit of 50 tags per resource, which AWS Backup cannot exceed. When a backup or copy job aggregates tags from the plan and the source resource, it might discover more than 50 total tags, it will be unable to complete the job, and will fail the job. This is consistent with AWS-wide tagging best practices. To learn more, see Tag limits in the AWS General Reference Guide.

• Your resource has more than 50 tags after aggregating your backup job tags with your source resource tags. AWS supports up to 50 tags per resource. For more information, see Tag limits.
• The IAM role you provide to AWS Backup lacks permissions to read the source tags or set the destination tags. For more information and sample IAM role policies, see Managed Policies.

You can use your backup plan to create tags that contradict your source resource tags. When the two conflict, the tags from your backup plan take precedence. Use this technique if you prefer not to copy a tag value from your source resource. Specify the same tag key, but different or empty value, using your backup plan.

Permissions Required to assign tags to backups

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Required permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EFS file system</td>
<td>elasticfilesystem:DescribeTags</td>
</tr>
<tr>
<td>Amazon FSx file system</td>
<td>fsx:ListTagsForResource</td>
</tr>
<tr>
<td>Amazon RDS database and Amazon Aurora cluster</td>
<td>rds:AddTagsToResource</td>
</tr>
<tr>
<td></td>
<td>rds:ListTagsForResource</td>
</tr>
<tr>
<td>Storage Gateway volume</td>
<td>storagegateway:ListTagsForResource</td>
</tr>
<tr>
<td>Amazon EC2 instance and Amazon EBS volume</td>
<td>EC2:CreateTags</td>
</tr>
<tr>
<td></td>
<td>EC2:DescribeTags</td>
</tr>
</tbody>
</table>
DynamoDB does not support assigning tags to backups unless you first enable Advanced DynamoDB backup (p. 107).

When an Amazon EC2 backup creates an Image Recovery Point and a set of snapshots, AWS Backup copies tags to the resulting AMI. AWS Backup also copies the tags from the volumes associated with the Amazon EC2 instance to the resulting snapshots.

Access policies

A permissions policy describes who has access to what. Policies attached to an IAM identity are referred to as identity-based policies (IAM policies). Policies attached to a resource are referred to as resource-based policies. AWS Backup supports both identity-based policies and resource-based policies.

Note
This section discusses using IAM in the context of AWS Backup. It doesn't provide detailed information about the IAM service. For complete IAM documentation, see What Is IAM? in the IAM User Guide. For information about IAM policy syntax and descriptions, see IAM JSON Policy Reference in the IAM User Guide.

Identity-based policies (IAM policies)

Identity-based policies are policies that you can attach to IAM identities, such as users or roles. For example, you can define a policy that allows a user to view and back up AWS resources, but prevents them from restoring backups.

For more information about users, groups, roles, and permissions, see Identities (Users, Groups, and Roles) in the IAM User Guide.

For information about how to use IAM policies to control access to backups, see Managed policies (p. 246).

Resource-based policies

AWS Backup supports resource-based access policies for backup vaults. This enables you to define an access policy that can control which users have what kind of access to any of the backups organized in a backup vault. Resource-based access policies for backup vaults provide an easy way to control access to your backups.

Backup vault access policies control user access when you use AWS Backup APIs. Some backup types, such as Amazon Elastic Block Store (Amazon EBS) and Amazon Relational Database Service (Amazon RDS) snapshots, can also be accessed using those services' APIs. You can create separate access policies in IAM that control access to those APIs in order to fully control access to backups.

To learn how to create an access policy for backup vaults, see Set access policies on backup vaults (p. 62).

IAM service roles

An AWS Identity and Access Management (IAM) role is similar to a user, in that it is an AWS identity with permissions policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.

A service role is a role that an AWS service assumes to perform actions on your behalf. As a service that performs backup operations on your behalf, AWS Backup requires that you pass it a role to assume when performing backup operations on your behalf. For more information about IAM roles, see IAM Roles in the IAM User Guide.

The role that you pass to AWS Backup must have an IAM policy with the permissions that enable AWS Backup to perform actions associated with backup operations, such as creating, restoring, or expiring backups. Different permissions are required for each of the AWS services that AWS Backup supports. The role must also have AWS Backup listed as a trusted entity, which enables AWS Backup to assume the role.
When you assign resources to a backup plan, or if you perform an on-demand backup, copy, or restore, you must pass a service role that has access to perform the underlying operations on the specified resources. AWS Backup uses this role to create, tag, and delete resources in your account.

### Using AWS roles to control access to backups

You can use roles to control access to your backups by defining narrowly scoped roles and by specifying who can pass that role to AWS Backup. For example, you could create a role that only grants permissions to back up Amazon Relational Database Service (Amazon RDS) databases and only grant Amazon RDS database owners permission to pass that role to AWS Backup. AWS Backup provides several predefined managed policies for each of the supported services. You can attach these managed policies to roles that you create. This makes it easier to create service-specific roles that have the correct permissions that AWS Backup needs.

For more information about AWS managed policies for AWS Backup, see *Managed policies* (p. 246).

### Default service role for AWS Backup

When using the AWS Backup console for the first time, you can choose to have AWS Backup create a default service role for you. This role has the permissions that AWS Backup needs to perform backup operations for all the AWS services that it supports. To choose the default service role, follow any of the options in *Getting Started*.

**Note**

The default role is automatically created when you use the AWS Management Console. You can create the default role using the AWS Command Line Interface (AWS CLI), but it must be done manually.

If you prefer to use custom roles, such as separate roles for different resource types, you can also do that and pass your custom roles to AWS Backup. To view examples of roles that enable backup and restore for individual resource types, see the *Customer managed policies* (p. 247) table.

The default service role created by AWS Backup manages creating and restoring backups without working with custom roles. The default service role is called `AWSBackupDefaultServiceRole`.

`AWSBackupDefaultServiceRole` contains two managed policies, `AWSBackupServiceRolePolicyForBackup` and `AWSBackupServiceRolePolicyForRestores`.

`AWSBackupServiceRolePolicyForBackup` includes an IAM policy that grants AWS Backup permissions to describe the resource being backed up, the ability to create, delete, describe, or add tags to a backup regardless of the AWS KMS key with which it is encrypted. This IAM policy includes the necessary permissions for all the resource types that AWS Backup supports.

`AWSBackupServiceRolePolicyForRestores` includes an IAM policy that grants AWS Backup permissions to create, delete, or describe the new resource being created from a backup regardless of the AWS KMS key with which it is encrypted. It also includes permissions to tag the newly created resource. This IAM policy includes the necessary permissions for all the resource types that AWS Backup supports.

To restore an Amazon EC2 instance, you must launch a new instance.

### Creating the default service role in the console

Specific actions you take in the AWS Backup Console create the AWS Backup default service role.

**To create the AWS Backup default service role** `AWSBackupDefaultServiceRole` **in your AWS account:**

2. To create the role for your account, either assign resources to a backup plan or create an on-demand backup.
a. Create a backup plan and assign resources to the backup. See Create a scheduled backup.
b. Alternatively, create an on-demand backup. See Create an on-demand backup.

3. Verify that you have created the AWSBackupDefaultServiceRole in your account by following these steps:

a. Wait a few minutes. For more information, see Changes that I make are not always immediately visible in the AWS Identity and Access Management User Guide.
b. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/
c. In the left navigation menu, choose Roles.
d. In the search bar, type AWSBackupDefaultServiceRole. If this selection exists, you have created the AWS Backup default role and completed this procedure.
e. If AWSBackupDefaultServiceRole still does not appear, add the following permissions to either the IAM user or IAM role you use to access the console.

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
      ],
      "Resource":"*"
    }
  ]
}
```

For China Regions, replace aws with aws-cn. For AWS GovCloud (US) Regions, replace aws with aws-us-gov.
f. If you cannot add permissions to your IAM user or IAM role, ask your administrator to manually create a role with a name other than AWSBackupDefaultServiceRole and attach that role to these managed policies:

- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores

**Managed policies for AWS Backup**

**Managed policies**

Managed policies are standalone identity-based policies that you can attach to multiple users, groups, and roles in your AWS account.

*AWS managed policies* deliver an out-of-the-box experience for AWS Backup
Customer managed policies give you fine-grained controls to set access to backups in AWS Backup. For example, you can use them to give your database backup administrator access to Amazon RDS backups but not Amazon EFS ones.

For updates to managed policies, see Policy updates.

**Customer managed policies**

You can create standalone policies that you administer in your own AWS account. These policies are referred to as customer managed policies. You can then attach the policies to multiple principal entities in your AWS account. When you attach a policy to a principal entity, you give the entity the permissions that are defined in the policy.

One way to create a customer managed policy is to start by copying an existing AWS managed policy. That way you know that the policy is correct at the beginning, and all you need to do is customize it to your environment.

The following policies specify backup and restore permissions for individual AWS Backup-supported AWS services and third-party applications. They can be customized and attached to roles that you create to further limit access to AWS resources.

**Backup and restore policies for individual AWS Backup-supported resources**

```json

Resource

Backup policy

Amazon S3
Backup policy

{
  "Version":"2012-10-17",
  "Statement":
  [
    {
      "Sid":"S3BucketBackupPermissions",
      "Action":
    ]
}

"Version":"2012-10-17",

"Statement":
[

{

"Sid":"S3BucketBackupPermissions",

"Action":
]
Resource

backup

policy

"s3:GetBucketConfiguration",

"s3:GetBucketVersioning",

"s3:GetBucketLocation",

"s3:CreateBucket",

"s3:ListBucketVersions",

"s3:ListBucket",

"s3:GetBucketVersioning",

"s3:GetBucketNotification",

"s3:PutBucketNotification",

"s3:GetBucketLocation",

"s3:CreateBucket"

],

"Effect":"Allow",

"Resource":

["s3:GetBucketLocation", "s3:CreateBucket"]
Managed policies

Resource backup policy

"s3:GetBucketTagging",

"arn:aws:s3:::*"

"s3:GetBucketAcl"

"Sid":"S3ObjectBackupPermissions",

"Resource": [  
  "arn:aws:s3:::*"  
  "s3:GetObject",
  "s3:DeleteObject",
  "s3:GetObjectVersion",
  
  "s3:DeleteObject",
  "Sid":"S3ObjectBackupPermissions",

"s3:GetObject",
  
  "s3:DeleteObject",
  "Sid":"S3ObjectBackupPermissions",

"s3:GetObjectVersion",

}
Managed policies

Resource

backup policy

"s3:GetObjectVersionAcl",
"s3:PutObjectVersionAcl",
"s3:GetObjectVersionTagging",
"s3:GetObjectAcl",
"s3:PutObjectAcl",
"s3:GetObject",
"s3:PutObject",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"s3:GetObjectVersion",
"s3:GetObjectVersionTagging",
"s3:GetObjectVersionAcl",
"s3:PutObjectVersionAcl",
"s3:GetObjectTagging",
"s3:PutObjectAcl",
"s3:GetObjectVersion"
Managed policies

Resource

backup

policy

"s3:ListMultipartUploadParts"

"Effect":"Allow",
],

"Resource":
[
 "Effect":"Allow",

 "Resource":
 ["arn:aws:s3:::*/*
"
]
"

"arn:aws:s3:::*/*"
],

I

},

"Sid":"S3GlobalPermissions",

{

 "Action":
 ["Sid":"S3KMSPermissions",

 "Action":
 ["s3:ListAllMyBuckets"
Resource

backup policy

]

"kms:Decrypt",

"Effect":"Allow",

"kms:DescribeKey",

"Resource":

[

"kms:GenerateDataKey"

"*

,

]

]

"Effect":"Allow",

}

{

"Resource":"*


"Sid":"KMSBackupPermissions",

"Condition":

{

"Action":

[

"StringLike":

{

"kms:Decrypt",

"kms:Decrypt",

"kms:DescribeKey",

"Resource":

[

"kms:GenerateDataKey"

"*

,

]

]

"Effect":"Allow",

},

,

}
Managed policies

Resource

backup

policy

"kms:ViaService":**.amazonaws.com"

"kms:DescribeKey"

],

"Effect":"Allow",


"Condition":


"StringLike":


"kms:ViaService":**.amazonaws.com"
"Sid":"EventsPermissions",

"Action": [  
  "events:DescribeRule",
  "events:EnableRule",
  "events:PutRule",
  "events:DeleteRule",
  "events:DeleteRule",
]
Resource

Resource backup policy

"events:PutTargets",

"events:RemoveTargets",

"events:ListTargetsByRule",

"events:DisableRule"

],

"Effect":"Allow",

"Resource":"arn:aws:events:*:*:rule/AwsBackupManagedRule*"

},

{

"Sid":"EventsMetricsGlobalPermissions",
"Action":
[
  "cloudwatch:GetMetricData",
  "events:ListRules"
],
"Effect":"Allow",
"Resource":"*"
Resource backup policy

Virtual Machine backup policy

{

"Sid": "BackupGatewayBackupPermissions",

"Effect": "Allow",

"Action": 
[
"backup-gateway:Backup",
"backup-gateway:ListTagsForResource"
],

"Resource": "arn:aws:backup-gateway:*:*:vm/*"
},

{

"Sid": "GatewayRestorePermissions",

"Effect": "Allow",

"Action": 
["backup-gateway:Restore",
"backup-gateway:RestoreGateway",
"backup-gateway:ListTagsForResource"
],

"Resource": "arn:aws:backup-gateway:*:*:hypervisor/*"
}
Managed policies

Resource
backup
policy

)
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["ec2:CreateTags"],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "ec2:CreateVolume",
    },
    {
      "ec2:DeleteVolume"
      "Effect": "Allow",
    },
    {
      "Action": ["ec2:CreateTags"],
      "Resource": ["arn:aws:ec2:*::snapshot/*", "ec2:CreateVolume", "ec2:DeleteVolume"]
    }
  ]
}
```
Managed policies

```
Resource backup policy

"ec2:CreateSnapshot",
"arn:aws:ec2:*>*::snapshot/ *

"ec2:DeleteSnapshot"

"arn:aws:ec2:*>*::volume/ *

"Resource": [ ],

{
  "arn:aws:ec2:*>*::snapshot/ *
  "Effect":"Allow",

  "ec2:DescribeSnapshots",
  }

"ec2:DescribeVolumes"
```
Managed policies

Resource

backup

policy

"Effect":"Allow",
[

"Action":
["Resource":"*

}]
]
"
"ec2:DescribeVolumes",

"ec2:DescribeSnapshots",

"ec2:CopySnapshot",

"ec2:DescribeTags"

],

"Resource":"*"

},

}
"Action": [
  "tag:GetResources",
],

"Resource": "*",

"Effect": "Allow"
Resource
backup
policy

"backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"

],

"Resource":"arn:aws:backup:*:*:backup-vault:*"

}
]
}
Resource
backup
policy
Amazon
EFS
backup
policy

{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": ["elasticfilesystem:Backup",
      "elasticfilesystem:DescribeTags"
      "elasticfilesystem:Restore",
      "elasticfilesystem:DescribeFilesystems",
      "elasticfilesystem:CreateFilesystem",
      "elasticfilesystem:DeleteFilesystem",
      "arn:aws:elasticfilesystem:***:file-system/
      "elasticfilesystem:DescribeFilesystems",
      "elasticfilesystem:DeleteFilesystem"
    }
  ]
}

Resource
restore
policy
Amazon
EFS
restore
policy

{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": ["elasticfilesystem:Restore",
      "elasticfilesystem:CreateFilesystem",
      "elasticfilesystem:DescribeFilesystems"]
    }
  ]
}
Resource backup policy

}]},

I,

"Resource":"arn:aws:elasticfilesystem::*:filesystem/*"

}]
tag:GetResources"

],

"Resource":"*",

"Effect":"Allow"

],

{

"Effect":"Allow",

"Action": [

}
Resource
backup
policy

"backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"

],

"Resource":"arn:aws:backup:*:*:backup-vault:*"
Resource backup policy

Amazon RDS backup policy

{
  "Version":"2012-10-17",
  "Statement":
  [
    {
      "Effect":"Allow",
      "Action":
      [
        "rds:AddTagsToResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ]
    }
  ]
}
### Resource backup policy

```json
"rds:CopyDBSnapshot",

"rds:DescribeDBInstances",

"rds:CreateDBClusterSnapshot",

"rds:DescribeDBClusters",

"rds:DescribeDBClusterSnapshots",

"rds:CopyDBClusterSnapshot"

",

"Resource":"*"

```
"Effect":"Allow",

"Action": [

"rds:DeleteDBSnapshot",

"rds:ModifyDBSnapshotAttribute"
],

"Resource": [

"arn:aws:rds:*:*:snapshot:awsbackup:*"
]

}
"Effect": "Allow",

"Action": [
  "rds:DeleteDBClusterSnapshot",
  "rds:ModifyDBClusterSnapshotAttribute"
],

"Resource": [
  "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
]

"Action": [
  "tag:GetResources"
]
{
  "Resource": "backup",
  "Effect": "Allow",
}
,
{
  "Resource": "*",
  "Effect": "Allow",
}
,
{
  "Effect": "Allow",
  "Action": [
    "backup:DescribeBackupVault",
    "backup:CopyIntoBackupVault"
  ]
}
Managed policies

Resource
backup
policy

"Resource": "arn:aws:backup:*:*:backup-vault:*"

},

{

"Action": "kms:DescribeKey",

"Effect": "Allow",

"Resource": "*

}

]
Resource backup policy

Amazon Aurora backup policy

{
  "Version": "2012-10-17",
  "Statement": [

    {
      "Effect": "Allow",
      "Action": [
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:AddTagsToResource",
      ]
    },

    {
      "Effect": "Allow",
      "Action": [
        "rds:DeleteDBCluster",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:ListTagsForResource",
      ]
    }
  ]
}

"rds:CreateDBClusterSnapshot",

"rds:DescribeDBClusters",

"rds:RestoreDBClusterFromSnapshot",

"rds:ListTagsForResource",

"rds:AddTagsToResource"
Managed policies

**Resource backup policy**

```
"rds:AddTagsToResource",

],
"rds:CopyDBClusterSnapshot"

"Resource": "*

}

"Effect": "Allow",

"Action": [

"rds:DeleteDBClusterSnapshot"
```
### Managed policies

**Resource backup policy**

```json
{
    "Resource": [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    ],

    "Resource": [

        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    ]
}

{
    "Action": [

        "tag:GetResources"
    ],

    "Resource": "*",

    "Resource": "*"
}
```
Managed policies

```
{
  "Effect": "Allow",
  "Action": [
    "backup:DescribeBackupVault",
    "backup:CopyIntoBackupVault"
  ],
  "Resource": "arn:aws:backup:*:*:backup-vault:*"
},
```
Resource backup policy

{

"Action":"kms:DescribeKey",

"Effect":"Allow",

"Resource":"*

} ] ]}
Resource backup policy

Storage Gateway backup policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource": "arn:aws:storagegateway:*:*:gateway/*
    }
  ]
}

Storage Gateway restore policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource": "arn:aws:storagegateway:*:*:gateway/*
    }
  ]
}

"Resource": "arn:aws:storagegateway:*:*:gateway/*
"volume/*"
Managed policies

- **Resource**: 
  - Backup policy
    - "Resource": "arn:aws:storagegateway:*:*:gateway/*:volume/*"
    - "Effect": "Allow",
      - "Action": [
          "storagegateway:DescribeGatewayInformation",
          "ec2:DeleteSnapshot"
        ],
    - "storagegateway:CreateStorediSCSIVolume",
    - "Resource": "arn:aws:ec2:*::snapshot/*"
    - "storagegateway:CreateCachediSCSIVolume"
  - Restore policy
    - "Resource": "arn:aws:ec2:*::snapshot/*"
Resource backup policy

"Effect":"Allow",
"Resource":"arn:aws:storagegateway:*:*:gateway/*"

"Action": [  
  {  
    "ec2:DescribeSnapshots"
    "Effect":"Allow",
      },  
  "Action": [  
    {  
      "Resource":"*"
      "storagegateway:ListVolumes"
      [  
        ],  
    "Action": [  
      {  
        "Resource":"arn:aws:storagegateway:*:*:*"
        }  
      ]
    }  
  ]
  ]
"
tag:GetResources"
```json
{
    "Resource":"*",
    "Effect":"Allow",
}
{
    "Effect":"Allow",
    "Action": ["backup:DescribeBackupVault", "backup:CopyIntoBackupVault"],
    "Resource":"arn:aws:backup:*:*:backup-vault:*"
}
```
Managed policies

```json
Resource

backup

policy

}

]

}
```
Resource backup policy

Amazon FSx backup policy

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "fsx:DescribeBackups",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Action": "fsx:CreateFileSystemFromBackup",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

```
"Action": "EffectStateBackup",
"Effect": "Allow",
"Resource": "arn:aws:fsx:*:*:backup/*"
```
Resource
backup policy

<Resource>

"arn:aws:fsx::*:file-system/*",

"arn:aws:fsx::*:backup/*"

},

{

"Action":
"fsx:DescribeFileSystems",
"Effect":
"Allow",
"Resource":
"arn:aws:fsx::*:file-
Resource

backup policy

```json
{
    "Action": "fsx:ListTagsForResource",
    "Effect": "Allow",
    "Resource": "arn:aws:fsx:*:*:file-system/*",
}
{
    "Action": "fsx:DeleteBackup",
    "Effect": "Allow",
    "Resource": "arn:aws:fsx:*:*:file-system/*",
}
{
    "Action": "fsx:DescribeBackups",
    "Effect": "Allow",
    "Resource": "arn:aws:fsx:*:*:file-system/*",
}
{
    "Action": "fsx:DescribeBackups",
    "Effect": "Allow",
    "Resource": "arn:aws:fsx:*:*:backup/*",
}

"Action": "fsx:DescribeBackups",
"Effect": "Allow",
"Resource": "arn:aws:fsx:*:*:backup/*",
```

[ "Resource":
  "backup":
  "Policy":
  [ "Action":
    "fsx:DescribeBackups",
    "Effect": "Allow",
    "Resource": "arn:aws:fsx:*:*:backup/*",
  ]
]
### Resource backup policy

```
"arn:aws:fsx:*:*:backup/**"

```

},
"fsx:DeleteFileSystem",
{

"Effect":
"Allow",

},
"Action":
[

"Effect":
"Allow",

"fsx:ListTagsForResource",

"Resource":
"arn:aws:fsx:*:*:file-system/**",

"fsx:ManageBackupPrincipalAssociations",

"Condition":

"fsx:CopyBackup",

{

"fsx:TagResource"

"Null":
```
A Resource
backup
policy

{

"Resource":
"arn:aws:fsx:*:*:backup/
**"

} aws:ResourceTag/
aws:backup:source-
resource":
"false"

}

,

{

"Action":
"ds:DescribeDirectories",

"Effect":
"Allow",
```json

"Resource": "*"
```
Resource

backup
policy

Amazon EC2
backup
policy

{
  "Version":"2012-10-17",
  "Statement": [ 

    {
      "Effect":"Allow",
      "Action": [ "ec2:CreateTags", "ec2:DeleteSnapshot" ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },

    {
      "Effect":"Allow",
      "Action": [ "ec2:CreateVolume", "ec2:DeleteVolume" ],
      "Resource": [ ]
    }

  ]

  "Resource":"arn:aws:ec2:*::snapshot/*"
}
Resource

backup

policy

},

"arn:aws:ec2::*:snapshot/*",

"Effect":"Allow",

"arn:aws:ec2::*:volume/*"

"Action":
[
]

},

"ec2:CreateImage",

{

"Effect":"AllowImage"

"Action":
[

"Resource":"*

"ec2:DescribeSnapshots",
},

[

"ec2:DescribeVolumes"

"Effect":"Allow",


Resource
backup
policy

],
"Action":
[

"Resource":"

"ec2:CopyImage",
{

"ec2:CopySnapshot"
"Effect":"Allow",

"ec2:DescribeImages",
{

"ec2:DescribeInstances"
"Effect":"Allow",

],
"Action":
[

"Resource":"

"ec2:DescribeImages",
{

"ec2:DescribeInstances"
"Effect":"Allow",

},
"Action":
[

"Resource":"


AWS Backup Developer Guide
Managed policies

Resource
backup
policy

},
"ec2:CreateTags"

{

},
"Action": [
"Resource":"arn:aws:ec2:*:*:image/*"

},
"ec2:RunInstances"

{

},
"Effect":"Allow",
"Action": [
"ec2:DescribeSnapshots",

{

},
"ec2:DescribeTags",

"ec2:DescribeImages",

"ec2:DescribeImages"
Managed policies

Resource backup policy

"ec2:TerminateInstances"

"ec2:DescribeInstances",

"Effect":"Allow",
"ec2:DescribeInstanceAttribute",

"Resource":"arn:aws:ec2::*:instance/*"
"ec2:DescribeInstanceCreditSpecifications",
},

{
"ec2:DescribeNetworkInterfaces",

"Action":"iam:PassRole",

"ec2:DescribeElasticGpus",
"Resource":"arn:aws:iam::<account-id>:role/<role-name>",

"ec2:DescribeSpotInstanceRequests"

"Effect":"Allow"

},
]

"Resource":"*

293
Resource
backup
policy

},

[

"Effect": "Allow",

"Action": ["ec2:CreateSnapshot",

"ec2:DeleteSnapshot",

"ec2:DescribeVolumes",

"ec2:DescribeSnapshots"

],
Resource
backup
policy

"Resource":
[

"arn:aws:ec2:*::snapshot/*",

"arn:aws:ec2:*:*:volume/*"
]

},

{

"Action":
[

"tag:GetResources"
],

}
Managed policies

```
{
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Effect": "Allow",
    "Action": [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
    ],
    "Resource": "arn:aws:backup:*:*:backup-vault:*"
}
```
Resource
backup
policy

}
Windows VSS (Volume Shadow Copy Service) Backup Policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ]
    }
  ]
}
Managed policies

Resource
backup
policy

"Resource": "arn:aws:ec2:*::snapshot/*"

}

{

"Effect": "Allow",

"Action": [

"ec2:CreateImage",

"ec2:DeregisterImage"

],

"Resource": "*

}
Managed policies

Resource backup policy

"Effect":"Allow",

"Action": [ "ec2:CopyImage",
            "ec2:CopySnapshot"
          ],

"Resource":"*"

}
Resource

backup
policy

"ec2:CreateTags"

],

"Resource":"arn:aws:ec2:*:*:image/*"

},

{

"Effect":"Allow",

"Action": [ "ec2:DescribeSnapshots", "ec2:DescribeTags",}
Managed policies

Resource backup policy

"ec2:DescribeImages",

"ec2:DescribeInstances",

"ec2:DescribeInstanceAttribute",

"ec2:DescribeInstanceCreditSpecifications",

"ec2:DescribeNetworkInterfaces",

"ec2:DescribeElasticGpus",

"ec2:DescribeSpotInstanceRequests"
Resource backup policy

"Resource": "*"

,

{

"Effect": "Allow",

"Action": [

"ec2:CreateSnapshot",

"ec2:DeleteSnapshot",

"ec2:DescribeVolumes",

"ec2:DescribeSnapshots"

]
Managed policies

```
Resource
backup
policy

]

"Resource":
[

"arn:aws:ec2:*::snapshot/*",

"arn:aws:ec2:*:*:volume/*"

]

},

},

{

"Action":
[

"tag:GetResources"

]```
Resource
backups
policy

"Resource":"*",

"Effect":"Allow"

"Action": [ "backup:DescribeBackupVault",
            "backup:CopyIntoBackupVault" ]

}
### Resource

**backup policy**

```
"Resource":"arn:aws:backup:*::*:backup-vault::*"
```

},

`,

{

"Effect":"Allow",

"Action": [

"ssm:CancelCommand",

"ssm:GetCommandInvocation"

],

"Resource":"
```

},

{

"Resource":"
```
To restore an encrypted backup, do one of the following:

- Add your role to the allowlist for the AWS Key Management Service (AWS KMS) key policy, or
AWS Backup Developer Guide
Managed policies

• Attach this policy to your IAM role for restores:

```json
{
  "Action": [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:ReEncrypt*"
  ],
  "Effect": "Allow",
  "Resource": "*"
}
```

AWS managed policies

An **AWS managed policy** is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases. AWS managed policies make it easier for you to assign appropriate permissions to users, groups, and roles than if you had to write the policies yourself.

However, you can't change the permissions defined in AWS managed policies. AWS occasionally updates the permissions defined in an AWS managed policy. When this occurs, the update affects all principal entities (users, groups, and roles) that the policy is attached to.

AWS Backup provides several AWS managed policies for common use cases. These policies make it easier to define the right permissions and control access to your backups. There are two types of managed policies. One type is designed to be assigned to users to control their access to AWS Backup. The other type of managed policy is designed to be attached to roles that you pass to AWS Backup. The following table lists all the managed policies that AWS Backup provides and describes how they are defined. You can find these managed policies in the **Policies** section of the IAM console.

<table>
<thead>
<tr>
<th>Policy name</th>
<th>IAM-managed policy name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Backup Data Transfer Access</td>
<td>AWSBackupDataTransferAccess</td>
<td>This policy provides permissions for AWS Backup storage plane data transfer APIs, allowing the AWS Backint agent to complete backup data transfer with the AWS Backup storage plane. Users can attach this policy to roles assumed by Amazon EC2 instances running SAP HANA with the Backint agent.</td>
</tr>
<tr>
<td>AWS Backup Restore Access For SAP HANA</td>
<td>AWSBackupRestoreAccessForSAPHANA</td>
<td>This policy provides AWS Backup permission to restore a backup of SAP HANA on Amazon EC2.</td>
</tr>
<tr>
<td>AWS Backup For Amazon S3 Backup Policy</td>
<td>AWSBackupServiceRolePolicyForS3Backup</td>
<td>This policy contains the permissions necessary for AWS Backup to back up any S3 bucket. This includes access to all objects in a bucket and any associated AWS KMS key.</td>
</tr>
<tr>
<td>AWS Backup For Amazon S3 Restore Policy</td>
<td>AWSBackupServiceRolePolicyForS3Restore</td>
<td>This policy contains permissions necessary for AWS Backup</td>
</tr>
</tbody>
</table>

308
## Managed policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>IAM-managed policy name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To restore an S3 backup to a bucket. This includes read and write permissions to the buckets and the usage of any AWS KMS key in regards to S3 operations.</td>
<td>AWSBackupAuditAccess</td>
<td>This policy grants permissions for users to create controls and frameworks that define their expectations for AWS Backup resources and activities, and to audit AWS Backup resources and activities against their defined controls and frameworks. This policy grants permissions to AWS Config and similar services to describe user expectations perform the audits. This policy also grants permissions to deliver audit reports to Amazon S3 and similar services, and enables users to find and open their audit reports.</td>
</tr>
<tr>
<td>AWS Service Role Policy for Backup Reports</td>
<td>AWSServiceRolePolicyForBackupReports</td>
<td>AWS Backup uses this policy for the AWSServiceRoleForBackupReports service-linked role. This service-linked role gives AWS Backup permissions to monitor and report on the compliance of your backup settings, jobs, and resources with your frameworks.</td>
</tr>
<tr>
<td>Backup Administrator IAM Policy</td>
<td>AWSBackupFullAccess</td>
<td>The backup administrator has full access to AWS Backup operations, including creating or editing backup plans, assigning AWS resources to backup plans, and restoring backups. Backup administrators are responsible for determining and enforcing backup compliance by defining backup plans that meet their organization's business and regulatory requirements. Backup administrators also ensure that their organization's AWS resources are assigned to the appropriate plan.</td>
</tr>
<tr>
<td>Policy name</td>
<td>IAM-managed policy name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup Operator IAM Policy</td>
<td>AWSBackupOperatorAccess</td>
<td>Backup operators are users that are responsible for ensuring the resources that they are responsible for are properly backed up. Backup operators have permissions to assign AWS resources to the backup plans that the backup administrator creates. They also have permissions to create on-demand backups of their AWS resources and to configure the retention period of on-demand backups. Backup operators do not have permissions to create or edit backup plans or to delete scheduled backups after they are created. Backup operators can restore backups. You can limit the resource types that a backup operator can assign to a backup plan or restore from a backup. You do this by allowing only certain service roles to be passed to AWS Backup that have permissions for a certain resource type.</td>
</tr>
<tr>
<td>Backup Administrator AWS Organizations Policy</td>
<td>AWSBackupOrganizationAdminAccess</td>
<td>The organization administrator has full access to AWS Organizations operations, including creating, editing, or deleting backup policies, assigning backup policies to accounts and organizational units, and monitoring backup activities within the organization. Organization administrators are responsible for protecting accounts in their organization by defining and assigning backup policies that meet their organization's business and regulatory requirements.</td>
</tr>
<tr>
<td>Default Service Role Policy for Backups</td>
<td>AWSBackupServiceRolePolicyForBackups</td>
<td>Provides AWS Backup permissions to create backups of all supported resource types on your behalf.</td>
</tr>
</tbody>
</table>
Policy name | IAM-managed policy name | Description
---|---|---
Default Service Role Policy for Restores | AWSBackupServiceRolePolicyForRestores | Provides AWS Backup permissions to restore backups of all supported resource types on your behalf. For EC2 instance restores, you must also include the following permissions to launch the EC2 instance:

"Action":"iam:PassRole",
"Resource":"arn:aws:iam::account-id:role/role-name",
"Effect":"Allow"

Policy updates for AWS Backup

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the ReadOnlyAccess AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the IAM User Guide.

View details about updates to AWS managed policies for AWS Backup since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Backup Document history page.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWSBackupFullAccess</td>
<td>Added permission to get Resource Share Associations for new vault type.</td>
<td>August 8, 2023</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the action <code>iam:GetResourceShareAssociations</code> to grant the user permission to get resource share associations for new vault type.</td>
<td></td>
</tr>
</tbody>
</table>

311
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AWSBackupOperatorAccess</strong></td>
<td>Added permission to get Resource Share Associations for new vault type.</td>
<td>August 8, 2023</td>
</tr>
<tr>
<td></td>
<td>AWS Backup requires this additional permission to interact with AWS RAM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the action <code>ram:GetResourceShareAssociations</code> to grant the user permission to get resource share associations for new vault type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS Backup requires this additional permission to interact with AWS RAM.</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForS3Backup</strong></td>
<td>Added new permission to support Amazon S3 backup</td>
<td>August 1, 2023</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the permission <code>s3:PutInventoryConfiguration</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS Backup needs this permission to enhance backup performance speeds by using a bucket inventory.</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong></td>
<td>Added permissions to add tags to resources during a restore job.</td>
<td>May 22, 2023</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following actions to grant the user permissions to add tags to restore resources: <code>storagegateway:AddTagsToResource</code>, <code>elasticfilesystem:TagResource</code>, <code>ec2:CreateTags</code> for only <code>ec2:CreateAction</code> that includes either <code>RunInstances</code> or <code>CreateVolume</code>, <code>fsx:TagResource</code>, and <code>cloudformation:TagResource</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>These added permissions are necessary for AWS Backup to add tags to resources during the restore process.</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupAuditAccess</strong></td>
<td>Replaced resource selection</td>
<td>April 11, 2023</td>
</tr>
<tr>
<td></td>
<td>AWS Backup replaced the resource selection within the API <code>config:DescribeComplianceByConfigRule</code> with a wildcard resource.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This expanded resource selection makes it easier for a user to select a resource with fewer errors.</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong></td>
<td>Added permissions to support encrypted Amazon Elastic File System restores.</td>
<td>March 27, 2023</td>
</tr>
<tr>
<td>The following permission to restore Amazon EFS using a customer managed key: kms:GenerateDataKeyWithoutPlaintext. This update is necessary to help ensure users have required permissions to restore Amazon EFS resources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AWSServiceRolePolicyForBackupReports</strong></td>
<td>Updated action</td>
<td>March 9, 2023</td>
</tr>
<tr>
<td>AWS Backup added the following permissions to allow AWS Backup Audit Manager to access AWS Backup Audit Manager-managed AWS Config rules: config:DescribeConfigRules and config:DescribeConfigRuleEvaluationStatus. AWS Backup requires this update to interact with AWS Config.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForS3Restore</strong></td>
<td>Adding new permission for restores involving AWS KMS encryptions</td>
<td>February 13, 2023</td>
</tr>
<tr>
<td>AWS Backup added the following permissions: kms:Decrypt, s3:PutBucketOwnershipControls, and s3:GetBucketOwnershipControls to the policy AWSBackupServiceRolePolicyForS3Restore. These permissions are necessary to support restores of objects when KMS encryption is used in the original backup and for restoring objects when object ownership is configured on the original bucket instead of ACL.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>AWSBackupFullAccess</strong> — Added new permissions to support VMware backup operations</td>
<td>AWS Backup added the following permissions: <code>backup-gateway:GetHypervisorPropertyMappings</code>, <code>backup-gateway:GetVirtualMachine</code>, <code>backup-gateway:PutHypervisorPropertyMappings</code>, <code>backup-gateway:GetHypervisor</code>, <code>backup-gateway:StartVirtualMachinesMetadataSync</code>, <code>backup-gateway:GetBandwidthRateLimitSchedule</code>, and <code>backup-gateway:PutBandwidthRateLimitSchedule</code>. These permissions are necessary for AWS Backup to schedule backups using VMware tags of virtual machines and to support schedule-based bandwidth throttling.</td>
<td>December 15, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupOperatorAccess</strong> — Added new permissions to support backup operations</td>
<td>AWS Backup added the following permissions: <code>backup-gateway:GetHypervisorPropertyMappings</code>, <code>backup-gateway:GetVirtualMachine</code>, <code>backup-gateway:PutHypervisorPropertyMappings</code>, <code>backup-gateway:GetHypervisor</code>, and <code>backup-gateway:GetBandwidthRateLimitSchedule</code>. These permissions are necessary for AWS Backup to schedule backups using VMware tags of virtual machines and to support schedule-based bandwidth throttling.</td>
<td>December 15, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync</strong> — Added new policy with permissions to support AWS Backup Gateway sync with virtual machines.</td>
<td>AWS Backup introduced this policy and within it, the following permissions: <code>backup-gateway:ListTagsForResource</code>, <code>backup-gateway:TagResource</code>, and <code>backup-gateway:UntagResource</code>. These permissions are necessary for AWS Backup Gateway to sync the metadata of virtual machines in on-premise networks with Backup Gateway.</td>
<td>December 15, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForBackup — Added permissions to allow AWS Backup to backup Amazon Timestream resources.</td>
<td>AWS Backup added the following permissions: <code>timestream:StartAwsBackupJob</code>, <code>timestream:GetAwsBackupStatus</code>, <code>timestream:ListTables</code>, <code>timestream:ListDatabases</code>, <code>timestream:ListTagsForResource</code>, <code>timestream:DescribeTable</code>, <code>timestream:DescribeDatabase</code>, and <code>timestream:DescribeEndpoints</code>. These permissions are necessary for AWS Backup to support Timestream backup jobs.</td>
<td>December 13, 2022</td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForRestores — Added permissions to allow AWS Backup to restore Amazon Timestream resources.</td>
<td>AWS Backup added the following permissions: <code>timestream:StartAwsRestoreJob</code>, <code>timestream:GetAwsRestoreStatus</code>, <code>timestream:ListTables</code>, <code>timestream:ListTagsForResource</code>, <code>timestream:ListDatabases</code>, <code>timestream:DescribeTable</code>, <code>timestream:DescribeDatabase</code>, <code>s3:GetBucketAcl</code>, and <code>timestream:DescribeEndpoints</code>. These permissions are necessary for AWS Backup to support Timestream restore jobs.</td>
<td>December 13, 2022</td>
</tr>
<tr>
<td>AWSBackupFullAccess — Added permissions to allow AWS Backup to support Amazon Timestream resources.</td>
<td>AWS Backup added the following permissions: <code>timestream:ListTables</code>, <code>timestream:ListDatabases</code>, <code>s3:ListAllMyBuckets</code> and <code>timestream:DescribeEndpoints</code>. These permissions are necessary for AWS Backup to support Timestream resources.</td>
<td>December 13, 2022</td>
</tr>
<tr>
<td>AWSBackupOperatorAccess — Added permissions to allow AWS Backup to support Amazon Timestream resources.</td>
<td>AWS Backup added the following permissions: <code>timestream:ListDatabases</code>, <code>timestream:ListTables</code>, <code>s3:ListAllMyBuckets</code>, and <code>timestream:DescribeEndpoints</code>. These permissions are necessary for AWS Backup to support Timestream resources.</td>
<td>December 13, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>AWSBackupServiceLinkedRolePolicy</strong></td>
<td>Updated managed policy permission allows AWS Backup to have necessary access to Timestream resources for backup functions.</td>
<td>December 13, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupFullAccess</strong></td>
<td>Added permissions to allow AWS Backup to support Amazon Redshift resources.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupOperatorAccess</strong></td>
<td>Added permissions for AWS Backup to support Amazon Redshift resources.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForRestores</td>
<td>Added permissions to allow AWS Backup to access Amazon Redshift resources.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permissions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:RestoreFromClusterSnapshot,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:RestoreTableFromClusterSnapshot,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeClusters,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeTableRestoreStatus.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS Backup needs these permissions for its support of Amazon Redshift restore jobs.</td>
<td></td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForBackup</td>
<td>Added permissions to allow AWS Backup to access Amazon Redshift resources.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permissions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:CreateClusterSnapshot,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeClusterSnapshots,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeTags,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DeleteClusterSnapshot,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeClusters,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:CreateTags.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS Backup needs these permissions for its support of Amazon Redshift backup jobs.</td>
<td></td>
</tr>
<tr>
<td>AWSBackupFullAccess</td>
<td>Added permission to allow AWS Backup to support AWS CloudFormation resources.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permission:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cloudformation:ListStacks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This permission is necessary for Backup to support CloudFormation resources.</td>
<td></td>
</tr>
<tr>
<td>AWSBackupOperatorAccess</td>
<td>Added permission to allow AWS Backup to support AWS CloudFormation resources.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permission:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cloudformation:ListStacks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This permission is necessary for Backup to support CloudFormation resources.</td>
<td></td>
</tr>
<tr>
<td>AWSBackupServiceLinkedRolePolicyForBackup</td>
<td>Added permissions to allow AWS Backup to support AWS CloudFormation resources.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permissions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeClusterSnapshots,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeTags,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DeleteClusterSnapshot,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>redshift:DescribeClusters,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>These permissions are necessary for Backup to support CloudFormation resources.</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForBackup</strong></td>
<td>Added permissions to allow AWS Backup to access AWS CloudFormation resources.</td>
<td>November 16, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permissions: <code>cloudformation:GetTemplate</code>, <code>cloudformation:DescribeStacks</code>, and <code>cloudformation:ListStackResources</code>. These permissions are necessary for AWS Backup to support AWS CloudFormation application stack backup jobs.</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong></td>
<td>Added permissions to allow AWS Backup to access AWS CloudFormation resources.</td>
<td>November 16, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permissions: <code>cloudformation:CreateChangeSet</code> and <code>cloudformation:DescribeChangeSet</code>. These permissions are necessary for AWS Backup to support AWS CloudFormation application stack restore jobs.</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupOrganizationAdminAccess</strong></td>
<td>AWS Backup added permissions to this policy for Delegated Administrator functions.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permissions to this policy: <code>organizations:ListDelegatedAdministrator</code>, <code>organizations:RegisterDelegatedAdministrator</code>, and <code>organizations:DeregisterDelegatedAdministrator</code>. These permissions are necessary to allow organization administrators to use the Delegated Administrator feature.</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForBackup</strong></td>
<td>Added permissions to allow AWS Backup to support SAP HANA on Amazon EC2 instances.</td>
<td>November 20, 2022</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added the following permissions: <code>ssm-sap:GetOperation</code>, <code>ssm-sap:ListDatabases</code>, <code>ssm-sap:BackupDatabase</code>, <code>ssm-sap:UpdateHanaBackupSettings</code>, <code>ssm-sap:GetDatabase</code>, and <code>ssm-sap:ListTagsForResource</code>. These permissions are necessary for Backup to support SAP HANA on Amazon EC2 instances.</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>AWSBackupFullAccess</strong> — Added permissions to allow AWS Backup support of SAP HANA on Amazon EC2 instances.</td>
<td>AWS Backup added the following permissions: <code>ssm-sap:GetOperation</code>, <code>ssm-sap:ListDatabases</code>, <code>ssm-sap:GetDatabase</code>, and <code>ssm-sap:ListTagsForResource</code>. These permissions are necessary for Backup to support SAP HANA on Amazon EC2 instances.</td>
<td>November 20, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupOperatorAccess</strong> — Added permissions to allow AWS Backup support of SAP HANA on Amazon EC2 instances.</td>
<td>AWS Backup added the following permissions: <code>ssm-sap:GetOperation</code>, <code>ssm-sap:ListDatabases</code>, <code>ssm-sap:GetDatabase</code>, and <code>ssm-sap:ListTagsForResource</code>. These permissions are necessary for Backup to support SAP HANA on Amazon EC2 instances.</td>
<td>November 20, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupServiceLinkedRolePolicyForBackup</strong> — Added permission to allow AWS Backup support of SAP HANA on Amazon EC2 instances.</td>
<td>AWS Backup added the following permission: <code>ssm-sap:GetOperation</code>. This permission is necessary for Backup to support SAP HANA on Amazon EC2 instances.</td>
<td>November 20, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong> — Added permissions to allow AWS Backup to access Amazon EC2 resources.</td>
<td>AWS Backup added the following permission: <code>ec2:CreateTags</code>. This permission is necessary for AWS Backup to support Backup gateway restore jobs to an EC2 instance.</td>
<td>November 20, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>AWSBackupDataTransferAccess</strong> — Added permissions to allow AWS Backup to support secure storage data transfer for SAP HANA on Amazon EC2 instance resources.</td>
<td>AWS Backup added the following permissions: backup-storage:StartObject, backup-storage:PutChunk, backup-storage:GetChunk, backup-storage:ListChunks, backup-storage:ListObjects, backup-storage:GetObjectMetadata, and backup-storage:NotifyObjectComplete. These permissions are necessary for AWS Backup to support secure storage data transfer for SAP HANA On Amazon EC2 resources.</td>
<td>November 20, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForS3Backup</strong> — Added new permission to support Amazon S3 backup</td>
<td>AWS Backup added the permission s3:GetBucketAcl. AWS Backup needs this permission for backup operations of AWS Backup for S3.</td>
<td>August 24, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong></td>
<td>AWS Backup added the following actions to grant access to create a database instance: rds:CreateDBInstance. AWS Backup needed this permission for its support of Amazon RDS multi- Availability Zone (Multi-AZ) functionality.</td>
<td>July 20, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupServiceLinkedRolePolicyForBackup</strong></td>
<td>AWS Backup added the s3:GetBucketTagging permission to grant the user permission to select buckets to backup with a resource wildcard. Without this permission, users who select which buckets to backup with a resource wildcard will be unsuccessful. AWS Backup needed that permission for its support of Amazon S3 data.</td>
<td>May 6, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForBackup</strong></td>
<td>AWS Backup added volume resources in the scope of existing fsx:CreateBackup and fsx:ListTagsForResource actions, and added new action fsx:DescribeVolumes to support FSx for ONTAP volume level backups. AWS Backup needed this permission for its support of FSx for ONTAP.</td>
<td>April 27, 2022</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong></td>
<td>AWS Backup added the following actions to grant the users permissions to restore FSx for ONTAP volumes: fsx:DescribeVolumes, fsx:CreateVolumeFromBackup, fsx:DeleteVolume, and fsx:UntagResource. AWS Backup needed this permission for its support of FSx for ONTAP.</td>
<td>April 27, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForS3Backup</td>
<td>AWS Backup added the following actions to grant the user permissions to receive notifications of changes to their Amazon S3 buckets during backup operations: s3:GetBucketNotification and s3:PutBucketNotification. AWS Backup needed those permissions for its support of Amazon S3 data.</td>
<td>February 25, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForS3Backup</td>
<td>AWS Backup added the following actions to grant the user permissions to back up their Amazon S3 buckets: <code>s3:GetInventoryConfiguration</code>, <code>s3:PutInventoryConfiguration</code>, <code>s3:ListBucketVersions</code>, <code>s3:ListBucket</code>, <code>s3:GetBucketTagging</code>, <code>s3:GetBucketVersioning</code>, <code>s3:GetBucketNotification</code>, <code>s3:GetBucketLocation</code>, and <code>s3:ListAllMyBuckets</code>. AWS Backup added the following actions to grant the user permissions to back up their Amazon S3 objects: <code>s3:GetObject</code>, <code>s3:GetObjectAcl</code>, <code>s3:GetObjectVersionTagging</code>, <code>s3:GetObjectVersionAcl</code>, <code>s3:GetObjectTagging</code>, and <code>s3:GetObjectVersion</code>. AWS Backup added the following actions to grant the user permissions to back up their encrypted Amazon S3 data: <code>kms:Decrypt</code> and <code>kms:DescribeKey</code>. AWS Backup added the following actions to grant the user permissions to take incremental backups of their Amazon S3 data using Amazon EventBridge rules: <code>events:DescribeRule</code>, <code>events:EnableRule</code>, <code>events:PutRule</code>, <code>events:DeleteRule</code>, <code>events:PutTargets</code>, <code>events:RemoveTargets</code>, <code>events:ListTargetsByRule</code>, <code>events:DisableRule</code>, <code>cloudwatch:GetMetricData</code>, and <code>events:ListRules</code>. AWS Backup needed those permissions for its support of Amazon S3 data.</td>
<td>February 17, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForS3Restore</strong></td>
<td>In the new AWS Backup Service Role Policy for S3 Restore, AWS added the following permissions to grant the user permissions to restore their Amazon S3 buckets: s3:CreateBucket, s3:ListBucketVersions, s3:ListBucket, s3:GetBucketVersioning, s3:GetBucketLocation, and s3:PutBucketVersioning.</td>
<td>February 17, 2022</td>
</tr>
<tr>
<td>— Added new AWS Managed Policy to support Amazon S3 restore</td>
<td>AWS Backup added the following actions to grant the user permissions to restore their Amazon S3 buckets: s3:GetObject, s3:GetObjectVersion, s3:DeleteObject, s3:PutObjectVersionAcl, s3:GetObjectVersionAcl, s3:GetObjectTagging, s3:PutObjectTagging, s3:GetObjectAcl, s3:PutObjectAcl, and s3:ListMultipartUploadParts.</td>
<td></td>
</tr>
<tr>
<td>— Added new AWS Managed Policy to support Amazon S3 restore</td>
<td>AWS Backup needed those permissions for its support of Amazon S3 data.</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceLinkedRolePolicyForBackup</strong></td>
<td>AWS Backup added s3:ListAllMyBuckets to grant the user permissions to view a list of their buckets and choose which ones to assign to a backup plan.</td>
<td>February 14, 2022</td>
</tr>
<tr>
<td>— Added permission to support Amazon S3 backup</td>
<td>AWS Backup needed that permission for its support of Amazon S3 data.</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>AWSBackupServiceLinkedRolePolicyForBackup</td>
<td>— Added permission to list AWS Backup Gateway resources</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added backup-gateway:ListVirtualMachines to grant the user permissions to view a list of their virtual machines and choose which ones to assign to a backup plan. AWS Backup also added backup-gateway:ListTagsForResource to grant the user permissions to list the tags for their virtual machines. AWS Backup needed these permission for its support of virtual machines, which launched November 30, 2021.</td>
<td></td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForBackup</td>
<td>— Added permissions to back up virtual machines</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added backup-gateway:Backup to grant the user permissions restore their virtual machine backups. AWS Backup also added backup-gateway:ListTagsForResource to grant the user permissions to list the tags assigned to their virtual machine backups. AWS Backup needed this permission for its support of virtual machines, which launched November 30, 2021.</td>
<td></td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForRestores</td>
<td>— Added permission to restore virtual machines</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td></td>
<td>AWS Backup added backup-gateway:Restore to grant the user permissions restore their virtual machine backups. AWS Backup needed this permission for its support of virtual machines, which launched November 30, 2021.</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>

AWS Backup needed this permission for its support of AWS Backup Gateway, which launched November 30, 2021.
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AWSBackupOperatorAccess</strong> — Added permission to list AWS Backup Gateway resources</td>
<td>AWS Backup added the following actions to grant the user permissions to back up their virtual machines: <code>backup-gateway:ListGateways</code>, <code>backup-gateway:ListHypervisors</code>, <code>backup-gateway:ListTagsForResource</code>, and <code>backup-gateway:ListVirtualMachines</code>. AWS Backup needed this permission for its support of virtual machines, which launched November 30, 2021.</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td><strong>AWSBackupServiceLinkedRolePolicyForBackup</strong> — Added permission to back up Amazon DynamoDB tables</td>
<td>AWS Backup added <code>dynamodb:ListTagsOfResource</code> to grant the user permissions to list tags of their DynamoDB tables to back up using AWS Backup's advanced DynamoDB backup features. AWS Backup needed this permission for its advanced DynamoDB backup features, which launched November 23, 2021.</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForBackup</strong> — Added permissions to back up Amazon DynamoDB tables</td>
<td>AWS Backup added <code>dynamodb:StartAwsBackupJob</code> to grant the user permissions to back up their DynamoDB tables using advanced backup features. AWS Backup also added <code>dynamodb:ListTagsOfResource</code> to grant the user to permissions to copy tags from their source DynamoDB tables to their backups. AWS Backup needed these permission for its advanced DynamoDB backup features, which launched November 23, 2021.</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>AWSBackupServiceLinkedRolePolicyForRestores</td>
<td>— Added permissions to restore Amazon DynamoDB tables</td>
<td>November 23, 2021</td>
</tr>
</tbody>
</table>

AWS Backup added `dynamodb:RestoreTableFromAwsBackup` to grant the user permissions to restore their DynamoDB tables backed up using AWS Backup's advanced DynamoDB advanced backup features.

AWS Backup needed this permission to restore backups created using AWS Backup's advanced DynamoDB features, which launched November 23, 2021.

| AWSBackupServiceRolePolicyForRestores | — Added permissions to restore Amazon DynamoDB tables | November 23, 2021 |

AWS Backup added `dynamodb:RestoreTableFrom AwsBackup` to grant the user permissions to restore their DynamoDB tables backed up using AWS Backup's advanced DynamoDB advanced backup features.

AWS Backup needed this permission to restore backups created using AWS Backup's advanced DynamoDB features, which launched November 23, 2021.

| AWSBackupOperatorAccess | — Removed redundant actions | November 23, 2021 |

AWS Backup removed the existing actions `backup:GetRecoveryPointRestoreMetadata` and `rds:DescribeDBSnapshots` because they were redundant.

AWS Backup did not need both `backup:GetRecoveryPointRestoreMetadata` and `backup:Get*` as part of the AWSBackupOperatorAccess AWS Managed Policy. Also, AWS Backup did not need both `rds:DescribeDBSnapshots` and `rds:describeDBSnapshots` as part of the AWSBackupOperatorAccess AWS Managed Policy.
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWSBackupServiceLinkedRolePolicyForBackup</td>
<td>AWS Backup added the new actions elasticfilesystem:DescribeFileSystems, dynamodb:ListTables, storagegateway:ListVolumes, ec2:DescribeVolumes, ec2:DescribeInstances, rds:DescribeDBInstances, rds:DescribeDBClusters, and fsx:DescribeFileSystems to allow customers to view and choose from a list of their AWS Backup-supported resources when selecting which resources to assign to a backup plan. AWS Backup needed these permissions to give customers additional, flexible ways to assign their resources to their backup plans.</td>
<td>November 10, 2021</td>
</tr>
<tr>
<td>AWSBackupAuditAccess</td>
<td>AWS Backup added AWSBackupAuditAccess to grant the user permissions to use AWS Backup Audit Manager. Permissions include the ability to configure compliance frameworks and generate reports. AWS Backup needed this permission for AWS Backup Audit Manager, which launched August 24, 2021.</td>
<td>August 24, 2021</td>
</tr>
<tr>
<td>AWSServiceRolePolicyForBackupReports</td>
<td>AWS Backup added AWSServiceRolePolicyForBackupReports to grant permissions for a service-linked role to automate the monitoring of backup settings, jobs, and resources for compliance with frameworks configured by the user. AWS Backup needed this permission for AWS Backup Audit Manager, which launched August 24, 2021.</td>
<td>August 24, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>AWSBackupFullAccess — Added permission to</td>
<td>AWS Backup added iam:CreateServiceLinkedRole to create a service-linked role (on a best-effort basis) to automate the deletion of expired recovery points for you. Without this service-linked role, AWS Backup cannot delete expired recovery points after customers delete the original IAM role they used to create their recovery points. AWS Backup needed this permission as part of the DeleteRecoveryPoint API operation.</td>
<td>July 5, 2021</td>
</tr>
<tr>
<td>create service-linked role</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWSBackupServiceLinkedRolePolicy — Added</td>
<td>AWS Backup added the new action dynamodb:DeleteBackup to grant DeleteRecoveryPoint permission to automate the deletion of expired DynamoDB recovery points based on your backup plan lifecycle settings. AWS Backup needed this permission to delete DynamoDB tables as part of the DeleteRecoveryPoint API operation.</td>
<td>July 5, 2021</td>
</tr>
<tr>
<td>permission to support deletion of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DynamoDB recovery points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWSBackupOperatorAccess — Removed redundant</td>
<td>AWS Backup removed the existing actions backup:GetRecoveryPointRestoreMetadata and rds:DescribeDBSnapshots because they were redundant. AWS Backup did not need both backup:GetRecoveryPointRestoreMetadata and backup:Get* as part of the AWSBackupOperatorAccess AWS Managed Policy. Also, AWS Backup did not need both rds:DescribeDBSnapshots and rds:describeDBSnapshots as part of the AWSBackupOperatorAccess AWS Managed Policy.</td>
<td>May 25, 2021</td>
</tr>
<tr>
<td>actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>AWSBackupOperatorPolicy</strong> — Removed redundant actions</td>
<td>AWS Backup removed the existing actions backup:GetRecoveryPointRestoreMetadata and rds:DescribeDBSnapshots because they were redundant. AWS Backup did not need both backup:GetRecoveryPointRestoreMetadata and backup:Get* as part of the AWSBackupOperatorPolicy AWS Managed Policy. Also, AWS Backup did not need both rds:DescribeDBSnapshots and rds:describeDBSnapshots as part of the AWSBackupOperatorPolicy AWS Managed Policy.</td>
<td>May 25, 2021</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong> — Added permission to apply tags to Amazon FSx restores</td>
<td>AWS Backup added the new action fsx:TagResource to grant StartRestoreJob permission to allow you to apply tags to Amazon FSx file systems during the restore process. AWS Backup needed this permission to apply tags to Amazon FSx file systems as part of the StartRestoreJob API operation.</td>
<td>May 24, 2021</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForRestores</strong> — Added permission to perform Amazon EC2 restores</td>
<td>AWS Backup added the new actions ec2:DescribeImages and ec2:DescribeInstances to grant StartRestoreJob permission to allow you to restore Amazon EC2 instances from recovery points. AWS Backup needed this permission to restore Amazon EC2 instances from recovery points as part of the StartRestoreJob API operation.</td>
<td>May 24, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForBackup</strong></td>
<td>Added permission to perform Amazon FSx cross-Region and cross-account copies</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceLinkedRolePolicyForBackup</strong></td>
<td>Added permission to perform Amazon FSx cross-Region and cross-account copies</td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupServiceRolePolicyForBackup</strong></td>
<td>Added permissions to support encrypted DynamoDB table backup</td>
<td>March 10, 2021</td>
</tr>
</tbody>
</table>

AWS Backup added the new action `fsx:CopyBackup` to grant `StartCopyJob` permission to allow you to copy Amazon FSx recovery points across Regions and accounts.

AWS Backup needed this permission to copy Amazon FSx recovery points across Regions and accounts as part of the `StartCopyJob` API operation.

AWS Backup updated its AWS managed policies to comply with the following requirement:

For AWS Backup to create a backup of an encrypted DynamoDB table, you must add the permissions `kms:Decrypt` and `kms:GenerateDataKey` to the IAM role used for backup.
Using service-linked roles for AWS Backup

AWS Backup uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Backup. Service-linked roles are predefined by AWS Backup and include all the permissions that the service requires to call other AWS services on your behalf.

Topics

- Using roles to list resources to back up, copy across accounts, and automatically backup Amazon EFS (p. 333)
- Using roles for AWS Backup Audit Manager (p. 335)

Using roles to list resources to back up, copy across accounts, and automatically backup Amazon EFS

AWS Backup uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Backup. Service-linked roles are predefined by AWS Backup and include all the permissions that the service requires to call other AWS services on your behalf.
A service-linked role makes setting up AWS Backup easier because you don’t have to manually add the necessary permissions. AWS Backup defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Backup can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting its related resources. This protects your AWS Backup resources because you can’t inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have Yes in the Service-Linked Role column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-linked role permissions for AWS Backup

AWS Backup uses the service-linked role named AWSServiceRoleForBackup – Provides AWS Backup permissions to list resources you can back up, copy backups across accounts, and automatically backup Amazon EFS.

The AWSServiceRoleForBackup service-linked role trusts the following services to assume the role:

- AWS Backup

The role permissions policy allows AWS Backup to complete the following actions on the specified resources:

- Action: list, read, write, and tag on all resources AWS Backup supports

See the policy AWSBackupServiceLinkedRolePolicyForBackup in the AWS Identity and Access Management console for specific permissions.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a service-linked role for AWS Backup

You don’t need to manually create a service-linked role. When you list resources to back up, set up cross-account backup, or perform Amazon EFS automatic backup in the AWS Management Console, the AWS CLI, or the AWS API, AWS Backup creates the service-linked role for you.

Important

This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. To learn more, see A New Role Appeared in My IAM Account.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you list resources to back up, set up cross-account backup, or perform Amazon EFS automatic backup, AWS Backup creates the service-linked role for you again.

Editing a service-linked role for AWS Backup

AWS Backup does not allow you to edit the AWSServiceRoleForBackup service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the IAM User Guide.
Deleting a service-linked role for AWS Backup

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role. First, you must delete all your recovery points. Then, you must delete all your backup vaults.

Note
If the AWS Backup service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes, then try the operation again.

To delete AWS Backup resources used by the AWSServiceRoleForBackup (console)

1. To delete all your recovery points and backup vaults (except for your default vault), follow the procedure in Deleting a backup vault.
2. To delete your default vault, use the following command in the AWS CLI:

   ```sh
   aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
   ```

To delete AWS Backup resources used by the AWSServiceRoleForBackup (AWS CLI)

1. To delete all your recovery points, use `delete-recovery-point`.
2. To delete all your backup vaults, use `delete-backup-vault`.

To delete AWS Backup resources used by the AWSServiceRoleForBackup (API)

1. To delete all your recovery points, use `DeleteRecoveryPoint`.
2. To delete all your backup vaults, use `DeleteBackupVault`.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForBackup service-linked role. For more information, see Deleting a Service-Linked Role in the IAM User Guide.

Supported Regions for AWS Backup service-linked roles

AWS Backup supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Backup supported features and Regions.

Using roles for AWS Backup Audit Manager

AWS Backup uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Backup. Service-linked roles are predefined by AWS Backup and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up AWS Backup easier because you don't have to manually add the necessary permissions. AWS Backup defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Backup can assume its roles. The defined permissions include the trust...
policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting its related resources. This protects your AWS Backup resources because you can’t inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have Yes in the Service-Linked Role column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-linked role permissions for AWS Backup

AWS Backup uses the service-linked role named AWSServiceRoleForBackupReports – Provides AWS Backup with permission to create controls, frameworks, and reports.

The AWSServiceRoleForBackupReports service-linked role trusts the following services to assume the role:

• AWS Backup

The role permissions policy allows AWS Backup to complete the following actions on the specified resources:

• Action: list, read, and write on all resources AWS Backup supports.

See the policy AWSServiceRolePolicyForBackupReports in the AWS Identity and Access Management console for a list of specific permissions.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a service-linked role for AWS Backup

You don’t need to manually create a service-linked role. When you create a framework or a report plan in the AWS Management Console, the AWS CLI, or the AWS API, AWS Backup creates the service-linked role for you.

Important

This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. To learn more, see A New Role Appeared in My IAM Account.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a framework or a report plan, AWS Backup creates the service-linked role for you again.

Editing a service-linked role for AWS Backup

AWS Backup does not allow you to edit the AWSServiceRoleForBackupReports service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the IAM User Guide.

Deleting a service-linked role for AWS Backup

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don’t have an unused entity that is not actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.
Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role. You must delete all frameworks and report plans.

**Note**
If the AWS Backup service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes, then try the operation again.

**To delete AWS Backup resources used by the AWSServiceRoleForBackupReports (console)**

1. To delete all frameworks, see Deleting frameworks.
2. To delete all report plans, see Deleting report plans.

**To delete AWS Backup resources used by the AWSServiceRoleForBackupReports (AWS CLI)**

1. To delete all frameworks, use delete-framework.
2. To delete all report plans, use delete-report-plan.

**To delete AWS Backup resources used by the AWSServiceRoleForBackupReports (API)**

1. To delete all frameworks, use DeleteFramework.
2. To delete all report plans, use DeleteReportPlan.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForBackupReports service-linked role. For more information, see Deleting a Service-Linked Role in the IAM User Guide.

**Supported Regions for AWS Backup service-linked roles**

AWS Backup supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Backup supported features and Regions.

### Compliance validation for AWS Backup

Third-party auditors assess the security and compliance of AWS Backup as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact in the AWS Artifact User Guide.

Your compliance responsibility when using AWS Backup is determined by the sensitivity of your data, your organization's compliance objectives, and applicable laws and regulations. If your use of AWS Backup is subject to compliance with standards like HIPAA, PCI, or FedRAMP, AWS provides resources to help:

- **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- **Architecting for HIPAA Security and Compliance Whitepaper** – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
Resilience in AWS Backup

AWS Backup takes its resilience — and your data security — extremely seriously.

AWS Backup stores your backups with at least as much resilience and durability as your resource’s original AWS service would give you, if you backed it up there.

AWS Backup is designed to use the AWS global infrastructure to replicate your backups across multiple Availability Zones for durability of 99.999999999% (11 nines) in any given year, provided that you adhere to the current AWS Backup documentation.

AWS Backup encrypts your backup plans at rest and continuously backs them up. You can also restrict access to your backup plans using AWS Identity and Access Management (IAM) credentials and policies. For more information, see Authentication, Access Control, and Security Best Practices in IAM.

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. AWS Backup stores your backups across Availability Zones. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures. For more information, see AWS Backup Service Level Agreement (SLA).

Furthermore, AWS Backup empowers you to copy your backups across Regions for even greater resilience. For more information about the AWS Backup cross-Region copy feature, see Creating a Backup Copy.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in AWS Backup

As a managed service, AWS Backup is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access AWS Backup through the network. Clients must support Transport Layer Security (TLS) 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

AWS PrivateLink

AWS PrivateLink allows you to establish a private connection between your Virtual Private Cloud ("VPC") and AWS Backup endpoints by creating an interface VPC endpoint. Interface endpoints are powered by
AWS PrivateLink, a technology that enables you to privately access AWS Backup APIs by restricting all network traffic between your VPC and AWS Backup to the Amazon network.

AWS PrivateLink enables you to privately access AWS Backup operations without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with AWS Backup API endpoints. Your instances also don't need public IP addresses to use any of the available AWS Backup API and Backup gateway API operations. Traffic between your VPC and AWS Backup doesn't leave the Amazon network.

For more information about VPC endpoints, see Interface VPC endpoints (AWS PrivateLink) in the Amazon VPC User Guide.

Considerations for Amazon VPC endpoints

Before you set up an interface VPC endpoint for AWS Backup endpoints, review Interface endpoint properties and limitations in the Amazon VPC User Guide.

All AWS Backup operations relevant to managing Amazon Backup resources are available from your VPC using AWS PrivateLink.

VPC endpoint policies are supported for Backup endpoints. By default, full access to Backup operations is allowed through the endpoint. For more information, see Controlling access to services with VPC endpoints in the Amazon VPC User Guide.

Creating an AWS Backup VPC endpoint

You can create a VPC endpoint for AWS Backup using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Creating an interface endpoint in the Amazon VPC User Guide.

Create a VPC endpoint for AWS Backup using the service name com.amazonaws.region.backup.

In China (Beijing) Region and China (Ningxia) Region, the service name should be cn.com.amazonaws.region.backup.

For Backup gateway endpoints, use com.amazonaws.region.backup-gateway.

The following TCP ports must be allowed in the security group when creating a VPC endpoint for backup gateway:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Using a VPC endpoint

If you enable private DNS for the endpoint, you can make API requests to AWS Backup with the VPC endpoint using its default DNS name for the AWS Region, for example backup.us-east-1.amazonaws.com.

However, for the China (Beijing) Region and China (Ningxia) Region AWS Regions, API requests should be made with the VPC endpoint using backup.cn-north-1.amazonaws.com.cn and backup.cn-northwest-1.amazonaws.com.cn, respectively.
Creating a VPC endpoint policy

You can attach an endpoint policy to your VPC endpoint that controls access to the Amazon Backup API. The policy specifies:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

**Important**

When a non-default policy is applied to an interface VPC endpoint for AWS Backup, certain failed API requests, such as those failing from RequestLimitExceeded, might not be logged to AWS CloudTrail or Amazon CloudWatch.

For more information, see [Controlling access to services with VPC endpoints](https://docs.aws.amazon.com/vpc/latest/userguide/controlling-access.html) in the Amazon VPC User Guide.

**Example: VPC endpoint policy for AWS Backup actions**

The following is an example of an endpoint policy for AWS Backup. When attached to an endpoint, this policy grants access to the listed AWS Backup actions for all principles on all resources.

```json
{
   "Statement": [
      {
         "Action": "backup:*",
         "Effect": "Allow",
         "Principal": "*",
         "Resource": "*"
      }
   ]
}
```

**Example: VPC endpoint policy that denies all access from a specified AWS account**

The following VPC endpoint policy denies AWS account 123456789012 all access to resources using the endpoint. The policy allows all actions from other accounts.

```json
{
   "Id": "Policy1645236617225",
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Stmt1645236612384",
         "Action": "backup:*",
         "Effect": "Deny",
         "Resource": "*",
         "Principal": {
            "AWS": [
               "123456789012"
            ]
         }
      }
   ]
}
```
Availability AWS Backup currently supports VPC endpoints in the following AWS Regions:

- US East (Ohio) Region
- US East (N. Virginia) Region
- US West (Oregon) Region
- US West (N. California) Region
- Africa (Cape Town) Region
- Asia Pacific (Hong Kong) Region
- Asia Pacific (Mumbai) Region
- Asia Pacific (Osaka) Region
- Asia Pacific (Seoul) Region
- Asia Pacific (Singapore) Region
- Asia Pacific (Sydney) Region
- Asia Pacific (Tokyo) Region
- Canada (Central) Region
- Europe (Frankfurt) Region
- Europe (Ireland) Region
- Europe (London) Region
- Europe (Paris) Region
- Europe (Stockholm) Region
- Europe (Milan) Region
- Middle East (Bahrain) Region
- South America (São Paulo) Region
- Asia Pacific (Jakarta) Region
- Asia Pacific (Osaka) Region
- China (Beijing) Region
- China (Ningxia) Region
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

**Note**
AWS Backup for VMware is not available in China Regions (China (Beijing) Region and China (Ningxia) Region) or Asia Pacific (Jakarta) Region.
The following quotas apply when working with AWS Backup. Many AWS Backup quotas are adjustable if allowed by the resource type service. To request a quota adjustment, describe your use case to AWS Support.

### AWS Backup quotas

<table>
<thead>
<tr>
<th>Resource</th>
<th>Quota</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of backup vaults per Region per account</td>
<td>300</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of recovery points per backup vault</td>
<td>1,000,000</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of backup plans per Region per account</td>
<td>300</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of versions per backup plan</td>
<td>2,000</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of resource assignments per backup plan</td>
<td>100</td>
<td>You cannot request an adjustment.</td>
</tr>
<tr>
<td>Number of active backup jobs per account</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>Number of concurrent backup copies per account outbound to a destination Region</td>
<td>100</td>
<td>You can request an adjustment for certain resources (currently virtual machines, Advanced DynamoDB, Timestream, Amazon EFS and SAP HANA databases on Amazon EC2 instances)</td>
</tr>
<tr>
<td>Number of concurrent copies per destination backup vault in account after the limit (entry above) has been reached</td>
<td>5</td>
<td>You cannot request an adjustment.</td>
</tr>
<tr>
<td>Number of concurrent cross-account copies that can be made of the same resource to the same destination Region</td>
<td>30</td>
<td>Not adjustable.</td>
</tr>
<tr>
<td>Number of concurrent backup and copy jobs per resource</td>
<td>1</td>
<td>You cannot request an adjustment.</td>
</tr>
<tr>
<td>Number of metadata tags per backup</td>
<td>50</td>
<td>You cannot request an adjustment. AWS imposes this quota across all resources. See Tag naming limits and requirements in the AWS General Reference.</td>
</tr>
</tbody>
</table>

See Tag naming limits and requirements in the AWS General Reference.
<table>
<thead>
<tr>
<th>Resource</th>
<th>Quota</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of hypervisors</td>
<td>10</td>
<td>You cannot request an adjustment.</td>
</tr>
<tr>
<td>Number of legal holds</td>
<td>50 per accounts</td>
<td></td>
</tr>
</tbody>
</table>

**AWS Backup of Amazon Timestream resource quotas**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Quota</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of concurrent Timestream backup jobs per account</td>
<td>4</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of concurrent Timestream restore jobs per account</td>
<td>1</td>
<td>You can request an adjustment.</td>
</tr>
</tbody>
</table>

There are quotas on a single resource assignment in a single backup rule. You can create a backup plan with multiple backup rules.

**AWS Backup Audit Manager quotas**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Quota</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of frameworks per account per Region</td>
<td>10</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of controls per account per Region</td>
<td>50</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of report plans per account</td>
<td>20</td>
<td>You can request an adjustment.</td>
</tr>
<tr>
<td>Number of frameworks per report plan</td>
<td>1,000</td>
<td>You cannot request an adjustment.</td>
</tr>
<tr>
<td>Maximum number of accounts multiplied by Regions in a report plan</td>
<td>300</td>
<td>You cannot request an adjustment.</td>
</tr>
</tbody>
</table>

**AWS Backup gateway quotas**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Quota</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup or restore jobs per gateway</td>
<td>4</td>
<td>You cannot request an adjustment. Instead, create more gateways and connect them to your hypervisor.</td>
</tr>
</tbody>
</table>

When you manage backups across multiple accounts using AWS Organizations, you might encounter quotas that AWS Organizations imposes. For these quotas, see Quotas for AWS Organizations in the AWS Organizations User Guide.

You might also encounter quotas imposed by a AWS Backup-supported service, including:
• Amazon Elastic File System
• Amazon Elastic Block Store
• Amazon RDS
• Amazon Aurora
• Amazon EC2
• AWS Storage Gateway
• Amazon DynamoDB
• Amazon FSx for Lustre
• Amazon FSx for Windows File Server
• Amazon DocumentDB
• Amazon Neptune
• Amazon Simple Storage Service
• Amazon Timestream
Monitoring

AWS Backup works with other AWS tools to empower you to monitor its workloads. These tools include the following:

- Use **Amazon CloudWatch** and **Amazon EventBridge** to monitor AWS Backup processes.
  - You can use CloudWatch to track metrics, create alarms, and view dashboards.
  - You can use EventBridge to view and monitor AWS Backup events.

  For more information, see Monitoring AWS Backup events using EventBridge (p. 345) and AWS Backup metrics with Amazon CloudWatch (p. 367).

- Use **AWS CloudTrail** to monitor AWS Backup API calls. You can identify the time, source IP, users, and accounts making those calls. For more information, see Logging AWS Backup API calls with CloudTrail (p. 370).

- Use **Amazon Simple Notification Service** (Amazon SNS) to subscribe to AWS Backup-related topics such as backup, restore, and copy events. For more information, see Notification options with AWS Backup (p. 376).

---

**Monitoring AWS Backup events using EventBridge**

**Topics**

- Monitor events using EventBridge (p. 345)
- Differences with the AWS Backup notification API (p. 367)

**Monitor events using EventBridge**

You can use EventBridge to monitor AWS Backup events. A common use case is to receive an alarm when a backup job fails. AWS Backup emits events to EventBridge in a best-effort manner every 5 minutes.

The purpose of this documentation page is to provide you with the reference materials to use EventBridge to monitor AWS Backup. For how to track events using EventBridge, see Configure AWS Backup events to send to EventBridge at the halfway mark of blog Amazon CloudWatch Events and Metrics for AWS Backup or Creating a rule for an AWS service in the Amazon EventBridge User Guide.

**Note**

Some events report status: COMPLETED whereas other events report state: COMPLETED. This is consistent with the AWS Backup API.

You can track the following AWS Backup-related events in EventBridge.

<table>
<thead>
<tr>
<th>Event type</th>
<th>States</th>
<th>Event details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Job State Change</td>
<td>ABORTED, EXPIRED, RUNNING, PENDING</td>
<td>accountId, resources: recoveryPointArn, details, backupJobId, backupSizeInBytes, backupVaultName, backupVaultArn, bytesTransferred, completionDate, expectedCompletionDate, iAmRoleArn, percentDone,</td>
</tr>
<tr>
<td>Event type</td>
<td>States</td>
<td>Event details</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>resourceArn, resourceType, startBy, state, statusMessage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createdBy: backupPlanArn, createdBy: backupPlanId, createdBy: backupPlanVersion, createdBy: backupRuleId</td>
</tr>
<tr>
<td>Backup Job State Change</td>
<td>COMPLETED, FAILED</td>
<td>accountId, resources: recoveryPointArn, details, backupJobId, backupSizeInBytes, backupVaultName, backupVaultArn, bytesTransferred, completionDate, expectedCompletionDate, iAmRoleArn, percentDone, retryCount, resourceArn, resourceType, startBy, state, statusMessage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createdBy: backupPlanArn, createdBy: backupPlanId, createdBy: backupPlanVersion, createdBy: backupRuleId</td>
</tr>
<tr>
<td></td>
<td>CREATED</td>
<td>accountId, resources: recoveryPointArn, details, backupJobId, state, creationDate</td>
</tr>
<tr>
<td>Copy Job State Change</td>
<td>COMPLETED, FAILED, RUNNING</td>
<td>accountId, resources: recoveryPointArn, details, backupSizeInBytes, completionDate, copyJobId, creationDate, destinationBackupVaultArn, destinationRecoveryPointArn, iAmRoleArn, resourceArn, resourceType, state, statusMessage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createdBy: backupPlanArn, createdBy: backupPlanId, createdBy: backupPlanVersion, createdBy: backupRuleId</td>
</tr>
<tr>
<td></td>
<td>CREATED</td>
<td>accountId, resources: recoveryPointArn, details, state, creationDate, sourceBackupVaultArn, destinationBackupVaultArn</td>
</tr>
<tr>
<td>Restore Job State Change</td>
<td>CREATED, COMPLETED, FAILED, PENDING, RUNNING, STOPPED</td>
<td>accountId, resources: recoveryPointArn, details, state, creationDate, restoreJobId</td>
</tr>
</tbody>
</table>
### Event type | States | Event details
---|---|---
Recovery Point State Change | COMPLETED, PARTIAL, EXPIRED | accountId, resources: recoveryPointArn, resources: backupVaultArn, details, backupSizeInBytes, backupVaultName, calculatedLifecycle: deleteAt, calculatedLifecycle: moveToColdStorageAt, completionDate, creationDate, encryptionKeyArn, iAmRoleArn, isEncrypted, lastRestoreTime, lifecycle: deleteAfterDays, lifecycle: moveToColdStorageAfterDays, resourceArn, resourceType, status, storageClass, createdBy: backupPlanArn, createdBy: backupPlanId, createdBy: backupPlanVersion, createdBy: backupRuleId
Recovery Point State Change | FAILED, COMPLETED, RUNNING, ABORTED, PENDING | accountId, resources: recoveryPointArn, details, backupSizeInBytes, completionDate, createdResourceArn, creationDate, expectedCompletionTimeMinutes, iAmRoleArn, percentDone, restoreJobId, status, statusMessage
Recovery Point State Change | MODIFIED, DELETED | accountId, resources: recoveryPointArn, resources: backupVaultArn, details, lifecycle, calculatedLifecycle, state
Backup Vault State Change | CREATED, DELETED, MODIFIED | accountId, resources: backupVaultArn, details, backupVaultName, state
Region Settings State Change | MODIFIED | accountId, details, modifiedAt, state, resourceTypeOptInPreference
Backup Plan State Change | CREATED, DELETED, MODIFIED | accountId, resources: backupPlanArn, details, backupPlanId, versionId, creationDate, deletionDate

Use these sample JSON payloads if you would like to use these events programmatically.

### Event state | JSON payload
---|---
Backup Job: FAILED | {  

### Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;version&quot;: &quot;0&quot;,</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;710b0398-d48e-f3c3-afca-cfeb2fdaa656&quot;,</td>
</tr>
<tr>
<td>&quot;detail-type&quot;: &quot;Backup Job State Change&quot;,</td>
</tr>
<tr>
<td>&quot;source&quot;: &quot;aws.backup&quot;,</td>
</tr>
<tr>
<td>&quot;account&quot;: &quot;111233445566&quot;,</td>
</tr>
<tr>
<td>&quot;time&quot;: &quot;2020-07-29T20:15:26Z&quot;,</td>
</tr>
<tr>
<td>&quot;region&quot;: &quot;us-east-1&quot;,</td>
</tr>
<tr>
<td>&quot;resources&quot;: [],</td>
</tr>
<tr>
<td>&quot;detail&quot;: {</td>
</tr>
<tr>
<td>&quot;backupJobId&quot;: &quot;34176239-e96d-4e1d-9fad-cfeb2fdaa656&quot;,</td>
</tr>
<tr>
<td>&quot;backupVaultName&quot;: &quot;9ab3e749-82c6-4342-9320-5edbf4918b86_beta&quot;,</td>
</tr>
<tr>
<td>&quot;bytesTransferred&quot;: &quot;0&quot;,</td>
</tr>
<tr>
<td>&quot;creationDate&quot;: &quot;2020-07-29T20:13:07.392Z&quot;,</td>
</tr>
<tr>
<td>&quot;iamRoleArn&quot;:</td>
</tr>
<tr>
<td>&quot;arn:aws:iam::111233445566:role/MockRCBackupIntegTestRole&quot;,</td>
</tr>
<tr>
<td>&quot;resourceType&quot;: &quot;CryoTestClient&quot;,</td>
</tr>
<tr>
<td>&quot;state&quot;: &quot;FAILED&quot;,</td>
</tr>
<tr>
<td>&quot;statusMessage&quot;: &quot;Backup job failed because backup vault arn:aws:backup:us-west-2:111233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86_beta does not exist.&quot;,</td>
</tr>
<tr>
<td>&quot;startBy&quot;: &quot;2020-07-30T04:13:07.392Z&quot;,</td>
</tr>
<tr>
<td>&quot;percentDone&quot;: 0,</td>
</tr>
<tr>
<td>&quot;retryCount&quot;: 3</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>]</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>
Monitor events using EventBridge

<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Backup Job: COMPLETED | {
  "version": "0",
  "id": "d4d54a13f",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "111223445566",
  "time": "2020-07-15T21:41:17Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
    "backupSizeInBytes": "36048",
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a_beta",
    "bytesTransferred": "36048",
    "creationDate": "2020-07-15T21:40:31.207Z",
    "iamRoleArn": "arn:aws:iam::111223445566:role/MockRCBackupIntegTestRole",
    "resourceType": "CryoTestClient",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T21:40:31.207Z",
    "startBy": "2020-07-16T05:40:31.207Z",
    "percentDone": 100,
    "retryCount": 3
  }
}
<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Backup Job: RUNNING | ```json
{
  "version": "0",
  "id": "46946c39-b519-3505-44e6-ba74afeb2e30",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "111223344566",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
    "backupSizeInBytes": "3221225472",
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1d183b15_beta",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::111223344566:role/FullBackupIntegTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:111223344566:volume/vol-0b5ae24f2ee72d926",
    "resourceType": "EBS",
    "state": "RUNNING",
    "startBy": "2020-07-15T05:00:00Z",
    "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
    "percentDone": 99,
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeea-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:111223344566:backup-plan:bde0f455-4e24-4668-aeea-4932a97f5cc5_beta",
      "backupPlanVersion": "YTkzNmM0MmUtMWRlM0ZlNzUyY2RkLTJmZGUtNjA5NTc4NGM1YTI5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    }
  }
} ```
<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Backup Job: ABORTED | ```json
{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:33:16Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
    "backupVaultName": "f59bffcd-2538-4bbe-8343-1c60dae27c27_beta",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:33:00.803Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupIntegTestRole",
    "resourceType": "CryoTestClient",
    "state": "ABORTED",
    "statusMessage": "Backup job was stopped by user."
  }
}
```
### Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup Job: EXPIRED</strong></td>
</tr>
<tr>
<td>`{</td>
</tr>
</tbody>
</table>
|   "version": "0",
|   "id": "1d7bc04-6120-1145-13b9-49b0af465328",
|   "detail-type": "Backup Job State Change",
|   "source": "aws.backup",
|   "account": "111223445566",
|   "time": "2020-07-29T13:04:57Z",
|   "region": "us-east-1",
|   "resources": [],
|   "detail": { |
|     "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
|     "backupVaultName": "aws/backup/AutomatedBackupVaultDel2_beta",
|     "bytesTransferred": "0",
|     "creationDate": "2020-07-29T05:10:20.077Z",
|     "iamRoleArn": "arn:aws:iam::111223445566:role/MockRCBackupIntegTestRole",
|     "resourceType": "CryoTestClient",
|     "state": "EXPIRED",
|     "statusMessage": "Backup job failed because there was a running job for the same resource.",
|     "completionDate": "2020-07-29T13:02:15.234Z",
|     "startBy": "2020-07-29T13:00:00Z",
|     "percentDone": 0,
|     "createdBy": { |
|       "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
|       "backupPlanVersion": "NjBjOTUzZjYtYzZ1N00NjhlLWIzMTExNjOWY2Nj2Vj",
|       "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11d2c"
|     } |
|   } |
| } |
| } |
### Event state

<table>
<thead>
<tr>
<th>Backup Job: PENDING</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON payload</td>
</tr>
<tr>
<td><img src="" alt="JSON payload" /></td>
</tr>
</tbody>
</table>

### Backup Job: CREATED

| JSON payload        |
| ![JSON payload](data:image/json;base64,iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAYAAAAfS9TAAAAA3NCSVQICAjb4U/gAAAACXBIWXMAAAsTAAALEwEAmpwYAAALoJREFUeNrs4TgIAwSEAAzEzBiRQIAAAABJRU5ErkJggg==) |
### Event state

**Copy Job: FAILED**

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
</table>
| `
"version": "0",
"id": "4660bc92-a44d-c939-4542-cda503f14855",
"detail-type": "Copy Job State Change",
"source": "aws.backup",
"account": "1112233445566",
"time": "2020-07-15T20:37:34Z",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5",
],
"detail": {
  "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
  "backupSizeInBytes": 22548578304,
  "creationDate": "2020-07-15T20:36:13.239Z",
  "iamRoleArn": 
  "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
  "resourceArn": 
  "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515ae7de03f58e1",
  "resourceType": "EC2",
  "sourceBackupVaultArn": 
  "state": "FAILED",
  "statusMessage": "Access denied exception while trying to list tags",
  "completionDate": "2020-07-15T20:37:28.704Z",
  "destinationBackupVaultArn": 
  "destinationRecoveryPointArn": {}
}``
### Event state

**Copy Job: RUNNING**

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{</td>
</tr>
</tbody>
</table>
|     "version": "0",
|     "id": "d17480ae-7042-edb2-0f6b-8b9482dc5864",
|     "detail-type": "Copy Job State Change",
|     "source": "aws.backup",
|     "account": "111223344566",
|     "time": "2020-07-15T22:07:48Z",
|     "region": "us-east-1",
|     "resources": [ |
|         "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9" |
|     ],
|     "detail": { |
|         "copyJobId": "0175DE71-5784-589F-DBAC-541ACCB4AC8",
|         "backupSizeInBytes": 3221225472,
|         "creationDate": "2020-07-15T22:06:27.234Z",
|         "iamRoleArn": |
|             "arn:aws:iam::111223344566:role/OrganizationCanaryTestRole",
|         "resourceArn": |
|             "arn:aws:ec2:us-west-2:111223344566:volume/vol-050e8ba1ee4d5c001",
|         "resourceType": "EBS",
|         "sourceBackupVaultArn": |
|         "state": "RUNNING",
|         "destinationBackupVaultArn": |
|         "destinationRecoveryPointArn": {},
|         "createdBy": { |
|             "backupPlanId": "b58e3621-1c53-4997-ad8a-acf3347a850e",
|             "backupPlanArn": |
|             "backupPlanVersion": |
|                 "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWOQ4",
|             "backupPlanRuleId": |
|                 "78e356d3-1a11-4f61-8585-af56b69bb18" |
|         } |
|     } |
| } |
| } |
## Event state

**Copy Job: COMPLETED**

<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;version&quot;: &quot;0&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;id&quot;: &quot;47deb974-6473-aef1-56c2-52c3aedfceb&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;detail-type&quot;: &quot;Copy Job State Change&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;source&quot;: &quot;aws.backup&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;account&quot;: &quot;1112233445566&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;time&quot;: &quot;2020-07-15T22:08:04Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;region&quot;: &quot;us-east-1&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;resources&quot;: [</td>
</tr>
<tr>
<td></td>
<td>&quot;arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9&quot;</td>
</tr>
<tr>
<td></td>
<td>]</td>
</tr>
<tr>
<td></td>
<td>&quot;detail&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;copyJobId&quot;: &quot;0175DE71-5784-589FD8AC-541ACCCB4AC8&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupSizeInBytes&quot;: 3221225472,</td>
</tr>
<tr>
<td></td>
<td>&quot;creationDate&quot;: &quot;2020-07-15T22:06:27.234Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;iamRoleArn&quot;: &quot;arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;resourceArn&quot;: &quot;arn:aws:ec2:us-west-2::volume/vol-050eba21ee4d5c001&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;resourceType&quot;: &quot;EBS&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;state&quot;: &quot;COMPLETED&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;completionDate&quot;: &quot;2020-07-15T22:07:58.111Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;destinationRecoveryPointArn&quot;: &quot;arn:aws:ec2:us-west-2::snapshot/snap-0726fe70935586180&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;createdBy&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;backupPlanId&quot;: &quot;b58e3621-1c53-4997-ad8a-afc3347a850e&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupPlanVersion&quot;: &quot;Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOmNwY2IwMTYvMTYuNQ4&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupPlanRuleId&quot;: &quot;78e356d3-1a11-4f61-8585-af5d66b69bb18&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
### Event state

**Copy Job: CREATED**

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
</table>
| {  
|   "version": "0",  
|   "id": "8398a4c4-8fe8-2b49-a4b9-fd4fcd34a4e",  
|   "detail-type": "Copy Job State Change",  
|   "source": "aws.backup",  
|   "account": "111223445566",  
|   "time": "2020-06-22T21:06:32Z",  
|   "region": "us-east-1",  
|   "resources": [  
|     "arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"  
|   ],  
|   "detail": {  
|     "creationDate": "2020-06-22T21:06:25.754Z",  
|     "state": "CREATED",  
|     "destinationBackupVaultArn": "arn:aws:backup:us-west-2:111223445566:backup-vault:ef09da5a-21a6-461fa98f-857e9e621a17_beta"  
|   }  
| }  
|
### Event state

