# 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 ........................................................................................................... 3  
Feature overview ........................................................................................................................................... 5  
  Centralized backup management ............................................................................................................... 5  
  Policy-based backup ................................................................................................................................. 5  
  Tag-based backup policies ......................................................................................................................... 5  
  Lifecycle management policies ................................................................................................................ 6  
  Cross-Region backup ................................................................................................................................. 6  
  Cross-account management and cross-account backup ............................................................................ 6  
  Auditing and reporting with AWS Backup Audit Manager .................................................................... 6  
  Incremental backups ............................................................................................................................... 7  
  Full AWS Backup management ................................................................................................................. 7  
  Backup activity monitoring ....................................................................................................................... 7  
  Secure your data in backup vaults ............................................................................................................ 8  
  Support for compliance obligations ....................................................................................................... 8  
Getting started .............................................................................................................................................. 8  
  Step 1: Create a backup plan by modifying an existing one .................................................................... 8  
  Step 2: Assign resources to a backup plan ............................................................................................ 23  
  Step 3: Create a backup vault ................................................................................................................. 23  
  Next steps ................................................................................................................................................ 22  
How it works ................................................................................................................................................... 9  
  Working with supported AWS services .................................................................................................. 9  
  Opt in to managing services with AWS Backup ....................................................................................... 9  
  Working with Amazon DynamoDB ........................................................................................................ 10  
  Working with Amazon FSx file systems ................................................................................................. 10  
  Working with Amazon EC2 ...................................................................................................................... 11  
  Working with Amazon EFS ....................................................................................................................... 12  
  Working with Amazon EBS ....................................................................................................................... 12  
  Working with Amazon RDS and Aurora ................................................................................................. 12  
  Working with AWS Storage Gateway .................................................................................................... 12  
  Working with Amazon DocumentDB .................................................................................................. 12  
  Working with Amazon Neptune ............................................................................................................. 13  
  How AWS services back up their own resources .................................................................................... 13  
Metering, costs, and billing ............................................................................................................................... 13  
  AWS Backup pricing ............................................................................................................................... 13  
  AWS Backup billing ............................................................................................................................... 13  
  Cost allocation tags ............................................................................................................................... 14  
  AWS Backup Audit Manager pricing .................................................................................................. 14  
Blogs, videos, tutorials, and other resources .................................................................................................. 14  
Setting up AWS for the first time .................................................................................................................... 16  