<table>
<thead>
<tr>
<th>Restore Job: FAILED</th>
</tr>
</thead>
</table>

### JSON payload

```json
{
  "version": "0",
  "id": "29605cc-6ad4-32f2-
  fb86-4e66c7aebe7",
  "detail-type": "Restore Job State
  Change",
  "source": "aws.backup",
  "account": "111233445566",
  "time": "2020-07-15T20:29Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-06b9894dfb1cf48"
  ],
  "detail": {
    "restoreJobId": "9B333A28-526B-01CD-4A77-9785A08922FD",
    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "iamRoleArn": "arn:aws:iam::111233445566:role/CanaryAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile
to an EC2 instance. Please restore using the backed up instance profile."
  }
}
```
## Event state

**Restore Job: RUNNING**

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
</table>
| `{  
  "version": "0",  
  "id": "6137a1f0-33f3-99ee-a01a-3d8b96fe2ad6",  
  "detail-type": "Restore Job State Change",  
  "source": "aws.backup",  
  "account": "1112233445566",  
  "time": "2020-07-29T20:26:06Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe679ca138cfad2c"  
  ],  
  "detail": {  
    "restoreJobId": "F143178C-A866-4782-3B19-BF776A1A790C",  
    "backupSizeInBytes": "3221225472",  
    "creationDate": "2020-07-29T20:26:00.098Z",  
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",  
    "percentDone": 0,  
    "resourceType": "EBS",  
    "status": "RUNNING"  
  }  
}`
Monitor events using EventBridge

<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Restore Job: COMPLETED | ```
{
  "version": "0",
  "id": "8939bc73-dcf1-418c-9420-b9c5e097f0fb",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "111223345556",
  "time": "2020-07-15T03:14:58Z",
  "region": "us-east-1",
  "resources": ["arn:aws:rds:us-west-2:111223345556:snapshot:awsbackup:job-f2094617-4fe0-47e3-969e-a652d02b475"],
  "detail": {
    "restoreJobId": "EF332640-02A5-5978-693F-987970F09961",
    "backupSizeInBytes": "0",
    "creationDate": "2020-07-15T03:10:01.742Z",
    "iamRoleArn": "arn:aws:iam::111223345556:role/CanaryAWSBackupRole",
    "percentDone": 0,
    "resourceType": "RDS",
    "status": "COMPLETED",
    "completionDate": "2020-07-15T03:14:53.128Z"
  }
}
```
<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Job: PENDING</td>
<td>{&quot;version&quot;: &quot;0&quot;, &quot;id&quot;: &quot;0586085f-3079-cd79-10b7-908d3c3a2lea&quot;, &quot;detail-type&quot;: &quot;Restore Job State Change&quot;, &quot;source&quot;: &quot;aws.backup&quot;, &quot;account&quot;: &quot;1112233445566&quot;, &quot;time&quot;: &quot;2020-07-29T00:26Z&quot;, &quot;region&quot;: &quot;us-east-1&quot;, &quot;resources&quot;: [&quot;arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-b29f4ed6b7b1_beta&quot;], &quot;detail&quot;: {&quot;restoreJobId&quot;: &quot;EB9CE5CB-2892-8866-FD16-9829F4DAAD07&quot;, &quot;backupSizeInBytes&quot;: &quot;36048&quot;, &quot;creationDate&quot;: &quot;2020-07-29T00:21.083Z&quot;, &quot;iamRoleArn&quot;: &quot;arn:aws:iam::1112233445566:role/MockRCBackupIntegTestRole&quot;, &quot;percentDone&quot;: 0, &quot;resourceType&quot;: &quot;CryoTestClient&quot;, &quot;status&quot;: &quot;PENDING&quot;}}</td>
</tr>
<tr>
<td>Restore Job: CREATED</td>
<td>{&quot;version&quot;: &quot;0&quot;, &quot;id&quot;: &quot;af32977e-378f-2122-f985-fca4596f0709&quot;, &quot;detail-type&quot;: &quot;Restore Job State Change&quot;, &quot;source&quot;: &quot;aws.backup&quot;, &quot;account&quot;: &quot;1112233445566&quot;, &quot;time&quot;: &quot;2020-06-22T00:25Z&quot;, &quot;region&quot;: &quot;us-east-1&quot;, &quot;resources&quot;: [&quot;arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-b29f4ed6b7b1_beta&quot;], &quot;detail&quot;: {&quot;restoreJobId&quot;: &quot;EB9CE5CB-2892-8866-FD16-9829F4DAAD07&quot;, &quot;backupSizeInBytes&quot;: &quot;36048&quot;, &quot;creationDate&quot;: &quot;2020-06-22T00:21.083Z&quot;, &quot;iamRoleArn&quot;: &quot;arn:aws:iam::1112233445566:role/MockRCBackupIntegTestRole&quot;, &quot;percentDone&quot;: 0, &quot;resourceType&quot;: &quot;CryoTestClient&quot;, &quot;status&quot;: &quot;PENDING&quot;}}</td>
</tr>
</tbody>
</table>
## Event state

### Recovery Point: COMPLETED

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
</tr>
</tbody>
</table>
|   "version": "0",
|   "id": "ec6f75cc-989c-faaf-a642-dd0f1c95bff0",
|   "detail-type": "Recovery Point Change",
|   "source": "aws.backup",
|   "account": "1112233445566",
|   "time": "2020-07-15T21:39:07Z",
|   "region": "us-east-1",
|   "resources": [          |
|     "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-d60e-00c2-5c3b-49960142d03b"
|   ],                     |
|   "detail": {            |
|     "backupVaultName":  |
|       "e6625738-0655-4aa9-bd37-6ec1dd183b15_beta",
|     "backupVaultArn":    |
|     "creationDate":      |
|     "iamRoleArn":        |
|       "arn:aws:iam::1112233445566:role/FullBackupIntegTestRole",
|     "resourceType": "Aurora",
|     "resourceArn":       |
|       "arn:aws:rds:us-west-2:1112233445566:cluster:cryo-aurora-14029f40-b0b6-4a61-9fd2-9886f2771add",
|     "status": "COMPLETED",
|     "isEncrypted": "false",
|     "storageClass": "WARM",
|     "completionDate":    |
|       "2020-07-15T21:39:05.689Z",
|     "createdBy": {       |
|       "backupPlanId":    |
|       "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
|       "backupPlanArn":   |
|       "arn:aws:backup:us-west-2:1112233445566:backup-plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5_beta",
|       "backupPlanVersion": |
|       "YTkzNmM0MmhUtMWRhNS00Y2RkLThmZGUtNjAxNTc4NGM1YTa5",
|       "backupPlanRuleId": |
|       "1f97baFa-14d6-4f39-94fd-94b51bd6d0d5"
|     },                   |
|     "lifecycle": {       |
|       "deleteAfterDays": 100
|     },                   |
|     "calculatedLifeCycle": { |
|       "deleteAt":        |
|       "2020-10-23T21:38:31.152Z"    |
|     }                     |
|   }                      |
| }                         |
### Event state | JSON payload
--- | ---
Recovery Point: DELETED | 
{
"version": "0",
"id": "6089ee76-d856-0d7c-cee7-0a451cd43343",
"detail-type": "Recovery Point Change",
"source": "aws.backup",
"account": "111223345566",
"time": "2020-07-29T22:38:49Z",
"region": "us-east-1",
"resources": [
],
"detail": {
  "state": "DELETED",
  "lifecycle": {
    "deleteAfterDays": 300
  },
  "calculatedLifeCycle": {
    "deletedAt": "2021-05-25T22:29:02.452Z"
  }
}

Recovery Point: MODIFIED | 
{
"version": "0",
"id": "14365bb1-adef-bc00-lee3-8fac188d1996",
"detail-type": "Recovery Point Change",
"source": "aws.backup",
"account": "111223345566",
"time": "2020-07-02T23:33:57Z",
"region": "us-east-1",
"resources": [
],
"detail": {
  "calculatedLifeCycle": {
    "toColdStorageAfterDays": "Fri Dec 04 22:55:11 UTC 2020"
  },
  "state": "MODIFIED"
}
### Event state

#### JSON payload

**Backup Vault: CREATED**

```
{
    "version": "0",
    "id": "d415609e-5f35-d9a2-76d1-613685e4e024",
    "detail-type": "Backup Vault State Change",
    "source": "aws.backup",
    "account": "112233445566",
    "time": "2020-06-24T23:18:19Z",
    "region": "us-east-1",
    "resources": [
    ],
    "detail": {
        "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
        "state": "CREATED"
    }
}
```

**Backup Vault: MODIFIED**

```
{
    "version": "0",
    "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
    "detail-type": "Backup Vault State Change",
    "source": "aws.backup",
    "account": "112233445566",
    "time": "2020-06-24T23:18:19Z",
    "region": "Region",
    "resources": [
        "arn:aws:backup:Region:112233445566:backup-vault:[nameOfTestBackup]"
    ],
    "detail": {
        "backupVaultName": "[vaultName]",
        "state": "MODIFIED",
        "isLocked": 'true'
    }
}
```
<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Backup Vault: DELETED | ```json
{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f8246029ad",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "111233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}
``` |
| Backup Plan: MODIFIED | ```json
{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "111233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "backupPlanId": "85fcb8ee-2d93-42ac-b06f-591565f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "modifiedAt": "2020-06-24T23:18:19.168Z",
    "state": "MODIFIED"
  }
}
``` |
### Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup Plan: DELETED</strong></td>
</tr>
<tr>
<td>`{   &quot;version&quot;: &quot;0&quot;,   &quot;id&quot;: &quot;33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c&quot;,   &quot;detail-type&quot;: &quot;Backup Plan State Change&quot;,   &quot;source&quot;: &quot;aws.backup&quot;,   &quot;account&quot;: &quot;1112233445566&quot;,   &quot;time&quot;: &quot;2020-06-24T23:18:25Z&quot;,   &quot;region&quot;: &quot;us-east-1&quot;,   &quot;resources&quot;: [     &quot;arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-b06f-591563f5f8de_beta&quot;   ],   &quot;detail&quot;: {     &quot;backupPlanId&quot;: &quot;83fcb8ee-2d93-42ac-b06f-591563f5f8de&quot;,     &quot;versionId&quot;: &quot;NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0&quot;,     &quot;deletionDate&quot;: &quot;2020-06-24T23:18:19.411Z&quot;,     &quot;state&quot;: &quot;DELETED&quot;   }}</td>
</tr>
<tr>
<td><strong>Backup Plan: CREATED</strong></td>
</tr>
<tr>
<td>`{   &quot;version&quot;: &quot;0&quot;,   &quot;id&quot;: &quot;b64fb2d0-ae16-ff9a-faf6-0bdd0d4bdef&quot;,   &quot;detail-type&quot;: &quot;Backup Plan State Change&quot;,   &quot;source&quot;: &quot;aws.backup&quot;,   &quot;account&quot;: &quot;1112233445566&quot;,   &quot;time&quot;: &quot;2020-06-24T23:18:19Z&quot;,   &quot;region&quot;: &quot;us-east-1&quot;,   &quot;resources&quot;: [     &quot;arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-d3afa4c84f59_beta&quot;   ],   &quot;detail&quot;: {     &quot;backupPlanId&quot;: &quot;2c103c5f-6d6e-4cac-9147-d3afa4c84f59&quot;,     &quot;versionId&quot;: &quot;N2Q4OTczMzEtZmY1MjVlNjQwMDI1NDIzOTk0&quot;,     &quot;creationDate&quot;: &quot;2020-06-24T23:18:15.318Z&quot;,     &quot;state&quot;: &quot;CREATED&quot;   }}</td>
</tr>
</tbody>
</table>
Differences with the AWS Backup notification API

You can also use the AWS Backup notification API to track AWS Backup events with Amazon Simple Notification Service (Amazon SNS). However, EventBridge tracks more changes than the notification API, including changes to backup vaults, copy job state, Region settings, and the number of cold or warm recovery points.

AWS Backup metrics with Amazon CloudWatch

Topics
- CloudWatch Dashboard (p. 367)
- Metrics with CloudWatch (p. 368)

CloudWatch Dashboard

Your AWS Backup console includes a dashboard to see metrics on completed or failed backup, copy, and restore jobs. Within this dashboard, you can view job status by time period, customized to the time frame you desire.

TO ACCESS THE DASHBOARD

2. Select Dashboard in the left-hand navigation pane.

VIEW AND UNDERSTAND THE DASHBOARD

The CloudWatch dashboard displays several widgets. Each widget shows job metrics by count. Each widget shows several line graphs. Each line corresponds to a protected resource (if you do not see an expected resource displayed, ensure the resource is turned on in Settings). The displays do not show in-progress jobs.
The y-axis (vertical values) shows the count. The x-axis (horizontal values) shows points in time. If there are no data points to visualize in the selected job status, the value will be set to 0 with a horizontal line on the x-axis. The legend showing the resources will still be visible.

The metrics display account-specific and Region-specific information related to the current login. To see other accounts or Regions, you must login under the chosen account.

**CUSTOMIZE THE DASHBOARD**

By default, the displayed time frame is one week. Along the top menu, there are options for redefining the displayed time frame. You can choose from among 1 hour, 3 hours, 12 hours, 1 day, 3 days, and 1 week. Additionally, you can select **Custom** to specify a different value. Customization will temporarily change the current view to your specifications.

You can hover over a widget, which will display a **Enlarge** button in the top right of the widget. Click on **Enlarge** to open the widget in full-screen view. In full screen, there are more options for customizing the graph display, such as changing the period (the time between every data point). Any changes will not be retained once the full-screen view is closed.

To view only one resource type at a time, click on the label text of the resource type you wish to view in the graph legend. This will deselect other all resource types. To reverse this, click on a resource type color box in the legend. To go back to default view of all resource types with all the labels selected, click again on the label text of any resource type selected.

Clicking the three vertical dots in the top right corner of a widgets opens up a drop down menu with options to refresh, enlarge, view in metrics and view in logs. “View in metrics” opens up the metric used in the widget in CloudWatch console. You can make any changes to the widget there and add the widget to a custom dashboard in CloudWatch dashboard. Any changes you make in the CloudWatch dashboard will not be reflected on the dashboard in AWS Backup Console. “View as logs” opens up the logs view page in CloudWatch console.

To add widgets displayed to your own custom CloudWatch dashboard, click on the **Add to dashboard** button located on the top right of the dashboard. This will open up the CloudWatch console where you can select in which custom dashboard to add all the six widgets.

For more information, see [Using Amazon CloudWatch metrics](#).

# Metrics with CloudWatch

You can use CloudWatch to monitor AWS Backup metrics. The AWS/Backup namespace allows you to track the following metrics. AWS Backup emits updated metrics to CloudWatch every 5 minutes.

The purpose of this documentation page is to provide you with the reference materials to use CloudWatch to monitor AWS Backup. To learn how to monitor a metric using CloudWatch, see the blog [Amazon CloudWatch Events and Metrics for AWS Backup](#) or [Focus on Metrics and Alarms in a Single AWS Service](#) in the [CloudWatch User Guide](#). To set alarms, see [Using Amazon CloudWatch Alarms](#) in the [CloudWatch User Guide](#).

<table>
<thead>
<tr>
<th>Category</th>
<th>Metrics</th>
<th>Example dimensions</th>
<th>Example use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jobs</td>
<td>Number of backup, restore, and copy jobs across each state, including CREATED, PENDING, RUNNING, ABORTED, COMPLETED, FAILED, and EXPIRED.</td>
<td>Resource type, vault name. The vault name of copy jobs is that of their destination vault.</td>
<td>Monitor the number of failed backup jobs within one or more specific backup vaults. When there are more than five failed jobs within 1 hour, send</td>
</tr>
</tbody>
</table>
Different job types have different available states.

**Example dimensions**

Resource type, vault name.

**Example use case**

an email or SMS using Amazon SNS or open a ticket to the engineering team to investigate.

**Reporting criteria:**

There is a nonzero value

---

<table>
<thead>
<tr>
<th>Category</th>
<th>Metrics</th>
<th>Example dimensions</th>
<th>Example use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery points</td>
<td>Number of warm and cold recovery points across each state: MODIFIED, COMPLETED, PARTIAL, EXPIRED, DELETED.</td>
<td>Resource type, vault name.</td>
<td>Track the number of deleted recovery points for your Amazon EBS volumes, and separately track the number of warm and cold recovery points in each backup vault. <strong>Reporting criteria:</strong> There is a nonzero value</td>
</tr>
</tbody>
</table>

The following table lists all the metrics available to you.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NumberOfBackupJobsCreated</td>
<td>The number of backup jobs that AWS Backup created.</td>
</tr>
<tr>
<td>NumberOfBackupJobsPending</td>
<td>The number of backup jobs about to run in AWS Backup.</td>
</tr>
<tr>
<td>NumberOfBackupJobsRunning</td>
<td>The number of backup jobs currently running in AWS Backup.</td>
</tr>
<tr>
<td>NumberOfBackupJobsAborted</td>
<td>The number of user cancelled backup jobs.</td>
</tr>
<tr>
<td>NumberOfBackupJobsCompleted</td>
<td>The number of backup jobs that AWS Backup finished.</td>
</tr>
<tr>
<td>NumberOfBackupJobsFailed</td>
<td>The number of backup jobs with status of Failed. Often caused by scheduling a backup job during or 1 hour before a database resource or 4 hours before or during a Amazon FSx maintenance window or automated backup window and not using AWS Backup to perform continuous backup for point-in-time restores. See <strong>Point-in-Time Recovery</strong> for a list of supported services and instructions on how to use AWS Backup to take continuous backups, or reschedule your backup jobs.</td>
</tr>
<tr>
<td>NumberOfBackupJobsExpired</td>
<td>The number of backup jobs that AWS Backup attempted to delete based on your backup retention lifecycle, but could not delete. You are billed for the storage that expired backups consume and should delete them manually.</td>
</tr>
</tbody>
</table>
### Metric Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NumberOfCopyJobsCreated</td>
<td>The number of cross-account and cross-Region copy jobs that AWS Backup created.</td>
</tr>
<tr>
<td>NumberOfCopyJobsRunning</td>
<td>The number of cross-account and cross-Region copy jobs currently running in AWS Backup.</td>
</tr>
<tr>
<td>NumberOfCopyJobsCompleted</td>
<td>The number of cross-account and cross-Region copy jobs that AWS Backup finished.</td>
</tr>
<tr>
<td>NumberOfCopyJobsFailed</td>
<td>The number of cross-account and cross-Region copy jobs that AWS Backup attempted but could not complete.</td>
</tr>
<tr>
<td>NumberOfRestoreJobsPending</td>
<td>The number of restore jobs about to run in AWS Backup.</td>
</tr>
<tr>
<td>NumberOfRestoreJobsRunning</td>
<td>The number of restore jobs currently running in AWS Backup.</td>
</tr>
<tr>
<td>NumberOfRestoreJobsCompleted</td>
<td>The number of restore jobs that AWS Backup finished.</td>
</tr>
<tr>
<td>NumberOfRestoreJobsFailed</td>
<td>The number of restore jobs that AWS Backup attempted but could not complete.</td>
</tr>
<tr>
<td>NumberOfRecoveryPointsCompleted</td>
<td>The number of recovery points that AWS Backup created.</td>
</tr>
<tr>
<td>NumberOfRecoveryPointsPartial</td>
<td>The number of recovery points that AWS Backup started to create but could not finish. AWS retries the process later, but because the retry occurs at the later time, it retains the partial recovery point.</td>
</tr>
<tr>
<td>NumberOfRecoveryPointsExpired</td>
<td>The number of recovery points that AWS Backup attempted to delete based on your backup retention lifecycle, but could not delete. You are billed for the storage that expired backups consume and should delete them manually.</td>
</tr>
<tr>
<td>NumberOfRecoveryPointsDeleting</td>
<td>The number of recovery points that AWS Backup is deleting.</td>
</tr>
<tr>
<td>NumberOfRecoveryPointsCold</td>
<td>The number of recovery points that AWS Backup tiered to cold storage.</td>
</tr>
</tbody>
</table>

More dimensions are available beyond those listed in the table. To view all the dimensions of a metric, type the name of that metric into the AWS/Backup namespace of the Metrics section of the CloudWatch console.

---

**Logging AWS Backup API calls with CloudTrail**

AWS Backup is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Backup. CloudTrail captures all API calls for AWS Backup as events. The calls captured include calls from the AWS Backup console and code calls to the AWS Backup API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Backup. If you don't configure a trail, you can still view the most recent
events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Backup, the IP address from which the request was made, who made the request, when it was made, and additional details. To learn more about CloudTrail, see the [AWS CloudTrail User Guide](https://docs.aws.amazon.com/AmazonCloudTrail/latest/userguide/).

**Topics**

- AWS Backup information in CloudTrail (p. 371)
- Understanding AWS Backup log file entries (p. 372)
- Logging cross-account management events (p. 374)

**Important**

In accounts logging data read events, S3 buckets with CloudTrail logs enabled need their access logs saved to a different target bucket; if CloudTrail logs are saved in the same bucket they log, an infinite loop forms. This loop can trigger unexpected and unwanted charges. For more information, see **Data events** in the *CloudTrail User Guide*.

**AWS Backup information in CloudTrail**

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS Backup, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. AWS Backup generates these CloudTrail events when it performs backups, restores, copies, or notifications:

- BackupDeleted
- BackupJobCompleted
- BackupJobStarted
- BackupSelectionDeletedDueToSLRDeletion
- BackupTransitionedToCold
- CopyJobCompleted
- CopyJobStarted
- ReportJobCompleted
- ReportJobStarted
- RestoreCompleted
- RestoreStarted
- PutBackupVaultNotifications

These events are not necessarily generated by use of the AWS Backup public APIs. Rather, they are generated through AWS Backup asynchronously executing your jobs. For example, your [StartBackupJob](https://docs.aws.amazon.com/AWSSimpleBackup/latest/APIReference/API_StartBackupJob.html) API call could generate the BackupJobStarted event, but a scheduled job from a backup plan could also generate the BackupJobStarted event.

For more information, see [Viewing Events with CloudTrail Event History](https://docs.aws.amazon.com/AmazonCloudTrail/latest/userguide/).

For an ongoing record of events in your AWS account, including events for AWS Backup, create a trail. A [trail](https://docs.aws.amazon.com/AmazonCloudTrail/latest/userguide/creating-trail.html) enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- [Overview for Creating a Trail](https://docs.aws.amazon.com/AmazonCloudTrail/latest/userguide/creating-trail.html)
Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail `userIdentity` Element.

**Understanding AWS Backup log file entries**

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `StartBackupJob`, `StartRestoreJob`, and `DeleteRecoveryPoint` actions and also the `BackupJobCompleted` event.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "account-id",
        "accessKeyId": "access-key",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465 Linux/4.9.124-0.1.ac.198.73.329.metall.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/vol-00a422a05b9c6asad3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": "60"
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    }
}
```
AWS Backup Developer Guide
Understanding AWS Backup log file entries

```
{
  "requestID": "98cf6d59-8c76-49f7-9201-790743951234",
  "eventID": "fe8146a5-7812-4a95-90ad-074698be1234",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-id"
},
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "account-id",
    "accessKeyId": "access-key",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-01-10T12:24:50Z"
      }
    }
  },
  "eventTime": "2019-01-10T13:49:50Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "StartRestoreJob",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "12.34.567.89",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.465 Linux/4.9.124-0.1.ac.198.73.329.metal1.86_64 OpenJDK_64-Bit_Server_VM/25.192-b12 java/1.8.0_192",
  "requestParameters": {
    "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
    "metadata": {
      "volumeType": "gp2",
      "availabilityZone": "us-east-1b",
      "volumeSize": "100"
    },
    "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
    "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
    "resourceType": "EBS"
  },
  "responseElements": {
    "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
  },
  "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
  "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-id"
},
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "account-id",
    "accessKeyId": "access-key",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-01-10T12:24:50Z"
      }
    }
  },
  "eventTime": "2019-01-10T14:52:42Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "DeleteRecoveryPoint",
```

373
Logging cross-account management events

Using AWS Backup, you can manage your backups across all AWS accounts inside your AWS Organizations structure. AWS Backup generates these CloudTrail events when you create, update, or delete an AWS Organizations backup policy (that applies backup plans to your member accounts):

- CreateOrganizationalBackupPlan
- UpdateOrganizationalBackupPlan
- DeleteOrganizationalBackupPlan
Example: AWS Backup log file entries for cross-account management

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the CreateOrganizationalBackupPlan action.

```
{
"*eventVersion*": "1.05",
"*userIdentity*": {
  "*accountId*": "account-id",
  "*invokedBy*": "backup.amazonaws.com",
  "*eventTime*": "2020-06-02T00:34:00Z",
  "*eventSource*": "backup.amazonaws.com",
  "*eventName*": "CreateOrganizationalBackupPlan",
  "*awsRegion*": "ca-central-1",
  "*sourceIPAddress*": "backup.amazonaws.com",
  "*userAgent*": "backup.amazonaws.com",
  "*requestParameters*": null,
  "*responseElements*": null,
  "*eventID*": "f2642255-af77-4203-8c37-7ca19d898e84",
  "*readOnly*": false,
  "*eventType*": "AwsServiceEvent",
  "*recipientAccountId*": "account-id",
  "*serviceEventDetails*": {
    "*backupPlanId*": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "*backupPlanVersionId*": "ZTA1Y2ZjZDYtNmRjMi00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
    "*backupPlanName*": "mybackupplan",
    "*backupRules*": 
      [{"id":"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2", "name":"hourly","description":null,"cryopodArn":"arn:aws:backup:ca-central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault","scheduleExpression ":\"cron(0 0/1 ? * * *)\","startWindow":"PT1H","completionWindow":"PT2H","lifecycle":{"moveToColdStorageAfterDays":null,"deleteAfterDays":null},"tags 
":null,\"copyActions\":[]}],
    "*backupSelections*": 
      [{"name":"selectiondatatype","arn":null},
        \"arn\":\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3d49-926d-a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",\n        \"resources\":[],\"notResources\":[]},
        \"conditions\":null,\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",\"value\":\"PII\",\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",\"value\":\"RED\"},
    "*creationDate*": "2020-06-02T00:34:00.695Z",
    "*creatorRequestId":null
  }
}
```

The following example shows a CloudTrail log entry that demonstrates the DeleteOrganizationalBackupPlan action.

```
{
"*eventVersion*": "1.05",
"*userIdentity*": {
  "*accountId*": "account-id",
  "*invokedBy*": "backup.amazonaws.com",
  "*eventTime*": "2020-06-02T00:34:00Z",
  "*eventSource*": "backup.amazonaws.com",
  "*eventName*": "DeleteOrganizationalBackupPlan",
  "*awsRegion*": "ca-central-1",
  "*sourceIPAddress*": "backup.amazonaws.com",
  "*userAgent*": "backup.amazonaws.com",
  "*requestParameters*": null,
  "*responseElements*": null,
  "*eventID*": "f2642255-af77-4203-8c37-7ca19d898e84",
  "*readOnly*": false,
  "*eventType*": "AwsServiceEvent",
  "*recipientAccountId*": "account-id",
  "*serviceEventDetails*": {
    "*backupPlanId*": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "*backupPlanName*": "mybackupplan",
    "*backupRules*": [],
    "*backupSelections*": [],
    "*creationDate*": "2020-06-02T00:34:00.695Z",
    "*creatorRequestId":null
  }
}
```
Notification options with AWS Backup

There are two ways to receive notifications about AWS Backup:

- AWS User Notifications can send notifications, including Amazon CloudWatch alarms, AWS Support, and other services' notifications.
- Amazon Simple Notification Service can notify you of AWS Backup events.

AWS User Notifications and AWS Backup

AWS Backup supports management of your backup notifications from the AWS User Notifications console. With AWS User Notifications, you can view the progress of your backup, copy, and restore jobs and changes to your backup policies, vaults, recovery points, and settings from the User Notifications Notification Center.

Amazon CloudWatch, Amazon EventBridge alarms, and AWS Support case updates are among other types of notifications you can manage from the console. Additionally, you can set up several delivery options, including email, AWS Chatbot notifications, and AWS Console Mobile Application push notifications.

Amazon SNS and AWS Backup events

AWS Backup takes advantage of the robust notifications delivered by Amazon Simple Notification Service (Amazon SNS). You can configure Amazon SNS to notify you of AWS Backup events from the Amazon SNS console.
Common use cases

- Set up notifications for failed backup jobs by following the steps in How can I get notifications for AWS Backup jobs that failed? from AWS Premium Support.
- Review sample Amazon SNS notification JSONs for completed, failed, and expired backup jobs in the Examples of events table below.

For more information about Amazon SNS generally, see Getting Started with Amazon SNS in the Amazon Simple Notification Service Developer Guide.

Note
While the Amazon SNS service allows cross-account notifications, AWS Backup does not currently support this feature. You must specify your own AWS account ID and the resource ARN of your topic.

AWS Backup notification APIs

After creating your topics using the Amazon SNS console or AWS Command Line Interface (AWS CLI), you can use the following AWS Backup API operations to manage your backup notifications.

- **DeleteBackupVaultNotifications** (p. 429) — Deletes event notifications for the specified backup vault.
- **GetBackupVaultNotifications** (p. 492) — Lists all event notifications for the specified backup vault.
- **PutBackupVaultNotifications** (p. 556) — Turns on notifications for the specified topic and events.

AWS Backup supports the following events:

<table>
<thead>
<tr>
<th>Job type</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup job</td>
<td>BACKUP_JOB_STARTED</td>
</tr>
<tr>
<td>Copy job</td>
<td>COPY_JOB_STARTED</td>
</tr>
<tr>
<td>Restore job</td>
<td>RESTORE_JOB_STARTED</td>
</tr>
<tr>
<td>Recovery point</td>
<td>RECOVERY_POINT_MODIFIED</td>
</tr>
</tbody>
</table>

AWS Backup for S3 supports two additional events:

- **S3_BACKUP_OBJECT_FAILED** notifies you of any S3 object that AWS Backup failed to back up during a backup job.
- **S3_RESTORE_OBJECT_FAILED** notifies you of any S3 object that AWS Backup failed to restore during a restore job.

Examples of events

<table>
<thead>
<tr>
<th>Event</th>
<th>Amazon SNS Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup job completed</td>
<td>{ &quot;Records&quot;: [] }</td>
</tr>
</tbody>
</table>
### Amazon SNS Notification

```
"EventSource": "aws: sns",
"EventVersion": "1.0",
"EventSubscriptionArn":
  "arn:aws:sns:...
"Sns": {
  "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
  "Subject": "Notification from AWS Backup",
  "Timestamp": "2019-08-02T18:46:02.788Z",
  "MessageAttributes": {
    "EventType": {
      "Type": "String",
      "Value": "BACKUP_JOB",
    },
    "State": {
      "Type": "String",
      "Value": "COMPLETED",
    },
    "AccountId": {
      "Type": "String",
      "Value": "123456789012",
    },
    "Id": {
      "Type": "String",
      "Value": "1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
    },
    "StartTime": {
      "Type": "String",
      "Value": "2019-09-02T13:48:52.226Z"
    }
  }
}
```
### Event

**Backup job failed**

<table>
<thead>
<tr>
<th>Amazon SNS Notification</th>
</tr>
</thead>
</table>
| `{  
  "Records": [[[  
"EventSource": "aws: sns",  
"EventVersion": "1.0",  
"EventSubscriptionArn":  
"arn:aws:sns::-a3802a1ed45",  
"Sns": {  
  "Type": "Notification",  
  "MessageId": "12345678-abcd-123a-def0-abcd1a234567",  
  "Subject": "Notification from AWS Backup",  
  "Timestamp": "2019-08-02T18:46:02.788Z",  
  ...  
  "MessageAttributes": {  
    "EventType": {  
      "Type": "String", "Value": "BACKUP_JOB"},  
    "State": {  
      "Type": "String", "Value": "FAILED"},  
    "AccountId": {  
      "Type": "String", "Value": "123456789012"},  
    "Id": {  
      "Type": "String", "Value": "1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},  
    "StartTime": {  
      "Type": "String", "Value": "2019-09-02T13:48:52.226Z"}  
  }  
}  
}  
]}`
Amazon SNS and AWS Backup events

<table>
<thead>
<tr>
<th>Event</th>
<th>Amazon SNS Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup job could not complete during the backup window</td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>&quot;Records&quot;: [[</td>
</tr>
<tr>
<td></td>
<td>&quot;EventSource&quot;: &quot;aws: sns&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;EventVersion&quot;: &quot;1.0&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;EventSubscriptionArn&quot;: &quot;arn:aws:sns:....-a3802a1ed45&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;Sns&quot;: {</td>
</tr>
<tr>
<td></td>
<td>&quot;Type&quot;: &quot;Notification&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;MessageId&quot;: &quot;12345678-abcd-123a-def0-abcd1a234567&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;Subject&quot;: &quot;Notification from AWS Backup&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;Message&quot;: &quot;An AWS Backup job failed to complete in time. Resource ARN :</td>
</tr>
<tr>
<td></td>
<td>arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :</td>
</tr>
<tr>
<td></td>
<td>1b2345b2-f22c-4db5-5eb6-bbc7890ed123&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;Timestamp&quot;: &quot;2019-08-02T18:46:02.788Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>&quot;MessageAttributes&quot; : {</td>
</tr>
<tr>
<td></td>
<td>&quot;EventType&quot; : &quot;BACKUP_JOB&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;State&quot; : &quot;EXPIRED&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;AccountId&quot; : &quot;123456789012&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;Id&quot; : &quot;1b2345b2-f22c-4db5-5eb6-bbc7890ed123&quot; }</td>
</tr>
<tr>
<td></td>
<td>]</td>
</tr>
</tbody>
</table>

AWS Backup notification command examples

You can use AWS CLI commands to subscribe to, list, and delete Amazon SNS notifications for your AWS Backup events.

**Example put backup vault notification**

The following command subscribes to an Amazon SNS topic for the specified backup vault that notifies you when a restore job is started or completed, or when a recovery point is modified.

```bash
aws backup put-backup-vault-notifications
   --backup-vault-name myBackupVault
   --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED RECOVERY_POINT_MODIFIED
```
Example get backup vault notification

The following command lists all events currently subscribed to an Amazon SNS topic for the specified backup vault.

```
aws backup get-backup-vault-notifications
   --backup-vault-name myVault
```

The sample output is as follows:

```
{
  "BackupVaultEvents": [
    "RESTORE_JOB_STARTED",
    "RESTORE_JOB_COMPLETED",
    "RECOVERY_POINT_MODIFIED"
  ],
  "BackupVaultName": "myVault",
}
```

Example delete backup vault notification

The following command unsubscribes from an Amazon SNS topic for the specified backup vault.

```
aws backup delete-backup-vault-notifications
   --backup-vault-name myVault
```

Specifying AWS Backup as a service principal

**Note**

To allow AWS Backup to publish SNS topics on your behalf, you must specify AWS Backup as a service principal.

Include the following JSON in the access policy of the Amazon SNS topic that you use to track AWS Backup events. You must specify the resource Amazon Resource Name (ARN) of your topic.

```
{
  "Sid": "My-statement-id",
  "Effect": "Allow",
  "Principal": {
    "Service": "backup.amazonaws.com"
  },
  "Action": "SNS:Publish",
}
```

For more information about specifying a service principal in an Amazon SNS access policy, see [Allowing Any AWS Resource to Publish to a Topic](https://docs.aws.amazon.com/sns/latest/dg/sns-allow-publish.html) in the *Amazon Simple Notification Service Developer Guide*.

**Note**

If your topic is encrypted, you must include additional permissions in your policy to allow AWS Backup to publish to it. For more information about enabling services to publish to encrypted topics, see [Enable Compatibility between Event Sources from AWS Services and Encrypted Topics](https://docs.aws.amazon.com/sns/latest/dg/sns-topic-encryption.html) in the *Amazon Simple Notification Service Developer Guide*.
Troubleshooting AWS Backup

When you use AWS Backup, you might encounter issues. The following sections can help you troubleshoot some common issues that might occur.

For general questions about AWS Backup, see the AWS Backup FAQ. You can also search for answers and post questions in the AWS Backup forum.

**Topics**
- Troubleshooting general issues (p. 382)
- Troubleshoot creating resources (p. 382)
- Troubleshooting deleting resources (p. 383)
- Troubleshooting restoring resources (p. 383)

**Troubleshooting general issues**

When you back up and restore resources, you not only need permission to use AWS Backup, you must also have permission to access the resources that you want to protect. The easiest way to have the proper permissions is to choose the Default role when you assign resources to a backup plan. For more information about access control using AWS Identity and Access Management (IAM) with AWS Backup, see Access control (p. 240).

If you run into issues with backing up and restoring a particular resource type, it can be helpful to review the backup and restore troubleshooting topic for that resource. For more information, see the links under How AWS Backup works with supported AWS services.

If AWS Backup fails to create or delete a resource, you can learn more about the issue by using AWS CloudTrail to view error messages or logs. For more information about using CloudTrail with AWS Backup, see Logging AWS Backup API calls with CloudTrail (p. 370).

**Troubleshoot creating resources**

The following information can help you troubleshoot problems with creating backups.

- In general, AWS database services cannot start backups 1 hour before or during their maintenance window or automatic backup window. Amazon FSx cannot start backups 4 hours before or during the maintenance window or automatic backup window (Amazon Aurora is exempt from this maintenance window restriction). Snapshot backups scheduled during those times will fail. One exception: when you opt in to using AWS Backup for both snapshot and continuous backups for a supported service, you no longer need to worry about those windows because AWS Backup will schedule them for you. See Point-in-Time Recovery for a list of supported services and instructions on how to use AWS Backup to take continuous backups.
- Creating backups for DynamoDB tables will fail while tables are being created. Creating a DynamoDB table typically takes a couple of minutes.
- Backing up Amazon EFS file systems can take up to 7 days when the file systems are very large. Only one concurrent backup at a time can be queued for an Amazon EFS file system. If a subsequent backup is queued while a previous one is still in progress, the backup window can expire and no backup is created.
• **Amazon EBS** has a soft quota of 100,000 backups per AWS Region per account, and additional backups fail when this quota is reached. If you reach this quota, you can delete excess backups or request a quota increase. For more information about requesting a quota increase, see [AWS Service Quotas](https://aws.amazon.com/service-quotas).

• When creating **Amazon Relational Database Service (RDS) backups**, consider the following:
  - If you do not use AWS Backup to manage both Amazon RDS snapshots and continuous backups with point-in-time recovery, your backups will fail if initiated if scheduled or made on-demand during the daily, user-configurable 30-minute backup window. For more information about automated Amazon RDS backups, see [Working With Backups](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/WorkingWithBackups.html) in the *Amazon RDS User Guide*. You can avoid this limitation by using AWS Backup to manage both Amazon RDS snapshots and continuous backups with point-in-time recovery.
  - If you initiate a backup job from the Amazon RDS console, this can conflict with an Aurora clusters backup job, causing the error *Backup job expired before completion.* If this occurs, configure a longer backup window in AWS Backup.
  - AWS Backup does not currently pass on the TDE option group when a copy job is created. If you intend to use this option group for copy job creation, you must use the Amazon RDS console or Amazon RDS API instead of AWS Backup tools. See [Copying an option group](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/WorkingWithOptionGroups.html) in the *Amazon Relational Database Service User Guide* for more information.
  - **ERROR:** On-demand backups complete but scheduled backups fail with error "The source snapshot KMS key does not exist, is not enabled or you do not have permissions to access it." The on-demand job is completed because it uses the API call CopyDBSnapshot, which doesn’t require KMS access.

  **REMEDY:** Add the IAM role to your KMS key. This can be done by allowing the role on your KMS key policy.

  To edit your policy,
  1. Open the [KMS console](https://console.aws.amazon.com/kms/).
  2. Select **customer managed keys** in the left navigation.
  3. Click the customer managed key you wish to edit.
  4. Under **Key policy**, click **Switch to policy view**.
  5. Click **Edit**.
  6. Add the role.

### Troubleshooting deleting resources

Recovery points that are created by AWS Backup cannot be deleted in the console window of the protected resource. You can delete them on the AWS Backup console by selecting them in the vault where they are stored and then choosing **Delete**.

To delete a recovery point or a backup vault, you need the appropriate permissions. For more information about access control using IAM with AWS Backup, see [Access control (p. 240)](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/ManagingAccessControl.html).

### Troubleshooting restoring resources

**Restoring using API**

To restore a backup programmatically, use the [StartRestoreJob](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/WorkingWithBackups.html#WorkingWithBackups.RestoreBackup) API operation.

To get the configuration metadata that your backup was created with, you can call [GetRecoveryPointRestoreMetadata](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/WorkingWithBackups.html#WorkingWithBackups.RetrieveBackup).
See [Restoring a backup](#) for more information.

**Restoring using the Console**

- [Restoring Amazon S3 data](#)
- [Restoring a virtual machine](#)
- [Restoring an Amazon FSx file system](#)
- [Restoring an Amazon EBS volume](#)
- [Restoring an Amazon EFS file system](#)
- [Restoring an Amazon DynamoDB table](#)
- [Restoring an Amazon RDS database](#)
- [Restoring an Aurora cluster](#)
- [Restoring an Amazon EC2 instance](#)
- [Restoring a Storage Gateway volume](#)
- [Restoring a Amazon DocumentDB cluster](#)
- [Restoring a Neptune cluster](#)
AWS Backup API

In addition to using the console, you can use the AWS Backup API actions and data types to programmatically configure and manage AWS Backup and its resources. This section describes AWS Backup actions and data types. It contains the API reference for AWS Backup.

AWS Backup API

- AWS Backup Actions
- AWS Backup Data Types

Actions

The following actions are supported by AWS Backup:

- CancelLegalHold (p. 390)
- CreateBackupPlan (p. 392)
- CreateBackupSelection (p. 396)
- CreateBackupVault (p. 399)
- CreateFramework (p. 402)
- CreateLegalHold (p. 406)
- CreateLogicallyAirGappedBackupVault (p. 410)
- CreateReportPlan (p. 414)
- DeleteBackupPlan (p. 418)
- DeleteBackupSelection (p. 421)
- DeleteBackupVault (p. 423)
- DeleteBackupVaultAccessPolicy (p. 425)
- DeleteBackupVaultLockConfiguration (p. 427)
- DeleteBackupVaultNotifications (p. 429)
- DeleteFramework (p. 431)
- DeleteRecoveryPoint (p. 433)
- DeleteReportPlan (p. 435)
- DescribeBackupJob (p. 437)
- DescribeBackupVault (p. 442)
- DescribeCopyJob (p. 446)
- DescribeFramework (p. 448)
- DescribeGlobalSettings (p. 451)
- DescribeProtectedResource (p. 453)
- DescribeRecoveryPoint (p. 455)
- DescribeRegionSettings (p. 461)
- DescribeReportJob (p. 463)
- DescribeReportPlan (p. 465)
- DescribeRestoreJob (p. 467)
- DisassociateRecoveryPoint (p. 471)
• **DisassociateRecoveryPointFromParent** (p. 473)
• **ExportBackupPlanTemplate** (p. 475)
• **GetBackupPlan** (p. 477)
• **GetBackupPlanFromJSON** (p. 481)
• **GetBackupPlanFromTemplate** (p. 484)
• **GetBackupSelection** (p. 487)
• **GetBackupVaultAccessPolicy** (p. 490)
• **GetBackupVaultNotifications** (p. 492)
• **GetLegalHold** (p. 495)
• **GetRecoveryPointRestoreMetadata** (p. 498)
• **GetSupportedResourceTypes** (p. 501)
• **ListBackupJobs** (p. 503)
• **ListBackupPlans** (p. 507)
• **ListBackupPlanTemplates** (p. 510)
• **ListBackupPlanVersions** (p. 512)
• **ListBackupSelections** (p. 515)
• **ListBackupVaults** (p. 517)
• **ListCopyJobs** (p. 520)
• **ListFrameworks** (p. 524)
• **ListLegalHolds** (p. 526)
• **ListProtectedResources** (p. 528)
• **ListProtectedResourcesByBackupVault** (p. 530)
• **ListRecoveryPointsByBackupVault** (p. 533)
• **ListRecoveryPointsByLegalHold** (p. 536)
• **ListRecoveryPointsByResource** (p. 538)
• **ListReportJobs** (p. 541)
• **ListReportPlans** (p. 544)
• **ListRestoreJobs** (p. 546)
• **ListTags** (p. 549)
• **PutBackupVaultAccessPolicy** (p. 551)
• **PutBackupVaultLockConfiguration** (p. 553)
• **PutBackupVaultNotifications** (p. 556)
• **StartBackupJob** (p. 559)
• **StartCopyJob** (p. 564)
• **StartReportJob** (p. 568)
• **StartRestoreJob** (p. 570)
• **StopBackupJob** (p. 574)
• **TagResource** (p. 576)
• **UntagResource** (p. 578)
• **UpdateBackupPlan** (p. 580)
• **UpdateFramework** (p. 583)
• **UpdateGlobalSettings** (p. 587)
• **UpdateRecoveryPointLifecycle** (p. 589)
• **UpdateRegionSettings** (p. 592)
• **UpdateReportPlan** (p. 594)
The following actions are supported by AWS Backup gateway:

- AssociateGatewayToServer (p. 598)
- CreateGateway (p. 600)
- DeleteGateway (p. 603)
- DeleteHypervisor (p. 605)
- DisassociateGatewayFromServer (p. 607)
- GetBandwidthRateLimitSchedule (p. 609)
- GetGateway (p. 611)
- GetHypervisor (p. 613)
- GetHypervisorPropertyMappings (p. 615)
- GetVirtualMachine (p. 618)
- ImportHypervisorConfiguration (p. 620)
- ListGateways (p. 623)
- ListHypervisors (p. 626)
- ListTagsForResource (p. 629)
- ListVirtualMachines (p. 631)
- PutBandwidthRateLimitSchedule (p. 634)
- PutHypervisorPropertyMappings (p. 637)
- PutMaintenanceStartTime (p. 640)
- StartVirtualMachinesMetadataSync (p. 643)
- TagResource (p. 645)
- TestHypervisorConfiguration (p. 647)
- UntagResource (p. 650)
- UpdateGatewayInformation (p. 652)
- UpdateGatewaySoftwareNow (p. 654)
- UpdateHypervisor (p. 656)

AWS Backup

The following actions are supported by AWS Backup:

- CancelLegalHold (p. 390)
- CreateBackupPlan (p. 392)
- CreateBackupSelection (p. 396)
- CreateBackupVault (p. 399)
- CreateFramework (p. 402)
- CreateLegalHold (p. 406)
- CreateLogicallyAirGappedBackupVault (p. 410)
- CreateReportPlan (p. 414)
- DeleteBackupPlan (p. 418)
- DeleteBackupSelection (p. 421)
- DeleteBackupVault (p. 423)
- DeleteBackupVaultAccessPolicy (p. 425)
- DeleteBackupVaultLockConfiguration (p. 427)
- DeleteBackupVaultNotifications (p. 429)
• **PutBackupVaultNotifications (p. 556)**
• **StartBackupJob (p. 559)**
• **StartCopyJob (p. 564)**
• **StartReportJob (p. 568)**
• **StartRestoreJob (p. 570)**
• **StopBackupJob (p. 574)**
• **TagResource (p. 576)**
• **UntagResource (p. 578)**
• **UpdateBackupPlan (p. 580)**
• **UpdateFramework (p. 583)**
• **UpdateGlobalSettings (p. 587)**
• **UpdateRecoveryPointLifecycle (p. 589)**
• **UpdateRegionSettings (p. 592)**
• **UpdateReportPlan (p. 594)**
CancelLegalHold
Service: AWS Backup

This action removes the specified legal hold on a recovery point. This action can only be performed by a user with sufficient permissions.