  Sign up for AWS ................................................................................................................................. 16  
  Create an IAM user ............................................................................................................................... 16  
  Create an IAM role ............................................................................................................................... 18  
Getting started .............................................................................................................................................. 19  
  Prerequisites .......................................................................................................................................... 19  
  Getting started 1: Service Opt-in ......................................................................................................... 20  
    Next steps ............................................................................................................................................ 20  
  Getting started 2: Create an on-demand backup .................................................................................. 20  
    Next steps ............................................................................................................................................ 22  
  Getting started 3: Create a scheduled backup ..................................................................................... 22  
    Step 1: Create a backup plan by modifying an existing one ............................................................... 22  
    Step 2: Assign resources to a backup plan ......................................................................................... 23  
    Step 3: Create a backup vault ............................................................................................................ 23  
    Next steps ............................................................................................................................................ 24  
  Getting started 4: Create Amazon EFS automatic backups ................................................................. 24
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing backups across multiple accounts with AWS Organizations</td>
<td>130</td>
</tr>
<tr>
<td>Viewing a list of backups</td>
<td>79</td>
</tr>
<tr>
<td>Listing backups by protected resource</td>
<td>79</td>
</tr>
<tr>
<td>Listing backups by backup vault</td>
<td>79</td>
</tr>
<tr>
<td>Editing a backup</td>
<td>79</td>
</tr>
<tr>
<td>Deleting backups</td>
<td>80</td>
</tr>
<tr>
<td>Deleting backups manually</td>
<td>80</td>
</tr>
<tr>
<td>Troubleshooting manual deletions</td>
<td>81</td>
</tr>
<tr>
<td>Restoring a backup</td>
<td>81</td>
</tr>
<tr>
<td>Restoring an Amazon FSx file system</td>
<td>82</td>
</tr>
<tr>
<td>Restoring an EBS volume</td>
<td>85</td>
</tr>
<tr>
<td>Restoring an EFS file system</td>
<td>86</td>
</tr>
<tr>
<td>Restoring a DynamoDB database</td>
<td>88</td>
</tr>
<tr>
<td>Restoring an Amazon RDS database</td>
<td>90</td>
</tr>
<tr>
<td>Restoring an Aurora cluster</td>
<td>91</td>
</tr>
<tr>
<td>Restoring an EC2 instance</td>
<td>93</td>
</tr>
<tr>
<td>Restoring an AWS Storage Gateway volume</td>
<td>95</td>
</tr>
<tr>
<td>Restoring a Amazon DocumentDB cluster</td>
<td>96</td>
</tr>
<tr>
<td>Restoring a Amazon Neptune cluster</td>
<td>97</td>
</tr>
<tr>
<td>Audit backups and create reports with AWS Backup Audit Manager</td>
<td>6</td>
</tr>
<tr>
<td>Working with audit frameworks</td>
<td>99</td>
</tr>
<tr>
<td>Choosing your controls</td>
<td>99</td>
</tr>
<tr>
<td>Turning on resource tracking</td>
<td>100</td>
</tr>
<tr>
<td>Creating frameworks using the AWS Backup console</td>
<td>105</td>
</tr>
<tr>
<td>Creating frameworks using the AWS Backup API</td>
<td>106</td>
</tr>
<tr>
<td>Viewing framework compliance status</td>
<td>110</td>
</tr>
<tr>
<td>Finding non-compliant resources</td>
<td>111</td>
</tr>
<tr>
<td>Updating audit frameworks</td>
<td>111</td>
</tr>
<tr>
<td>Deleting audit frameworks</td>
<td>112</td>
</tr>
<tr>
<td>Working with audit reports</td>
<td>112</td>
</tr>
<tr>
<td>Choosing your report template</td>
<td>112</td>
</tr>
<tr>
<td>Creating report plans using the AWS Backup console</td>
<td>117</td>
</tr>
<tr>
<td>Creating report plans using the AWS Backup API</td>
<td>118</td>
</tr>
<tr>
<td>Creating on-demand reports</td>
<td>119</td>
</tr>
<tr>
<td>Viewing audit reports</td>
<td>120</td>
</tr>
<tr>
<td>Updating report plans</td>
<td>120</td>
</tr>
<tr>
<td>Deleting report plans</td>
<td>120</td>
</tr>
<tr>
<td>Using AWS CloudFormation to deploy AWS Backup Audit Manager resources</td>
<td>121</td>
</tr>
<tr>
<td>Turn on resource tracking</td>
<td>105</td>
</tr>
<tr>
<td>Deploy default controls</td>
<td>125</td>
</tr>
<tr>
<td>Exempt IAM roles from control evaluation</td>
<td>125</td>
</tr>
<tr>
<td>Create a report plan</td>
<td>126</td>
</tr>
<tr>
<td>Using AWS Backup Audit Manager with AWS Audit Manager</td>
<td>126</td>
</tr>
<tr>
<td>AWS Backup Audit Manager controls and remediation</td>
<td>127</td>
</tr>
<tr>
<td>Backup resources protected by backup plan</td>
<td>127</td>
</tr>
<tr>
<td>Backup plan minimum frequency and minimum retention</td>
<td>127</td>
</tr>
<tr>
<td>Backup prevent recovery point manual deletion</td>
<td>128</td>
</tr>
<tr>
<td>Backup recovery point encrypted</td>
<td>128</td>
</tr>
<tr>
<td>Backup recovery point minimum retention</td>
<td>129</td>
</tr>
<tr>
<td>Managing backups across multiple accounts with AWS Organizations</td>
<td>130</td>
</tr>
<tr>
<td>Creating a management account in Organizations</td>
<td>131</td>
</tr>
<tr>
<td>Enabling cross-account management</td>
<td>131</td>
</tr>
<tr>
<td>Creating a backup policy</td>
<td>131</td>
</tr>
<tr>
<td>Monitoring activities in multiple AWS accounts</td>
<td>134</td>
</tr>
<tr>
<td>Resource opt-in rules</td>
<td>135</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Defining policies, policy syntax, and policy inheritance</td>
<td>135</td>
</tr>
<tr>
<td>Using AWS CloudFormation to provision AWS Backup resources</td>
<td>136</td>
</tr>
<tr>
<td>In general</td>
<td>136</td>
</tr>
<tr>
<td>Deploying a backup vault, backup plan, and resource assignment with AWS CloudFormation</td>
<td>136</td>
</tr>
<tr>
<td>Deploying backup plans with AWS CloudFormation</td>
<td>136</td>
</tr>
<tr>
<td>Deploying AWS Backup Audit Manager frameworks and report plans with AWS CloudFormation</td>
<td>136</td>
</tr>
<tr>
<td>Using AWS CloudFormation with AWS Organizations</td>
<td>137</td>
</tr>
<tr>
<td>Learning more</td>
<td>137</td>
</tr>
<tr>
<td>Security</td>
<td>138</td>
</tr>
<tr>
<td>Data protection</td>
<td>138</td>
</tr>
<tr>
<td>Encryption for backups in AWS Backup</td>
<td>139</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>142</td>
</tr>
<tr>
<td>Authentication</td>
<td>142</td>
</tr>
<tr>
<td>Access control</td>
<td>143</td>
</tr>
<tr>
<td>IAM service roles</td>
<td>147</td>
</tr>
<tr>
<td>Managed policies</td>
<td>148</td>
</tr>
<tr>
<td>Using service-linked roles</td>
<td>210</td>
</tr>
<tr>
<td>Cross-service confused deputy prevention</td>
<td>214</td>
</tr>
<tr>
<td>Compliance validation</td>
<td>215</td>
</tr>
<tr>
<td>Resilience</td>
<td>215</td>
</tr>
<tr>
<td>Infrastructure security</td>
<td>216</td>
</tr>
<tr>
<td>Quotas</td>
<td>217</td>
</tr>
<tr>
<td>Monitoring</td>
<td>219</td>
</tr>
<tr>
<td>Monitoring AWS Backup events using EventBridge</td>
<td>219</td>
</tr>
<tr>
<td>Monitor events using EventBridge</td>
<td>219</td>
</tr>
<tr>
<td>Differences with the AWS Backup notification API</td>
<td>240</td>
</tr>
<tr>
<td>Monitoring AWS Backup metrics with CloudWatch</td>
<td>241</td>
</tr>
<tr>
<td>Monitor metrics with CloudWatch</td>
<td>241</td>
</tr>
<tr>
<td>Differences with the AWS Backup dashboard</td>
<td>243</td>
</tr>
<tr>
<td>Logging AWS Backup API calls with CloudTrail</td>
<td>243</td>
</tr>
<tr>
<td>AWS Backup information in CloudTrail</td>
<td>244</td>
</tr>
<tr>
<td>Understanding AWS Backup log file entries</td>
<td>244</td>
</tr>
<tr>
<td>Logging cross-account management events</td>
<td>247</td>
</tr>
<tr>
<td>Using Amazon SNS to Track Events</td>
<td>249</td>
</tr>
<tr>
<td>Common use cases</td>
<td>249</td>
</tr>
<tr>
<td>AWS Backup notification APIs</td>
<td>249</td>
</tr>
<tr>
<td>Examples of events</td>
<td>250</td>
</tr>
<tr>
<td>AWS Backup notification command examples</td>
<td>252</td>
</tr>
<tr>
<td>Specifying AWS Backup as a service principal</td>
<td>253</td>
</tr>
<tr>
<td>Troubleshooting AWS Backup</td>
<td>255</td>
</tr>
<tr>
<td>Troubleshooting general issues</td>
<td>255</td>
</tr>
<tr>
<td>Troubleshooting creating resources</td>
<td>255</td>
</tr>
<tr>
<td>Troubleshooting deleting resources</td>
<td>256</td>
</tr>
<tr>
<td>AWS Backup API</td>
<td>257</td>
</tr>
<tr>
<td>Actions</td>
<td>257</td>
</tr>
<tr>
<td>CreateBackupPlan</td>
<td>259</td>
</tr>
<tr>
<td>CreateBackupSelection</td>
<td>263</td>
</tr>
<tr>
<td>CreateBackupVault</td>
<td>266</td>
</tr>
<tr>
<td>CreateFramework</td>
<td>269</td>
</tr>
<tr>
<td>CreateReportPlan</td>
<td>273</td>
</tr>
<tr>
<td>DeleteBackupPlan</td>
<td>277</td>
</tr>
<tr>
<td>DeleteBackupSelection</td>
<td>280</td>
</tr>
<tr>
<td>DeleteBackupVault</td>
<td>282</td>
</tr>
<tr>
<td>DeleteBackupVaultAccessPolicy</td>
<td>284</td>
</tr>
<tr>
<td>DeleteBackupVaultLockConfiguration</td>
<td>286</td>
</tr>
<tr>
<td>DeleteBackupVaultNotifications</td>
<td>288</td>
</tr>
<tr>
<td>DeleteFramework</td>
<td>290</td>
</tr>
<tr>
<td>Concept</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>BackupPlan</td>
<td>443</td>
</tr>
<tr>
<td>BackupPlanInput</td>
<td>444</td>
</tr>
<tr>
<td>BackupPlansListMember</td>
<td>445</td>
</tr>
<tr>
<td>BackupPlanTemplatesListMember</td>
<td>447</td>
</tr>
<tr>
<td>BackupRule</td>
<td>448</td>
</tr>
<tr>
<td>BackupRuleInput</td>
<td>450</td>
</tr>
<tr>
<td>BackupSelection</td>
<td>452</td>
</tr>
<tr>
<td>BackupSelectionsListMember</td>
<td>454</td>
</tr>
<tr>
<td>BackupVaultListMember</td>
<td>456</td>
</tr>
<tr>
<td>CalculatedLifecycle</td>
<td>459</td>
</tr>
<tr>
<td>Condition</td>
<td>460</td>
</tr>
<tr>
<td>ConditionParameter</td>
<td>461</td>
</tr>
<tr>
<td>Conditions</td>
<td>462</td>
</tr>
<tr>
<td>ControlInputParameter</td>
<td>463</td>
</tr>
<tr>
<td>ControlScope</td>
<td>464</td>
</tr>
<tr>
<td>CopyAction</td>
<td>465</td>
</tr>
<tr>
<td>CopyJob</td>
<td>466</td>
</tr>
<tr>
<td>Framework</td>
<td>469</td>
</tr>
<tr>
<td>FrameworkControl</td>
<td>471</td>
</tr>
<tr>
<td>Lifecycle</td>
<td>472</td>
</tr>
<tr>
<td>ProtectedResource</td>
<td>473</td>
</tr>
<tr>
<td>RecoveryPointByBackupVault</td>
<td>474</td>
</tr>
<tr>
<td>RecoveryPointByResource</td>
<td>478</td>
</tr>
<tr>
<td>RecoveryPointCreator</td>
<td>480</td>
</tr>
<tr>
<td>ReportDeliveryChannel</td>
<td>481</td>
</tr>
<tr>
<td>ReportDestination</td>
<td>482</td>
</tr>
<tr>
<td>ReportJob</td>
<td>483</td>
</tr>
<tr>
<td>ReportPlan</td>
<td>485</td>
</tr>
<tr>
<td>ReportSetting</td>
<td>487</td>
</tr>
<tr>
<td>RestoreJobsListMember</td>
<td>488</td>
</tr>
<tr>
<td>Common Errors</td>
<td>490</td>
</tr>
<tr>
<td>AWS glossary</td>
<td>492</td>
</tr>
<tr>
<td>Document history</td>
<td>493</td>
</tr>
</tbody>
</table>
What is AWS Backup?