Request Syntax

```
DELETE /legal-holds/{legalHoldId}?
cancelDescription={CancelDescription}&retainRecordInDays={RetainRecordInDays} HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

- **CancelDescription (p. 390)**
  - String describing the reason for removing the legal hold.
  - Required: Yes

- **legalHoldId (p. 390)**
  - Legal hold ID required to remove the specified legal hold on a recovery point.
  - Required: Yes

- **RetainRecordInDays (p. 390)**
  - The integer amount in days specifying amount of days after this API operation to remove legal hold.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 201
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

- **InvalidParameterValueException**
  - Indicates that something is wrong with a parameter's value. For example, the value is out of range.
  - HTTP Status Code: 400

- **InvalidResourceStateException**
  - AWS Backup is already performing an action on this recovery point. It can't perform the action you requested until the first action finishes. Try again later.
  - HTTP Status Code: 400
**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
CreateBackupPlan

Service: AWS Backup

Creates a backup plan using a backup plan name and backup rules. A backup plan is a document that contains information that AWS Backup uses to schedule tasks that create recovery points for resources.

If you call CreateBackupPlan with a plan that already exists, you receive an AlreadyExistsException exception.

Request Syntax

```json
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string": "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlanName": "string",
    "Rules": [
      {
        "CompletionWindowMinutes": number,
        "CopyActions": [
          {
            "DestinationBackupVaultArn": "string",
            "Lifecycle": {
              "DeleteAfterDays": number,
              "MoveToColdStorageAfterDays": number
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "Lifecycle": {
          "DeleteAfterDays": number,
          "MoveToColdStorageAfterDays": number
        },
        "RecoveryPointTags": {
          "string": "string"
        },
        "RuleName": "string",
        "ScheduleExpression": "string",
        "StartWindowMinutes": number,
        "TargetBackupVaultName": "string"
      }
    ],
    "BackupPlanTags": {
      "string": "string"
    },
    "CreatorRequestId": "string"
  }
}
```

URI Request Parameters

The request does not use any URI parameters.
Request Body

The request accepts the following data in JSON format.

**BackupPlan** *(p. 392)*

Specifies the body of a backup plan. Includes a BackupPlanName and one or more sets of Rules.

**Type:** [BackupPlanInput](p. 667) object

**Required:** Yes

**BackupPlanTags** *(p. 392)*

To help organize your resources, you can assign your own metadata to the resources that you create. Each tag is a key-value pair. The specified tags are assigned to all backups created with this plan.

**Type:** String to string map

**Required:** No

**CreatorRequestId** *(p. 392)*

Identifies the request and allows failed requests to be retried without the risk of running the operation twice. If the request includes a CreatorRequestId that matches an existing backup plan, that plan is returned. This parameter is optional.

If used, this parameter must contain 1 to 50 alphanumeric or '_,_' characters.

**Type:** String

**Required:** No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "AdvancedBackupSettings": [
    {
      "BackupOptions": {
        "string": "string"
      },
      "ResourceType": "string"
    },
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "CreationDate": number,
    "VersionId": "string"
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**AdvancedBackupSettings** *(p. 393)*

A list of BackupOptions settings for a resource type. This option is only available for Windows Volume Shadow Copy Service (VSS) backup jobs.
Type: Array of AdvancedBackupSetting (p. 661) objects

**BackupPlanArn (p. 393)**

An Amazon Resource Name (ARN) that uniquely identifies a backup plan; for example, arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50.

Type: String

**BackupPlanId (p. 393)**

Uniquely identifies a backup plan.

Type: String

**CreationDate (p. 393)**

The date and time that a backup plan is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**VersionId (p. 393)**

Unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. They cannot be edited.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**AlreadyExistsException**

The required resource already exists.

HTTP Status Code: 400

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**LimitExceededException**

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateBackupSelection
Service: AWS Backup

Creates a JSON document that specifies a set of resources to assign to a backup plan. For examples, see Assigning resources programmatically.

Request Syntax

```json
PUT /backup/plans/{backupPlanId}/selections/ HTTP/1.1
Content-type: application/json

{
  "BackupSelection": {
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      ],
      "StringLike": [
        {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      ],
      "StringNotEquals": [
        {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      ],
      "StringNotLike": [
        {
          "ConditionKey": "string",
          "ConditionValue": "string"
        }
      ],
      "IamRoleArn": "string",
      "ListOfTags": [
        {
          "ConditionKey": "string",
          "ConditionType": "string",
          "ConditionValue": "string"
        }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
    },
    "CreatorRequestId": "string"
  }
}
```

URI Request Parameters

The request uses the following URI parameters.

**backupPlanId (p. 396)**

Uniquely identifies the backup plan to be associated with the selection of resources.

Required: Yes
Request Body

The request accepts the following data in JSON format.

**BackupSelection (p. 396)**

Specifies the body of a request to assign a set of resources to a backup plan.

Type: **BackupSelection (p. 676)** object

Required: Yes

**CreatorRequestId (p. 396)**

A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice. This parameter is optional.

If used, this parameter must contain 1 to 50 alphanumeric or '-_.' characters.

Type: String

Required: No

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
    "BackupPlanId": "string",
    "CreationDate": number,
    "SelectionId": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupPlanId (p. 397)**

Uniquely identifies a backup plan.

Type: String

**CreationDate (p. 397)**

The date and time a backup selection is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**SelectionId (p. 397)**

Uniquely identifies the body of a request to assign a set of resources to a backup plan.

Type: String
Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

AlreadyExistsException

The required resource already exists.

HTTP Status Code: 400

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

LimitExceededException

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateBackupVault
Service: AWS Backup

Creates a logical container where backups are stored. A CreateBackupVault request includes a name, optionally one or more resource tags, an encryption key, and a request ID.

**Note**
Do not include sensitive data, such as passport numbers, in the name of a backup vault.

Request Syntax

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string": "String"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

**backupVaultName (p. 399)**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-\_]\{2,50}\$

Required: Yes

Request Body

The request accepts the following data in JSON format.

**BackupVaultTags (p. 399)**

Metadata that you can assign to help organize the resources that you create. Each tag is a key-value pair.

Type: String to string map

Required: No

**CreatorRequestId (p. 399)**

A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice. This parameter is optional.

If used, this parameter must contain 1 to 50 alphanumeric or ‘_-’ characters.

Type: String

Required: No
EncryptionKeyArn (p. 399)

The server-side encryption key that is used to protect your backups; for example, arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab.

Type: String

Required: No

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
    "BackupVaultArn": "string",
    "BackupVaultName": "string",
    "CreationDate": "number"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupVaultArn (p. 400)

An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

BackupVaultName (p. 400)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: ^[a-zA-Z0-9\-\_]{2,50}$

CreationDate (p. 400)

The date and time a backup vault is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

AlreadyExistsException

The required resource already exists.

HTTP Status Code: 400
InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

LimitExceededException

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateFramework
Service: AWS Backup

Creates a framework with one or more controls. A framework is a collection of controls that you can use to evaluate your backup practices. By using pre-built customizable controls to define your policies, you can evaluate whether your backup practices comply with your policies and which resources are not yet in compliance.

Request Syntax

```json
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ],
      "ControlName": "string",
      "ControlScope": {
        "ComplianceResourceIds": [ "string" ],
        "ComplianceResourceTypes": [ "string" ],
        "Tags": {
          "string": "string"
        }
      }
    }
  ],
  "FrameworkDescription": "string",
  "FrameworkName": "string",
  "FrameworkTags": {
    "string": "string"
  },
  "IdempotencyToken": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

**FrameworkControls (p. 402)**

A list of the controls that make up the framework. Each control in the list has a name, input parameters, and scope.

Type: Array of FrameworkControl (p. 697) objects

Required: Yes

**FrameworkDescription (p. 402)**

An optional description of the framework with a maximum of 1,024 characters.

Type: String
Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: .\S.*

Required: No

**FrameworkName (p. 402)**

The unique name of the framework. The name must be between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][_a-zA-Z0-9]*

Required: Yes

**FrameworkTags (p. 402)**

Metadata that you can assign to help organize the frameworks that you create. Each tag is a key-value pair.

Type: String to string map

Required: No

**IdempotencyToken (p. 402)**

A customer-chosen string that you can use to distinguish between otherwise identical calls to CreateFrameworkInput. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

**Response Syntax**

HTTP/1.1 200
Content-type: application/json

{
  "FrameworkArn": "string",
  "FrameworkName": "string"
}

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**FrameworkArn (p. 403)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String
FrameworkName (p. 403)

The unique name of the framework. The name must be between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][_a-zA-Z0-9]*

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

AlreadyExistsException

The required resource already exists.

HTTP Status Code: 400

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

LimitExceededException

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateLegalHold
Service: AWS Backup

This action creates a legal hold on a recovery point (backup). A legal hold is a restraint on altering or deleting a backup until an authorized user cancels the legal hold. Any actions to delete or disassociate a recovery point will fail with an error if one or more active legal holds are on the recovery point.

Request Syntax

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
    "Description": "string",
    "IdempotencyToken": "string",
    "RecoveryPointSelection": {
        "DateRange": {
            "FromDate": number,
            "ToDate": number
        },
        "ResourceIdentifiers": [ "string" ],
        "VaultNames": [ "string" ]
    },
    "Tags": {
        "string" : "string"
    },
    "Title": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

**Description (p. 406)**

This is the string description of the legal hold.

Type: String

Required: Yes

**IdempotencyToken (p. 406)**

This is a user-chosen string used to distinguish between otherwise identical calls. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

**RecoveryPointSelection (p. 406)**

This specifies criteria to assign a set of resources, such as resource types or backup vaults.

Type: [RecoveryPointSelection (p. 710)] object

Required: No
**Tags (p. 406)**

Optional tags to include. A tag is a key-value pair you can use to manage, filter, and search for your resources. Allowed characters include UTF-8 letters, numbers, spaces, and the following characters: + - . _ : /.

Type: String to string map

Required: No

**Title (p. 406)**

This is the string title of the legal hold.

Type: String

Required: Yes

**Response Syntax**

```
HTTP/1.1 200
Content-type: application/json
{
    "CreationDate": number,
    "Description": "string",
    "LegalHoldArn": "string",
    "LegalHoldId": "string",
    "RecoveryPointSelection": {
        "DateRange": {
            "FromDate": number,
            "ToDate": number
        },
        "ResourceIdentifiers": [ "string" ],
        "VaultNames": [ "string" ]
    },
    "Status": "string",
    "Title": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**CreationDate (p. 407)**

Time in number format when legal hold was created.

Type: Timestamp

**Description (p. 407)**

This is the returned string description of the legal hold.

Type: String

**LegalHoldArn (p. 407)**

This is the ARN (Amazon Resource Number) of the created legal hold.

Type: String
LegalHoldId (p. 407)
Legal hold ID returned for the specified legal hold on a recovery point.
Type: String

RecoveryPointSelection (p. 407)
This specifies criteria to assign a set of resources, such as resource types or backup vaults.
Type: RecoveryPointSelection (p. 710) object

Status (p. 407)
This displays the status of the legal hold returned after creating the legal hold. Statuses can be ACTIVE, PENDING, CANCELED, CANCELLING, or FAILED.
Type: String
Valid Values: CREATING | ACTIVE | CANCELING | CANCELED

Title (p. 407)
This is the string title of the legal hold returned after creating the legal hold.
Type: String

Errors
For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.
HTTP Status Code: 400

LimitExceededException
A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.
HTTP Status Code: 400

MissingParameterValueException
Indicates that a required parameter is missing.
HTTP Status Code: 400

ServiceUnavailableException
The request failed due to a temporary failure of the server.
HTTP Status Code: 500

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
CreateLogicallyAirGappedBackupVault

Service: AWS Backup

This request creates a logical container to where backups may be copied.

This request includes a name, the Region, the maximum number of retention days, the minimum number of retention days, and optionally can include tags and a creator request ID.

**Note**
Do not include sensitive data, such as passport numbers, in the name of a backup vault.

**Request Syntax**

```
PUT /logically-air-gapped-backup-vaults/{backupVaultName} HTTP/1.1
Content-type: application/json

{
    "BackupVaultTags": {
        "string" : "string"
    },
    "CreatorRequestId": "string",
    "MaxRetentionDays": number,
    "MinRetentionDays": number
}
```

**URI Request Parameters**

The request uses the following URI parameters.

**backupVaultName (p. 410)**

This is the name of the vault that is being created.

Pattern: ^[a-zA-Z0-9\-_\ ]{2,50}$

Required: Yes

**Request Body**

The request accepts the following data in JSON format.

**BackupVaultTags (p. 410)**

These are the tags that will be included in the newly-created vault.

Type: String to string map

Required: No

**CreatorRequestId (p. 410)**

This is the ID of the creation request.

Type: String

Required: No

**MaxRetentionDays (p. 410)**

This is the setting that specifies the maximum retention period that the vault retains its recovery points. If this parameter is not specified, AWS Backup does not enforce a maximum retention period on the recovery points in the vault (allowing indefinite storage).
If specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or shorter than the maximum retention period. If the job retention period is longer than that maximum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault.

Type: Long
Required: Yes

MinRetentionDays (p. 410)

This setting specifies the minimum retention period that the vault retains its recovery points. If this parameter is not specified, no minimum retention period is enforced.

If specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or longer than the minimum retention period. If a job retention period is shorter than that minimum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault.

Type: Long
Required: Yes

Response Syntax

HTTP/1.1 200
Content-type: application/json

```json
{
    "BackupVaultArn": "string",
    "BackupVaultName": "string",
    "CreationDate": number,
    "VaultState": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupVaultArn (p. 411)

This is the ARN (Amazon Resource Name) of the vault being created.

Type: String

BackupVaultName (p. 411)

The name of a logical container where backups are stored. Logically air-gapped backup vaults are identified by names that are unique to the account used to create them and the Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: ^[a-zA-Z0-9\-\_]{2,50}$

CreationDate (p. 411)

The date and time when the vault was created.
This value is in Unix format, Coordinated Universal Time (UTC), and accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

VaultState (p. 411)
This is the current state of the vault.
Type: String
Valid Values: CREATING | AVAILABLE | FAILED

Errors
For information about the errors that are common to all actions, see Common Errors (p. 742).

AlreadyExistsException
The required resource already exists.
HTTP Status Code: 400

InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.
HTTP Status Code: 400

InvalidRequestException
Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.
HTTP Status Code: 400

LimitExceededException
A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.
HTTP Status Code: 400

MissingParameterValueException
Indicates that a required parameter is missing.
HTTP Status Code: 400

ServiceUnavailableException
The request failed due to a temporary failure of the server.
HTTP Status Code: 500

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
CreateReportPlan
Service: AWS Backup

Creates a report plan. A report plan is a document that contains information about the contents of the report and where AWS Backup will deliver it.

If you call CreateReportPlan with a plan that already exists, you receive an AlreadyExistsException exception.

Request Syntax

POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
  "IdempotencyToken": "string",
  "ReportDeliveryChannel": {
    "Formats": [ "string" ],
    "S3BucketName": "string",
    "S3KeyPrefix": "string"
  },
  "ReportPlanDescription": "string",
  "ReportPlanName": "string",
  "ReportPlanTags": {
    "string": "string"
  },
  "ReportSetting": {
    "Accounts": [ "string" ],
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "OrganizationUnits": [ "string" ],
    "Regions": [ "string" ],
    "ReportTemplate": "string"
  }
}

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

IdempotencyToken (p. 414)

A customer-chosen string that you can use to distinguish between otherwise identical calls to CreateReportPlanInput. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

ReportDeliveryChannel (p. 414)

A structure that contains information about where and how to deliver your reports, specifically your Amazon S3 bucket name, S3 key prefix, and the formats of your reports.

Type: ReportDeliveryChannel (p. 711) object
Required: Yes

**ReportPlanDescription (p. 414)**

An optional description of the report plan with a maximum of 1,024 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: \.*\S.*

Required: No

**ReportPlanName (p. 414)**

The unique name of the report plan. The name must be between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z]_[a-zA-Z0-9]*

Required: Yes

**ReportPlanTags (p. 414)**

Metadata that you can assign to help organize the report plans that you create. Each tag is a key-value pair.

Type: String to string map

Required: No

**ReportSetting (p. 414)**

Identifies the report template for the report. Reports are built using a report template. The report templates are:

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

If the report template is RESOURCE_COMPLIANCE_REPORT or CONTROL_COMPLIANCE_REPORT, this API resource also describes the report coverage by AWS Regions and frameworks.

Type: ReportSetting (p. 717) object

Required: Yes

**Response Syntax**

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "ReportPlanArn": "string",
  "ReportPlanName": "string"
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**CreationTime (p. 415)**

The date and time a backup vault is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationTime` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**ReportPlanArn (p. 415)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

**ReportPlanName (p. 415)**

The unique name of the report plan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][\_a-zA-Z0-9]*

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**AlreadyExistsException**

The required resource already exists.

HTTP Status Code: 400

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**LimitExceededException**

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteBackupPlan

Service: AWS Backup

Deletes a backup plan. A backup plan can only be deleted after all associated selections of resources have been deleted. Deleting a backup plan deletes the current version of a backup plan. Previous versions, if any, will still exist.

Request Syntax

DELETE /backup/plans/{backupPlanId} HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

`backupPlanId` (p. 418)

- Uniquely identifies a backup plan.
- Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "DeletionDate": number,
  "VersionId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupPlanArn (p. 418)

An Amazon Resource Name (ARN) that uniquely identifies a backup plan; for example, arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50.

Type: String

BackupPlanId (p. 418)

- Uniquely identifies a backup plan.
- Type: String
**DeletionDate (p. 418)**

The date and time a backup plan is deleted, in Unix format and Coordinated Universal Time (UTC). The value of **DeletionDate** is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**VersionId (p. 418)**

Unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. Version IDs cannot be edited.

Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**InvalidRequestException**

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
• AWS SDK for Python
• AWS SDK for Ruby V3
DeleteBackupSelection
Service: AWS Backup

Deletes the resource selection associated with a backup plan that is specified by the SelectionId.

Request Syntax

```
DELETE /backup/plans/{backupPlanId}/selections/{selectionId} HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

- **backupPlanId (p. 421)**
  - Uniquely identifies a backup plan.
  - Required: Yes
- **selectionId (p. 421)**
  - Uniquely identifies the body of a request to assign a set of resources to a backup plan.
  - Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

- **InvalidParameterValueException**
  - Indicates that something is wrong with a parameter's value. For example, the value is out of range.
  - HTTP Status Code: 400
- **MissingParameterValueException**
  - Indicates that a required parameter is missing.
  - HTTP Status Code: 400
- **ResourceNotFoundException**
  - A resource that is required for the action doesn't exist.
  - HTTP Status Code: 400
ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteBackupVault
Service: AWS Backup

Deletes the backup vault identified by its name. A vault can be deleted only if it is empty.

Request Syntax

```
DELETE /backup-vaults/<backupVaultName> HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 423)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

InvalidRequestException

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.
HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
DeleteBackupVaultAccessPolicy

Service: AWS Backup

Deletes the policy document that manages permissions on a backup vault.

Request Syntax

DELETE /backup-vaults/{backupVaultName}/access-policy HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

{backupVaultName} (p. 425)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-_\[2, 50]$^$

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.
HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteBackupVaultLockConfiguration
Service: AWS Backup

Deletes AWS Backup Vault Lock from a backup vault specified by a backup vault name.

If the Vault Lock configuration is immutable, then you cannot delete Vault Lock using API operations, and you will receive an InvalidRequestException if you attempt to do so. For more information, see Vault Lock in the AWS Backup Developer Guide.

Request Syntax

DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 427)
- The name of the backup vault from which to delete AWS Backup Vault Lock.
- Pattern: ^[a-zA-Z0-9-\-_]{2,50}$
- Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException
- Indicates that something is wrong with a parameter's value. For example, the value is out of range.
  - HTTP Status Code: 400

InvalidRequestException
- Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.
  - HTTP Status Code: 400

MissingParameterValueException
- Indicates that a required parameter is missing.
HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
DeleteBackupVaultNotifications
Service: AWS Backup

Deletes event notifications for the specified backup vault.

Request Syntax

```
DELETE /backup-vaults/{backupVaultName}/notification-configuration HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**backupVaultName** *(p. 429)*

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: `^[a-zA-Z0-9\-_\]\{2,50}\$

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors *(p. 742)*.

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.


HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteFramework
Service: AWS Backup

Deletes the framework specified by a framework name.

Request Syntax

DELETE /audit/frameworks/{frameworkName} HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

frameworkName (p. 431)

The unique name of a framework.

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z]_[a-zA-Z0-9]*

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

ConflictException

AWS Backup can't perform the action that you requested until it finishes performing a previous action. Try again later.

HTTP Status Code: 400

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400
ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteRecoveryPoint
Service: AWS Backup

Deletes the recovery point specified by a recovery point ID.

If the recovery point ID belongs to a continuous backup, calling this endpoint deletes the existing continuous backup and stops future continuous backup.

When an IAM role's permissions are insufficient to call this API, the service sends back an HTTP 200 response with an empty HTTP body, but the recovery point is not deleted. Instead, it enters an EXPIRED state.

EXPIRED recovery points can be deleted with this API once the IAM role has the iam:CreateServiceLinkedRole action. To learn more about adding this role, see Troubleshooting manual deletions.

If the user or role is deleted or the permission within the role is removed, the deletion will not be successful and will enter an EXPIRED state.

Request Syntax

```
DELETE /backup-vaults/{backupVaultName}/recovery-points/{recoveryPointArn} HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**backupVaultName** (p. 433)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: `^[a-zA-Z0-9\-_]{2,50}$`

Required: Yes

**recoveryPointArn** (p. 433)

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

InvalidRequestException

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

InvalidResourceStateException

AWS Backup is already performing an action on this recovery point. It can't perform the action you requested until the first action finishes. Try again later.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
DeleteReportPlan
Service: AWS Backup

Deletes the report plan specified by a report plan name.

Request Syntax

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

`reportPlanName` *(p. 435)*

- The unique name of a report plan.
- Pattern: `[a-zA-Z]_[a-zA-Z0-9]*`
- Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors *(p. 742).*

**ConflictException**

AWS Backup can’t perform the action that you requested until it finishes performing a previous action. Try again later.

HTTP Status Code: 400

**InvalidParameterValueException**

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400
ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeBackupJob

Service: AWS Backup

Returns backup job details for the specified BackupJobId.

Request Syntax

GET /backup-jobs/{backupJobId} HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**backupJobId (p. 437)**

- Uniquely identifies a request to AWS Backup to back up a resource.
- Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

```json
{
    "AccountId": "string",
    "BackupJobId": "string",
    "BackupOptions": {
        "string": "string"
    },
    "BackupSizeInBytes": number,
    "BackupType": "string",
    "BackupVaultArn": "string",
    "BackupVaultName": "string",
    "BytesTransferred": number,
    "ChildJobsInState": {
        "string": number
    },
    "CompletionDate": number,
    "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
    },
    "CreationDate": number,
    "ExpectedCompletionDate": number,
    "IamRoleArn": "string",
    "IsParent": boolean,
    "NumberOfChildJobs": number,
    "ParentJobId": "string",
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string"
}
```
"StartBy": number,
"State": "string",
"StatusMessage": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Accountld (p. 437)**

- Returns the account ID that owns the backup job.
- Type: String
- Pattern: \^[0-9]{12}\$

**BackupJobld (p. 437)**

- Uniquely identifies a request to AWS Backup to back up a resource.
- Type: String

**BackupOptions (p. 437)**

- Represents the options specified as part of backup plan or on-demand backup job.
- Type: String to string map
- Key Pattern: \^[a-zA-Z0-9\-_\.]{1,50}\$
- Value Pattern: \^[a-zA-Z0-9\-_\.]{1,50}\$

**BackupSizeInBytes (p. 437)**

- The size, in bytes, of a backup.
- Type: Long

**BackupType (p. 437)**

- Represents the actual backup type selected for a backup job. For example, if a successful Windows Volume Shadow Copy Service (VSS) backup was taken, BackupType returns "WindowsVSS". If BackupType is empty, then the backup type was a regular backup.
- Type: String

**BackupVaultArn (p. 437)**

- An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.
- Type: String

**BackupVaultName (p. 437)**

- The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.
- Type: String
- Pattern: \^[a-zA-Z0-9\-_\ ]{2,50}\$
BytesTransferred (p. 437)

The size in bytes transferred to a backup vault at the time that the job status was queried.

Type: Long

ChildJobsInState (p. 437)

This returns the statistics of the included child (nested) backup jobs.

Type: String to long map

Valid Keys: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

CompletionDate (p. 437)

The date and time that a job to create a backup job is completed, in Unix format and Coordinated Universal Time (UTC). The value of CompletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

CreatedBy (p. 437)

Contains identifying information about the creation of a backup job, including the BackupPlanArn, BackupPlanId, BackupPlanVersion, and BackupRuleId of the backup plan that is used to create it.

Type: RecoveryPointCreator (p. 708) object

CreationDate (p. 437)

The date and time that a backup job is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

ExpectedCompletionDate (p. 437)

The date and time that a job to back up resources is expected to be completed, in Unix format and Coordinated Universal Time (UTC). The value of ExpectedCompletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

IamRoleArn (p. 437)

Specifies the IAM role ARN used to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

IsParent (p. 437)

This returns the boolean value that a backup job is a parent (composite) job.

Type: Boolean

NumberOfChildJobs (p. 437)

This returns the number of child (nested) backup jobs.

Type: Long
**ParentJobId (p. 437)**

This returns the parent (composite) resource backup job ID.

Type: String

**PercentDone (p. 437)**

Contains an estimated percentage that is complete of a job at the time the job status was queried.

Type: String

**RecoveryPointArn (p. 437)**

An ARN that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type: String

**ResourceArn (p. 437)**

An ARN that uniquely identifies a saved resource. The format of the ARN depends on the resource type.

Type: String

**ResourceName (p. 437)**

This is the non-unique name of the resource that belongs to the specified backup.

Type: String

**ResourceType (p. 437)**

The type of AWS resource to be backed up; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database.

Type: String

Pattern: `^[a-zA-Z0-9-\-_\.]{1,50}$`

**StartBy (p. 437)**

Specifies the time in Unix format and Coordinated Universal Time (UTC) when a backup job must be started before it is canceled. The value is calculated by adding the start window to the scheduled time. So if the scheduled time were 6:00 PM and the start window is 2 hours, the StartBy time would be 8:00 PM on the date specified. The value of StartBy is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**State (p. 437)**

The current state of a backup job.

Type: String

Valid Values: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

**StatusMessage (p. 437)**

A detailed message explaining the status of the job to back up a resource.

Type: String
Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

DependencyFailureException

A dependent AWS service or resource returned an error to the AWS Backup service, and the action cannot be completed.

HTTP Status Code: 500

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeBackupVault
Service: AWS Backup

Returns metadata about a backup vault specified by its name.

Request Syntax

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**BackupVaultAccountId (p. 442)**

This is the account ID of the specified backup vault.

**backupVaultName (p. 442)**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": "number",
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string",
  "LockDate": "number",
  "Locked": "boolean",
  "MaxRetentionDays": "number",
  "MinRetentionDays": "number",
  "NumberOfRecoveryPoints": "number",
  "VaultType": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupVaultArn (p. 442)**

An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.
**BackupVaultName (p. 442)**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the Region where they are created. They consist of lowercase letters, numbers, and hyphens.

**CreationDate (p. 442)**

The date and time that a backup vault is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

**CreatorRequestId (p. 442)**

A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice.

**EncryptionKeyArn (p. 442)**

The server-side encryption key that is used to protect your backups; for example, arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab.

**LockDate (p. 442)**

The date and time when AWS Backup Vault Lock configuration cannot be changed or deleted.

If you applied Vault Lock to your vault without specifying a lock date, you can change any of your Vault Lock settings, or delete Vault Lock from the vault entirely, at any time.

This value is in Unix format, Coordinated Universal Time (UTC), and accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

**Locked (p. 442)**

A Boolean that indicates whether AWS Backup Vault Lock is currently protecting the backup vault. True means that Vault Lock causes delete or update operations on the recovery points stored in the vault to fail.

**MaxRetentionDays (p. 442)**

The AWS Backup Vault Lock setting that specifies the maximum retention period that the vault retains its recovery points. If this parameter is not specified, Vault Lock does not enforce a maximum retention period on the recovery points in the vault (allowing indefinite storage).

If specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or shorter than the maximum retention period. If the job's retention period is longer than that maximum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault. Recovery points already stored in the vault prior to Vault Lock are not affected.

Type: Long
MinRetentionDays (p. 442)

The AWS Backup Vault Lock setting that specifies the minimum retention period that the vault retains its recovery points. If this parameter is not specified, Vault Lock does not enforce a minimum retention period.

If specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or longer than the minimum retention period. If the job's retention period is shorter than that minimum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault. Recovery points already stored in the vault prior to Vault Lock are not affected.

Type: Long

NumberOfRecoveryPoints (p. 442)

The number of recovery points that are stored in a backup vault.

Type: Long

VaultType (p. 442)

This is the type of vault described.

Type: String

Valid Values: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeCopyJob
Service: AWS Backup

Returns metadata associated with creating a copy of a resource.

Request Syntax

GET /copy-jobs/copyJobId HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

copyJobId (p. 446)

Uniquely identifies a copy job.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{  "CopyJob": {    "AccountId": "string",    "BackupSizeInBytes": number,    "ChildJobsInState": {      "string": number    },    "CompletionDate": number,    "CompositeMemberIdentifier": "string",    "CopyJobId": "string",    "CreatedBy": {      "BackupPlanArn": "string",      "BackupPlanId": "string",      "BackupPlanVersion": "string",      "BackupRuleId": "string"    },    "CreationDate": number,    "DestinationBackupVaultArn": "string",    "DestinationRecoveryPointArn": "string",    "IamRoleArn": "string",    "IsParent": boolean,    "NumberOfChildJobs": number,    "ParentJobId": "string",    "ResourceArn": "string",    "ResourceName": "string",    "ResourceType": "string",    "SourceBackupVaultArn": "string",    "SourceRecoveryPointArn": "string",    "State": "string",    "StatusMessage": "string"  }
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**CopyJob (p. 446)**

Contains detailed information about a copy job.

Type: [CopyJob (p. 690)] object

Errors

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
DescribeFramework
Service: AWS Backup

Returns the framework details for the specified FrameworkName.

Request Syntax

GET /audit/frameworks/frameworkName HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

frameworkName (p. 448)

The unique name of a framework.

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][_a-zA-Z0-9]*

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{  
  "CreationTime": number,
  "DeploymentStatus": "string",
  "FrameworkArn": "string",
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ],
      "ControlName": "string",
      "ControlScope": {
        "ComplianceResourceIds": [ "string" ],
        "ComplianceResourceTypes": [ "string" ],
        "Tags": {
          "string": "string"
        }
      }
    }
  ],
  "FrameworkDescription": "string",
  "FrameworkName": "string",
  "FrameworkStatus": "string",
  "IdempotencyToken": "string"
}
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CreationTime (p. 448)

The date and time that a framework is created, in ISO 8601 representation. The value of CreationTime is accurate to milliseconds. For example, 2020-07-10T15:00:00.000-08:00 represents the 10th of July 2020 at 3:00 PM 8 hours behind UTC.

Type: Timestamp

DeploymentStatus (p. 448)

The deployment status of a framework. The statuses are:

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED

Type: String

FrameworkArn (p. 448)

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

FrameworkControls (p. 448)

A list of the controls that make up the framework. Each control in the list has a name, input parameters, and scope.

Type: Array of FrameworkControl (p. 697) objects

FrameworkDescription (p. 448)

An optional description of the framework.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: .\S.*

FrameworkName (p. 448)

The unique name of a framework.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][_a-zA-Z0-9]*

FrameworkStatus (p. 448)

A framework consists of one or more controls. Each control governs a resource, such as backup plans, backup selections, backup vaults, or recovery points. You can also turn AWS Config recording on or off for each resource. The statuses are:

• ACTIVE when recording is turned on for all resources governed by the framework.
• PARTIALLY_ACTIVE when recording is turned off for at least one resource governed by the framework.
• INACTIVE when recording is turned off for all resources governed by the framework.
• UNAVAILABLE when AWS Backup is unable to validate recording status at this time.

Type: String

IdempotencyToken (p. 448)

A customer-chosen string that you can use to distinguish between otherwise identical calls to DescribeFrameworkOutput. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn’t exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

• AWS Command Line Interface
• AWS SDK for .NET
• AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
DescribeGlobalSettings

Service: AWS Backup

Describes whether the AWS account is opted in to cross-account backup. Returns an error if the account is not a member of an Organizations organization. Example: describe-global-settings --region us-west-2

Request Syntax

GET /global-settings HTTP/1.1

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string": "string"
   },
   "LastUpdateTime": number
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

GlobalSettings (p. 451)

The status of the flag isCrossAccountBackupEnabled.

Type: String to string map

LastUpdateTime (p. 451)

The date and time that the flag isCrossAccountBackupEnabled was last updated. This update is in Unix format and Coordinated Universal Time (UTC). The value of LastUpdateTime is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).
InvalidRequestException

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeProtectedResource

Service: AWS Backup

Returns information about a saved resource, including the last time it was backed up, its Amazon Resource Name (ARN), and the AWS service type of the saved resource.

Request Syntax

```
GET /resources/resourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

<table>
<thead>
<tr>
<th>resourceArn (p. 453)</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.</td>
</tr>
<tr>
<td>Required: Yes</td>
</tr>
</tbody>
</table>

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "LastBackupTime": number,
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

LastBackupTime (p. 453)

The date and time that a resource was last backed up, in Unix format and Coordinated Universal Time (UTC). The value of LastBackupTime is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

ResourceArn (p. 453)

An ARN that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

ResourceName (p. 453)

This is the non-unique name of the resource that belongs to the specified backup.
Type: String

**ResourceType (p. 453)**

The type of AWS resource saved as a recovery point; for example, an Amazon EBS volume or an Amazon RDS database.

Type: String

Pattern: `^[a-zA-Z0-9\-\._\.]\{1,50}\$`

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
DescribeRecoveryPoint
Service: AWS Backup

Returns metadata associated with a recovery point, including ID, status, encryption, and lifecycle.

Request Syntax

GET /backup-vaults/<backupVaultName>/recovery-points/<recoveryPointArn>?backupVaultAccountId=<BackupVaultAccountId> HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

BackupVaultAccountId (p. 455)

This is the account ID of the specified backup vault.

Pattern: ^[0-9]{12}$

backupVaultName (p. 455)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

Required: Yes

recoveryPointArn (p. 455)

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
    "BackupSizeInBytes": number,
    "BackupVaultArn": string,
    "BackupVaultName": string,
    "CalculatedLifecycle": {
        "DeleteAt": number,
        "MoveToColdStorageAt": number
    },
    "CompletionDate": number,
    "CompositeMemberIdentifier": string,
    "CreatedBy": {
        "BackupPlanArn": string
    }
}
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupSizeInBytes (p. 455)**

The size, in bytes, of a backup.

Type: Long

**BackupVaultArn (p. 455)**

An ARN that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

**Backup Vault Name (p. 455)**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: ^[a-zA-Z0-9-\_]{2,50}$

**CalculatedLifecycle (p. 455)**

A CalculatedLifecycle object containing DeleteAt and MoveToColdStorageAt timestamps.

Type: CalculatedLifecycle (p. 683) object

**CompletionDate (p. 455)**

The date and time that a job to create a recovery point is completed, in Unix format and Coordinated Universal Time (UTC). The value of CompletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp

**CompositeMemberIdentifier (p. 455)**

This is the identifier of a resource within a composite group, such as nested (child) recovery point belonging to a composite (parent) stack. The ID is transferred from the logical ID within a stack.

Type: String

**CreatedBy (p. 455)**

Contains identifying information about the creation of a recovery point, including the BackupPlanArn, BackupPlanId, BackupPlanVersion, and BackupRuleId of the backup plan used to create it.

Type: RecoveryPointCreator (p. 708) object

**CreationDate (p. 455)**

The date and time that a recovery point is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**EncryptionKeyArn (p. 455)**

The server-side encryption key used to protect your backups; for example, arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab.

Type: String

**IamRoleArn (p. 455)**

Specifies the IAM role ARN used to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

**IsEncrypted (p. 455)**

A Boolean value that is returned as TRUE if the specified recovery point is encrypted, or FALSE if the recovery point is not encrypted.

Type: Boolean

**IsParent (p. 455)**

This returns the boolean value that a recovery point is a parent (composite) job.

Type: Boolean

**LastRestoreTime (p. 455)**

The date and time that a recovery point was last restored, in Unix format and Coordinated Universal Time (UTC). The value of LastRestoreTime is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**Lifecycle (p. 455)**

The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define. Backups that are transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the "retention" setting must be 90 days greater than the "transition to cold after
days" setting. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 700) object

ParentRecoveryPointArn (p. 455)

This is an ARN that uniquely identifies a parent (composite) recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type: String

RecoveryPointArn (p. 455)

An ARN that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type: String

ResourceArn (p. 455)

An ARN that uniquely identifies a saved resource. The format of the ARN depends on the resource type.

Type: String

ResourceName (p. 455)

This is the non-unique name of the resource that belongs to the specified backup.

Type: String

ResourceType (p. 455)

The type of AWS resource to save as a recovery point; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database.

Type: String

Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$

SourceBackupVaultArn (p. 455)

An Amazon Resource Name (ARN) that uniquely identifies the source vault where the resource was originally backed up in; for example, arn:aws:backup:us-east-1:123456789012:vault:BackupVault. If the recovery is restored to the same AWS account or Region, this value will be null.

Type: String

Status (p. 455)

A status code specifying the state of the recovery point.

PARTIAL status indicates AWS Backup could not create the recovery point before the backup window closed. To increase your backup plan window using the API, see UpdateBackupPlan. You can also increase your backup plan window using the Console by choosing and editing your backup plan.

EXPIRED status indicates that the recovery point has exceeded its retention period, but AWS Backup lacks permission or is otherwise unable to delete it. To manually delete these recovery points, see Step 3: Delete the recovery points in the Clean up resources section of Getting started.
STOPPED status occurs on a continuous backup where a user has taken some action that causes the continuous backup to be disabled. This can be caused by the removal of permissions, turning off versioning, turning off events being sent to EventBridge, or disabling the EventBridge rules that are put in place by AWS Backup.

To resolve STOPPED status, ensure that all requested permissions are in place and that versioning is enabled on the S3 bucket. Once these conditions are met, the next instance of a backup rule running will result in a new continuous recovery point being created. The recovery points with STOPPED status do not need to be deleted.

For SAP HANA on Amazon EC2 STOPPED status occurs due to user action, application misconfiguration, or backup failure. To ensure that future continuous backups succeed, refer to the recovery point status and check SAP HANA for details.

Type: String

Valid Values: COMPLETED | PARTIAL | DELETING | EXPIRED

**StatusMessage (p. 455)**

A status message explaining the status of the recovery point.

Type: String

**StorageClass (p. 455)**

Specifies the storage class of the recovery point. Valid values are WARM or COLD.

Type: String

Valid Values: WARM | COLD | DELETED

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](https://docs.aws.amazon.com/backup/latest/devguide/backup-errors.html).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:
- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeRegionSettings
Service: AWS Backup

Returns the current service opt-in settings for the Region. If service opt-in is enabled for a service, AWS Backup tries to protect that service's resources in this Region, when the resource is included in an on-demand backup or scheduled backup plan. Otherwise, AWS Backup does not try to protect that service's resources in this Region.

Request Syntax

GET /account-settings HTTP/1.1

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{  
  "ResourceTypeManagementPreference": {  
    "string": boolean  
  },  
  "ResourceTypeOptInPreference": {  
    "string": boolean  
  }  
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ResourceTypeManagementPreference (p. 461)

Returns whether AWS Backup fully manages the backups for a resource type.

For the benefits of full AWS Backup management, see Full AWS Backup management.

For a list of resource types and whether each supports full AWS Backup management, see the Feature availability by resource table.

If "DynamoDB": false, you can enable full AWS Backup management for DynamoDB backup by enabling AWS Backup's advanced DynamoDB backup features.

Type: String to boolean map

Key Pattern: ^[a-zA-Z0-9-\.\-_]{1,50}$

ResourceTypeOptInPreference (p. 461)

Returns a list of all services along with the opt-in preferences in the Region.
Type: String to boolean map

Key Pattern: ^[a-zA-Z0-9\-\._\[\].]{1,50}$

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeReportJob
Service: AWS Backup

Returns the details associated with creating a report as specified by its ReportJobId.

Request Syntax

GET /audit/report-jobs/reportJobId HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

reportJobId (p. 463)

The identifier of the report job. A unique, randomly generated, Unicode, UTF-8 encoded string that is at most 1,024 bytes long. The report job ID cannot be edited.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{   "ReportJob": {       "CompletionTime": number,       "CreationTime": number,       "ReportDestination": {           "S3BucketName": "string",           "S3Keys": ["string"]       },       "ReportJobId": "string",       "ReportPlanArn": "string",       "ReportTemplate": "string",       "Status": "string",       "StatusMessage": "string"   }
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ReportJob (p. 463)

A list of information about a report job, including its completion and creation times, report destination, unique report job ID, Amazon Resource Name (ARN), report template, status, and status message.

Type: ReportJob (p. 713) object
Errors

For information about the errors that are common to all actions, see [Common Errors](p. 742).

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeReportPlan
Service: AWS Backup

Returns a list of all report plans for an AWS account and AWS Region.

Request Syntax

GET /audit/report-plans/{reportPlanName} HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**reportPlanName** (p. 465)
The unique name of a report plan.

Length Constraints: Minimum length of 1. Maximum length of 256.
Pattern: [a-zA-Z][_a-zA-Z0-9]*
Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

```
{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "OrganizationUnits": [ "string" ],
         "Regions": [ "string" ],
         "ReportTemplate": "string"
      }
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.
The following data is returned in JSON format by the service.

**ReportPlan (p. 465)**

Returns details about the report plan that is specified by its name. These details include the report plan's Amazon Resource Name (ARN), description, settings, delivery channel, deployment status, creation time, and last attempted and successful run times.

Type: ReportPlan (p. 715) object

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DescribeRestoreJob
Service: AWS Backup

Returns metadata associated with a restore job that is specified by a job ID.