AWS Backup is a fully-managed data protection service that makes it easy to centralize and automate 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 instances)</td>
</tr>
<tr>
<td>Windows Volume Shadow Copy Service (VSS)</td>
<td>Windows VSS-supported applications (including Windows Server, Microsoft SQL Server, and Microsoft Exchange Server) on Amazon EC2</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 databases (including all database engines)</td>
</tr>
<tr>
<td>Amazon Aurora</td>
<td>Amazon 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 Windows File Server file systems</td>
</tr>
<tr>
<td>FSx for Windows File Server</td>
<td>FSx for Windows File Server 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>
<tr>
<td>Amazon Neptune</td>
<td>Amazon Neptune clusters</td>
</tr>
</tbody>
</table>
Features available for all supported resources

To use a 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
- AWS KMS-integrated backup encryption
- Cross-Region backup
- Cross-account management with AWS Organizations
- Cross-account backup
- Automated backup audits and reports with AWS Backup Audit Manager
- Write-once, read-many (WORM) with AWS Backup Vault Lock

Feature availability by resource

<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>EBS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDS</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>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>Windows VSS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AWS Backup supports Cross-Region backup, Cross-account backup, AWS Backup Audit Manager, Increment backup, Continuous backup and point-in-time restore (PITR), Full AWS Backup management, Lifecycle to cold storage, and Item-level restore.