Request Syntax

```
GET /restore-jobs/<restoreJobId> HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

`restoreJobId (p. 467)`

Uniquely identifies the job that restores a recovery point.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupSizeInBytes": number,
  "CompletionDate": number,
  "CreatedResourceArn": "string",
  "CreationDate": number,
  "ExpectedCompletionTimeMinutes": number,
  "IamRoleArn": "string",
  "PercentDone": "string",
  "RecoveryPointArn": "string",
  "ResourceType": "string",
  "RestoreJobId": "string",
  "Status": "string",
  "StatusMessage": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

`AccountId (p. 467)`

Returns the account ID that owns the restore job.

Type: String

Pattern: `^[0-9]{12}$`
**BackupSizeInBytes (p. 467)**

The size, in bytes, of the restored resource.

Type: Long

**CompletionDate (p. 467)**

The date and time that a job to restore a recovery point is completed, in Unix format and Coordinated Universal Time (UTC). The value of CompletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**CreatedResourceArn (p. 467)**

An Amazon Resource Name (ARN) that uniquely identifies a resource whose recovery point is being restored. The format of the ARN depends on the resource type of the backed-up resource.

Type: String

**CreationDate (p. 467)**

The date and time that a restore job is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**ExpectedCompletionTimeMinutes (p. 467)**

The amount of time in minutes that a job restoring a recovery point is expected to take.

Type: Long

**IamRoleArn (p. 467)**

Specifies the IAM role ARN used to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

**PercentDone (p. 467)**

Contains an estimated percentage that is complete of a job at the time the job status was queried.

Type: String

**RecoveryPointArn (p. 467)**

An ARN that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type: String

**ResourceType (p. 467)**

Returns metadata associated with a restore job listed by resource type.

Type: String

Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$

**RestoreJobId (p. 467)**

Uniquely identifies the job that restores a recovery point.

Type: String
Status (p. 467)
Status code specifying the state of the job that is initiated by AWS Backup to restore a recovery point.

Type: String

Valid Values: PENDING | RUNNING | COMPLETED | ABORTED | FAILED

StatusMessage (p. 467)
A message showing the status of a job to restore a recovery point.

Type: String

Errors
For information about the errors that are common to all actions, see Common Errors (p. 742).

DependencyFailureException
A dependent AWS service or resource returned an error to the AWS Backup service, and the action cannot be completed.

HTTP Status Code: 500

InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException
Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException
A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException
The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
DisassociateRecoveryPoint
Service: AWS Backup

Deletes the specified continuous backup recovery point from AWS Backup and releases control of that continuous backup to the source service, such as Amazon RDS. The source service will continue to create and retain continuous backups using the lifecycle that you specified in your original backup plan.

Does not support snapshot backup recovery points.

Request Syntax

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**backupVaultName (p. 471)**

The unique name of an AWS Backup vault.

Pattern: `^[a-zA-Z0-9-\._]{2,50}$`

Required: Yes

**recoveryPointArn (p. 471)**

An Amazon Resource Name (ARN) that uniquely identifies an AWS Backup recovery point.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**InvalidRequestException**

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.
HTTP Status Code: 400
**InvalidResourceStateException**
AWS Backup is already performing an action on this recovery point. It can't perform the action you requested until the first action finishes. Try again later.

HTTP Status Code: 400
**MissingParameterValueException**
Indicates that a required parameter is missing.

HTTP Status Code: 400
**ResourceNotFoundException**
A resource that is required for the action doesn't exist.

HTTP Status Code: 400
**ServiceUnavailableException**
The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
DisassociateRecoveryPointFromParent
Service: AWS Backup

This action to a specific child (nested) recovery point removes the relationship between the specified recovery point and its parent (composite) recovery point.

Request Syntax

DELETE /backup-vaults/{backupVaultName}/recovery-points/{recoveryPointArn}/parentAssociation
HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 473)
This is the name of a logical container where the child (nested) recovery point is stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-_\[]\{2,50\}$
Required: Yes

recoveryPointArn (p. 473)
This is the Amazon Resource Name (ARN) that uniquely identifies the child (nested) recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 204

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

InvalidRequestException
Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.
HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
ExportBackupPlanTemplate
Service: AWS Backup

Returns the backup plan that is specified by the plan ID as a backup template.

Request Syntax

GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupPlanId (p. 475)
Uniquely identifies a backup plan.
Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupPlanTemplateJson (p. 475)
The body of a backup plan template in JSON format.

Note
This is a signed JSON document that cannot be modified before being passed to GetBackupPlanFromJSON.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400
MissingParameterValueException
Indicates that a required parameter is missing.
HTTP Status Code: 400

ResourceNotFoundException
A resource that is required for the action doesn't exist.
HTTP Status Code: 400

ServiceUnavailableException
The request failed due to a temporary failure of the server.
HTTP Status Code: 500

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetBackupPlan
Service: AWS Backup

Returns BackupPlan details for the specified BackupPlanId. The details are the body of a backup plan in JSON format, in addition to plan metadata.

Request Syntax

GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupPlanId (p. 477)
Uniquely identifies a backup plan.
Required: Yes

VersionId (p. 477)
Unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. Version IDs cannot be edited.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{  "AdvancedBackupSettings":  [    {      "BackupOptions": {       "string": "string"      },      "ResourceType": "string"    }  ],  "BackupPlan": {    "AdvancedBackupSettings": [      {        "BackupOptions": {         "string": "string"        },        "ResourceType": "string"      }    ],    "BackupPlanName": "string",    "Rules": [      {        "CompletionWindowMinutes": number,        "CopyActions": [          {            "DestinationBackupVaultArn": "string",          ...
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AdvancedBackupSettings (p. 477)

Contains a list of BackupOptions for each resource type. The list is populated only if the advanced option is set for the backup plan.

Type: Array of AdvancedBackupSetting (p. 661) objects

BackupPlan (p. 477)

Specifies the body of a backup plan. Includes a BackupPlanName and one or more sets of Rules.

Type: BackupPlan (p. 666) object

BackupPlanArn (p. 477)

An Amazon Resource Name (ARN) that uniquely identifies a backup plan; for example, arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50.

Type: String

BackupPlanId (p. 477)

Uniquely identifies a backup plan.

Type: String
**CreationDate (p. 477)**

The date and time that a backup plan is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**CreatorRequestId (p. 477)**

A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice.

Type: String

**DeletionDate (p. 477)**

The date and time that a backup plan is deleted, in Unix format and Coordinated Universal Time (UTC). The value of DeletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**LastExecutionDate (p. 477)**

The last time a job to back up resources was run with this backup plan. A date and time, in Unix format and Coordinated Universal Time (UTC). The value of LastExecutionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**VersionId (p. 477)**

Unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. Version IDs cannot be edited.

Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.
HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetBackupPlanFromJSON

Service: AWS Backup

Returns a valid JSON document specifying a backup plan or an error.

Request Syntax

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
    "BackupPlanTemplateJson": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

**BackupPlanTemplateJson (p. 481)**

A customer-supplied backup plan document in JSON format.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "BackupPlan": {
        "AdvancedBackupSettings": [
            {
                "BackupOptions": {
                    "string": "string"
                },
                "ResourceType": "string"
            }
        ],
        "BackupPlanName": "string",
        "Rules": [
            {
                "CompletionWindowMinutes": number,
                "CopyActions": [
                    {
                        "DestinationBackupVaultArn": "string",
                        "Lifecycle": {
                            "DeleteAfterDays": number,
                            "MoveToColdStorageAfterDays": number
                        }
                    }
                ],
                "EnableContinuousBackup": boolean,
                "Lifecycle": {
```

481
```json
  "DeleteAfterDays": number,
  "MoveToColdStorageAfterDays": number
},
  "RecoveryPointTags": {
    "string": "string"
  },
  "RuleId": "string",
  "RuleName": "string",
  "ScheduleExpression": "string",
  "StartWindowMinutes": number,
  "TargetBackupVaultName": "string"

```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupPlan (p. 481)**

Specifies the body of a backup plan. Includes a BackupPlanName and one or more sets of Rules.

Type: BackupPlan (p. 666) object

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**InvalidRequestException**

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

**LimitExceededException**

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetBackupPlanFromTemplate
Service: AWS Backup

Returns the template specified by its templateId as a backup plan.

Request Syntax

GET /backup/template/plans/templateId/toPlan HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

templateId (p. 484)

Uniquely identifies a stored backup plan template.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

```json
{
    "BackupPlanDocument": {
        "AdvancedBackupSettings": [
            {
                "BackupOptions": {
                    "string": "string",
                    "ResourceType": "string"
                }
            },
            "BackupPlanName": "string",
            "Rules": [
                {
                    "CompletionWindowMinutes": number,
                    "CopyActions": [
                        {
                            "DestinationBackupVaultArn": "string",
                            "Lifecycle": {
                                "DeleteAfterDays": number,
                                "MoveToColdStorageAfterDays": number
                            }
                        }
                    ],
                    "EnableContinuousBackup": boolean,
                    "Lifecycle": {
                        "DeleteAfterDays": number,
                        "MoveToColdStorageAfterDays": number
                    },
                    "RecoveryPointTags": {
                        "string": "string"
                    },
                    "RuleId": "string"
                }
            ]
        }
    }
}
```
"RuleName": "string",
"ScheduleExpression": "string",
"StartWindowMinutes": number,
"TargetBackupVaultName": "string"
]
]
]

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupPlanDocument (p. 484)

Returns the body of a backup plan based on the target template, including the name, rules, and backup vault of the plan.

Type: BackupPlan (p. 666) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
GetBackupSelection
Service: AWS Backup

Returns selection metadata and a document in JSON format that specifies a list of resources that are associated with a backup plan.

Request Syntax

GET /backup/plans/{backupPlanId}/selections/{selectionId} HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupPlanId (p. 487)

Uniquely identifies a backup plan.

Required: Yes

selectionId (p. 487)

Uniquely identifies the body of a request to assign a set of resources to a backup plan.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanId": "string",
  "BackupSelection": {
    "Conditions": {
      "StringEquals": [ {
        "ConditionKey": "string",
        "ConditionValue": "string"
      } ],
      "StringLike": [ {
        "ConditionKey": "string",
        "ConditionValue": "string"
      } ],
      "StringNotEquals": [ {
        "ConditionKey": "string",
        "ConditionValue": "string"
      } ],
      "StringNotLike": [ {
        "ConditionKey": "string",
        "ConditionValue": "string"
      } ]
    }
  }
}
"ConditionValue": "string"
}
],
"IamRoleArn": "string",
"ListOfTags": [
{
 "ConditionKey": "string",
 "ConditionType": "string",
 "ConditionValue": "string"
}
],
"NotResources": [ "string" ],
"Resources": [ "string" ],
"SelectionName": "string"
}
"CreationDate": number,
"CreatorRequestId": "string",
"SelectionId": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupPlanId (p. 487)

- Uniquely identifies a backup plan.
  - Type: String

BackupSelection (p. 487)

- Specifies the body of a request to assign a set of resources to a backup plan.
  - Type: BackupSelection (p. 676) object

CreationDate (p. 487)

- The date and time a backup selection is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.
  - Type: Timestamp

CreatorRequestId (p. 487)

- A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice.
  - Type: String

SelectionId (p. 487)

- Uniquely identifies the body of a request to assign a set of resources to a backup plan.
  - Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).
InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.
HTTP Status Code: 400

MissingParameterValueException
Indicates that a required parameter is missing.
HTTP Status Code: 400

ResourceNotFoundException
A resource that is required for the action doesn't exist.
HTTP Status Code: 400

ServiceUnavailableException
The request failed due to a temporary failure of the server.
HTTP Status Code: 500

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetBackupVaultAccessPolicy
Service: AWS Backup

Returns the access policy document that is associated with the named backup vault.

Request Syntax

GET /backup-vaults/backupVaultName/access-policy HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 490)
The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-_\~]{2,50}$

Required: Yes

Response Syntax

HTTP/1.1 200
Content-type: application/json

{  
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupVaultArn (p. 490)
An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012: vault:aBackupVault.

Type: String

BackupVaultName (p. 490)
The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String
Pattern: ^[a-zA-Z0-9\-\_]{2,50}$

**Policy (p. 490)**

The backup vault access policy document in JSON format.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetBackupVaultNotifications

Service: AWS Backup

Returns event notifications for the specified backup vault.

Request Syntax

GET /backup-vaults/{backupVaultName}/notification-configuration HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 492)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-_\[]\(2,50\)$

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultEvents": [ "string" ],
  "BackupVaultName": "string",
  "SNSTopicArn": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupVaultArn (p. 492)

An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

BackupVaultEvents (p. 492)

An array of events that indicate the status of jobs to back up resources to the backup vault.

Type: Array of strings
Valid Values: BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

**BackupVaultName (p. 492)**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: ^[a-zA-Z0-9\-\_]\{2,50}$

**SNSTopicArn (p. 492)**

An ARN that uniquely identifies an Amazon Simple Notification Service (Amazon SNS) topic; for example, arn:aws:sns:us-west-2:111122223333:MyTopic.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
GetLegalHold
Service: AWS Backup

This action returns details for a specified legal hold. The details are the body of a legal hold in JSON format, in addition to metadata.

Request Syntax

GET `/legal-holds/`\_\_legalHoldId\_\_ HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

legalHoldId (p. 495)

This is the ID required to use `GetLegalHold`. This unique ID is associated with a specific legal hold.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

```
{
    "CancelDescription": "string",
    "CancellationDate": number,
    "CreationDate": number,
    "Description": "string",
    "LegalHoldArn": "string",
    "LegalHoldId": "string",
    "RecoveryPointSelection": {
        "DateRange": {
            "FromDate": number,
            "ToDate": number
        },
        "ResourceIdentifiers": [ "string" ],
        "VaultNames": [ "string" ]
    },
    "RetainRecordUntil": number,
    "Status": "string",
    "Title": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CancelDescription (p. 495)

String describing the reason for removing the legal hold.
Type: String
CancellationDate (p. 495)
Time in number when legal hold was cancelled.
Type: Timestamp
CreationDate (p. 495)
Time in number format when legal hold was created.
Type: Timestamp
Description (p. 495)
This is the returned string description of the legal hold.
Type: String
LegalHoldArn (p. 495)
This is the returned framework ARN for the specified legal hold. An Amazon Resource Name (ARN) uniquely identifies a resource. The format of the ARN depends on the resource type.
Type: String
LegalHoldId (p. 495)
This is the returned ID associated with a specified legal hold.
Type: String
RecoveryPointSelection (p. 495)
This specifies criteria to assign a set of resources, such as resource types or backup vaults.
Type: RecoveryPointSelection (p. 710) object
RetainRecordUntil (p. 495)
This is the date and time until which the legal hold record will be retained.
Type: Timestamp
Status (p. 495)
This is the status of the legal hold. Statuses can be ACTIVE, CREATING, CANCELED, and CANCELING.
Type: String
Valid Values: CREATING | ACTIVE | CANCELING | CANCELED
Title (p. 495)
This is the string title of the legal hold.
Type: String

Errors
For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.
HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
GetRecoveryPointRestoreMetadata
Service: AWS Backup

Returns a set of metadata key-value pairs that were used to create the backup.

Request Syntax

```
GET /backup-vaults/{backupVaultName}/recovery-points/{recoveryPointArn}/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**BackupVaultAccountId (p. 498)**

This is the account ID of the specified backup vault.

Pattern: `^[0-9]{12}$`

**backupVaultName (p. 498)**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: `^[a-zA-Z0-9\-_\]{2,50}$`

Required: Yes

**recoveryPointArn (p. 498)**

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "RestoreMetadata": {
      "string": "String"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.
The following data is returned in JSON format by the service.

**BackupVaultArn (p. 498)**

An ARN that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

**RecoveryPointArn (p. 498)**

An ARN that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108848880D45.

Type: String

**RestoreMetadata (p. 498)**

The set of metadata key-value pairs that describe the original configuration of the backed-up resource. These values vary depending on the service that is being restored.

Type: String to string map

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
GetSupportedResourceTypes
Service: AWS Backup

Returns the AWS resource types supported by AWS Backup.

Request Syntax

GET /supported-resource-types HTTP/1.1

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ResourceTypes (p. 501)

Contains a string with the supported AWS resource types:

- Aurora for Amazon Aurora
- DynamoDB for Amazon DynamoDB
- EBS for Amazon Elastic Block Store
- EC2 for Amazon Elastic Compute Cloud
- EFS for Amazon Elastic File System
- FSX for Amazon FSx
- RDS for Amazon Relational Database Service
- Storage Gateway for Storage Gateway
- DocDB for Amazon DocumentDB (with MongoDB compatibility)
- Neptune for Amazon Neptune

Type: Array of strings

Pattern: ^[a-zA-Z0-9\-\.]{1,50}$

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).
ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListBackupJobs
Service: AWS Backup

Returns a list of existing backup jobs for an authenticated account for the last 30 days. For a longer period of time, consider using these monitoring tools.

Request Syntax

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&parentJobId=ByParentJobId&resourceArn=ByResourceArn&resourceType=ByResourceType&state=ByState
```

HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**ByAccountId (p. 503)**

The account ID to list the jobs from. Returns only backup jobs associated with the specified account ID.

If used from an AWS Organizations management account, passing * returns all jobs across the organization.

Pattern: ^\[0-9]{12}$

**ByBackupVaultName (p. 503)**

Returns only backup jobs that will be stored in the specified backup vault. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^\[a-zA-Z0-9\-_\\]{2,50}$

**ByCompleteAfter (p. 503)**

Returns only backup jobs completed after a date expressed in Unix format and Coordinated Universal Time (UTC).

**ByCompleteBefore (p. 503)**

Returns only backup jobs completed before a date expressed in Unix format and Coordinated Universal Time (UTC).

**ByCreatedAfter (p. 503)**

Returns only backup jobs that were created after the specified date.

**ByCreatedBefore (p. 503)**

Returns only backup jobs that were created before the specified date.

**ByParentJobId (p. 503)**

This is a filter to list child (nested) jobs based on parent job ID.

**ByResourceArn (p. 503)**

Returns only backup jobs that match the specified resource Amazon Resource Name (ARN).

**ByResourceType (p. 503)**

Returns only backup jobs for the specified resources:

- **Aurora** for Amazon Aurora
- DocumentDB for Amazon DocumentDB (with MongoDB compatibility)
- DynamoDB for Amazon DynamoDB
- EBS for Amazon Elastic Block Store
- EC2 for Amazon Elastic Compute Cloud
- EFS for Amazon Elastic File System
- FSx for Amazon FSx
- Neptune for Amazon Neptune
- RDS for Amazon Relational Database Service
- Storage Gateway for AWS Storage Gateway
- S3 for Amazon S3
- VirtualMachine for virtual machines

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

**ByState (p. 503)**

Returns only backup jobs that are in the specified state.

Valid Values: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

**MaxResults (p. 503)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 503)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

**Request Body**

The request does not have a request body.

**Response Syntax**

```json
HTTP/1.1 200
Content-type: application/json

{
  "BackupJobs": [
  {
    "AccountId": "string",
    "BackupJobId": "string",
    "BackupOptions": {
      "string": "string"
    },
    "BackupSizeInBytes": number,
    "BackupType": "string",
    "BackupVaultArn": "string",
    "BackupVaultName": "string",
    "BytesTransferred": number,
    "CompletionDate": number,
    "CreatedBy": {
      "BackupPlanArn": "string"
    }
  }
  ]
}
```

504
"BackupPlanId": "string",
"BackupPlanVersion": "string",
"BackupRuleId": "string"
},
"CreationDate": number,
"ExpectedCompletionDate": number,
"IamRoleArn": "string",
"IsParent": boolean,
"ParentJobId": "string",
"PercentDone": "string",
"RecoveryPointArn": "string",
"ResourceArn": "string",
"ResourceName": "string",
"ResourceType": "string",
"StartBy": number,
"State": "string",
"StatusMessage": "string"
}
"NextToken": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupJobs (p. 504)**

An array of structures containing metadata about your backup jobs returned in JSON format.

Type: Array of [BackupJob (p. 662)] objects

**NextToken (p. 504)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:
- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListBackupPlans
Service: AWS Backup

Returns a list of all active backup plans for an authenticated account. The list contains information such as Amazon Resource Names (ARNs), plan IDs, creation and deletion dates, version IDs, plan names, and creator request IDs.

Request Syntax

```
GET /backup/plans/?includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken
```

HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**IncludeDeleted (p. 507)**

A Boolean value with a default value of FALSE that returns deleted backup plans when set to TRUE.

**MaxResults (p. 507)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 507)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlansList": [
    {
      "AdvancedBackupSettings": [
        {
          "BackupOptions": {
            "string": "string"
          },
          "ResourceType": "string"
        }
      ],
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "DeletionDate": number,
      "LastExecutionDate": number,
      "VersionId": "string"
    }
  ]
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupPlansList (p. 507)**

An array of backup plan list items containing metadata about your saved backup plans.

Type: Array of *BackupPlansListMember (p. 668)* objects

**NextToken (p. 507)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**Errors**

For information about the errors that are common to all actions, see *Common Errors (p. 742).*

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
ListBackupPlanTemplates
Service: AWS Backup

Returns metadata of your saved backup plan templates, including the template ID, name, and the creation and deletion dates.

Request Syntax

GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

MaxResults (p. 510)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 510)

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{  
  "BackupPlanTemplatesList": [
    
    
    ],
  "NextToken": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupPlanTemplatesList (p. 510)

An array of template list items containing metadata about your saved templates.

Type: Array of BackupPlanTemplatesListMember (p. 670) objects
**NextToken (p. 510)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListBackupPlanVersions
Service: AWS Backup

Returns version metadata of your backup plans, including Amazon Resource Names (ARNs), backup plan IDs, creation and deletion dates, plan names, and version IDs.

Request Syntax

GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**backupPlanId** *(p. 512)*

Uniquely identifies a backup plan.

Required: Yes

**MaxResults** *(p. 512)*

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken** *(p. 512)*

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

```json
{
    "BackupPlanVersionsList": [
        {
            "AdvancedBackupSettings": [
                {
                    "BackupOptions": {
                        "string": "string"
                    },
                    "ResourceType": "string"
                }
            ],
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanName": "string",
            "CreationDate": number,
            "CreatorRequestId": "string",
            "DeletionDate": number,
            "LastExecutionDate": number,
            "VersionId": "string"
        }
    ]
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupPlanVersionsList (p. 512)**

An array of version list items containing metadata about your backup plans.

Type: Array of [BackupPlansListMember (p. 668)](p. 668) objects

**NextToken (p. 512)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors (p. 742)](p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListBackupSelections
Service: AWS Backup

Returns an array containing metadata of the resources associated with the target backup plan.

Request Syntax

```
GET /backup/plans/{backupPlanId}/selections/?maxResults={MaxResults}&nextToken={NextToken}
HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

- **backupPlanId** (p. 515)
  - Uniquely identifies a backup plan.
  - Required: Yes

- **MaxResults** (p. 515)
  - The maximum number of items to be returned.
  - Valid Range: Minimum value of 1. Maximum value of 1000.

- **NextToken** (p. 515)
  - The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "BackupSelectionsList": [
       {
            "BackupPlanId": "string",
            "CreationDate": number,
            "CreatorRequestId": "string",
            "IamRoleArn": "string",
            "SelectionId": "string",
            "SelectionName": "string"
       },
       ...
    ],
    "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.
The following data is returned in JSON format by the service.

**BackupSelectionsList (p. 515)**

An array of backup selection list items containing metadata about each resource in the list.

Type: Array of BackupSelectionsListMember (p. 678) objects

**NextToken (p. 515)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListBackupVaults

Service: AWS Backup

Returns a list of recovery point storage containers along with information about them.

**Request Syntax**

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**ByShared (p. 517)**

This parameter will sort the list of vaults by shared vaults.

**ByVaultType (p. 517)**

This parameter will sort the list of vaults by vault type.

Valid Values: BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

**MaxResults (p. 517)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 517)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultList": [
      {
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "EncryptionKeyArn": "string",
         "LockDate": number,
         "Locked": boolean,
         "MaxRetentionDays": number,
         "MinRetentionDays": number,
         "NumberOfRecoveryPoints": number
      }
   ],
   "NextToken": "string"
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupVaultList (p. 517)**

An array of backup vault list members containing vault metadata, including Amazon Resource Name (ARN), display name, creation date, number of saved recovery points, and encryption information if the resources saved in the backup vault are encrypted.

Type: Array of [BackupVaultListMember (p. 680)] objects

**NextToken (p. 517)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
ListCopyJobs
Service: AWS Backup

Returns metadata about your copy jobs.

Request Syntax

GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&destinationVaultArn=ByDestinationVaultArn&maxResults=MaxResults&nextToken=NextToken&parentJobId=ByParentJobId&resourceArn=ByResourceArn&resourceType=ByResourceType&state=ByState

HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**ByAccountId (p. 520)**

The account ID to list the jobs from. Returns only copy jobs associated with the specified account ID.

Pattern: ^[0-9]{12}$

**ByCompleteAfter (p. 520)**

Returns only copy jobs completed after a date expressed in Unix format and Coordinated Universal Time (UTC).

**ByCompleteBefore (p. 520)**

Returns only copy jobs completed before a date expressed in Unix format and Coordinated Universal Time (UTC).

**ByCreatedAfter (p. 520)**

Returns only copy jobs that were created after the specified date.

**ByCreatedBefore (p. 520)**

Returns only copy jobs that were created before the specified date.

**ByDestinationVaultArn (p. 520)**

An Amazon Resource Name (ARN) that uniquely identifies a source backup vault to copy from; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

**ByParentJobId (p. 520)**

This is a filter to list child (nested) jobs based on parent job ID.

**ByResourceArn (p. 520)**

Returns only copy jobs that match the specified resource Amazon Resource Name (ARN).

**ByResourceType (p. 520)**

Returns only backup jobs for the specified resources:

- **Aurora** for Amazon Aurora
- **DocumentDB** for Amazon DocumentDB (with MongoDB compatibility)
- **DynamoDB** for Amazon DynamoDB
- **EBS** for Amazon Elastic Block Store
- **EC2** for Amazon Elastic Compute Cloud
- **EFS** for Amazon Elastic File System
- **FSx** for Amazon FSx
AWS Backup Developer Guide
AWS Backup

- Neptune for Amazon Neptune
- RDS for Amazon Relational Database Service
- Storage Gateway for AWS Storage Gateway
- S3 for Amazon S3
- VirtualMachine for virtual machines

Pattern: ^[a-zA-Z0-9\-\._\-\.]\{1,50}\$

ByState (p. 520)

Returns only copy jobs that are in the specified state.

Valid Values: CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

MaxResults (p. 520)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 520)

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

```json
HTTP/1.1 200
Content-type: application/json

{
  "CopyJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "ChildJobsInState": {
        "string": number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
      "CopyJobId": "string",
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "IsParent": boolean,
      "NumberOfChildJobs": number,
      "ParentJobId": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string"
    }
  ]
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**CopyJobs (p. 521)**

An array of structures containing metadata about your copy jobs returned in JSON format.

- Type: Array of [CopyJob (p. 690)] objects

**NextToken (p. 521)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

- Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

- HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

- HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
ListFrameworks
Service: AWS Backup

Returns a list of all frameworks for an AWS account and AWS Region.

Request Syntax

GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

MaxResults (p. 524)

The number of desired results from 1 to 1000. Optional. If unspecified, the query will return 1 MB of data.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 524)

An identifier that was returned from the previous call to this operation, which can be used to return the next set of items in the list.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
  "Frameworks": [
    {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "FrameworkArn": "string",
      "FrameworkDescription": "string",
      "FrameworkName": "string",
      "NumberOfControls": number
    }
  ],
  "NextToken": "string"
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Frameworks (p. 524)

A list of frameworks with details for each framework, including the framework name, Amazon Resource Name (ARN), description, number of controls, creation time, and deployment status.
Type: Array of Framework (p. 695) objects

**NextToken (p. 524)**

An identifier that was returned from the previous call to this operation, which can be used to return the next set of items in the list.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListLegalHolds
Service: AWS Backup

This action returns metadata about active and previous legal holds.

Request Syntax

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken  HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**MaxResults (p. 526)**

The maximum number of resource list items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 526)**

The next item following a partial list of returned resources. For example, if a request is made to return $maxResults$ number of resources, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "LegalHolds": [
      {
         "CancellationDate": number,
         "CreationDate": number,
         "Description": "string",
         "LegalHoldArn": "string",
         "LegalHoldId": "string",
         "Status": "string",
         "Title": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**LegalHolds (p. 526)**

This is an array of returned legal holds, both active and previous.
Type: Array of LegalHold (p. 698) objects

**NextToken (p. 526)**

The next item following a partial list of returned resources. For example, if a request is made to return maxResults number of resources, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListProtectedResources
Service: AWS Backup

Returns an array of resources successfully backed up by AWS Backup, including the time the resource was
saved, an Amazon Resource Name (ARN) of the resource, and a resource type.

Request Syntax

GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

MaxResults (p. 528)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 528)

The next item following a partial list of returned items. For example, if a request is made to return
maxResults number of items, NextToken allows you to return more items in your list starting at
the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 528)

The next item following a partial list of returned items. For example, if a request is made to return
maxResults number of items, NextToken allows you to return more items in your list starting at
the location pointed to by the next token.
Type: String

**Results (p. 528)**

An array of resources successfully backed up by AWS Backup including the time the resource was saved, an Amazon Resource Name (ARN) of the resource, and a resource type.

Type: Array of [ProtectedResource (p. 701)] objects

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
ListProtectedResourcesByBackupVault

Service: AWS Backup

This request lists the protected resources corresponding to each backup vault.

Request Syntax

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**BackupVaultAccountId (p. 530)**

This is the list of protected resources by backup vault within the vault(s) you specify by account ID.

Pattern: `^[0-9]{12}$`

**backupVaultName (p. 530)**

This is the list of protected resources by backup vault within the vault(s) you specify by name.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: Yes

**MaxResults (p. 530)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 530)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "LastBackupTime": number,
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string"
    }
  ]
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**NextToken (p. 530)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**Results (p. 530)**

These are the results returned for the request ListProtectedResourcesByBackupVault.

Type: Array of ProtectedResource (p. 701) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListRecoveryPointsByBackupVault

Service: AWS Backup

Returns detailed information about the recovery points stored in a backup vault.

Request Syntax

```
GET /backup-vaults/{backupVaultName}/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore
&maxResults=MaxResults&nextToken=NextToken&parentRecoveryPointArn=ByParentRecoveryPointArn&resourceArn=ByResourceArn&resourceType=ByResourceType
```

<table>
<thead>
<tr>
<th>Request Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| **BackupVaultAccountId** (p. 533)   | This parameter will sort the list of recovery points by account ID. | ^[{0-9}][12]$
| **backupVaultName** (p. 533)       | The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens. | ^{[a-zA-Z0-9-\_.]2,50}$
| **Note**                            | Backup vault name might not be available when a supported service creates the backup. | |
| **ByBackupPlanId** (p. 533)        | Returns only recovery points that match the specified backup plan ID. | |
| **ByCreatedAfter** (p. 533)        | Returns only recovery points that were created after the specified timestamp. | |
| **ByCreatedBefore** (p. 533)       | Returns only recovery points that were created before the specified timestamp. | |
| **ByParentRecoveryPointArn** (p. 533) | This returns only recovery points that match the specified parent (composite) recovery point Amazon Resource Name (ARN). | |
| **ByResourceArn** (p. 533)         | Returns only recovery points that match the specified resource Amazon Resource Name (ARN). | |
| **ByResourceType** (p. 533)        | Returns only recovery points that match the specified resource type. | ^{[a-zA-Z0-9-\_.]1,50}$
| **MaxResults** (p. 533)            | The maximum number of items to be returned. | Valid Range: Minimum value of 1. Maximum value of 1000. |
**NextToken (p. 533)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

**Request Body**

The request does not have a request body.

**Response Syntax**

```json
HTTP/1.1 200
Content-type: application/json
{
    "NextToken": "string",
    "RecoveryPoints": [
        {
            "BackupSizeInBytes": number,
            "BackupVaultArn": "string",
            "BackupVaultName": "string",
            "CalculatedLifecycle": {
                "DeleteAt": number,
                "MoveToColdStorageAt": number
            },
            "CompletionDate": number,
            "CompositeMemberIdentifier": "string",
            "CreatedBy": {
                "BackupPlanArn": "string",
                "BackupPlanId": "string",
                "BackupPlanVersion": "string",
                "BackupRuleId": "string"
            },
            "CreationDate": number,
            "EncryptionKeyArn": "string",
            "IamRoleArn": "string",
            "IsEncrypted": boolean,
            "IsParent": boolean,
            "LastRestoreTime": number,
            "Lifecycle": {
                "DeleteAfterDays": number,
                "MoveToColdStorageAfterDays": number
            },
            "ParentRecoveryPointArn": "string",
            "RecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string",
            "SourceBackupVaultArn": "string",
            "Status": "string",
            "StatusMessage": "string"
        }
    ]
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
**NextToken (p. 534)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**RecoveryPoints (p. 534)**

An array of objects that contain detailed information about recovery points saved in a backup vault.

Type: Array of `RecoveryPointByBackupVault (p. 702)` objects

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

- **InvalidParameterValueException**
  
  Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

  HTTP Status Code: 400

- **MissingParameterValueException**
  
  Indicates that a required parameter is missing.

  HTTP Status Code: 400

- **ResourceNotFoundException**
  
  A resource that is required for the action doesn't exist.

  HTTP Status Code: 400

- **ServiceUnavailableException**
  
  The request failed due to a temporary failure of the server.

  HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
ListRecoveryPointsByLegalHold
Service: AWS Backup

This action returns recovery point ARNs (Amazon Resource Names) of the specified legal hold.

Request Syntax

GET /legal-holds/<legalHoldId>/recovery-points?maxResults=<MaxResults>&nextToken=<NextToken>
HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

* **legalHoldId (p. 536)**
  
  This is the ID of the legal hold.

  Required: Yes

* **MaxResults (p. 536)**
  
  This is the maximum number of resource list items to be returned.

  Valid Range: Minimum value of 1. Maximum value of 1000.

* **NextToken (p. 536)**
  
  This is the next item following a partial list of returned resources. For example, if a request is made to return maxResults number of resources, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json

```json
{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "BackupVaultName": "string",
      "RecoveryPointARN": "string",
      "ResourceArn": "string",
      "ResourceType": "string"
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
**NextToken (p. 536)**

This return is the next item following a partial list of returned resources.

Type: String

**RecoveryPoints (p. 536)**

This is a list of the recovery points returned by ListRecoveryPointsByLegalHold.

Type: Array of [RecoveryPointMember (p. 709)] objects

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
ListRecoveryPointsByResource

Service: AWS Backup

Returns detailed information about all the recovery points of the type specified by a resource Amazon Resource Name (ARN).

**Note**

For Amazon EFS and Amazon EC2, this action only lists recovery points created by AWS Backup.

**Request Syntax**

```plaintext
GET /resources/resourceArn/recovery-points/?maxResults=MaxResults&nextToken=NextToken
HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**MaxResults (p. 538)**

The maximum number of items to be returned.

**Note**

Amazon RDS requires a value of at least 20.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 538)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

**resourceArn (p. 538)**

An ARN that uniquely identifies a resource. The format of the ARN depends on the resource type.

Required: Yes

**Request Body**

The request does not have a request body.

**Response Syntax**

```plaintext
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "BackupSizeBytes": number,
      "BackupVaultName": "string",
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "IsParent": boolean,
      "ParentRecoveryPointArn": "string",
      "RecoveryPointArn": "string",
      "ResourceName": "string",
      "Status": "string",
    }
  ]
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**NextToken (p. 538)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**RecoveryPoints (p. 538)**

An array of objects that contain detailed information about recovery points of the specified resource type.

Note

Only Amazon EFS and Amazon EC2 recovery points return BackupVaultName.

Type: Array of RecoveryPointByResource (p. 706) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
• AWS SDK for .NET
• AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
ListReportJobs
Service: AWS Backup

Returns details about your report jobs.

Request Syntax

GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=NextToken
HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

ByCreationAfter (p. 541)

Returns only report jobs that were created after the date and time specified in Unix format and
Coordinated Universal Time (UTC). For example, the value 1516925490 represents Friday, January
26, 2018 12:11:30 AM.

ByCreationBefore (p. 541)

Returns only report jobs that were created before the date and time specified in Unix format and
Coordinated Universal Time (UTC). For example, the value 1516925490 represents Friday, January
26, 2018 12:11:30 AM.

ByReportPlanName (p. 541)

Returns only report jobs with the specified report plan name.

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z]_[a-zA-Z0-9]*

ByStatus (p. 541)

Returns only report jobs that are in the specified status. The statuses are:

CREATED | RUNNING | COMPLETED | FAILED

MaxResults (p. 541)

The number of desired results from 1 to 1000. Optional. If unspecified, the query will return 1 MB of
data.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 541)

An identifier that was returned from the previous call to this operation, which can be used to return
the next set of items in the list.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
Content-type: application/json
{
  "NextToken": "string",
  "ReportJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
        "S3BucketName": "string",
        "S3Keys": ["string"]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 541)

An identifier that was returned from the previous call to this operation, which can be used to return the next set of items in the list.

Type: String

ReportJobs (p. 541)

Details about your report jobs in JSON format.

Type: Array of ReportJob (p. 713) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:
- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListReportPlans
Service: AWS Backup

Returns a list of your report plans. For detailed information about a single report plan, use DescribeReportPlan.

Request Syntax

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**MaxResults (p. 544)**

The number of desired results from 1 to 1000. Optional. If unspecified, the query will return 1 MB of data.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 544)**

An identifier that was returned from the previous call to this operation, which can be used to return the next set of items in the list.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "NextToken": "string",
    "ReportPlans": [
        {
            "CreationTime": number,
            "DeploymentStatus": "string",
            "LastAttemptedExecutionTime": number,
            "LastSuccessfulExecutionTime": number,
            "ReportDeliveryChannel": {
                "Formats": [ "string" ],
                "S3BucketName": "string",
                "S3KeyPrefix": "string"
            },
            "ReportPlanArn": "string",
            "ReportPlanDescription": "string",
            "ReportPlanName": "string",
            "ReportSetting": {
                "Accounts": [ "string" ],
                "FrameworkArns": [ "string" ],
                "NumberOfFrameworks": number,
                "OrganizationUnits": [ "string" ],
                "Regions": [ "string" ],
                "ReportTemplate": "string"
            }
        }
    ]
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 544)
An identifier that was returned from the previous call to this operation, which can be used to return the next set of items in the list.

Type: String

ReportPlans (p. 544)
A list of your report plans with detailed information for each plan. This information includes the Amazon Resource Name (ARN), report plan name, description, settings, delivery channel, deployment status, creation time, and last times the report plan attempted to and successfully ran.

Type: Array of ReportPlan (p. 715) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException
Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

ServiceUnavailableException
The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListRestoreJobs
Service: AWS Backup

Returns a list of jobs that AWS Backup initiated to restore a saved resource, including details about the recovery process.

Request Syntax

GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&maxResults=MaxResults&nextToken=NextToken&status=ByStatus

HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

ByAccountId (p. 546)

The account ID to list the jobs from. Returns only restore jobs associated with the specified account ID.

Pattern: ^[0-9]{12}$

ByCompleteAfter (p. 546)

Returns only copy jobs completed after a date expressed in Unix format and Coordinated Universal Time (UTC).

ByCompleteBefore (p. 546)

Returns only copy jobs completed before a date expressed in Unix format and Coordinated Universal Time (UTC).

ByCreatedAfter (p. 546)

Returns only restore jobs that were created after the specified date.

ByCreatedBefore (p. 546)

Returns only restore jobs that were created before the specified date.

ByStatus (p. 546)

Returns only restore jobs associated with the specified job status.

Valid Values: PENDING | RUNNING | COMPLETED | ABORTED | FAILED

MaxResults (p. 546)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 546)

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.
Response Syntax

HTTP/1.1 200
Content-type: application/json

{  
  "NextToken": "string",
  "RestoreJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "CompletionDate": number,
      "CreatedResourceArn": "string",
      "CreationDate": number,
      "ExpectedCompletionTimeMinutes": number,
      "IamRoleArn": "string",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
      "ResourceType": "string",
      "RestoreJobId": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**NextToken (p. 547)**

The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**RestoreJobs (p. 547)**

An array of objects that contain detailed information about jobs to restore saved resources.

Type: Array of RestoreJobsListMember (p. 719) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400
ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
**ListTags**  
Service: AWS Backup

Returns a list of key-value pairs assigned to a target recovery point, backup plan, or backup vault.

ListTags only works for resource types that support full AWS Backup management of their backups. Those resource types are listed in the "Full AWS Backup management" section of the Feature availability by resource table.

**Request Syntax**

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

- **MaxResults (p. 549)**
  - The maximum number of items to be returned.
  - Valid Range: Minimum value of 1. Maximum value of 1000.

- **NextToken (p. 549)**
  - The next item following a partial list of returned items. For example, if a request is made to return maxResults number of items, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

- **resourceArn (p. 549)**
  - An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the type of resource. Valid targets for ListTags are recovery points, backup plans, and backup vaults.
  - Required: Yes

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200  
Content-type: application/json
{
    "NextToken": "string",
    "Tags": {
        "string": "string"
    }
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
**NextToken (p. 549)**

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

**Tags (p. 549)**

To help organize your resources, you can assign your own metadata to the resources you create. Each tag is a key-value pair.

Type: String to string map

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
**PutBackupVaultAccessPolicy**

Service: AWS Backup

Sets a resource-based policy that is used to manage access permissions on the target backup vault. Requires a backup vault name and an access policy document in JSON format.

**Request Syntax**

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

**URI Request Parameters**

The request uses the following URI parameters.

* backupVaultName (p. 551)
  
  The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.
  
  Pattern: `^[a-zA-Z0-9\-_\_][2,50]$`
  
  Required: Yes

**Request Body**

The request accepts the following data in JSON format.

* Policy (p. 551)
  
  The backup vault access policy document in JSON format.
  
  Type: String
  
  Required: No

**Response Syntax**

```
HTTP/1.1 200
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

* InvalidParameterValueException
  
  Indicates that something is wrong with a parameter's value. For example, the value is out of range.
HTTP Status Code: 400
**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400
**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400
**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

### See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
PutBackupVaultLockConfiguration
Service: AWS Backup

Applies AWS Backup Vault Lock to a backup vault, preventing attempts to delete any recovery point stored in or created in a backup vault. Vault Lock also prevents attempts to update the lifecycle policy that controls the retention period of any recovery point currently stored in a backup vault. If specified, Vault Lock enforces a minimum and maximum retention period for future backup and copy jobs that target a backup vault.

Note
AWS Backup Vault Lock has been assessed by Cohasset Associates for use in environments that are subject to SEC 17a-4, CFTC, and FINRA regulations. For more information about how AWS Backup Vault Lock relates to these regulations, see the [Cohasset Associates Compliance Assessment](#).

Request Syntax

```
PUT /backup-vaults/[backupVaultName]/vault-lock HTTP/1.1
Content-type: application/json

{
  "ChangeableForDays": number,
  "MaxRetentionDays": number,
  "MinRetentionDays": number
}
```

URI Request Parameters

The request uses the following URI parameters.

**backupVaultName (p. 553)**

The AWS Backup Vault Lock configuration that specifies the name of the backup vault it protects.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: Yes

Request Body

The request accepts the following data in JSON format.

**ChangeableForDays (p. 553)**

The AWS Backup Vault Lock configuration that specifies the number of days before the lock date. For example, setting `ChangeableForDays` to 30 on Jan. 1, 2022 at 8pm UTC will set the lock date to Jan. 31, 2022 at 8pm UTC.

AWS Backup enforces a 72-hour cooling-off period before Vault Lock takes effect and becomes immutable. Therefore, you must set `ChangeableForDays` to 3 or greater.

Before the lock date, you can delete Vault Lock from the vault using `DeleteBackupVaultLockConfiguration` or change the Vault Lock configuration using `PutBackupVaultLockConfiguration`. On and after the lock date, the Vault Lock becomes immutable and cannot be changed or deleted.

If this parameter is not specified, you can delete Vault Lock from the vault using `DeleteBackupVaultLockConfiguration` or change the Vault Lock configuration using `PutBackupVaultLockConfiguration` at any time.
The AWS Backup Vault Lock configuration that specifies the maximum retention period that the vault retains its recovery points. This setting can be useful if, for example, your organization's policies require you to destroy certain data after retaining it for four years (1460 days).

If this parameter is not included, Vault Lock does not enforce a maximum retention period on the recovery points in the vault. If this parameter is included without a value, Vault Lock will not enforce a maximum retention period.

If this parameter is specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or shorter than the maximum retention period. If the job's retention period is longer than that maximum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault. The longest maximum retention period you can specify is 36500 days (approximately 100 years). Recovery points already saved in the vault prior to Vault Lock are not affected.

The AWS Backup Vault Lock configuration that specifies the minimum retention period that the vault retains its recovery points. This setting can be useful if, for example, your organization's policies require you to retain certain data for at least seven years (2555 days).

If this parameter is not specified, Vault Lock will not enforce a minimum retention period.

If this parameter is specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or longer than the minimum retention period. If the job's retention period is shorter than that minimum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault. The shortest minimum retention period you can specify is 1 day. Recovery points already saved in the vault prior to Vault Lock are not affected.

Response Syntax

HTTP/1.1 200

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.
HTTP Status Code: 400

**InvalidRequestException**

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
PutBackupVaultNotifications
Service: AWS Backup

Turns on notifications on a backup vault for the specified topic and events.

Request Syntax

| PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1 |
| Content-type: application/json | |
| { |
| "BackupVaultEvents": [ "string" ], |
| "SNSTopicArn": "string" |
| } |

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 556)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-\_]\{2,50}\$

Required: Yes

Request Body

The request accepts the following data in JSON format.

BackupVaultEvents (p. 556)

An array of events that indicate the status of jobs to back up resources to the backup vault.

For common use cases and code samples, see Using Amazon SNS to track AWS Backup events.

The following events are supported:

• BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED
• COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED
• RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RECOVERY_POINT_MODIFIED
• S3_BACKUP_OBJECT FAILED | S3_RESTORE_OBJECT FAILED

Note
The list below shows items that are deprecated events (for reference) and are no longer in use. They are no longer supported and will not return statuses or notifications. Refer to the list above for current supported events.

Type: Array of strings

Valid Values: BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED |
RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

Required: Yes

**SNSTopicArn (p. 556)**

The Amazon Resource Name (ARN) that specifies the topic for a backup vault's events; for example, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Type: String

Required: Yes

**Response Syntax**

```plaintext
HTTP/1.1 200
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](https://aws.amazon.com/Documentation/).

*InvalidParameterValueException*

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

*MissingParameterValueException*

Indicates that a required parameter is missing.

HTTP Status Code: 400

*ResourceNotFoundException*

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

*ServiceUnavailableException*

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](https://aws.amazon.com/Documentation/)
- [AWS SDK for .NET](https://aws.amazon.com/Documentation/)
- [AWS SDK for C++](https://aws.amazon.com/Documentation/)
- [AWS SDK for Go](https://aws.amazon.com/Documentation/)
- [AWS SDK for Java V2](https://aws.amazon.com/Documentation/)
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
StartBackupJob
Service: AWS Backup

Starts an on-demand backup job for the specified resource.

Request Syntax

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
    "BackupOptions": {
        "string": "string"
    },
    "BackupVaultName": "string",
    "CompleteWindowMinutes": number,
    "IamRoleArn": "string",
    "IdempotencyToken": "string",
    "Lifecycle": {
        "DeleteAfterDays": number,
        "MoveToColdStorageAfterDays": number
    },
    "RecoveryPointTags": {
        "string": "string"
    },
    "ResourceArn": "string",
    "StartWindowMinutes": number
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

**BackupOptions (p. 559)**

Specifies the backup option for a selected resource. This option is only available for Windows Volume Shadow Copy Service (VSS) backup jobs.

Valid values: Set to "WindowsVSS":"enabled" to enable the WindowsVSS backup option and create a Windows VSS backup. Set to "WindowsVSS":"disabled" to create a regular backup. The WindowsVSS option is not enabled by default.

Type: String to string map

Key Pattern: ^[a-zA-Z0-9-\-\_\.]{1,50}$

Value Pattern: ^[a-zA-Z0-9-\-\_\.]{1,50}$

Required: No

**BackupVaultName (p. 559)**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String
CompleteWindowMinutes (p. 559)

A value in minutes during which a successfully started backup must complete, or else AWS Backup will cancel the job. This value is optional. This value begins counting down from when the backup was scheduled. It does not add additional time for StartWindowMinutes, or if the backup started later than scheduled.

Like StartWindowMinutes, this parameter has a maximum value of 100 years (52,560,000 minutes).

Type: Long

Required: No

IamRoleArn (p. 559)

Specifies the IAM role ARN used to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

Required: Yes

IdempotencyToken (p. 559)

A customer-chosen string that you can use to distinguish between otherwise identical calls to StartBackupJob. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

Lifecycle (p. 559)

The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup will transition and expire backups automatically according to the lifecycle that you define.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the "retention" setting must be 90 days greater than the "transition to cold after days" setting. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

This parameter has a maximum value of 100 years (36,500 days).

Type: Lifecycle (p. 700) object

Required: No

RecoveryPointTags (p. 559)

To help organize your resources, you can assign your own metadata to the resources that you create. Each tag is a key-value pair.

Type: String to string map
Required: No

**ResourceArn (p. 559)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

Required: Yes

**StartWindowMinutes (p. 559)**

A value in minutes after a backup is scheduled before a job will be canceled if it doesn’t start successfully. This value is optional, and the default is 8 hours. If this value is included, it must be at least 60 minutes to avoid errors.

This parameter has a maximum value of 100 years (52,560,000 minutes).

During the start window, the backup job status remains in CREATED status until it has successfully begun or until the start window time has run out. If within the start window time AWS Backup receives an error that allows the job to be retried, AWS Backup will automatically retry to begin the job at least every 10 minutes until the backup successfully begins (the job status changes to RUNNING) or until the job status changes to EXPIRED (which is expected to occur when the start window time is over).

Type: Long

Required: No

---

### Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "BackupJobId": "string",
    "CreationDate": number,
    "IsParent": boolean,
    "RecoveryPointArn": "string"
}
```

### Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupJobId (p. 561)**

Uniquely identifies a request to AWS Backup to back up a resource.

Type: String

**CreationDate (p. 561)**

The date and time that a backup job is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp
IsParent (p. 561)

This is a returned boolean value indicating this is a parent (composite) backup job.

Type: Boolean

RecoveryPointArn (p. 561)

Note: This field is only returned for Amazon EFS and Advanced DynamoDB resources.

An ARN that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108848880D45.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

InvalidRequestException

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

LimitExceededException

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
**StartCopyJob**

Service: AWS Backup

Starts a job to create a one-time copy of the specified resource.

Does not support continuous backups.

**Request Syntax**

```plaintext
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
   "DestinationBackupVaultArn": "string",
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number
   },
   "RecoveryPointArn": "string",
   "SourceBackupVaultName": "string"
}
```

**URI Request Parameters**

The request does not use any URI parameters.

**Request Body**

The request accepts the following data in JSON format.

**DestinationBackupVaultArn (p. 564)**

An Amazon Resource Name (ARN) that uniquely identifies a destination backup vault to copy to; for example, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

Required: Yes

**IamRoleArn (p. 564)**

Specifies the IAM role ARN used to copy the target recovery point; for example, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

Required: Yes

**IdempotencyToken (p. 564)**

A customer-chosen string that you can use to distinguish between otherwise identical calls to `StartCopyJob`. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No
Lifecycle (p. 564)

Contains an array of Transition objects specifying how long in days before a recovery point transitions to cold storage or is deleted.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, on the console, the "retention" setting must be 90 days greater than the "transition to cold after days" setting. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 700) object

Required: No

RecoveryPointArn (p. 564)

An ARN that uniquely identifies a recovery point to use for the copy job; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-10B8B48BB0D45.

Type: String

Required: Yes

SourceBackupVaultName (p. 564)

The name of a logical source container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

Required: Yes

Response Syntax

HTTP/1.1 200
Content-type: application/json

{  
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CopyJobId (p. 565)

Uniquely identifies a copy job.
**Type**: String  
**CreationDate (p. 565)**

The date and time that a copy job is created, in Unix format and Coordinated Universal Time (UTC). The value of **CreationDate** is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

**Type**: Timestamp  
**IsParent (p. 565)**

This is a returned boolean value indicating this is a parent (composite) copy job.

**Type**: Boolean

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

- **InvalidParameterValueException**
  
  Indicates that something is wrong with a parameter's value. For example, the value is out of range.
  
  HTTP Status Code: 400

- **InvalidRequestException**
  
  Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.
  
  HTTP Status Code: 400

- **LimitExceededException**
  
  A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.
  
  HTTP Status Code: 400

- **MissingParameterValueException**
  
  Indicates that a required parameter is missing.
  
  HTTP Status Code: 400

- **ResourceNotFoundException**
  
  A resource that is required for the action doesn't exist.
  
  HTTP Status Code: 400

- **ServiceUnavailableException**
  
  The request failed due to a temporary failure of the server.
  
  HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
• AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
StartReportJob
Service: AWS Backup

Starts an on-demand report job for the specified report plan.

Request Syntax

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

**reportPlanName (p. 568)**

The unique name of a report plan.

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z]_[a-zA-Z0-9]*

Required: Yes

Request Body

The request accepts the following data in JSON format.

**IdempotencyToken (p. 568)**

A customer-chosen string that you can use to distinguish between otherwise identical calls to StartReportJobInput. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
**ReportJobId (p. 568)**

The identifier of the report job. A unique, randomly generated, Unicode, UTF-8 encoded string that is at most 1,024 bytes long. The report job ID cannot be edited.

Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
StartRestoreJob
Service: AWS Backup

Recovers the saved resource identified by an Amazon Resource Name (ARN).

Request Syntax

```json
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
  "CopySourceTagsToRestoredResource": boolean,
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Metadata": {
    "string": "string"
  },
  "RecoveryPointArn": "string",
  "ResourceType": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

**CopySourceTagsToRestoredResource (p. 570)**

This is an optional parameter. If this equals True, tags included in the backup will be copied to the restored resource.

This can only be applied to backups created through AWS Backup.

Type: Boolean

Required: No

**IamRoleArn (p. 570)**

The Amazon Resource Name (ARN) of the IAM role that AWS Backup uses to create the target resource; for example: arn:aws:iam::123456789012:role/S3Access.

Type: String

Required: No

**IdempotencyToken (p. 570)**

A customer-chosen string that you can use to distinguish between otherwise identical calls to StartRestoreJob. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

**Metadata (p. 570)**

A set of metadata key-value pairs. Contains information, such as a resource name, required to restore a recovery point.
You can get configuration metadata about a resource at the time it was backed up by calling `GetRecoveryPointRestoreMetadata`. However, values in addition to those provided by `GetRecoveryPointRestoreMetadata` might be required to restore a resource. For example, you might need to provide a new resource name if the original already exists.

You need to specify specific metadata to restore an Amazon Elastic File System (Amazon EFS) instance:

- **file-system-id**: The ID of the Amazon EFS file system that is backed up by AWS Backup. Returned in `GetRecoveryPointRestoreMetadata`.
- **Encrypted**: A Boolean value that, if true, specifies that the file system is encrypted. If `KmsKeyId` is specified, `Encrypted` must be set to true.
- **KmsKeyId**: Specifies the AWS KMS key that is used to encrypt the restored file system. You can specify a key from another AWS account provided that key is properly shared with your account via AWS KMS.
- **PerformanceMode**: Specifies the throughput mode of the file system.
- **CreationToken**: A user-supplied value that ensures the uniqueness (idempotency) of the request.
- **newFileSystem**: A Boolean value that, if true, specifies that the recovery point is restored to a new Amazon EFS file system.
- **ItemsToRestore**: An array of one to five strings where each string is a file path. Use `ItemsToRestore` to restore specific files or directories rather than the entire file system. This parameter is optional. For example, "itemsToRestore": "\"/my.test\"".

Type: String to string map

Required: Yes

**RecoveryPointArn (p. 570)**

An ARN that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

Required: Yes

**ResourceType (p. 570)**

Starts a job to restore a recovery point for one of the following resources:

- **Aurora** for Amazon Aurora
- **DocumentDB** for Amazon DocumentDB (with MongoDB compatibility)
- **CloudFormation** for AWS CloudFormation
- **DynamoDB** for Amazon DynamoDB
- **EBS** for Amazon Elastic Block Store
- **EC2** for Amazon Elastic Compute Cloud
- **EFS** for Amazon Elastic File System
- **FSx** for Amazon FSx
- **Neptune** for Amazon Neptune
- **RDS** for Amazon Relational Database Service
- **Redshift** for Amazon Redshift
- **Storage Gateway** for AWS Storage Gateway
- **S3** for Amazon S3
- **Timestream** for Amazon Timestream
- **VirtualMachine** for virtual machines
Type: String
Pattern: {}^a-zA-Z0-9\-\_\.\{1,50\}$
Required: No

**Response Syntax**

```json
HTTP/1.1 200
Content-type: application/json
{
    "RestoreJobId": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**RestoreJobId (p. 572)**

Uniquely identifies the job that restores a recovery point.

Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**InvalidRequestException**

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
StopBackupJob
Service: AWS Backup

Attempts to cancel a job to create a one-time backup of a resource.

This action is not supported for the following services: Amazon FSx for Windows File Server, Amazon FSx for Lustre, FSx for ONTAP, Amazon FSx for OpenZFS, Amazon DocumentDB (with MongoDB compatibility), Amazon RDS, Amazon Aurora, and Amazon Neptune.

Request Syntax

```
POST /backup-jobs/{backupJobId} HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**backupJobId (p. 574)**

Uniquely identifies a request to AWS Backup to back up a resource.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**InvalidRequestException**

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400
ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
TagResource
Service: AWS Backup

Assigns a set of key-value pairs to a recovery point, backup plan, or backup vault identified by an Amazon Resource Name (ARN).

Request Syntax

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

**resourceArn** *(p. 576)*

An ARN that uniquely identifies a resource. The format of the ARN depends on the type of the tagged resource.

Required: Yes

Request Body

The request accepts the following data in JSON format.

**Tags** *(p. 576)*

Key-value pairs that are used to help organize your resources. You can assign your own metadata to the resources you create. For clarity, this is the structure to assign tags:

```
[{
   "Key": "string",
   "Value": "string"
}]
```

Type: String to string map

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors *(p. 742).*

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.
HTTP Status Code: 400

**LimitExceededException**

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
UntagResource
Service: AWS Backup

Removes a set of key-value pairs from a recovery point, backup plan, or backup vault identified by an Amazon Resource Name (ARN)

Request Syntax

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json
{
    "TagKeyList": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn (p. 578)

An ARN that uniquely identifies a resource. The format of the ARN depends on the type of the tagged resource.

Required: Yes

Request Body

The request accepts the following data in JSON format.

TagKeyList (p. 578)

A list of keys to identify which key-value tags to remove from a resource.

Type: Array of strings

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400
MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateBackupPlan
Service: AWS Backup

Updates an existing backup plan identified by its backupPlanId with the input document in JSON format. The new version is uniquely identified by a VersionId.

Request Syntax

POST /backup/plans/backupPlanId HTTP/1.1
Content-type: application/json

```
{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string": "string",
          "ResourceType": "string"
        },
        "BackupPlanName": "string",
        "Rules": [
          {
            "CompletionWindowMinutes": number,
            "CopyActions": [
              {
                "DestinationBackupVaultArn": "string",
                "Lifecycle": {
                  "DeleteAfterDays": number,
                  "MoveToColdStorageAfterDays": number
                }
              }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
              "DeleteAfterDays": number,
              "MoveToColdStorageAfterDays": number
            },
            "RecoveryPointTags": {
              "string": "string"
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
          }
        ]
      }
    }
  }
}
```

URI Request Parameters

The request uses the following URI parameters.

**backupPlanId (p. 580)**

Uniquely identifies a backup plan.

Required: Yes
Request Body

The request accepts the following data in JSON format.

**BackupPlan (p. 580)**

Specifies the body of a backup plan. Includes a BackupPlanName and one or more sets of Rules.

Type: **BackupPlanInput (p. 667)** object

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "AdvancedBackupSettings": [
        {
            "BackupOptions": {
                "string": "string"
            },
            "ResourceType": "string"
        }
    ],
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "CreationDate": number,
    "VersionId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**AdvancedBackupSettings (p. 581)**

Contains a list of BackupOptions for each resource type.

Type: Array of **AdvancedBackupSetting (p. 661)** objects

**BackupPlanArn (p. 581)**

An Amazon Resource Name (ARN) that uniquely identifies a backup plan; for example, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B95D-B3360DC80C50`.

Type: String

**BackupPlanId (p. 581)**

Uniquely identifies a backup plan.

Type: String

**CreationDate (p. 581)**

The date and time a backup plan is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value `1516925490.087` represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp

**VersionId (p. 581)**

Unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. Version Ids cannot be edited.

Type: String

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
UpdateFramework
Service: AWS Backup

Updates an existing framework identified by its FrameworkName with the input document in JSON format.

Request Syntax

```json
PUT /audit/frameworks/\{frameworkName\} HTTP/1.1
Content-type: application/json

{
    "FrameworkControls": [
        {
            "ControlInputParameters": [
                {
                    "ParameterName": "string",
                    "ParameterValue": "string"
                }
            ],
            "ControlName": "string",
            "ControlScope": {
                "ComplianceResourceIds": ["string"],
                "ComplianceResourceTypes": ["string"],
                "Tags": {
                    "string": "string"
                }
            }
        },
        {
            "FrameworkDescription": "string",
            "IdempotencyToken": "string"
        }
    ]
}
```

URI Request Parameters

The request uses the following URI parameters.

**frameworkName (p. 583)**

The unique name of a framework. This name is between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `[a-zA-Z][_a-zA-Z0-9]*`

Required: Yes

**Request Body**

The request accepts the following data in JSON format.

**FrameworkControls (p. 583)**

A list of the controls that make up the framework. Each control in the list has a name, input parameters, and scope.

Type: Array of FrameworkControl (p. 697) objects
Required: No

**FrameworkDescription (p. 583)**

An optional description of the framework with a maximum 1,024 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: .*\S.*

Required: No

**IdempotencyToken (p. 583)**

A customer-chosen string that you can use to distinguish between otherwise identical calls to UpdateFrameworkInput. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

**Response Syntax**

```json
HTTP/1.1 200
Content-type: application/json

{
    "CreationTime": number,
    "FrameworkArn": "string",
    "FrameworkName": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**CreationTime (p. 584)**

The date and time that a framework is created, in ISO 8601 representation. The value of CreationTime is accurate to milliseconds. For example, 2020-07-10T15:00:00.000-08:00 represents the 10th of July 2020 at 3:00 PM 8 hours behind UTC.

Type: Timestamp

**FrameworkArn (p. 584)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

**FrameworkName (p. 584)**

The unique name of a framework. This name is between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Type: String
Length Constraints: Minimum length of 1. Maximum length of 256.
Pattern: [a-zA-Z][a-zA-Z0-9]*

**Errors**

For information about the errors that are common to all actions, see [Common Errors](p. 742).

**AlreadyExistsException**

The required resource already exists.

HTTP Status Code: 400

**ConflictException**

AWS Backup can't perform the action that you requested until it finishes performing a previous action. Try again later.

HTTP Status Code: 400

**InvalidParameterValueException**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**LimitExceededException**

A limit in the request has been exceeded; for example, a maximum number of items allowed in a request.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateGlobalSettings
Service: AWS Backup

Updates whether the AWS account is opted in to cross-account backup. Returns an error if the account is not an Organizations management account. Use the DescribeGlobalSettings API to determine the current settings.

Request Syntax

```plaintext
PUT /global-settings HTTP/1.1
Content-type: application/json
{
   "GlobalSettings": {
      "string": "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GlobalSettings (p. 587)

Type: String to string map

Required: No

Response Syntax

HTTP/1.1 200

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException
Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

InvalidRequestException
Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.
HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

### See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
UpdateRecoveryPointLifecycle
Service: AWS Backup

Sets the transition lifecycle of a recovery point.

The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the "retention" setting must be 90 days greater than the "transition to cold after days" setting. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

This operation does not support continuous backups.

Request Syntax

POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number
   }
}

URI Request Parameters

The request uses the following URI parameters.

backups VaultName (p. 589)

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Pattern: ^[a-zA-Z0-9\-_\_][2,50]$

Required: Yes

recoveryPointArn (p. 589)

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9E80-435A-A80B-108B488B0D45.

Required: Yes

Request Body

The request accepts the following data in JSON format.

Lifecycle (p. 589)

The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.
Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the "retention" setting must be 90 days greater than the "transition to cold after days" setting. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

Type: Lifecycle (p. 700) object

Required: No

**Response Syntax**

HTTP/1.1 200
Content-type: application/json

```
{
  "BackupVaultArn": "string",
  "CalculatedLifecycle": {
    "DeleteAt": number,
    "MoveToColdStorageAt": number
  },
  "Lifecycle": {
    "DeleteAfterDays": number,
    "MoveToColdStorageAfterDays": number
  },
  "RecoveryPointArn": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BackupVaultArn (p. 590)**

An ARN that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

**CalculatedLifecycle (p. 590)**

A CalculatedLifecycle object containing DeleteAt and MoveToColdStorageAt timestamps.

Type: CalculatedLifecycle (p. 683) object

**Lifecycle (p. 590)**

The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the "retention" setting must be 90 days greater than the "transition to cold after days" setting. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 700) object
RecoveryPointArn (p. 590)

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

InvalidRequestException

Indicates that something is wrong with the input to the request. For example, a parameter is of the wrong type.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ResourceNotFoundException

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateRegionSettings
Service: AWS Backup

Updates the current service opt-in settings for the Region. If service-opt-in is enabled for a service, AWS Backup tries to protect that service's resources in this Region, when the resource is included in an on-demand backup or scheduled backup plan. Otherwise, AWS Backup does not try to protect that service's resources in this Region. Use the DescribeRegionSettings API to determine the resource types that are supported.

Request Syntax

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
  "ResourceTypeManagementPreference": {
    "string": boolean
  },
  "ResourceTypeOptInPreference": {
    "string": boolean
  }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

**ResourceTypeManagementPreference (p. 592)**

Enables or disables full AWS Backup management of backups for a resource type. To enable full AWS Backup management for DynamoDB along with AWS Backup's advanced DynamoDB backup features, follow the procedure to enable advanced DynamoDB backup programmatically.

Type: String to boolean map

Key Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

Required: No

**ResourceTypeOptInPreference (p. 592)**

Updates the list of services along with the opt-in preferences for the Region.

Type: String to boolean map

Key Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

Required: No

Response Syntax

```
HTTP/1.1 200
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InvalidParameterValueException

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

MissingParameterValueException

Indicates that a required parameter is missing.

HTTP Status Code: 400

ServiceUnavailableException

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateReportPlan
Service: AWS Backup

Updates an existing report plan identified by its ReportPlanName with the input document in JSON format.

Request Syntax

```
PUT /audit/report-plans/{reportPlanName} HTTP/1.1
Content-type: application/json

{
    "IdempotencyToken": "string",
    "ReportDeliveryChannel": {
        "Formats": [ "string" ],
        "S3BucketName": "string",
        "S3KeyPrefix": "string"
    },
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "Accounts": [ "string" ],
        "FrameworkArns": [ "string" ],
        "NumberOfFrameworks": number,
        "OrganizationUnits": [ "string" ],
        "Regions": [ "string" ],
        "ReportTemplate": "string"
    }
}
```

URI Request Parameters

The request uses the following URI parameters.

**reportPlanName (p. 594)**

The unique name of the report plan. This name is between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][a-zA-Z0-9]*

Required: Yes

Request Body

The request accepts the following data in JSON format.

**IdempotencyToken (p. 594)**

A customer-chosen string that you can use to distinguish between otherwise identical calls to UpdateReportPlanInput. Retrying a successful request with the same idempotency token results in a success message with no action taken.

Type: String

Required: No

**ReportDeliveryChannel (p. 594)**

A structure that contains information about where to deliver your reports, specifically your Amazon S3 bucket name, S3 key prefix, and the formats of your reports.
Type: **ReportDeliveryChannel (p. 711)** object

Required: No

**ReportPlanDescription (p. 594)**

An optional description of the report plan with a maximum 1,024 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*\S.*`

Required: No

**ReportSetting (p. 594)**

Identifies the report template for the report. Reports are built using a report template. The report templates are:

- RESOURCE_COMPLIANCE_REPORT
- CONTROL_COMPLIANCE_REPORT
- BACKUP_JOB_REPORT
- COPY_JOB_REPORT
- RESTORE_JOB_REPORT

If the report template is RESOURCE_COMPLIANCE_REPORT or CONTROL_COMPLIANCE_REPORT, this API resource also describes the report coverage by AWS Regions and frameworks.

Type: **ReportSetting (p. 717)** object

Required: No

**Response Syntax**

```json
HTTP/1.1 200
Content-type: application/json
{
    "CreationTime": number,
    "ReportPlanArn": "string",
    "ReportPlanName": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**CreationTime (p. 595)**

The date and time that a report plan is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationTime is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**ReportPlanArn (p. 595)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String
**ReportPlanName (p. 595)**

The unique name of the report plan.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][_a-zA-Z0-9]*

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

**ConflictException**

AWS Backup can't perform the action that you requested until it finishes performing a previous action. Try again later.

HTTP Status Code: 400

**InvalidParameterValueException**

Indicates that something is wrong with a parameter’s value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueException**

Indicates that a required parameter is missing.

HTTP Status Code: 400

**ResourceNotFoundException**

A resource that is required for the action doesn't exist.

HTTP Status Code: 400

**ServiceUnavailableException**

The request failed due to a temporary failure of the server.

HTTP Status Code: 500

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
AWS Backup gateway

The following actions are supported by AWS Backup gateway:

- AssociateGatewayToServer (p. 598)
- CreateGateway (p. 600)
- DeleteGateway (p. 603)
- DeleteHypervisor (p. 605)
- DisassociateGatewayFromServer (p. 607)
- GetBandwidthRateLimitSchedule (p. 609)
- GetGateway (p. 611)
- GetHypervisor (p. 613)
- GetHypervisorPropertyMappings (p. 615)
- GetVirtualMachine (p. 618)
- ImportHypervisorConfiguration (p. 620)
- ListGateways (p. 623)
- ListHypervisors (p. 626)
- ListTagsForResource (p. 629)
- ListVirtualMachines (p. 631)
- PutBandwidthRateLimitSchedule (p. 634)
- PutHypervisorPropertyMappings (p. 637)
- PutMaintenanceStartTime (p. 640)
- StartVirtualMachinesMetadataSync (p. 643)
- TagResource (p. 645)
- TestHypervisorConfiguration (p. 647)
- UntagResource (p. 650)
- UpdateGatewayInformation (p. 652)
- UpdateGatewaySoftwareNow (p. 654)
- UpdateHypervisor (p. 656)
**AssociateGatewayToServer**

Service: AWS Backup gateway

Associates a backup gateway with your server. After you complete the association process, you can back up and restore your VMs through the gateway.

**Request Syntax**

```json
{
  "GatewayArn": "string",
  "ServerArn": "string"
}
```

**Request Parameters**

For information about the parameters that are common to all actions, see [Common Parameters (p. 741)](#).

The request accepts the following data in JSON format.

**GatewayArn (p. 598)**

The Amazon Resource Name (ARN) of the gateway. Use the ListGateways operation to return a list of gateways for your account and AWS Region.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway:[a-zA-Z0-9]\{3\}/[a-zA-Z0-9]+$`

Required: Yes

**ServerArn (p. 598)**

The Amazon Resource Name (ARN) of the server that hosts your virtual machines.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway:[a-zA-Z0-9]\{3\}/[a-zA-Z0-9]+$`

Required: Yes

**Response Syntax**

```json
{
  "GatewayArn": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
**GatewayArn (p. 598)**

The Amazon Resource Name (ARN) of a gateway.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](p.742).

**ConflictException**

The operation cannot proceed because it is not supported.

HTTP Status Code: 400

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](p.742)
- [AWS SDK for .NET](p.742)
- [AWS SDK for C++](p.742)
- [AWS SDK for Go](p.742)
- [AWS SDK for Java V2](p.742)
- [AWS SDK for JavaScript](p.742)
- [AWS SDK for PHP V3](p.742)
- [AWS SDK for Python](p.742)
- [AWS SDK for Ruby V3](p.742)
CreateGateway
Service: AWS Backup gateway

Creates a backup gateway. After you create a gateway, you can associate it with a server using the AssociateGatewayToServer operation.

Request Syntax

```json
{
  "ActivationKey": "string",
  "GatewayDisplayName": "string",
  "GatewayType": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**ActivationKey (p. 600)**

The activation key of the created gateway.

Type: String


Pattern: ^[0-9a-zA-Z\-]+$

Required: Yes

**GatewayDisplayName (p. 600)**

The display name of the created gateway.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: ^[a-zA-Z0-9-]+\$`

Required: Yes

**GatewayType (p. 600)**

The type of created gateway.

Type: String

Valid Values: BACKUP_VM

Required: Yes
**Tags (p. 600)**

A list of up to 50 tags to assign to the gateway. Each tag is a key-value pair.

Type: Array of [Tag (p. 734)] objects

Required: No

**Response Syntax**

```
{
  "GatewayArn": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**GatewayArn (p. 601)**

The Amazon Resource Name (ARN) of the gateway you create.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
AWS Backup Developer Guide
AWS Backup gateway

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteGateway
Service: AWS Backup gateway

Deletes a backup gateway.

Request Syntax

```
{
   "GatewayArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**GatewayArn (p. 603)**

The Amazon Resource Name (ARN) of the gateway to delete.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
   "GatewayArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**GatewayArn (p. 603)**

The Amazon Resource Name (ARN) of the gateway you deleted.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).
**InternalServerErrorException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
DeleteHypervisor

Service: AWS Backup gateway

Deletes a hypervisor.

Request Syntax

```json
{
  "HypervisorArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**HypervisorArn (p. 605)**

The Amazon Resource Name (ARN) of the hypervisor to delete.

- **Type:** String
- **Length Constraints:** Minimum length of 50. Maximum length of 500.
- **Pattern:** `arn:(aws|aws-cn|aws-us-gov):backup-gateway:[a-zA-Z-0-9]+\/[a-zA-Z-0-9]+`
- **Required:** Yes

Response Syntax

```json
{
  "HypervisorArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**HypervisorArn (p. 605)**

The Amazon Resource Name (ARN) of the hypervisor you deleted.

- **Type:** String
- **Length Constraints:** Minimum length of 50. Maximum length of 500.
- **Pattern:** `arn:(aws|aws-cn|aws-us-gov):backup-gateway:[a-zA-Z-0-9]+\/[a-zA-Z-0-9]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).
AccessDeniedException

The operation cannot proceed because you have insufficient permissions.

HTTP Status Code: 400

ConflictException

The operation cannot proceed because it is not supported.

HTTP Status Code: 400

InternalServerException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn't found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DisassociateGatewayFromServer
Service: AWS Backup gateway

Disassociates a backup gateway from the specified server. After the disassociation process finishes, the
gateway can no longer access the virtual machines on the server.

Request Syntax

```
{
    "GatewayArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common
Parameters (p. 741).

The request accepts the following data in JSON format.

**GatewayArn** (p. 607)

The Amazon Resource Name (ARN) of the gateway to disassociate.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
    "GatewayArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**GatewayArn** (p. 607)

The Amazon Resource Name (ARN) of the gateway you disassociated.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).
ConflictException

The operation cannot proceed because it is not supported.

HTTP Status Code: 400

InternalServerException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn't found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetBandwidthRateLimitSchedule
Service: AWS Backup gateway

Retrieves the bandwidth rate limit schedule for a specified gateway. By default, gateways do not have bandwidth rate limit schedules, which means no bandwidth rate limiting is in effect. Use this to get a gateway's bandwidth rate limit schedule.

Request Syntax

```json
{
  "GatewayArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**GatewayArn (p. 609)**

The Amazon Resource Name (ARN) of the gateway. Use the ListGateways operation to return a list of gateways for your account and AWS Region.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```json
{
  "BandwidthRateLimitIntervals": [
    {
      "AverageUploadRateLimitInBitsPerSec": number,
      "DaysOfWeek": [ number ],
      "EndHourOfDay": number,
      "EndMinuteOfHour": number,
      "StartHourOfDay": number,
      "StartMinuteOfHour": number
    }
  ],
  "GatewayArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**BandwidthRateLimitIntervals (p. 609)**

An array containing bandwidth rate limit schedule intervals for a gateway. When no bandwidth rate limit intervals have been scheduled, the array is empty.
Type: Array of BandwidthRateLimitInterval (p. 722) objects

Array Members: Minimum number of 0 items. Maximum number of 20 items.

**GatewayArn (p. 609)**

The Amazon Resource Name (ARN) of the gateway. Use the `ListGateways` operation to return a list of gateways for your account and AWS Region.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetGateway
Service: AWS Backup gateway

By providing the ARN (Amazon Resource Name), this API returns the gateway.

Request Syntax

```json
{
   "GatewayArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**GatewayArn (p. 611)**

The Amazon Resource Name (ARN) of the gateway.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```json
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
         "DayOfWeek": number,
         "HourOfDay": number,
         "MinuteOfHour": number
      },
      "NextUpdateAvailabilityTime": number,
      "VpcEndpoint": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Gateway (p. 611)**

By providing the ARN (Amazon Resource Name), this API returns the gateway.
Type: GatewayDetails (p. 726) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InternalServerException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn’t found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetHypervisor
Service: AWS Backup gateway

This action requests information about the specified hypervisor to which the gateway will connect. A hypervisor is hardware, software, or firmware that creates and manages virtual machines, and allocates resources to them.

Request Syntax

```
{
   "HypervisorArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**HypervisorArn (p. 613)**

The Amazon Resource Name (ARN) of the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
      "LatestMetadataSyncStatus": "string",
      "LatestMetadataSyncStatusMessage": "string",
      "LogGroupArn": "string",
      "Name": "string",
      "State": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Hypervisor (p. 613)**

Details about the requested hypervisor.
Type: HypervisorDetails (p. 730) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InternalServerErrorException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn't found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetHypervisorPropertyMappings
Service: AWS Backup gateway

This action retrieves the property mappings for the specified hypervisor. A hypervisor property mapping displays the relationship of entity properties available from the hypervisor to the properties available in AWS.

Request Syntax

```
{
  "HypervisorArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**HypervisorArn (p. 615)**

The Amazon Resource Name (ARN) of the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
  "HypervisorArn": "string",
  "IamRoleArn": "string",
  "VmwareToAwsTagMappings": [
    {
      "AwsTagKey": "string",
      "AwsTagValue": "string",
      "VmwareCategory": "string",
      "VmwareTagName": "string"
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**HypervisorArn (p. 615)**

The Amazon Resource Name (ARN) of the hypervisor.
Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


**IamRoleArn (p. 615)**

The Amazon Resource Name (ARN) of the IAM role.

Type: String


**VmwareToAwsTagMappings (p. 615)**

This is a display of the mappings of VMware tags to the AWS tags.

Type: Array of **VmwareToAwsTagMapping (p. 740)** objects

**Errors**

For information about the errors that are common to all actions, see *Common Errors (p. 742).*

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- **AWS Command Line Interface**
- **AWS SDK for .NET**
- **AWS SDK for C++**
- **AWS SDK for Go**
- **AWS SDK for Java V2**
- **AWS SDK for JavaScript**
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
GetVirtualMachine
Service: AWS Backup gateway

By providing the ARN (Amazon Resource Name), this API returns the virtual machine.

Request Syntax

```
{
  "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**ResourceArn (p. 618)**

The Amazon Resource Name (ARN) of the virtual machine.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
  "VirtualMachine": {
    "HostName": "string",
    "HypervisorId": "string",
    "LastBackupDate": "number",
    "Name": "string",
    "Path": "string",
    "ResourceArn": "string",
    "VmwareTags": [
      {
        "VmwareCategory": "string",
        "VmwareTagDescription": "string",
        "VmwareTagName": "string"
      }
    ]
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
VirtualMachine (p. 618)

This object contains the basic attributes of VirtualMachine contained by the output of GetVirtualMachine

Type: VirtualMachineDetails (p. 737) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InternalServerErrorException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn't found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ImportHypervisorConfiguration
Service: AWS Backup gateway

Connect to a hypervisor by importing its configuration.

Request Syntax

```json
{
  "Host": "string",
  "KmsKeyArn": "string",
  "Name": "string",
  "Password": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Username": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**Host (p. 620)**

The server host of the hypervisor. This can be either an IP address or a fully-qualified domain name (FQDN).

Type: String


Pattern: ^.+$

Required: Yes

**KmsKeyArn (p. 620)**

The AWS Key Management Service for the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

Pattern: ^(arn:(aws|aws-cn|aws-us-gov):kms:[a-zA-Z0-9-]+):(0-9)+:(key|alias)/(\S+)$|^(alias/(\S+)$)

Required: No

**Name (p. 620)**

The name of the hypervisor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[a-zA-Z0-9-]*$
Required: Yes
**Password (p. 620)**
The password for the hypervisor.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[ -~]*$
Required: No
**Tags (p. 620)**
The tags of the hypervisor configuration to import.
Type: Array of Tag (p. 734) objects
Required: No
**Username (p. 620)**
The username for the hypervisor.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[ -\-\.0-\[\]-\~]*[^!-\-\.0-\[\]-\~][ -\-\.0-\[\]-\~]*$
Required: No

**Response Syntax**

```
{
   "HypervisorArn" : "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.
The following data is returned in JSON format by the service.

**HypervisorArn (p. 621)**
The Amazon Resource Name (ARN) of the hypervisor you disassociated.
Type: String
Length Constraints: Minimum length of 50. Maximum length of 500.
AccessDeniedException
The operation cannot proceed because you have insufficient permissions.
HTTP Status Code: 400

ConflictException
The operation cannot proceed because it is not supported.
HTTP Status Code: 400

InternalServerException
The operation did not succeed because an internal error occurred. Try again later.
HTTP Status Code: 500

ThrottlingException
TPS has been limited to protect against intentional or unintentional high request volumes.
HTTP Status Code: 400

ValidationException
The operation did not succeed because a validation error occurred.
HTTP Status Code: 400

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListGateways
Service: AWS Backup gateway

Lists backup gateways owned by an AWS account in an AWS Region. The returned list is ordered by gateway Amazon Resource Name (ARN).

Request Syntax

```json
{
  "MaxResults": number,
  "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**MaxResults (p. 623)**

The maximum number of gateways to list.

- Type: Integer
- Valid Range: Minimum value of 1.
- Required: No

**NextToken (p. 623)**

The next item following a partial list of returned resources. For example, if a request is made to return `MaxResults` number of resources, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

- Type: String
- Pattern: `^\.+\$`
- Required: No

Response Syntax

```json
{
  "Gateways": [
    {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number
    },
    {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number
    },
    ...
  ],
  "NextToken": "string"
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Gateways (p. 623)**

A list of your gateways.

Type: Array of Gateway (p. 724) objects

**NextToken (p. 623)**

The next item following a partial list of returned resources. For example, if a request is made to return maxResults number of resources, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: ^\.+$ 

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListHypervisors
Service: AWS Backup gateway

Lists your hypervisors.

Request Syntax

```json
{
    "MaxResults": number,
    "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**MaxResults (p. 626)**

The maximum number of hypervisors to list.

Type: Integer

Valid Range: Minimum value of 1.

Required: No

**NextToken (p. 626)**

The next item following a partial list of returned resources. For example, if a request is made to return maxResults number of resources, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: ^.+$

Required: No

Response Syntax

```json
{
    "Hypervisors": [
        {
            "Host": "string",
            "HypervisorArn": "string",
            "KmsKeyArn": "string",
            "Name": "string",
            "State": "string"
        }
    ],
    "NextToken": "string"
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Hypervisors (p. 626)**

A list of your Hypervisor objects, ordered by their Amazon Resource Names (ARNs).

Type: Array of Hypervisor (p. 728) objects

**NextToken (p. 626)**

The next item following a partial list of returned resources. For example, if a request is made to return `maxResults` number of resources, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: ^.*$

Errors

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
• AWS SDK for Ruby V3
ListTagsForResource
Service: AWS Backup gateway

Lists the tags applied to the resource identified by its Amazon Resource Name (ARN).

Request Syntax

```
{
    "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**ResourceArn (p. 629)**

The Amazon Resource Name (ARN) of the resource's tags to list.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
    "ResourceArn": "string",
    "Tags": [
        {
            "Key": "string",
            "Value": "string"
        }
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**ResourceArn (p. 629)**

The Amazon Resource Name (ARN) of the resource's tags that you listed.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

**Tags (p. 629)**

A list of the resource's tags.

Type: Array of [Tag (p. 734)] objects

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)].

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface]
- [AWS SDK for .NET]
- [AWS SDK for C++]
- [AWS SDK for Go]
- [AWS SDK for Java V2]
- [AWS SDK for JavaScript]
- [AWS SDK for PHP V3]
- [AWS SDK for Python]
- [AWS SDK for Ruby V3]
ListVirtualMachines
Service: AWS Backup gateway
Lists your virtual machines.

Request Syntax

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**HypervisorArn (p. 631)**

The Amazon Resource Name (ARN) of the hypervisor connected to your virtual machine.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: No

**MaxResults (p. 631)**

The maximum number of virtual machines to list.

Type: Integer

Valid Range: Minimum value of 1.

Required: No

**NextToken (p. 631)**

The next item following a partial list of returned resources. For example, if a request is made to return maxResults number of resources, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: ^.+$

Required: No

Response Syntax

```
{
```

"NextToken": "string",
"VirtualMachines": [
  {
    "HostName": "string",
    "HypervisorId": "string",
    "LastBackupDate": number,
    "Name": "string",
    "Path": "string",
    "ResourceArn": "string"
  }
]
}

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 631)

The next item following a partial list of returned resources. For example, if a request is made to return maxResults number of resources, NextToken allows you to return more items in your list starting at the location pointed to by the next token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: ^.+$

VirtualMachines (p. 631)

A list of your VirtualMachine objects, ordered by their Amazon Resource Names (ARNs).

Type: Array of VirtualMachine (p. 735) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InternalServerException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:
• AWS Command Line Interface
• AWS SDK for .NET
• AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
PutBandwidthRateLimitSchedule

Service: AWS Backup gateway

This action sets the bandwidth rate limit schedule for a specified gateway. By default, gateways do not have a bandwidth rate limit schedule, which means no bandwidth rate limiting is in effect. Use this to initiate a gateway's bandwidth rate limit schedule.

Request Syntax

```
{
    "BandwidthRateLimitIntervals": [
        {
            "AverageUploadRateLimitInBitsPerSec": number,
            "DaysOfWeek": [ number ],
            "EndHourOfDay": number,
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
        }
    ],
    "GatewayArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](p. 741).

The request accepts the following data in JSON format.

**BandwidthRateLimitIntervals (p. 634)**

An array containing bandwidth rate limit schedule intervals for a gateway. When no bandwidth rate limit intervals have been scheduled, the array is empty.

Type: Array of [BandwidthRateLimitInterval (p. 722)] objects

Array Members: Minimum number of 0 items. Maximum number of 20 items.

Required: Yes

**GatewayArn (p. 634)**

The Amazon Resource Name (ARN) of the gateway. Use the [ListGateways](p. 452) operation to return a list of gateways for your account and AWS Region.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
    "GatewayArn": "string"
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response. The following data is returned in JSON format by the service.

**GatewayArn (p. 634)**

The Amazon Resource Name (ARN) of the gateway. Use the `ListGateways` operation to return a list of gateways for your account and AWS Region.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see [Common Errors (p. 742)](common-errors.html).

**InternalServerError**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](aws-cli.html)
- [AWS SDK for .NET](aws-sdk-net.html)
- [AWS SDK for C++](aws-sdk-c++.html)
- [AWS SDK for Go](aws-sdk-go.html)
- [AWS SDK for Java V2](aws-sdk-javav2.html)
- [AWS SDK for JavaScript](aws-sdk-javascript.html)
- [AWS SDK for PHP V3](aws-sdk-phpv3.html)
- AWS SDK for Python
- AWS SDK for Ruby V3
PutHypervisorPropertyMappings
Service: AWS Backup gateway

This action sets the property mappings for the specified hypervisor. A hypervisor property mapping displays the relationship of entity properties available from the hypervisor to the properties available in AWS.

Request Syntax

```
{
    "HypervisorArn": "string",
    "IamRoleArn": "string",
    "VmwareToAwsTagMappings": [
        {
            "AwsTagKey": "string",
            "AwsTagValue": "string",
            "VmwareCategory": "string",
            "VmwareTagName": "string"
        }
    ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**HypervisorArn (p. 637)**

The Amazon Resource Name (ARN) of the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

**IamRoleArn (p. 637)**

The Amazon Resource Name (ARN) of the IAM role.

Type: String


Required: Yes

**VmwareToAwsTagMappings (p. 637)**

This action requests the mappings of VMware tags to the AWS tags.

Type: Array of VmwareToAwsTagMapping (p. 740) objects

Required: Yes
Response Syntax

```json
{
    "HypervisorArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**HypervisorArn (p. 638)**

The Amazon Resource Name (ARN) of the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see `Common Errors (p. 742)`.

**AccessDeniedException**

The operation cannot proceed because you have insufficient permissions.

HTTP Status Code: 400

**ConflictException**

The operation cannot proceed because it is not supported.

HTTP Status Code: 400

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
PutMaintenanceStartTime
Service: AWS Backup gateway

Set the maintenance start time for a gateway.

Request Syntax

```
{
  "DayOfMonth": number,
  "DayOfWeek": number,
  "GatewayArn": "string",
  "HourOfDay": number,
  "MinuteOfHour": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**DayOfMonth (p. 640)**

The day of the month start maintenance on a gateway.

Valid values range from Sunday to Saturday.

Type: Integer


Required: No

**DayOfWeek (p. 640)**

The day of the week to start maintenance on a gateway.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 6.

Required: No

**GatewayArn (p. 640)**

The Amazon Resource Name (ARN) for the gateway, used to specify its maintenance start time.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

**HourOfDay (p. 640)**

The hour of the day to start maintenance on a gateway.

Type: Integer
Valid Range: Minimum value of 0. Maximum value of 23.
Required: Yes

**MinuteOfHour (p. 640)**

The minute of the hour to start maintenance on a gateway.
Type: Integer
Valid Range: Minimum value of 0. Maximum value of 59.
Required: Yes

**Response Syntax**

```json
{
   "GatewayArn": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**GatewayArn (p. 641)**

The Amazon Resource Name (ARN) of a gateway for which you set the maintenance start time.
Type: String
Length Constraints: Minimum length of 50. Maximum length of 500.
Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z0-9\-]+){3}\/[a-zA-Z0-9]+$

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 742).

**ConflictException**

The operation cannot proceed because it is not supported.
HTTP Status Code: 400

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.
HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.
HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.
HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
StartVirtualMachinesMetadataSync
Service: AWS Backup gateway

This action sends a request to sync metadata across the specified virtual machines.

Request Syntax

```
{
    "HypervisorArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**HypervisorArn (p. 643)**

The Amazon Resource Name (ARN) of the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
    "HypervisorArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**HypervisorArn (p. 643)**

The Amazon Resource Name (ARN) of the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).
AccessDeniedException

The operation cannot proceed because you have insufficient permissions.

HTTP Status Code: 400

InternalServerErrorException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn't found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
TagResource
Service: AWS Backup gateway

Tag the resource.

Request Syntax

```json
{
    "ResourceARN": "string",
    "Tags": [
        {
            "Key": "string",
            "Value": "string"
        }
    ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**ResourceARN (p. 645)**

The Amazon Resource Name (ARN) of the resource to tag.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

**Tags (p. 645)**

A list of tags to assign to the resource.

Type: Array of Tag (p. 734) objects

Required: Yes

Response Syntax

```json
{
    "ResourceARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**ResourceARN (p. 645)**

The Amazon Resource Name (ARN) of the resource you tagged.
Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- **AWS Command Line Interface**
- **AWS SDK for .NET**
- **AWS SDK for C++**
- **AWS SDK for Go**
- **AWS SDK for Java V2**
- **AWS SDK for JavaScript**
- **AWS SDK for PHP V3**
- **AWS SDK for Python**
- **AWS SDK for Ruby V3**
TestHypervisorConfiguration
Service: AWS Backup gateway

Tests your hypervisor configuration to validate that backup gateway can connect with the hypervisor and its resources.

Request Syntax

```
{
    "GatewayArn": "string",
    "Host": "string",
    "Password": "string",
    "Username": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](p. 741).

The request accepts the following data in JSON format.

**GatewayArn (p. 647)**

The Amazon Resource Name (ARN) of the gateway to the hypervisor to test.

- Type: String
- Required: Yes

**Host (p. 647)**

The server host of the hypervisor. This can be either an IP address or a fully-qualified domain name (FQDN).

- Type: String
- Pattern: ^.+$
- Required: Yes

**Password (p. 647)**

The password for the hypervisor.

- Type: String
- Pattern: ^[ -~]+$
- Required: No

**Username (p. 647)**

The username for the hypervisor.
Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: ^[ -\0-\[\]-~]*[!-\0-\[\]-~][ -\0-\[\]-~]*$

Required: No

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 742)](#).

**ConflictException**

The operation cannot proceed because it is not supported.

HTTP Status Code: 400

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)
UntagResource
Service: AWS Backup gateway
Removes tags from the resource.

Request Syntax

```
{
    "ResourceARN": "string",
    "TagKeys": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**ResourceARN (p. 650)**

The Amazon Resource Name (ARN) of the resource from which to remove tags.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

**TagKeys (p. 650)**

The list of tag keys specifying which tags to remove.

Type: Array of strings


Pattern: `^([\p{L}\p{Z}\p{N}_.:=/-@]*)$`

Required: Yes

Response Syntax

```
{
    "ResourceARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**ResourceARN (p. 650)**

The Amazon Resource Name (ARN) of the resource from which you removed tags.
Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

InternalServerException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn't found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateGatewayInformation
Service: AWS Backup gateway

Updates a gateway's name. Specify which gateway to update using the Amazon Resource Name (ARN) of the gateway in your request.

Request Syntax

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](p. 741).

The request accepts the following data in JSON format.

**GatewayArn (p. 652)**

The Amazon Resource Name (ARN) of the gateway to update.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

**GatewayDisplayName (p. 652)**

The updated display name of the gateway.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `^[a-zA-Z0-9-]*$`

Required: No

Response Syntax

```
{
   "GatewayArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**GatewayArn (p. 652)**

The Amazon Resource Name (ARN) of the gateway you updated.
Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

ConflictException

The operation cannot proceed because it is not supported.

HTTP Status Code: 400

InternalServerException

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

ResourceNotFoundException

A resource that is required for the action wasn't found.

HTTP Status Code: 400

ThrottlingException

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

ValidationException

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateGatewaySoftwareNow
Service: AWS Backup gateway

Updates the gateway virtual machine (VM) software. The request immediately triggers the software update.

**Note**
When you make this request, you get a 200 OK success response immediately. However, it might take some time for the update to complete.

Request Syntax

```
{
  "GatewayArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

**GatewayArn (p. 654)**

The Amazon Resource Name (ARN) of the gateway to be updated.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

Response Syntax

```
{
  "GatewayArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**GatewayArn (p. 654)**

The Amazon Resource Name (ARN) of the gateway you updated.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

**InternalServerException**

The operation did not succeed because an internal error occurred. Try again later.

HTTP Status Code: 500

**ResourceNotFoundException**

A resource that is required for the action wasn't found.

HTTP Status Code: 400

**ThrottlingException**

TPS has been limited to protect against intentional or unintentional high request volumes.

HTTP Status Code: 400

**ValidationException**

The operation did not succeed because a validation error occurred.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateHypervisor
Service: AWS Backup gateway

Updates a hypervisor metadata, including its host, username, and password. Specify which hypervisor to update using the Amazon Resource Name (ARN) of the hypervisor in your request.

Request Syntax

```json
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 741).

The request accepts the following data in JSON format.

**Host (p. 656)**

The updated host of the hypervisor. This can be either an IP address or a fully-qualified domain name (FQDN).

Type: String


Pattern: ^.+$

Required: No

**HypervisorArn (p. 656)**

The Amazon Resource Name (ARN) of the hypervisor to update.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: Yes

**LogGroupArn (p. 656)**

The Amazon Resource Name (ARN) of the group of gateways within the requested log.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.


Required: No
Required: No

**Name (p. 656)**

The updated name for the hypervisor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `^[a-zA-Z0-9-]*$`

Required: No

**Password (p. 656)**

The updated password for the hypervisor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `^[ -~]*$`

Required: No

**Username (p. 656)**

The updated username for the hypervisor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: `^[ -\.0-\[\]-~]*[!-\~\[\]-~][ -\.0-\[\]-~]*$`

Required: No

**Response Syntax**

```json
{
   "HypervisorArn": "string"
}
```

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**HypervisorArn (p. 657)**

The Amazon Resource Name (ARN) of the hypervisor you updated.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 742).

AccessDeniedException
The operation cannot proceed because you have insufficient permissions.
HTTP Status Code: 400

ConflictException
The operation cannot proceed because it is not supported.
HTTP Status Code: 400

InternalServerException
The operation did not succeed because an internal error occurred. Try again later.
HTTP Status Code: 500

ResourceNotFoundException
A resource that is required for the action wasn't found.
HTTP Status Code: 400

ThrottlingException
TPS has been limited to protect against intentional or unintentional high request volumes.
HTTP Status Code: 400

ValidationException
The operation did not succeed because a validation error occurred.
HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The following data types are supported by AWS Backup:

- AdvancedBackupSetting (p. 661)
The following data types are supported by AWS Backup gateway:

- **BackupJob** (p. 662)
- **BackupPlan** (p. 666)
- **BackupPlanInput** (p. 667)
- **BackupPlansListMember** (p. 668)
- **BackupPlanTemplatesListMember** (p. 670)
- **BackupRule** (p. 671)
- **BackupRuleInput** (p. 674)
- **BackupSelection** (p. 676)
- **BackupSelectionsListMember** (p. 678)
- **BackupVaultListMember** (p. 680)
- **CalculatedLifecycle** (p. 683)
- **Condition** (p. 684)
- **ConditionParameter** (p. 685)
- **Conditions** (p. 686)
- **ControlInputParameter** (p. 687)
- **CopyAction** (p. 689)
- **CopyJob** (p. 690)
- **DateRange** (p. 694)
- **Framework** (p. 695)
- **FrameworkControl** (p. 697)
- **LegalHold** (p. 698)
- **Lifecycle** (p. 700)
- **ProtectedResource** (p. 701)
- **RecoveryPointByBackupVault** (p. 702)
- **RecoveryPointByResource** (p. 706)
- **RecoveryPointCreator** (p. 708)
- **RecoveryPointMember** (p. 709)
- **RecoveryPointSelection** (p. 710)
- **ReportDeliveryChannel** (p. 711)
- **ReportDestination** (p. 712)
- **ReportJob** (p. 713)
- **ReportPlan** (p. 715)
- **ReportSetting** (p. 717)
- **RestoreJobsListMember** (p. 719)

The following data types are supported by AWS Backup gateway:

- **BandwidthRateLimitInterval** (p. 722)
- **Gateway** (p. 724)
- **GatewayDetails** (p. 726)
- **Hypervisor** (p. 728)
- **HypervisorDetails** (p. 730)
- **MaintenanceStartTime** (p. 732)
- **Tag** (p. 734)
- **VirtualMachine** (p. 735)
AWS Backup

The following data types are supported by AWS Backup:

- AdvancedBackupSetting (p. 661)
- BackupJob (p. 662)
- BackupPlan (p. 666)
- BackupPlanInput (p. 667)
- BackupPlansListMember (p. 668)
- BackupPlanTemplatesListMember (p. 670)
- BackupRule (p. 671)
- BackupRuleInput (p. 674)
- BackupSelection (p. 676)
- BackupSelectionsListMember (p. 678)
- BackupVaultListMember (p. 680)
- CalculatedLifecycle (p. 683)
- Condition (p. 684)
- ConditionParameter (p. 685)
- Conditions (p. 686)
- ControlInputParameter (p. 687)
- ControlScope (p. 688)
- CopyAction (p. 689)
- CopyJob (p. 690)
- DateRange (p. 694)
- Framework (p. 695)
- FrameworkControl (p. 697)
- LegalHold (p. 698)
- Lifecycle (p. 700)
- ProtectedResource (p. 701)
- RecoveryPointByBackupVault (p. 702)
- RecoveryPointByResource (p. 706)
- RecoveryPointCreator (p. 708)
- RecoveryPointMember (p. 709)
- RecoveryPointSelection (p. 710)
- ReportDeliveryChannel (p. 711)
- ReportDestination (p. 712)
- ReportJob (p. 713)
- ReportPlan (p. 715)
- ReportSetting (p. 717)
- RestoreJobsListMember (p. 719)
AdvancedBackupSetting
Service: AWS Backup

A list of backup options for each resource type.

Contents

BackupOptions

Specifies the backup option for a selected resource. This option is only available for Windows VSS backup jobs.

Valid values:

Set to "WindowsVSS":"enabled" to enable the WindowsVSS backup option and create a Windows VSS backup.

Set to "WindowsVSS":"disabled" to create a regular backup. The WindowsVSS option is not enabled by default.

If you specify an invalid option, you get an InvalidParameterValueException exception.

For more information about Windows VSS backups, see Creating a VSS-Enabled Windows Backup.

Type: String to string map

Key Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$

Value Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$

Required: No

ResourceType

Specifies an object containing resource type and backup options. The only supported resource type is Amazon EC2 instances with Windows Volume Shadow Copy Service (VSS). For a CloudFormation example, see the sample CloudFormation template to enable Windows VSS in the AWS Backup User Guide.

Valid values: EC2.

Type: String

Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
BackupJob
Service: AWS Backup

Contains detailed information about a backup job.

Contents

AccountId
The account ID that owns the backup job.
Type: String
Pattern: ^[0-9]{12}$
Required: No

BackupJobId
Uniquely identifies a request to AWS Backup to back up a resource.
Type: String
Required: No

BackupOptions
Specifies the backup option for a selected resource. This option is only available for Windows Volume Shadow Copy Service (VSS) backup jobs.

Valid values: Set to "WindowsVSS": "enabled" to enable the WindowsVSS backup option and create a Windows VSS backup. Set to "WindowsVSS": "disabled" to create a regular backup. If you specify an invalid option, you get an InvalidParameterValueException exception.
Type: String to string map
Key Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$
Value Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$
Required: No

BackupSizeInBytes
The size, in bytes, of a backup.
Type: Long
Required: No

BackupType
Represents the type of backup for a backup job.
Type: String
Required: No

BackupVaultArn
An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.
Type: String
Required: No

**BackupVaultName**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: `^[a-zA-Z0-9\-_\.]\{2,50}$`

Required: No

**Bytes Transferred**

The size in bytes transferred to a backup vault at the time that the job status was queried.

Type: Long

Required: No

**CompletionDate**

The date and time a job to create a backup job is completed, in Unix format and Coordinated Universal Time (UTC). The value of `CompletionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**CreatedBy**

Contains identifying information about the creation of a backup job, including the `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, and `BackupRuleId` of the backup plan used to create it.

Type: `RecoveryPointCreator (p. 708)` object

Required: No

**CreationDate**

The date and time a backup job is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**ExpectedCompletionDate**

The date and time a job to back up resources is expected to be completed, in Unix format and Coordinated Universal Time (UTC). The value of `ExpectedCompletionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**IamRoleArn**

Specifies the IAM role ARN used to create the target recovery point. IAM roles other than the default role must include either `AWSBackup` or `AwsBackup` in the role name. For example,
arn::aws:iam::123456789012:role/AWSBackupRDSAccess. Role names without those strings lack permissions to perform backup jobs.

Type: String
Required: No

IsParent
This is a boolean value indicating this is a parent (composite) backup job.

Type: Boolean
Required: No

ParentJobId
This uniquely identifies a request to AWS Backup to back up a resource. The return will be the parent (composite) job ID.

Type: String
Required: No

PercentDone
Contains an estimated percentage complete of a job at the time the job status was queried.

Type: String
Required: No

RecoveryPointArn
An ARN that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type: String
Required: No

ResourceArn
An ARN that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String
Required: No

ResourceName
This is the non-unique name of the resource that belongs to the specified backup.

Type: String
Required: No

ResourceType
The type of AWS resource to be backed up; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database. For Windows Volume Shadow Copy Service (VSS) backups, the only supported resource type is Amazon EC2.

Type: String
Pattern: ^[a-zA-Z0-9\-\_.]{1,50}$
Required: No

**StartBy**

Specifies the time in Unix format and Coordinated Universal Time (UTC) when a backup job must be started before it is canceled. The value is calculated by adding the start window to the scheduled time. So if the scheduled time were 6:00 PM and the start window is 2 hours, the StartBy time would be 8:00 PM on the date specified. The value of StartBy is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp
Required: No

**State**

The current state of a backup job.

Type: String

Valid Values: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

Required: No

**StatusMessage**

A detailed message explaining the status of the job to back up a resource.

Type: String
Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
BackupPlan
Service: AWS Backup

Contains an optional backup plan display name and an array of BackupRule objects, each of which specifies a backup rule. Each rule in a backup plan is a separate scheduled task and can back up a different selection of AWS resources.

Contents

BackupPlanName

The display name of a backup plan. Must contain 1 to 50 alphanumeric or ‘-_.’ characters.

Type: String
Required: Yes

Rules

An array of BackupRule objects, each of which specifies a scheduled task that is used to back up a selection of resources.

Type: Array of BackupRule objects
Required: Yes

AdvancedBackupSettings

Contains a list of BackupOptions for each resource type.

Type: Array of AdvancedBackupSetting objects
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
BackupPlanInput
Service: AWS Backup

Contains an optional backup plan display name and an array of BackupRule objects, each of which specifies a backup rule. Each rule in a backup plan is a separate scheduled task.

Contents

BackupPlanName

The display name of a backup plan. Must contain 1 to 50 alphanumeric or ‘-.’ characters.

Type: String

Required: Yes

Rules

An array of BackupRule objects, each of which specifies a scheduled task that is used to back up a selection of resources.

Type: Array of BackupRuleInput (p. 674) objects

Required: Yes

AdvancedBackupSettings

Specifies a list of BackupOptions for each resource type. These settings are only available for Windows Volume Shadow Copy Service (VSS) backup jobs.

Type: Array of AdvancedBackupSetting (p. 661) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
**BackupPlansListMember**
Service: AWS Backup

Contains metadata about a backup plan.

**Contents**

**AdvancedBackupSettings**

Contains a list of BackupOptions for a resource type.

Type: Array of [AdvancedBackupSetting](p. 661) objects

Required: No

**BackupPlanArn**

An Amazon Resource Name (ARN) that uniquely identifies a backup plan; for example, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type: String

Required: No

**BackupPlanId**

Uniquely identifies a backup plan.

Type: String

Required: No

**BackupPlanName**

The display name of a saved backup plan.

Type: String

Required: No

**CreationDate**

The date and time a resource backup plan is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**CreatorRequestId**

A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice. This parameter is optional.

If used, this parameter must contain 1 to 50 alphanumeric or ‘-_.’ characters.

Type: String

Required: No

**DeletionDate**

The date and time a backup plan is deleted, in Unix format and Coordinated Universal Time (UTC). The value of DeletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp
Required: No

**LastExecutionDate**

The last time a job to back up resources was run with this rule. A date and time, in Unix format and Coordinated Universal Time (UTC). The value of `LastExecutionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp
Required: No

**VersionId**

Unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. Version IDs cannot be edited.

Type: String
Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)
BackupPlanTemplatesListMember

Service: AWS Backup

An object specifying metadata associated with a backup plan template.

Contents

BackupPlanTemplateId

Uniquely identifies a stored backup plan template.

Type: String
Required: No

BackupPlanTemplateName

The optional display name of a backup plan template.

Type: String
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
BackupRule
Service: AWS Backup

Specifies a scheduled task used to back up a selection of resources.

Contents

RuleName
A display name for a backup rule. Must contain 1 to 50 alphanumeric or '-' '_' characters.
Type: String
Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$
Required: Yes

TargetBackupVaultName
The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.
Type: String
Pattern: ^[a-zA-Z0-9\-\_\-]{2,50}$
Required: Yes

CompletionWindowMinutes
A value in minutes after a backup job is successfully started before it must be completed or it will be canceled by AWS Backup. This value is optional.
Type: Long
Required: No

CopyActions
An array of CopyAction objects, which contains the details of the copy operation.
Type: Array of CopyAction (p. 689) objects
Required: No

EnableContinuousBackup
Specifies whether AWS Backup creates continuous backups. True causes AWS Backup to create continuous backups capable of point-in-time restore (PITR). False (or not specified) causes AWS Backup to create snapshot backups.
Type: Boolean
Required: No

Lifecycle
The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the "retention" setting must be 90 days greater than the "transition to cold after days"
setting. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 700) object

Required: No

RecoveryPointTags

An array of key-value pair strings that are assigned to resources that are associated with this rule when restored from backup.

Type: String to string map

Required: No

RuleId

Uniquely identifies a rule that is used to schedule the backup of a selection of resources.

Type: String

Required: No

ScheduleExpression

A cron expression in UTC specifying when AWS Backup initiates a backup job. For more information about AWS cron expressions, see Schedule Expressions for Rules in the Amazon CloudWatch Events User Guide. Two examples of AWS cron expressions are 15 * ? * * * (take a backup every hour at 15 minutes past the hour) and 0 12 * * ? * (take a backup every day at 12 noon UTC). For a table of examples, click the preceding link and scroll down the page.

Type: String

Required: No

StartWindowMinutes

A value in minutes after a backup is scheduled before a job will be canceled if it doesn't start successfully. This value is optional. If this value is included, it must be at least 60 minutes to avoid errors.

During the start window, the backup job status remains in CREATED status until it has successfully begun or until the start window time has run out. If within the start window time AWS Backup receives an error that allows the job to be retried, AWS Backup will automatically retry to begin the job at least every 10 minutes until the backup successfully begins (the job status changes to RUNNING) or until the job status changes to EXPIRED (which is expected to occur when the start window time is over).

Type: Long

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for Ruby V3
BackupRuleInput
Service: AWS Backup

Specifies a scheduled task used to back up a selection of resources.

Contents

RuleName
A display name for a backup rule. Must contain 1 to 50 alphanumeric or ‘-_.’ characters.
Type: String
Pattern: ^[a-zA-Z0-9-\._\.]\{1,50}\$
Required: Yes

TargetBackupVaultName
The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.
Type: String
Pattern: ^[a-zA-Z0-9-\._\.\_]\{2,50}\$
Required: Yes

CompletionWindowMinutes
A value in minutes after a backup job is successfully started before it must be completed or it will be canceled by AWS Backup. This value is optional.
Type: Long
Required: No

CopyActions
An array of CopyAction objects, which contains the details of the copy operation.
Type: Array of CopyAction (p. 689) objects
Required: No

EnableContinuousBackup
Specifies whether AWS Backup creates continuous backups. True causes AWS Backup to create continuous backups capable of point-in-time restore (PITR). False (or not specified) causes AWS Backup to create snapshot backups.
Type: Boolean
Required: No

Lifecycle
The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup will transition and expire backups automatically according to the lifecycle that you define.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the “retention” setting must be 90 days greater than the “transition to cold after days”
setting. The “transition to cold after days” setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

This parameter has a maximum value of 100 years (36,500 days).

Type: Lifecycle (p. 700) object

Required: No

RecoveryPointTags

To help organize your resources, you can assign your own metadata to the resources that you create. Each tag is a key-value pair.

Type: String to string map

Required: No

ScheduleExpression

A CRON expression in UTC specifying when AWS Backup initiates a backup job.

Type: String

Required: No

StartWindowMinutes

A value in minutes after a backup is scheduled before a job will be canceled if it doesn't start successfully. This value is optional. If this value is included, it must be at least 60 minutes to avoid errors.

This parameter has a maximum value of 100 years (52,560,000 minutes).

During the start window, the backup job status remains in CREATED status until it has successfully begun or until the start window time has run out. If within the start window time AWS Backup receives an error that allows the job to be retried, AWS Backup will automatically retry to begin the job at least every 10 minutes until the backup successfully begins (the job status changes to RUNNING) or until the job status changes to EXPIRED (which is expected to occur when the start window time is over).

Type: Long

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
BackupSelection
Service: AWS Backup

Used to specify a set of resources to a backup plan.

Specifying your desired Conditions, ListOfTags, NotResources, and/or Resources is recommended. If none of these are specified, Backup will attempt to select all supported and opted-in storage resources, which could have unintended cost implications.

Contents

**IamRoleArn**

The ARN of the IAM role that AWS Backup uses to authenticate when backing up the target resource; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

Required: Yes

**SelectionName**

The display name of a resource selection document. Must contain 1 to 50 alphanumeric or '-_.' characters.

Type: String

Pattern: ^[a-zA-Z0-9\-\_.]{1,50}$

Required: Yes

**Conditions**

A list of conditions that you define to assign resources to your backup plans using tags. For example, "StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" },. Condition operators are case sensitive.

Conditions differs from ListOfTags as follows:
- When you specify more than one condition, you only assign the resources that match ALL conditions (using AND logic).
- Conditions supports StringEquals, StringLike, StringNotEquals, and StringNotLike. ListOfTags only supports StringEquals.

Type: [Conditions (p. 686)] object

Required: No

**ListOfTags**

A list of conditions that you define to assign resources to your backup plans using tags. For example, "StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" },. Condition operators are case sensitive.

ListOfTags differs from Conditions as follows:
- When you specify more than one condition, you assign all resources that match AT LEAST ONE condition (using OR logic).
- ListOfTags only supports StringEquals. Conditions supports StringEquals, StringLike, StringNotEquals, and StringNotLike.

Type: Array of [Condition (p. 684)] objects
**NotResources**

A list of Amazon Resource Names (ARNs) to exclude from a backup plan. The maximum number of ARNs is 500 without wildcards, or 30 ARNs with wildcards.

If you need to exclude many resources from a backup plan, consider a different resource selection strategy, such as assigning only one or a few resource types or refining your resource selection using tags.

Type: Array of strings  
Required: No

**Resources**

A list of Amazon Resource Names (ARNs) to assign to a backup plan. The maximum number of ARNs is 500 without wildcards, or 30 ARNs with wildcards.

If you need to assign many resources to a backup plan, consider a different resource selection strategy, such as assigning all resources of a resource type or refining your resource selection using tags.

Type: Array of strings  
Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](https://aws-sdk_cpp.github.io/)
- [AWS SDK for Go](https://github.com/aws/aws-sdk-go)
- [AWS SDK for Java V2](https://docs.aws.amazon.com/java/sdk-for-aws/latest/api/index.html)
- [AWS SDK for Ruby V3](https://github.com/aws/aws-sdk-ruby)
BackupSelectionsListMember
Service: AWS Backup

Contains metadata about a BackupSelection object.

Contents

BackupPlanId
Uniquely identifies a backup plan.
Type: String
Required: No

CreationDate
The date and time a backup plan is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp
Required: No

CreatorRequestId
A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice. This parameter is optional.
If used, this parameter must contain 1 to 50 alphanumeric or ‘-_.’ characters.
Type: String
Required: No

IamRoleArn
Specifies the IAM role Amazon Resource Name (ARN) to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.
Type: String
Required: No

SelectionId
Uniquely identifies a request to assign a set of resources to a backup plan.
Type: String
Required: No

SelectionName
The display name of a resource selection document.
Type: String
Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$
Required: No
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
**BackupVaultListMember**

*Service: AWS Backup*

Contains metadata about a backup vault.

**Contents**

**BackupVaultArn**

An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

Required: No

**BackupVaultName**

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: `^[a-zA-Z0-9\-_]{2,50}$`

Required: No

**CreationDate**

The date and time a resource backup is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationDate` is accurate to milliseconds. For example, the value `1516925490.087` represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**CreatorRequestId**

A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice. This parameter is optional.

If used, this parameter must contain 1 to 50 alphanumeric or `-_.` characters.

Type: String

Required: No

**EncryptionKeyArn**

A server-side encryption key you can specify to encrypt your backups from services that support full AWS Backup management; for example, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. If you specify a key, you must specify its ARN, not its alias. If you do not specify a key, AWS Backup creates a KMS key for you by default.

To learn which AWS Backup services support full AWS Backup management and how AWS Backup handles encryption for backups from services that do not yet support full AWS Backup, see [Encryption for backups in AWS Backup](#).

Type: String
Required: No

**LockDate**

The date and time when AWS Backup Vault Lock configuration becomes immutable, meaning it cannot be changed or deleted.

If you applied Vault Lock to your vault without specifying a lock date, you can change your Vault Lock settings, or delete Vault Lock from the vault entirely, at any time.

This value is in Unix format, Coordinated Universal Time (UTC), and accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**Locked**

A Boolean value that indicates whether AWS Backup Vault Lock applies to the selected backup vault. If true, Vault Lock prevents delete and update operations on the recovery points in the selected vault.

Type: Boolean

Required: No

**MaxRetentionDays**

The AWS Backup Vault Lock setting that specifies the maximum retention period that the vault retains its recovery points. If this parameter is not specified, Vault Lock does not enforce a maximum retention period on the recovery points in the vault (allowing indefinite storage).

If specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or shorter than the maximum retention period. If the job's retention period is longer than that maximum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault. Recovery points already stored in the vault prior to Vault Lock are not affected.

Type: Long

Required: No

**MinRetentionDays**

The AWS Backup Vault Lock setting that specifies the minimum retention period that the vault retains its recovery points. If this parameter is not specified, Vault Lock does not enforce a minimum retention period.

If specified, any backup or copy job to the vault must have a lifecycle policy with a retention period equal to or longer than the minimum retention period. If the job's retention period is shorter than that minimum retention period, then the vault fails the backup or copy job, and you should either modify your lifecycle settings or use a different vault. Recovery points already stored in the vault prior to Vault Lock are not affected.

Type: Long

Required: No

**NumberOfRecoveryPoints**

The number of recovery points that are stored in a backup vault.

Type: Long
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)
**CalculatedLifecycle**

Service: AWS Backup

Contains **DeleteAt** and **MoveToColdStorageAt** timestamps, which are used to specify a lifecycle for a recovery point.

The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the “retention” setting must be 90 days greater than the “transition to cold after days” setting. The “transition to cold after days” setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

**Contents**

**DeleteAt**

A timestamp that specifies when to delete a recovery point.

Type: Timestamp

Required: No

**MoveToColdStorageAt**

A timestamp that specifies when to transition a recovery point to cold storage.

Type: Timestamp

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)
Condition
Service: AWS Backup

Contains an array of triplets made up of a condition type (such as StringEquals), a key, and a value. Used to filter resources using their tags and assign them to a backup plan. Case sensitive.

Contents

ConditionKey

The key in a key-value pair. For example, in the tag Department: Accounting, Department is the key.

Type: String

Required: Yes

ConditionType

An operation applied to a key-value pair used to assign resources to your backup plan. Condition only supports StringEquals. For more flexible assignment options, including StringLike and the ability to exclude resources from your backup plan, use Conditions (with an "s" on the end) for your BackupSelection.

Type: String

Valid Values: STRINGEQUALS

Required: Yes

ConditionValue

The value in a key-value pair. For example, in the tag Department: Accounting, Accounting is the value.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
ConditionParameter
Service: AWS Backup

Includes information about tags you define to assign tagged resources to a backup plan.

Contents

ConditionKey

The key in a key-value pair. For example, in the tag Department: Accounting, Department is the key.

Type: String
Required: No

ConditionValue

The value in a key-value pair. For example, in the tag Department: Accounting, Accounting is the value.

Type: String
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
Conditions
Service: AWS Backup

Contains information about which resources to include or exclude from a backup plan using their tags. Conditions are case sensitive.

Contents

StringEquals

Filters the values of your tagged resources for only those resources that you tagged with the same value. Also called "exact matching."

Type: Array of ConditionParameter (p. 685) objects

Required: No

StringLike

Filters the values of your tagged resources for matching tag values with the use of a wildcard character (*) anywhere in the string. For example, "prod*" or "*rod*" matches the tag value "production".

Type: Array of ConditionParameter (p. 685) objects

Required: No

StringNotEquals

Filters the values of your tagged resources for only those resources that you tagged that do not have the same value. Also called "negated matching."

Type: Array of ConditionParameter (p. 685) objects

Required: No

StringNotLike

Filters the values of your tagged resources for non-matching tag values with the use of a wildcard character (*) anywhere in the string.

Type: Array of ConditionParameter (p. 685) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
**ControllInputParameter**

Service: AWS Backup

A list of parameters for a control. A control can have zero, one, or more than one parameter. An example of a control with two parameters is: "backup plan frequency is at least daily and the retention period is at least 1 year". The first parameter is daily. The second parameter is 1 year.

**Contents**

**ParameterName**

The name of a parameter, for example, BackupPlanFrequency.

- Type: String
- Required: No

**ParameterValue**

The value of parameter, for example, hourly.

- Type: String
- Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)
A framework consists of one or more controls. Each control has its own control scope. The control scope can include one or more resource types, a combination of a tag key and value, or a combination of one resource type and one resource ID. If no scope is specified, evaluations for the rule are triggered when any resource in your recording group changes in configuration.

**Note**
To set a control scope that includes all of a particular resource, leave the ControlScope empty or do not pass it when calling CreateFramework.

## Contents

**ComplianceResourceIds**

The ID of the only AWS resource that you want your control scope to contain.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Required: No

**ComplianceResourceTypes**

Describes whether the control scope includes one or more types of resources, such as EFS or RDS.

Type: Array of strings

Required: No

**Tags**

The tag key-value pair applied to those AWS resources that you want to trigger an evaluation for a rule. A maximum of one key-value pair can be provided. The tag value is optional, but it cannot be an empty string. The structure to assign a tag is: ["Key":"string", "Value":"string"].

Type: String to string map

Required: No

## See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](https://docs.aws.amazon.com/sdk-for-cpp/v1/reference/service/AWS_Backup.html)
- [AWS SDK for Go](https://docs.aws.amazon.com/sdk-for-golang/v1/reference/service/AWS_Backup.html)
- [AWS SDK for Java V2](https://docs.aws.amazon.com/sdk-for-java/v2/reference/service/AWS_Backup.html)
- [AWS SDK for Ruby V3](https://docs.aws.amazon.com/sdk-for-aws-reference/service/AWS_Backup.html)
CopyAction
Service: AWS Backup

The details of the copy operation.

Contents

DestinationBackupVaultArn

An Amazon Resource Name (ARN) that uniquely identifies the destination backup vault for the copied backup. For example, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String
Required: Yes

Lifecycle

Contains an array of Transition objects specifying how long in days before a recovery point transitions to cold storage or is deleted.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, on the console, the “retention” setting must be 90 days greater than the “transition to cold after days” setting. The “transition to cold after days” setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 700) object
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
CopyJob
Service: AWS Backup

Contains detailed information about a copy job.

Contents

**AccountId**
The account ID that owns the copy job.
Type: String
Pattern: `^[0-9]{12}$`
Required: No

**BackupSizeInBytes**
The size, in bytes, of a copy job.
Type: Long
Required: No

**ChildJobsInState**
This returns the statistics of the included child (nested) copy jobs.
Type: String to long map
Valid Keys: CREATED | RUNNING | COMPLETED | FAILED | PARTIAL
Required: No

**CompletionDate**
The date and time a copy job is completed, in Unix format and Coordinated Universal Time (UTC). The value of CompletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp
Required: No

**CompositeMemberIdentifier**
This is the identifier of a resource within a composite group, such as nested (child) recovery point belonging to a composite (parent) stack. The ID is transferred from the logical ID within a stack.
Type: String
Required: No

**CopyJobId**
Uniquely identifies a copy job.
Type: String
Required: No

**CreatedBy**
Contains information about the backup plan and rule that AWS Backup used to initiate the recovery point backup.
Type: **RecoveryPointCreator** *(p. 708)* object

**CreationDate**

The date and time a copy job is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

**DestinationBackupVaultArn**

An Amazon Resource Name (ARN) that uniquely identifies a destination copy vault; for example, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

**DestinationRecoveryPointArn**

An ARN that uniquely identifies a destination recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

**IamRoleArn**

Specifies the IAM role ARN used to copy the target recovery point; for example, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

**IsParent**

This is a boolean value indicating this is a parent (composite) copy job.

Type: Boolean

**NumberOfChildJobs**

This is the number of child (nested) copy jobs.

Type: Long

**ParentJobId**

This uniquely identifies a request to AWS Backup to copy a resource. The return will be the parent (composite) job ID.

Type: String

Required: No
**ResourceArn**

The AWS resource to be copied; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database.

Type: String

Required: No

**ResourceName**

This is the non-unique name of the resource that belongs to the specified backup.

Type: String

Required: No

**ResourceType**

The type of AWS resource to be copied; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database.

Type: String

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Required: No

**SourceBackupVaultArn**

An Amazon Resource Name (ARN) that uniquely identifies a source copy vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

Required: No

**SourceRecoveryPointArn**

An ARN that uniquely identifies a source recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type: String

Required: No

**State**

The current state of a copy job.

Type: String

Valid Values: CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

Required: No

**StatusMessage**

A detailed message explaining the status of the job to copy a resource.

Type: String

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:
• AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for Ruby V3
**DateRange**
Service: AWS Backup

This is a resource filter containing FromDate: DateTime and ToDate: DateTime. Both values are required. Future DateTime values are not permitted.

The date and time are in Unix format and Coordinated Universal Time (UTC), and it is accurate to milliseconds (milliseconds are optional). For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

**Contents**

**FromDate**

This value is the beginning date, inclusive.

The date and time are in Unix format and Coordinated Universal Time (UTC), and it is accurate to milliseconds (milliseconds are optional).

Type: Timestamp

Required: Yes

**ToDate**

This value is the end date, inclusive.

The date and time are in Unix format and Coordinated Universal Time (UTC), and it is accurate to milliseconds (milliseconds are optional).

Type: Timestamp

Required: Yes

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
Framework
Service: AWS Backup

Contains detailed information about a framework. Frameworks contain controls, which evaluate and report on your backup events and resources. Frameworks generate daily compliance results.

Contents

**CreationTime**

The date and time that a framework is created, in ISO 8601 representation. The value of CreationTime is accurate to milliseconds. For example, 2020-07-10T15:00:00.000-08:00 represents the 10th of July 2020 at 3:00 PM 8 hours behind UTC.

Type: Timestamp

Required: No

**DeploymentStatus**

The deployment status of a framework. The statuses are:

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED

Type: String

Required: No

**FrameworkArn**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

Required: No

**FrameworkDescription**

An optional description of the framework with a maximum 1,024 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: .*\S.*

Required: No

**FrameworkName**

The unique name of a framework. This name is between 1 and 256 characters, starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][\_a-zA-Z0-9]*

Required: No
**NumberOfControls**

The number of controls contained by the framework.

Type: Integer

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
FrameworkControl
Service: AWS Backup

Contains detailed information about all of the controls of a framework. Each framework must contain at least one control.

Contents

ControlName

The name of a control. This name is between 1 and 256 characters.

Type: String
Required: Yes

ControlInputParameters

A list of ParameterName and ParameterValue pairs.

Type: Array of ControlInputParameter (p. 687) objects
Required: No

ControlScope

The scope of a control. The control scope defines what the control will evaluate. Three examples of control scopes are: a specific backup plan, all backup plans with a specific tag, or all backup plans. For more information, see ControlScope.

Type: ControlScope (p. 688) object
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
**LegalHold**

Service: AWS Backup

A legal hold is an administrative tool that helps prevent backups from being deleted while under a hold. While the hold is in place, backups under a hold cannot be deleted and lifecycle policies that would alter the backup status (such as transition to cold storage) are delayed until the legal hold is removed. A backup can have more than one legal hold. Legal holds are applied to one or more backups (also known as recovery points). These backups can be filtered by resource types and by resource IDs.

**Contents**

**CancellationDate**

This is the time in number format when legal hold was cancelled.

Type: Timestamp

Required: No

**CreationDate**

This is the time in number format when legal hold was created.

Type: Timestamp

Required: No

**Description**

This is the description of a legal hold.

Type: String

Required: No

**LegalHoldArn**

This is an Amazon Resource Number (ARN) that uniquely identifies the legal hold; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

Required: No

**LegalHoldId**

ID of specific legal hold on one or more recovery points.

Type: String

Required: No

**Status**

This is the status of the legal hold. Statuses can be ACTIVE, CREATING, CANCELED, and CANCELING.

Type: String

Valid Values: CREATING | ACTIVE | CANCELING | CANCELED

Required: No

**Title**

This is the title of a legal hold.
Type: String
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
Lifecycle
Service: AWS Backup

Contains an array of Transition objects specifying how long in days before a recovery point transitions to cold storage or is deleted.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, on the console, the “retention” setting must be 90 days greater than the “transition to cold after days” setting. The “transition to cold after days” setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Contents

DeleteAfterDays

Specifies the number of days after creation that a recovery point is deleted. Must be greater than 90 days plus MoveToColdStorageAfterDays.

Type: Long
Required: No

MoveToColdStorageAfterDays

Specifies the number of days after creation that a recovery point is moved to cold storage.

Type: Long
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
ProtectedResource
Service: AWS Backup

A structure that contains information about a backed-up resource.

Contents

LastBackupTime

The date and time a resource was last backed up, in Unix format and Coordinated Universal Time (UTC). The value of LastBackupTime is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

ResourceArn

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

Required: No

ResourceName

This is the non-unique name of the resource that belongs to the specified backup.

Type: String

Required: No

ResourceType

The type of AWS resource; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database. For Windows Volume Shadow Copy Service (VSS) backups, the only supported resource type is Amazon EC2.

Type: String

Pattern: ^[a-zA-Z0-9\-\.\_\ ]{1,50}$

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
RecoveryPointByBackupVault

Service: AWS Backup

Contains detailed information about the recovery points stored in a backup vault.

Contents

BackupSizeInBytes

The size, in bytes, of a backup.

Type: Long

Required: No

BackupVaultArn

An ARN that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

Required: No

BackupVaultName

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

Required: No

CalculatedLifecycle

A CalculatedLifecycle object containing DeleteAt and MoveToColdStorageAt timestamps.

Type: CalculatedLifecycle (p. 683) object

Required: No

CompletionDate

The date and time a job to restore a recovery point is completed, in Unix format and Coordinated Universal Time (UTC). The value of CompletionDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

CompositeMemberIdentifier

This is the identifier of a resource within a composite group, such as nested (child) recovery point belonging to a composite (parent) stack. The ID is transferred from the logical ID within a stack.

Type: String

Required: No
CreatedBy
Contains identifying information about the creation of a recovery point, including the
BackupPlanArn, BackupPlanId, BackupPlanVersion, and BackupRuleId of the backup plan
that is used to create it.
Type: RecoveryPointCreator (p. 708) object
Required: No

CreationDate
The date and time a recovery point is created, in Unix format and Coordinated Universal Time (UTC).
The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087
represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp
Required: No

EncryptionKeyArn
The server-side encryption key that is used to protect your backups; for example,
Type: String
Required: No

IamRoleArn
Specifies the IAM role ARN used to create the target recovery point; for example,
arwn:aws:iam::123456789012:role/S3Access.
Type: String
Required: No

IsEncrypted
A Boolean value that is returned as TRUE if the specified recovery point is encrypted, or FALSE if the
recovery point is not encrypted.
Type: Boolean
Required: No

IsParent
This is a boolean value indicating this is a parent (composite) recovery point.
Type: Boolean
Required: No

LastRestoreTime
The date and time a recovery point was last restored, in Unix format and Coordinated Universal
Time (UTC). The value of LastRestoreTime is accurate to milliseconds. For example, the value
1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp
Required: No
Lifecycle

The lifecycle defines when a protected resource is transitioned to cold storage and when it expires. AWS Backup transitions and expires backups automatically according to the lifecycle that you define.

Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the “retention” setting must be 90 days greater than the “transition to cold after days” setting. The “transition to cold after days” setting cannot be changed after a backup has been transitioned to cold.

Resource types that are able to be transitioned to cold storage are listed in the "Lifecycle to cold storage" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 700) object
Required: No

ParentRecoveryPointArn

This is the Amazon Resource Name (ARN) of the parent (composite) recovery point.

Type: String
Required: No

RecoveryPointArn

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-188B488B0D45.

Type: String
Required: No

ResourceArn

An ARN that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String
Required: No

ResourceName

This is the non-unique name of the resource that belongs to the specified backup.

Type: String
Required: No

ResourceType

The type of AWS resource saved as a recovery point; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database. For Windows Volume Shadow Copy Service (VSS) backups, the only supported resource type is Amazon EC2.

Type: String
Pattern: ^[a-zA-Z0-9\-\.\_\_]\{1,50}\$
Required: No
SourceBackupVaultArn

The backup vault where the recovery point was originally copied from. If the recovery point is restored to the same account this value will be null.

Type: String
Required: No

Status

A status code specifying the state of the recovery point.

Type: String
Valid Values: COMPLETED | PARTIAL | DELETING | EXPIRED
Required: No

StatusMessage

A message explaining the reason of the recovery point deletion failure.

Type: String
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
RecoveryPointByResource
Service: AWS Backup

Contains detailed information about a saved recovery point.

Contents

BackupSizeBytes
The size, in bytes, of a backup.
Type: Long
Required: No

BackupVaultName
The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.
Type: String
Pattern: ^[a-zA-Z0-9\-_]{2,50}$
Required: No

CreationDate
The date and time a recovery point is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationDate is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.
Type: Timestamp
Required: No

EncryptionKeyArn
The server-side encryption key that is used to protect your backups; for example, arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab.
Type: String
Required: No

IsParent
This is a boolean value indicating this is a parent (composite) recovery point.
Type: Boolean
Required: No

ParentRecoveryPointArn
This is the Amazon Resource Name (ARN) of the parent (composite) recovery point.
Type: String
Required: No

RecoveryPointArn
An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-1088A88B0D45.
Type: String
Required: No

**ResourceName**
This is the non-unique name of the resource that belongs to the specified backup.

Type: String
Required: No

**Status**
A status code specifying the state of the recovery point.

Type: String

Valid Values: COMPLETED | PARTIAL | DELETING | EXPIRED

Required: No

**StatusMessage**
A message explaining the reason of the recovery point deletion failure.

Type: String
Required: No

**See Also**
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)
RecoveryPointCreator
Service: AWS Backup

Contains information about the backup plan and rule that AWS Backup used to initiate the recovery point backup.

Contents

BackupPlanArn

An Amazon Resource Name (ARN) that uniquely identifies a backup plan; for example, 

Type: String
Required: No

BackupPlanId

Uniquely identifies a backup plan.

Type: String
Required: No

BackupPlanVersion

Version IDs are unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. They cannot be edited.

Type: String
Required: No

BackupRuleId

Uniquely identifies a rule used to schedule the backup of a selection of resources.

Type: String
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
RecoveryPointMember
Service: AWS Backup

This is a recovery point which is a child (nested) recovery point of a parent (composite) recovery point. These recovery points can be disassociated from their parent (composite) recovery point, in which case they will no longer be a member.

Contents

BackupVaultName

This is the name of the backup vault (the logical container in which backups are stored).

Type: String

Pattern: ^[a-zA-Z0-9\-\_\\]\{2,50}$

Required: No

RecoveryPointArn

This is the Amazon Resource Name (ARN) of the parent (composite) recovery point.

Type: String

Required: No

ResourceArn

This is the Amazon Resource Name (ARN) that uniquely identifies a saved resource.

Type: String

Required: No

ResourceType

This is the AWS resource type that is saved as a recovery point.

Type: String

Pattern: ^[a-zA-Z0-9\-\_/\.\[]{1,50}$

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
RecoveryPointSelection
Service: AWS Backup

This specifies criteria to assign a set of resources, such as resource types or backup vaults.

Contents

DateRange

This is a resource filter containing FromDate: DateTime and ToDate: DateTime. Both values are required. Future DateTime values are not permitted.

The date and time are in Unix format and Coordinated Universal Time (UTC), and it is accurate to milliseconds ((milliseconds are optional). For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: DateRange (p. 694) object

Required: No

ResourceIdentifiers

These are the resources included in the resource selection (including type of resources and vaults).

Type: Array of strings

Required: No

VaultNames

These are the names of the vaults in which the selected recovery points are contained.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
ReportDeliveryChannel
Service: AWS Backup

Contains information from your report plan about where to deliver your reports, specifically your Amazon S3 bucket name, S3 key prefix, and the formats of your reports.

Contents

S3BucketName
The unique name of the S3 bucket that receives your reports.

Type: String
Required: Yes

Formats
A list of the format of your reports: CSV, JSON, or both. If not specified, the default format is CSV.

Type: Array of strings
Required: No

S3KeyPrefix
The prefix for where AWS Backup Audit Manager delivers your reports to Amazon S3. The prefix is this part of the following path: s3://your-bucket-name/prefix/Backup/us-west-2/year/month/day/report-name. If not specified, there is no prefix.

Type: String
Required: No

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
ReportDestination
Service: AWS Backup

Contains information from your report job about your report destination.

Contents

S3BucketName

The unique name of the Amazon S3 bucket that receives your reports.

Type: String
Required: No

S3Keys

The object key that uniquely identifies your reports in your S3 bucket.

Type: Array of strings
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
ReportJob
Service: AWS Backup

Contains detailed information about a report job. A report job compiles a report based on a report plan and publishes it to Amazon S3.

Contents

CompletionTime
The date and time that a report job is completed, in Unix format and Coordinated Universal Time (UTC). The value of CompletionTime is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

CreationTime
The date and time that a report job is created, in Unix format and Coordinated Universal Time (UTC). The value of CreationTime is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

ReportDestination
The S3 bucket name and S3 keys for the destination where the report job publishes the report.

Type: ReportDestination (p. 712) object

Required: No

ReportJobId
The identifier for a report job. A unique, randomly generated, Unicode, UTF-8 encoded string that is at most 1,024 bytes long. Report job IDs cannot be edited.

Type: String

Required: No

ReportPlanArn
An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

Required: No

ReportTemplate
Indicates the report template for the report. Reports are built using a report template. The report templates are:

- RESOURCE_COMPLIANCE_REPORT
- CONTROL_COMPLIANCE_REPORT
- BACKUP_JOB_REPORT
- COPY_JOB_REPORT
- RESTORE_JOB_REPORT

Type: String
Required: No

**Status**

The status of a report job. The statuses are:

- CREATED
- RUNNING
- COMPLETED
- FAILED

COMPLETED means that the report is available for your review at your designated destination. If the status is FAILED, review the **StatusMessage** for the reason.

Type: String

Required: No

**StatusMessage**

A message explaining the status of the report job.

Type: String

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](aws-sdk-cpp)
- [AWS SDK for Go](aws-sdk-go)
- [AWS SDK for Java V2](aws-sdk-java)
- [AWS SDK for Ruby V3](aws-sdk-ruby)


**ReportPlan**  
Service: AWS Backup

Contains detailed information about a report plan.

**Contents**

**CreationTime**

The date and time that a report plan is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationTime` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp  
Required: No

**DeploymentStatus**

The deployment status of a report plan. The statuses are:

- CREATE_IN_PROGRESS  
- UPDATE_IN_PROGRESS  
- DELETE_IN_PROGRESS  
- COMPLETED

Type: String  
Required: No

**LastAttemptedExecutionTime**

The date and time that a report job associated with this report plan last attempted to run, in Unix format and Coordinated Universal Time (UTC). The value of `LastAttemptedExecutionTime` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp  
Required: No

**LastSuccessfulExecutionTime**

The date and time that a report job associated with this report plan last successfully ran, in Unix format and Coordinated Universal Time (UTC). The value of `LastSuccessfulExecutionTime` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp  
Required: No

**ReportDeliveryChannel**

Contains information about where and how to deliver your reports, specifically your Amazon S3 bucket name, S3 key prefix, and the formats of your reports.

Type: `ReportDeliveryChannel` (p. 711) object  
Required: No

**ReportPlanArn**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String
Required: No

**ReportPlanDescription**

An optional description of the report plan with a maximum 1,024 characters.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: .*\S.*

Required: No

**ReportPlanName**

The unique name of the report plan. This name is between 1 and 256 characters starting with a letter, and consisting of letters (a-z, A-Z), numbers (0-9), and underscores (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: [a-zA-Z][a-zA-Z0-9]*

Required: No

**ReportSetting**

Identifies the report template for the report. Reports are built using a report template. The report templates are:

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

If the report template is RESOURCE_COMPLIANCE_REPORT or CONTROL_COMPLIANCE_REPORT, this API resource also describes the report coverage by AWS Regions and frameworks.

Type: ReportSetting (p. 717) object

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
ReportSetting
Service: AWS Backup

Contains detailed information about a report setting.

Contents

ReportTemplate

Identifies the report template for the report. Reports are built using a report template. The report templates are:

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

Type: String
Required: Yes

Accounts

These are the accounts to be included in the report.

Type: Array of strings
Required: No

FrameworkArns

The Amazon Resource Names (ARNs) of the frameworks a report covers.

Type: Array of strings
Required: No

NumberOfFrameworks

The number of frameworks a report covers.

Type: Integer
Required: No

OrganizationUnits

These are the Organizational Units to be included in the report.

Type: Array of strings
Required: No

Regions

These are the Regions to be included in the report.

Type: Array of strings
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
• **AWS SDK for Go**
• **AWS SDK for Java V2**
• **AWS SDK for Ruby V3**
**RestoreJobsListMember**

Service: AWS Backup

Contains metadata about a restore job.

**Contents**

**AccountId**

The account ID that owns the restore job.

Type: String

Pattern: `^[0-9]{12}$`

Required: No

**BackupSizeInBytes**

The size, in bytes, of the restored resource.

Type: Long

Required: No

**CompletionDate**

The date and time a job to restore a recovery point is completed, in Unix format and Coordinated Universal Time (UTC). The value of `CompletionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**CreatedResourceArn**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

Required: No

**CreationDate**

The date and time a restore job is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

**ExpectedCompletionTimeMinutes**

The amount of time in minutes that a job restoring a recovery point is expected to take.

Type: Long

Required: No

**IamRoleArn**

Specifies the IAM role ARN used to create the target recovery point; for example, `arn:aws:iam::123456789012:role/S3Access.`
Type: String
Required: No

**PercentDone**
Contains an estimated percentage complete of a job at the time the job status was queried.
Type: String
Required: No

**RecoveryPointArn**
An ARN that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.
Type: String
Required: No

**ResourceType**
The resource type of the listed restore jobs; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database. For Windows Volume Shadow Copy Service (VSS) backups, the only supported resource type is Amazon EC2.
Type: String
Pattern: `^[a-zA-Z0-9\-_\.]{1,50}$`
Required: No

**RestoreJobId**
Uniquely identifies the job that restores a recovery point.
Type: String
Required: No

**Status**
A status code specifying the state of the job initiated by AWS Backup to restore a recovery point.
Type: String
Valid Values: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`
Required: No

**StatusMessage**
A detailed message explaining the status of the job to restore a recovery point.
Type: String
Required: No

**See Also**
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for Ruby V3

AWS Backup gateway

The following data types are supported by AWS Backup gateway:

• BandwidthRateLimitInterval (p. 722)
• Gateway (p. 724)
• GatewayDetails (p. 726)
• Hypervisor (p. 728)
• HypervisorDetails (p. 730)
• MaintenanceStartTime (p. 732)
• Tag (p. 734)
• VirtualMachine (p. 735)
• VirtualMachineDetails (p. 737)
• VmwareTag (p. 739)
• VmwareToAwsTagMapping (p. 740)
**BandwidthRateLimitInterval**  
*Service: AWS Backup gateway*

Describes a bandwidth rate limit interval for a gateway. A bandwidth rate limit schedule consists of one or more bandwidth rate limit intervals. A bandwidth rate limit interval defines a period of time on one or more days of the week, during which bandwidth rate limits are specified for uploading, downloading, or both.

**Contents**

**DaysOfWeek**

The days of the week component of the bandwidth rate limit interval, represented as ordinal numbers from 0 to 6, where 0 represents Sunday and 6 represents Saturday.

*Type:* Array of integers

*Array Members:* Minimum number of 1 item. Maximum number of 7 items.

*Valid Range:* Minimum value of 0. Maximum value of 6.

*Required:* Yes

**EndHourOfDay**

The hour of the day to end the bandwidth rate limit interval.

*Type:* Integer

*Valid Range:* Minimum value of 0. Maximum value of 23.

*Required:* Yes

**EndMinuteOfHour**

The minute of the hour to end the bandwidth rate limit interval.

*Important*

The bandwidth rate limit interval ends at the end of the minute. To end an interval at the end of an hour, use the value 59.

*Type:* Integer

*Valid Range:* Minimum value of 0. Maximum value of 59.

*Required:* Yes

**StartHourOfDay**

The hour of the day to start the bandwidth rate limit interval.

*Type:* Integer

*Valid Range:* Minimum value of 0. Maximum value of 23.

*Required:* Yes

**StartMinuteOfHour**

The minute of the hour to start the bandwidth rate limit interval. The interval begins at the start of that minute. To begin an interval exactly at the start of the hour, use the value 0.

*Type:* Integer
Valid Range: Minimum value of 0. Maximum value of 59.

Required: Yes

**AverageUploadRateLimitInBitsPerSec**

The average upload rate limit component of the bandwidth rate limit interval, in bits per second. This field does not appear in the response if the upload rate limit is not set.

**Note**

For Backup Gateway, the minimum value is (Value).

Type: Long


Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
Gateway
Service: AWS Backup gateway

A gateway is an AWS Backup Gateway appliance that runs on the customer's network to provide seamless connectivity to backup storage in the AWS Cloud.

Contents

GatewayArn

The Amazon Resource Name (ARN) of the gateway. Use the ListGateways operation to return a list of gateways for your account and AWS Region.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.


Required: No

GatewayDisplayName

The display name of the gateway.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: ^[a-zA-Z0-9-]+$/

Required: No

GatewayType

The type of the gateway.

Type: String

Valid Values: BACKUP_VM

Required: No

HypervisorId

The hypervisor ID of the gateway.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Required: No

LastSeenTime

The last time AWS Backup gateway communicated with the gateway, in Unix format and UTC time.

Type: Timestamp

Required: No
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
GatewayDetails
Service: AWS Backup gateway

The details of gateway.

Contents

GatewayArn
The Amazon Resource Name (ARN) of the gateway. Use the ListGateways operation to return a list of gateways for your account and AWS Region.

Type: String
Length Constraints: Minimum length of 50. Maximum length of 500.
Required: No

GatewayDisplayName
The display name of the gateway.

Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern:^[a-zA-Z0-9-]*$
Required: No

GatewayType
The type of the gateway type.

Type: String
Valid Values: BACKUP_VM
Required: No

HypervisorId
The hypervisor ID of the gateway.

Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Required: No

LastSeenTime
Details showing the last time AWS Backup gateway communicated with the cloud, in Unix format and UTC time.

Type: Timestamp
Required: No

MaintenanceStartTime
Returns your gateway's weekly maintenance start time including the day and time of the week. Note that values are in terms of the gateway's time zone. Can be weekly or monthly.
Type: MaintenanceStartTime (p. 732) object

Required: No

NextUpdateAvailabilityTime

Details showing the next update availability time of the gateway.

Type: Timestamp

Required: No

VpcEndpoint

The DNS name for the virtual private cloud (VPC) endpoint the gateway uses to connect to the cloud for backup gateway.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
Hypervisor
Service: AWS Backup gateway

Represents the hypervisor's permissions to which the gateway will connect.

A hypervisor is hardware, software, or firmware that creates and manages virtual machines, and allocates resources to them.

Contents

Host
The server host of the hypervisor. This can be either an IP address or a fully-qualified domain name (FQDN).

Type: String
Pattern: ^.+$
Required: No

HypervisorArn
The Amazon Resource Name (ARN) of the hypervisor.

Type: String
Length Constraints: Minimum length of 50. Maximum length of 500.
Required: No

KmsKeyArn
The Amazon Resource Name (ARN) of the AWS Key Management Service used to encrypt the hypervisor.

Type: String
Length Constraints: Minimum length of 50. Maximum length of 500.
Pattern: ^arn:(aws|aws-cn|aws-us-gov):kms([a-zA-Z0-9-]+):([0-9]+):(key|alias)/([^\(\S\)+]*$)$
Required: No

Name
The name of the hypervisor.

Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[a-zA-Z-0-9-]+$
Required: No

State
The state of the hypervisor.
Type: String

Valid Values: PENDING | ONLINE | OFFLINE | ERROR

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
**HypervisorDetails**

Service: AWS Backup gateway

These are the details of the specified hypervisor. A hypervisor is hardware, software, or firmware that creates and manages virtual machines, and allocates resources to them.

**Contents**

**Host**

The server host of the hypervisor. This can be either an IP address or a fully-qualified domain name (FQDN).

Type: String


Pattern: ^\.$

Required: No

**HypervisorArn**

The Amazon Resource Name (ARN) of the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway:[a-zA-Z0-9-]+:[a-zA-Z0-9-]++$

Required: No

**KmsKeyArn**

The Amazon Resource Name (ARN) of the AWS KMS used to encrypt the hypervisor.

Type: String

Length Constraints: Minimum length of 50. Maximum length of 500.

Pattern: ^arn:(aws|aws-cn|aws-us-gov):kms:[a-zA-Z0-9-]+:[0-9]+:(key|alias)/([^/]+)$

Required: No

**LastSuccessfulMetadataSyncTime**

This is the time when the most recent successful sync of metadata occurred.

Type: Timestamp

Required: No

**LatestMetadataSyncStatus**

This is the most recent status for the indicated metadata sync.

Type: String

Valid Values: CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED

Required: No
**LatestMetadataSyncStatusMessage**

This is the most recent status for the indicated metadata sync.

Type: String

Required: No

**LogGroupArn**

The Amazon Resource Name (ARN) of the group of gateways within the requested log.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Pattern: ^\|^[a-zA-Z0-9-\+\,\-\./]*$  

Required: No

**Name**

This is the name of the specified hypervisor.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Pattern: ^[a-zA-Z0-9-]*$  

Required: No

**State**

This is the current state of the specified hypervisor.

The possible states are PENDING, ONLINE, OFFLINE, or ERROR.

Type: String

Valid Values: PENDING | ONLINE | OFFLINE | ERROR

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
MaintenanceStartTime
Service: AWS Backup gateway

This is your gateway's weekly maintenance start time including the day and time of the week. Note that values are in terms of the gateway's time zone. Can be weekly or monthly.

Contents

HourOfDay

The hour component of the maintenance start time represented as \( hh \), where \( hh \) is the hour (0 to 23). The hour of the day is in the time zone of the gateway.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 23.

Required: Yes

MinuteOfHour

The minute component of the maintenance start time represented as \( mm \), where \( mm \) is the minute (0 to 59). The minute of the hour is in the time zone of the gateway.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 59.

Required: Yes

DayOfMonth

The day of the month component of the maintenance start time represented as an ordinal number from 1 to 28, where 1 represents the first day of the month and 28 represents the last day of the month.

Type: Integer


Required: No

DayOfWeek

An ordinal number between 0 and 6 that represents the day of the week, where 0 represents Sunday and 6 represents Saturday. The day of week is in the time zone of the gateway.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 6.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
**Tag**
Service: AWS Backup gateway

A key-value pair you can use to manage, filter, and search for your resources. Allowed characters include UTF-8 letters, numbers, spaces, and the following characters: + - = . _ : /.

**Contents**

**Key**

The key part of a tag's key-value pair. The key can't start with `aws:`.

Type: String


Pattern: `^([\p{L}\p{Z}\p{N}\_\.:+/=\@]*$`

Required: Yes

**Value**

The value part of a tag's key-value pair.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `^[^\x00]*$`

Required: Yes

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
VirtualMachine
Service: AWS Backup gateway

A virtual machine that is on a hypervisor.

Contents

HostName
The host name of the virtual machine.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[a-zA-Z0-9-]*$  
Required: No

HypervisorId
The ID of the virtual machine's hypervisor.
Type: String
Required: No

LastBackupDate
The most recent date a virtual machine was backed up, in Unix format and UTC time.
Type: Timestamp
Required: No

Name
The name of the virtual machine.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[a-zA-Z0-9-]*$  
Required: No

Path
The path of the virtual machine.
Type: String
Pattern: ^[^\\x00]+$  
Required: No

ResourceArn
The Amazon Resource Name (ARN) of the virtual machine. For example, arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL.
Type: String
Length Constraints: Minimum length of 50. Maximum length of 500.


Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
VirtualMachineDetails
Service: AWS Backup gateway

Your VirtualMachine objects, ordered by their Amazon Resource Names (ARNs).

Contents

HostName
The host name of the virtual machine.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[a-zA-Z0-9-]+$
Required: No

HypervisorId
The ID of the virtual machine's hypervisor.
Type: String
Required: No

LastBackupDate
The most recent date a virtual machine was backed up, in Unix format and UTC time.
Type: Timestamp
Required: No

Name
The name of the virtual machine.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 100.
Pattern: ^[a-zA-Z0-9-]+$
Required: No

Path
The path of the virtual machine.
Type: String
Pattern: ^[^\x00]+$
Required: No

ResourceArn
The Amazon Resource Name (ARN) of the virtual machine. For example, arn:aws:backup-gateway:us-west-1:000000000000:vm/vm-0000ABCDEFGIJKL.
Type: String
Length Constraints: Minimum length of 50. Maximum length of 500.

Required: No

**VmwareTags**

These are the details of the VMware tags associated with the specified virtual machine.

Type: Array of [VmwareTag (p. 739)] objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)
VmwareTag
Service: AWS Backup gateway

A VMware tag is a tag attached to a specific virtual machine. A tag is a key-value pair you can use to manage, filter, and search for your resources.

The content of VMware tags can be matched to AWS tags.

Contents

VmwareCategory

The is the category of VMware.
Type: String
Required: No

VmwareTagDescription

This is a user-defined description of a VMware tag.
Type: String
Required: No

VmwareTagName

This is the user-defined name of a VMware tag.
Type: String
Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
VmwareToAwsTagMapping
Service: AWS Backup gateway

This displays the mapping of VMware tags to the corresponding AWS tags.

Contents

AwsTagKey
The key part of the AWS tag's key-value pair.
Type: String
Pattern: ^([p{L}p{Z}p{N}_.:=+\-@]*)$
Required: Yes

AwsTagValue
The value part of the AWS tag's key-value pair.
Type: String
Length Constraints: Minimum length of 0. Maximum length of 256.
Pattern: ^[^\x00]*$
Required: Yes

VmwareCategory
The is the category of VMware.
Type: String
Required: Yes

VmwareTagName
This is the user-defined name of a VMware tag.
Type: String
Required: Yes

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
## Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see [Signing AWS API requests](https://docs.aws.amazon.com/IAM/latest/UserGuide/elements.html) in the IAM User Guide.

### Action

The action to be performed.

*Type:* string  
*Required:* Yes

### Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

*Type:* string  
*Required:* Yes

### X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

*Type:* string

*Valid Values:* AWS4-HMAC-SHA256  
*Required:* Conditional

### X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: access_key/YYYYMMDD/region/service/aws4_request.

For more information, see [Create a signed AWS API request](https://docs.aws.amazon.com/IAM/latest/UserGuide/elements.html) in the IAM User Guide.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

*Type:* string  
*Required:* Conditional

### X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: 20120325T120000Z.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see [Elements of an AWS API request signature](https://docs.aws.amazon.com/IAM/latest/UserGuide/elements.html) in the IAM User Guide.

*Type:* string
Required: Conditional

**X-Amz-Security-Token**

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see [AWS services that work with IAM](https://docs.aws.amazon.com/iam/latest/userguide/services-supported-by-iam.html) in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, you must include the security token.

Type: string

Required: Conditional

**X-Amz-Signature**

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

**X-Amz-SignedHeaders**

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see [Create a signed AWS API request](https://docs.aws.amazon.com/iam/latest/userguide/create-signed-api-requests.html) in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

---

**Common Errors**

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**IncompleteSignature**

The request signature does not conform to AWS standards.

HTTP Status Code: 400

**InternalFailure**

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500
InvalidAction
The action or operation requested is invalid. Verify that the action is typed correctly.
HTTP Status Code: 400

InvalidClientTokenId
The X.509 certificate or AWS access key ID provided does not exist in our records.
HTTP Status Code: 403

NotAuthorized
You do not have permission to perform this action.
HTTP Status Code: 400

OptInRequired
The AWS access key ID needs a subscription for the service.
HTTP Status Code: 403

RequestExpired
The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.
HTTP Status Code: 400

ServiceUnavailable
The request has failed due to a temporary failure of the server.
HTTP Status Code: 503

ThrottlingException
The request was denied due to request throttling.
HTTP Status Code: 400

ValidationError
The input fails to satisfy the constraints specified by an AWS service.
HTTP Status Code: 400
AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS Glossary Reference.
# Document history for AWS Backup

- **API version:** August 8, 2023
- **Latest documentation update:** August 8, 2023

The following table lists all AWS Backup launches since the launch of the service in January 2019 to present. For notifications about updates to this documentation you can subscribe to the RSS feed above.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preview of logically air-gapped backup vault</td>
<td>AWS Backup now offers a preview of a new type of backup vault to help supplement data protection operations. For more information, see <a href="#">Logically air-gapped vaults (preview)</a>.</td>
<td>August 8, 2023</td>
</tr>
<tr>
<td>AWS Backup enhances Amazon S3 backups</td>
<td>AWS Backup has increased performance, size, and speed capabilities for S3 bucket backups. For more information, see <a href="#">Amazon S3 backups</a>.</td>
<td>August 1, 2023</td>
</tr>
<tr>
<td>Tag on restore feature now available in China Regions</td>
<td>Tags that are part of a backup can now be copied when you create a restore job in China (Beijing) or China (Ningxia) Regions. For more information, see <a href="#">Copy tags during a restore</a>.</td>
<td>July 17, 2023</td>
</tr>
<tr>
<td>AWS Backup now supports Amazon S3 in additional Regions</td>
<td>AWS Backup support for Amazon S3 is now available in Europe (Spain), Europe (Zurich), Asia Pacific (Hyderabad), and Asia Pacific (Melbourne) Regions. For more information, see <a href="#">Feature availability by Region</a>.</td>
<td>July 6, 2023</td>
</tr>
<tr>
<td>Cross-account copy expands to additional Regions</td>
<td>AWS Backup now supports cross-account backup copy of most resources in the following Regions: Asia Pacific (Jakarta), Middle East (Bahrain), Asia Pacific (Hong Kong), Africa (Cape Town), Europe (Milan), Asia Pacific (Osaka), Middle East (UAE), Europe (Spain), Europe (Zurich), Asia Pacific</td>
<td>July 5, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>(Hyderabad), and Asia Pacific (Melbourne).</td>
<td>For more information, see Feature availability by Region</td>
<td></td>
</tr>
<tr>
<td>Backup Audit Manager available in GovCloud Regions</td>
<td>AWS Backup has expanded AWS Backup Audit Manager into AWS GovCloud (US-East) and AWS GovCloud (US-West).</td>
<td>June 29, 2023</td>
</tr>
<tr>
<td>Cross-account management now available in GovCloud Regions</td>
<td>AWS Backup now supports cross-account management of resources in AWS GovCloud (US-East) and AWS GovCloud (US-West).</td>
<td>June 29, 2023</td>
</tr>
<tr>
<td>Support for cross-Region copies of Amazon Aurora in additional Regions</td>
<td>AWS Backup now supports cross-Region backup copies for Aurora clusters into and from the following Regions: Asia Pacific (Jakarta), Middle East (Bahrain), Asia Pacific (Hong Kong), Africa (Cape Town), Europe (Milan), Middle East (UAE), Europe (Spain), Europe (Zurich), Asia Pacific (Hyderabad), and Asia Pacific (Melbourne).</td>
<td>June 5, 2023</td>
</tr>
<tr>
<td>Copy tags when restoring</td>
<td>Tags that are part of a backup can now be copied when you create a restore job.</td>
<td>May 22, 2023</td>
</tr>
<tr>
<td>AWS Backup integrates with AWS User Notifications</td>
<td>You can now choose to receive notifications related to backup, copy, and restore events through the AWS User Notifications console.</td>
<td>May 10, 2023</td>
</tr>
<tr>
<td>Support for cross-Region copies of Amazon Aurora in additional Regions</td>
<td>AWS Backup now supports cross-Region backup copies for Aurora clusters into and from the following Regions: Asia Pacific (Jakarta), Middle East (Bahrain), Asia Pacific (Hong Kong), Africa (Cape Town), Europe (Milan), Middle East (UAE), Europe (Spain), Europe (Zurich), Asia Pacific (Hyderabad), and Asia Pacific (Melbourne).</td>
<td>June 5, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Cross-Region backups available in four new Regions</td>
<td>AWS Backup now supports cross-Region backup in Middle East (UAE) Region, Europe (Spain) Region, Europe (Zurich) Region, and Asia Pacific (Hyderabad) Region.</td>
<td>April 28, 2023</td>
</tr>
<tr>
<td>Expanded cross-Region AWS Backup copy support</td>
<td>Cross-Region backups of Amazon EFS, VMware, and DynamoDB resources can now be conducted within the following Regions: Asia Pacific (Jakarta), Middle East (Bahrain), Asia Pacific (Hong Kong), Africa (Cape Town), and Europe (Milan).</td>
<td>April 28, 2023</td>
</tr>
<tr>
<td>Amazon S3 backup and restore in South America (São Paulo) Region</td>
<td>AWS Backup support for Amazon S3 (Amazon Simple Storage Service) is now available in South America (São Paulo) Region. For more information, see Amazon S3 backups.</td>
<td>April 20, 2023</td>
</tr>
<tr>
<td>AWS Backup expands to Asia Pacific (Melbourne) Region</td>
<td>AWS Backup is now available in Asia Pacific (Melbourne) Region. For more information, see Feature availability by AWS Region.</td>
<td>April 20, 2023</td>
</tr>
<tr>
<td>Expanded Regional support for Amazon S3</td>
<td>AWS Backup support for Amazon S3 (Amazon Simple Storage Service) is now available in AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions For more information, see Amazon S3 backups.</td>
<td>April 19, 2023</td>
</tr>
<tr>
<td>Backup and restore SAP HANA databases on Amazon EC2 instances</td>
<td>AWS Backup now offers the ability to backup and restore SAP HANA databases running on Amazon EC2 instances in most Regions. For more information, see SAP HANA databases on Amazon EC2 instances backup.</td>
<td>April 17, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>AWS Backup now available in Europe (Spain), Europe (Zurich), and Asia Pacific (Hyderabad) Regions</td>
<td>AWS Backup support has expanded to new Regions, including Europe (Spain), Europe (Zurich), and Asia Pacific (Hyderabad). Supported resources can be backed up and restored within these Regions. For more information, see Feature availability by AWS Region.</td>
<td>April 13, 2023</td>
</tr>
<tr>
<td>Updated AWS managed policy AWSBackupAuditAccess</td>
<td>Updated AWS managed policy AWSBackupAuditAccess. AWS Backup replaced the resource selection within the API config:DescribeComplianceByConfigRule with a wildcard resource. For more information see Policy updates for AWS Backup.</td>
<td>April 11, 2023</td>
</tr>
<tr>
<td>Hypervisors with Amazon CloudWatch Logs</td>
<td>AWS Backup gateway users can now integrate hypervisors with CloudWatch Logs to maintain logs. For more information, see Editing a hypervisor configuration and CloudWatch Logs.</td>
<td>March 29, 2023</td>
</tr>
<tr>
<td>Expanded Regional support for Amazon S3</td>
<td>AWS Backup support for Amazon S3 is now available in Asia Pacific (Jakarta) and Middle East (UAE) Regions.</td>
<td>March 22, 2023</td>
</tr>
<tr>
<td>Virtual machine incremental backup improvement</td>
<td>VMware VM (virtual machine) backups that experience CBT (Changed Block Tracking) data issues now contain additional information to help remedy and troubleshoot. For more information, see Incremental VM backups and Troubleshoot your virtual machines.</td>
<td>March 15, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>AWS Backup support for multiple network adapters</td>
<td>AWS Backup gateway now supports configuring multiple network adapters. For more information on configuring your network adapters, see <a href="#">Configure your gateway for multiple NICs in VMware</a> in the AWS Backup Developer Guide.</td>
<td>March 8, 2023</td>
</tr>
<tr>
<td>AWS Backup support for vSphere 8</td>
<td>AWS Backup now supports backup and restore of virtual machines which run on VMware vSphere 8. For more information on supported VMware options, see <a href="#">Supported VMs</a> in the AWS Backup Developer Guide.</td>
<td>March 8, 2023</td>
</tr>
<tr>
<td>AWS Backup Audit Manager supports Amazon RDS Multi-AZ backups</td>
<td>Backup Audit Manager now offers support for Amazon Relational Database Service Multi-Availability Zone backups. For more information, see how to <a href="#">audit backups and create reports with AWS Backup Audit Manager</a>.</td>
<td>February 1, 2023</td>
</tr>
<tr>
<td>AWS Backup offers incremental backup for Amazon Timestream tables</td>
<td>AWS Backup now offers expanded backup capabilities for Timestream backups. Backup plans can now take incremental backups to lower the time required to backup Timestream resources and lower storage costs. For more information, see <a href="#">Amazon Timestream backups</a>.</td>
<td>January 23, 2023</td>
</tr>
<tr>
<td>AWS Backup now available in Dubai</td>
<td>AWS Backup has expanded to the Middle East (UAE) Region. Supported resources can be backed up and restored within this Region.</td>
<td>January 17, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| Cross-Region copying available in additional Regions | AWS Backup now offers cross-Region backups in Asia Pacific (Jakarta) Region, Middle East (Bahrain) Region, Asia Pacific (Hong Kong) Region, Africa (Cape Town) Region, and Europe (Milan) Region for most resources.  
For more information, see [Creating backup copies across AWS Regions](#). | December 21, 2022 |
| Backup Gateway Bandwidth Limits and Throttling  | AWS Backup Gateway now allows limits on the upload throughput from gateways to AWS Backup to control the amount of network bandwidth used by the gateway.  
To support this feature, AWS Backup has created and updated managed policies, including AWSBackupFullAccess and AWSBackupOperatorAccess.  
For more information, see [Backup Gateway bandwidth throttling](#). | December 15, 2022 |
| Backup Gateway VMware tag support            | AWS Backup Gateway now supports VMware tags. Users have the additional flexibility to create AWS tags that match tags used for virtual machines.  
To support this feature, AWS Backup has created and updated managed policies, including AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync, AWSBackupFullAccess, and AWSBackupOperatorAccess.  
For more information, see [VMware tags](#). | December 15, 2022 |
<p>| AWS Backup support for Amazon Timestream     | AWS Backup now supports backing up and restoring Amazon Timestream tables. For more information, see <a href="#">Amazon Timestream backup</a>. | December 13, 2022 |</p>
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Backup offers Legal Hold</td>
<td>AWS Backup introduces a new tool to help protect recovery points through a legal hold. For more information see <a href="https://aws.amazon.com">Legal hold</a>.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td>AWS Backup Audit Manager cross-Region and cross-account reporting</td>
<td>AWS Backup Audit Manager brings additional functionality to compliance and job reports. Users can generate reports incorporating multiple Regions and multiple accounts. For more information, see <a href="https://aws.amazon.com">Working with audit reports</a>.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td>AWS Backup supports Amazon Redshift</td>
<td>AWS Backup now offers support to backup Amazon Redshift clusters and to restore Amazon Redshift clusters and tables. For more information, see <a href="https://aws.amazon.com">Amazon Redshift backups</a>.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td>AWS Backup offers support to backup AWS CloudFormation application stacks</td>
<td>AWS Backup provides the capability to backup CloudFormation and restore applications containing multiple resources by backing up a stack and restoring the resources within it. For more information, see <a href="https://aws.amazon.com">Application stack backups</a>.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td>AWS Backup offers delegated administrator accounts and backup policy delegation</td>
<td>AWS Backup accounts enrolled in AWS Organizations can designate member accounts as delegated administrator accounts. For more information, see <a href="https://aws.amazon.com">Managing multiple accounts with AWS Organizations</a>.</td>
<td>November 27, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Public Preview of SAP HANA on Amazon EC2 Instances backup and restore</td>
<td>AWS Backup and AWS Backint are offering an integrated public preview of functionality to backup and restore SAP HANA databases on EC2 instances. For more information, see our Public Preview of SAP HANA on Amazon EC2 instances. To support this preview, AWS Backup has provided policy updates and new AWS Managed Policies for these features.</td>
<td>November 20, 2022</td>
</tr>
<tr>
<td>Restore VMware to Amazon EC2 instances</td>
<td>AWS Backup now offers the ability to restore virtual machines to Amazon EC2 instances, in addition to the ability to restore machines to EBS, VMware, VMware Cloud on AWS, and VMware Cloud on AWS Outposts. For more information, see documentation on how to Use the AWS Backup console to restore virtual machine recovery points.</td>
<td>November 9, 2022</td>
</tr>
<tr>
<td>Expanded AWS Backup Vault Lock functionality</td>
<td>AWS Backup Vault Lock can be now created in governance mode for additional IAM protections or in compliance mode to ensure immutability. Learn more at AWS Backup Vault Lock.</td>
<td>October 4, 2022</td>
</tr>
<tr>
<td>AWS Backup Audit Manager now available in Africa (Cape Town) Region and Europe (Milan) Region</td>
<td>AWS Backup Audit Manager has expanded to Africa (Cape Town) Region and Europe (Milan) Region. For more information on Backup Audit Manager, see Audit backups and create reports with AWS Backup Audit Manager.</td>
<td>September 14, 2022</td>
</tr>
<tr>
<td>AWS Backup brings Amazon CloudWatch metrics to Backup console dashboard</td>
<td>AWS Backup enhances its Backup console dashboard to display integrated Amazon CloudWatch metrics for backup and restore jobs for additional monitoring capability and flexibility.</td>
<td>September 8, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Support for additional Amazon EBS encryption flexibility during restore</td>
<td>AWS Backup now offers additional choices of encryption during restoration of Amazon EBS snapshots.</td>
<td>September 1, 2022</td>
</tr>
<tr>
<td>AWS Backup supports Amazon S3 cross-account and cross-Region backup copying</td>
<td>AWS Backup now offers cross-Region and cross-account backup copying for Amazon S3 backups. For more information see Amazon S3 backups.</td>
<td>July 28, 2022</td>
</tr>
<tr>
<td>AWS Backup Audit Manager offers additional control support for FSx for ONTAP</td>
<td>AWS Backup Audit Manager now offers additional controls to support monitoring and auditing FSx for ONTAP volumes, including Backup resources are protected by a backup plan and Last recovery point created. For more information, see AWS Backup Audit Manager controls and remediation.</td>
<td>July 22, 2022</td>
</tr>
<tr>
<td>AWS Backup adds support to backup and restore Amazon RDS Multi-AZ clusters for PostgreSQL and MySQL clusters</td>
<td>AWS Backup has added a Multi-Availability Zone cluster backup and restore option with one primary and two readable standby database instances. To learn more, see Amazon RDS Multi-AZ backups.</td>
<td>July 20, 2022</td>
</tr>
<tr>
<td>AWS Backup Audit Manager adds new control for recovery point creation</td>
<td>AWS Backup Audit Manager offers a new audit control for increased compliance support. Last recovery point created is an optional additional control to ensure recovery points are created within specified time frames. To learn more, see Last recovery point created control.</td>
<td>June 29, 2022</td>
</tr>
<tr>
<td>Added AWS Backup Gateway endpoint sample</td>
<td>AWS Backup Gateway provided a sample endpoint to assist users with connecting to VPNs (Virtual Private Networks). For more information, see Creating a AWS Backup VPC endpoint.</td>
<td>June 14, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>AWS Backup now offers Amazon VPC endpoints for VMware</td>
<td>AWS Backup now supports Amazon VPC endpoints for VMware, enabling you to use a virtual private network between your VMware environments and AWS using AWS PrivateLink. For more information, see Creating a gateway and AWS Backup and AWS PrivateLink.</td>
<td>June 1, 2022</td>
</tr>
<tr>
<td>AWS Backup Audit Manager offers additional control support for Amazon S3</td>
<td>Backup Audit Manager now offers support for the compliance control <strong>Backup resources protected by backup plan</strong> for S3 resource types. For more information, see AWS Backup Audit Manager controls and remediation.</td>
<td>May 25, 2022</td>
</tr>
<tr>
<td>AWS Backup Audit Manager offers additional control support for Storage Gateway</td>
<td>Backup Audit Manager now offers support for the compliance control <strong>Backup resources protected by backup plan</strong> for Storage Gateway resource types. For more information, see AWS Backup Audit Manager controls and remediation.</td>
<td>May 25, 2022</td>
</tr>
<tr>
<td>Support for Amazon FSx for OpenZFS</td>
<td>AWS Backup now offers added management of data protection for backing up and restoring to FSx for OpenZFS file systems.</td>
<td>May 18, 2022</td>
</tr>
<tr>
<td>AWS Backup Audit Manager support for VMware</td>
<td>AWS Backup now provides support for virtual machines in the Backup Audit Manager controls and remediation. For more information, see AWS Backup Audit Manager controls and remediation.</td>
<td>May 11, 2022</td>
</tr>
<tr>
<td>Amazon FSx now supported in Asia Pacific (Osaka) Region</td>
<td>AWS Backup now offers backing up Amazon FSx in, and cross-Region copies to and from, the Asia Pacific (Osaka) Region.</td>
<td>April 26, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Support for Amazon FSx for Lustre Persistent_2</td>
<td>AWS Backup now offers general availability of support for Amazon FSx for Lustre, which supports higher levels of throughput per storage unit as compared to Persistent_1 file systems.</td>
<td>April 5, 2022</td>
</tr>
<tr>
<td>VMware Enhancements</td>
<td>AWS Backup now offers restoring to Amazon EBS Volume, disk level restore, and support for VMWare on AWS Outposts. For more information, see <a href="#">Restoring a virtual machine</a>.</td>
<td>March 31, 2022</td>
</tr>
<tr>
<td>AWS Backup Availability for Asia Pacific (Jakarta)</td>
<td>AWS Backup is now available to customers in the Asia Pacific (Jakarta) Region.</td>
<td>March 17, 2022</td>
</tr>
<tr>
<td>New Controls for AWS Backup Audit Manager</td>
<td>AWS Backup Audit Manager introduces three new audit controls: Cross-Region copy, Cross-account copy, and Backup Vault Lock. For more information, see <a href="#">AWS Backup Audit Manager controls and remediation</a>.</td>
<td>March 17, 2022</td>
</tr>
<tr>
<td>Support for AWS PrivateLink</td>
<td>With AWS PrivateLink for AWS Backup, you can connect directly to AWS Backup using an interface endpoint in your VPC instead of connecting over the public internet. Interface endpoints are directly accessible from applications that are on premises or in a different AWS Region. For more information, see <a href="#">AWS Backup and AWS PrivateLink</a>.</td>
<td>February 28, 2022</td>
</tr>
<tr>
<td>Support for Amazon Simple Storage Service (Amazon S3)</td>
<td>General availability of AWS Backup for Amazon S3 in all AWS Regions is available except for China (Beijing) Region, China (Ningxia) Region, AWS GovCloud (US-West), and AWS GovCloud (US-East) Regions. For more information, see <a href="#">Working with Amazon S3 data</a>.</td>
<td>February 14, 2022</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Support for Advanced DynamoDB backup in AWS China Regions</td>
<td>Advanced DynamoDB backup is now available in China (Beijing) Region and China (Ningxia) Region. For more information, see <a href="#">Advanced DynamoDB backup</a>.</td>
<td>January 18, 2022</td>
</tr>
<tr>
<td>Public preview of support for Amazon S3</td>
<td>AWS Backup offers a public preview of Amazon S3 backups. For more information, see <a href="#">Working with Amazon S3 data</a>.</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td>Support for VMware virtual machines (VMs)</td>
<td>You can now use AWS Backup to automatically back up VMware VMs. For more information, see <a href="#">Virtual machine backups</a>.</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td>Support for advanced DynamoDB backup</td>
<td>You can now use AWS Backup to perform the following features for all new DynamoDB table backups you create: cold storage tiering, cost allocation tagging, cross-Region copy, cross-account copy, independent encryption, and copying tags from source DynamoDB tables. For more information, see <a href="#">Advanced DynamoDB backup</a> in the <em>Amazon DynamoDB Developer Guide</em> and <a href="#">Using AWS Backup with DynamoDB</a>.</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td>Support for AWS Backup resource assignment enhancement in AWS China Regions</td>
<td>AWS Backup resource assignment enhancement is now available in China (Beijing) Region and China (Ningxia) Region. For more information, see <a href="#">Assigning resources to a backup plan</a>.</td>
<td>November 16, 2021</td>
</tr>
<tr>
<td>Launch of AWS Backup resource assignment enhancement</td>
<td>Backup resource assignment enhancement gives you additional, fine-grained controls and new streamlined processes to deploy backup plans that protect hundreds of thousands of AWS resources. Use this feature to increase your speed, flexibility, and precision when protecting data using AWS Backup. For more information, see <a href="#">Assigning resources to a backup plan</a>.</td>
<td>November 10, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Support for Amazon Neptune</td>
<td>You can now use AWS Backup to back up Amazon Neptune clusters. To learn more, see <a href="#">What is AWS Backup?</a></td>
<td>November 5, 2021</td>
</tr>
<tr>
<td>Support for Amazon DocumentDB</td>
<td>You can now use AWS Backup to back up Amazon DocumentDB clusters. To learn more, see <a href="#">What is AWS Backup?</a></td>
<td>November 5, 2021</td>
</tr>
<tr>
<td>Support for AWS Backup Vault Lock in AWS China Regions</td>
<td>AWS Backup Vault Lock is now available in China (Beijing) Region and China (Ningxia) Region. For more information, see <a href="#">AWS Backup Vault Lock</a>.</td>
<td>November 3, 2021</td>
</tr>
<tr>
<td>Launch of AWS Backup Vault Lock</td>
<td>With AWS Backup Vault Lock, you can prevent deletion of backups stored in an AWS Backup backup vault. For more information, see <a href="#">AWS Backup Vault Lock</a>.</td>
<td>October 7, 2021</td>
</tr>
<tr>
<td>Launch of AWS Backup Audit Manager compliance reports</td>
<td>With compliance reports, you can generate daily reports on the compliance of your backup activity and resources against the controls you defined in your AWS Backup Audit Manager frameworks. For more information, see <a href="#">Compliance report templates</a>.</td>
<td>October 5, 2021</td>
</tr>
<tr>
<td>AWS CloudFormation support for AWS Backup Audit Manager</td>
<td>With AWS CloudFormation, you can now deploy AWS Backup Audit Manager frameworks, controls, and report plans in a safe, repeatable manner at scale. For more information, see <a href="#">Backup audit and reports with AWS Backup Audit Manager</a>.</td>
<td>October 4, 2021</td>
</tr>
<tr>
<td>Launch of AWS Backup Audit Manager</td>
<td>With AWS Backup Audit Manager, you can now define controls for your backup activity and resources, and identify the activities and resources that do not comply with your controls. You can also use AWS Backup Audit Manager to generate daily and on-demand reports that serve as evidence of compliance with your defined controls over time. For more information, see <a href="#">Backup audit and reports with AWS Backup Audit Manager</a>.</td>
<td>August 24, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Support for new asynchronous recovery point operations</td>
<td>AWS Backup now assumes a service-linked role to manage your backup lifecycle rules in the event that you modified or deleted your original IAM role. For more information, see Deleting backups.</td>
<td>August 23, 2021</td>
</tr>
<tr>
<td>Support for Amazon EBS multi-volume, crash-consistent backup</td>
<td>Now, when you use AWS Backup to protect your Amazon EC2 instances, AWS Backup takes multi-volume, crash-consistent backups of all the Amazon EBS volumes attached to each Amazon EC2 instance by default. For more information, see Creating Amazon EBS multi-volume, crash-consistent backup.</td>
<td>June 14, 2021</td>
</tr>
<tr>
<td>Support for Amazon FSx in additional AWS Regions</td>
<td>You can now use AWS Backup to protect your Amazon FSx file systems in the following Regions: AWS GovCloud (US), Europe (Milan) Region, Africa (Cape Town) Region, and Middle East (Bahrain) Region. For more information, see AWS Backup endpoints and quotas in the AWS General Reference.</td>
<td>April 15, 2021</td>
</tr>
<tr>
<td>Support for Amazon FSx cross-Region and cross-account backups</td>
<td>You can now use AWS Backup to copy Amazon FSx backups across AWS Regions and accounts. For more information, see Creating a Backup Copy. If you use customer managed policies, you should add the new permission fsx:CopyBackup to prevent existing backup jobs from failing. For that permission, see the last statement in the Amazon FSx backup policy in the Customer managed policies.</td>
<td>April 12, 2021</td>
</tr>
<tr>
<td>Support for cost allocation tags for Amazon EFS backups</td>
<td>You can now use cost allocation tags to track costs for your Amazon EFS backups on a detailed level, and view and filter those tags using AWS Cost Explorer. For more information, see Using Cost Allocation Tags.</td>
<td>April 7, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>FedRAMP High Authorization</td>
<td>AWS Backup is now authorized to support FedRAMP High workloads. For more information, see <a href="#">AWS Services in Scope by Compliance Program</a>.</td>
<td>March 25, 2021</td>
</tr>
<tr>
<td>New AWS Region</td>
<td>AWS Backup is now available in the Asia Pacific (Osaka) Region. In this Region, AWS Backup currently does not support Storage Gateway, Amazon FSx, and cross-account backup in this Region. For more information, see <a href="#">AWS Backup endpoints and quotas</a> in the <a href="#">AWS General Reference</a>.</td>
<td>March 25, 2021</td>
</tr>
<tr>
<td>Support for recovery point batch operations</td>
<td>You can now use the AWS Backup console to automate batch operations to clean up recovery points in your backup vaults. For more information, see <a href="#">Deleting backups</a>.</td>
<td>March 23, 2021</td>
</tr>
<tr>
<td>Support for restores to the Amazon EFS One Zone storage class</td>
<td>You can now restore your Amazon EFS backups to the Amazon EFS One Zone storage class. For more information, see <a href="#">Restoring an Amazon EFS file system</a>.</td>
<td>March 12, 2021</td>
</tr>
<tr>
<td>Support for Amazon Relational Database Service point-in-time restore and continuous backup</td>
<td>You can now use AWS Backup to automate Amazon RDS continuous backups and perform point-in-time restore (PITR), in addition to orchestrating your snapshot backups. For more information, see <a href="#">Restoring to a specified time using point-in-time recovery</a>.</td>
<td>March 10, 2021</td>
</tr>
<tr>
<td>Support for Amazon CloudWatch</td>
<td>You can now use CloudWatch to monitor AWS Backup metrics. For more information, see <a href="#">Monitoring Events and Metrics with Amazon CloudWatch and Amazon EventBridge</a>.</td>
<td>February 3, 2021</td>
</tr>
<tr>
<td>Support for Amazon EventBridge</td>
<td>You can now use EventBridge to monitor AWS Backup events. For more information, see <a href="#">Monitoring Events and Metrics with Amazon CloudWatch and Amazon EventBridge</a>.</td>
<td>February 3, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Support for cross-account backups</td>
<td>You can now use AWS Backup to back up your resources across multiple AWS accounts. For more information, see Creating backup copies across AWS accounts.</td>
<td>November 18, 2020</td>
</tr>
<tr>
<td>Support for backing up and restoring Amazon FSx file systems</td>
<td>You can now use AWS Backup to back up Amazon FSx file systems. For more information, see Working with Amazon FSx file systems.</td>
<td>November 9, 2020</td>
</tr>
<tr>
<td>New AWS Regions</td>
<td>AWS Backup is now available in the Africa (Cape Town) and Europe (Milan) AWS Regions. For more information, see AWS Backup endpoints and quotas in the AWS General Reference.</td>
<td>October 21, 2020</td>
</tr>
<tr>
<td>Support for VSS-Enabled Windows backup</td>
<td>You can now back up and restore VSS (Volume Shadow Copy Service)-enabled Windows applications running on Amazon EC2 instances. For more information, see Creating Windows VSS backups.</td>
<td>September 22, 2020</td>
</tr>
<tr>
<td>Support for Amazon EFS automatic backup</td>
<td>You can now use AWS Backup to automatically back up Amazon EFS file systems. For more information, see Getting started 4: Create Amazon EFS automatic backups.</td>
<td>July 16, 2020</td>
</tr>
<tr>
<td>New AWS Region</td>
<td>AWS Backup is now available in the AWS GovCloud (US) Region. For more information, see AWS Backup endpoints and quotas in the AWS General Reference.</td>
<td>June 24, 2020</td>
</tr>
<tr>
<td>Support for managing backups across multiple AWS accounts</td>
<td>You can now manage backups across multiple AWS accounts by using AWS Organizations. For more information, see How Cross-Account Management Works.</td>
<td>June 24, 2020</td>
</tr>
<tr>
<td>Support for Amazon Aurora added to AWS Backup</td>
<td>You can now configure AWS Backup to back up resources for Amazon Aurora. For information, see Overview of Backing Up and Restoring an Aurora DB Cluster in the Amazon Aurora User Guide.</td>
<td>June 10, 2020</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Support for configuring services to work with AWS Backup</td>
<td>You can now configure AWS Backup to back up resources for specific AWS services. For more information, see <a href="#">Opt in to managing services with AWS Backup</a>.</td>
<td>May 20, 2020</td>
</tr>
<tr>
<td>Support for backing up Amazon EC2 instances and also adds support for cross-Region backup</td>
<td>You can now back up entire Amazon EC2 instances and also copy resources across AWS Regions. For more information, see <a href="#">Creating backup copies across AWS Regions</a>.</td>
<td>January 13, 2020</td>
</tr>
<tr>
<td>New guide</td>
<td>AWS launches AWS Backup and the <a href="#">AWS Backup Developer Guide</a>.</td>
<td>January 15, 2019</td>
</tr>
</tbody>
</table>