<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>
<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 without AWS Backup advanced features</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>
</tbody>
</table>

* 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.

**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 management</th>
<th>Cross-account backup</th>
<th>AWS Backup Audit Manager</th>
<th>Storage Gateway and Amazon FSx</th>
</tr>
</thead>
<tbody>
<tr>
<td>South America (São Paulo) Region</td>
<td>✓</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>
<td>✓</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (Ireland) Region</td>
<td>✓</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>
<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>
<td>Storage Gateway and Amazon FSx</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Europe (London) Region</td>
<td>✓</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>
<td>✓</td>
</tr>
<tr>
<td>US West (N. California) Region</td>
<td>✓</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>
<td>✓</td>
</tr>
<tr>
<td>Europe (Paris) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (Stockholm) Region</td>
<td>✓</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>
<td>✓</td>
</tr>
<tr>
<td>Canada (Central) Region</td>
<td>✓</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>
<td>✓</td>
</tr>
<tr>
<td>US East (N. Virginia) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Europe (Frankfurt) Region</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>China (Beijing) Region</td>
<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>
<td>✓</td>
</tr>
</tbody>
</table>
### 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.

<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>
<th>Storage Gateway and Amazon FSx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middle East (Bahrain) Region</td>
<td>✓</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>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town) Region</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Milan) Region</td>
<td>✓</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>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-East)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For all the configuration options for backup plans, see Backup plan options and configuration (p. 32).

**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. 38).

**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. You can configure lifecycle policies that automatically transition backups from warm storage to cold storage according to a schedule that you define.

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.

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. 139) 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. 143) 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. 13) 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. 19).
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. 9)
- Metering, costs, and billing (p. 13)
- AWS Backup blogs, videos, tutorials, and other resources (p. 14)

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. 9)
- Working with Amazon DynamoDB (p. 10)
- Working with Amazon FSx file systems (p. 10)
- Working with Amazon EC2 (p. 11)
- Working with Amazon EFS (p. 12)
- Working with Amazon EBS (p. 12)
- Working with Amazon RDS and Aurora (p. 12)
- Working with AWS Storage Gateway (p. 12)
- Working with Amazon DocumentDB (p. 12)
- Working with Amazon Neptune (p. 13)
- How AWS services back up their own resources (p. 13)

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. Use the toggle switches to enable or disable the services used with AWS Backup.
4. Choose Confirm when your services are configured.

Note
Backups created with AWS Backup cannot be deleted using APIs that belong to the backed-up resource. For information about deleting recovery points using the AWS Backup API, see DeleteRecoveryPoint (p. 292).

Working with Amazon DynamoDB

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. 63).

• How to back up resources: Getting started with AWS Backup (p. 19)
• How to restore DynamoDB resources: Restoring an Amazon DynamoDB database (p. 88)

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. 19)
- How to restore Amazon FSx resources: Restoring an Amazon FSx file system (p. 82)

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. 67).

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.

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. 19)
- How to restore Amazon EC2 resources: Restoring an Amazon EC2 instance (p. 93)

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. 19)
- How to restore Amazon EFS resources: Restoring an Amazon EFS file system (p. 86)

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. 19)
- How to restore Amazon EBS volumes: Using AWS Backup to restore an Amazon EBS volume (p. 85)

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. 19)
- How to restore Amazon RDS resources: Restoring an Amazon RDS database (p. 90)
- How to restore Aurora clusters: Restoring an Amazon Aurora cluster (p. 91)

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.

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. 19)
- How to restore Storage Gateway resources: Restoring an AWS Storage Gateway volume (p. 95).

Working with Amazon DocumentDB

AWS Backup supports Amazon DocumentDB clusters.
• How to back up resources: Getting started with AWS Backup (p. 19)
• How to restore Storage Gateway resources: Restoring a Amazon DocumentDB cluster (p. 96).

Working with Amazon Neptune

AWS Backup supports Amazon Neptune clusters.

• How to back up resources: Getting started with AWS Backup (p. 19)
• How to restore Amazon Neptune clusters: Restoring a Amazon Neptune cluster (p. 97).

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
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, as long as the resource type supports full AWS Backup management. For a list of those resource types, see the Feature availability by resource (p. 2) table.

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.

AWS Backup blogs, videos, tutorials, and other resources

For more information about AWS Backup, see the following:

- Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup. With Karthik Vijayraghavan (Nov. 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 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).
• 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. 16)
2. Create an IAM user (p. 16)
3. Create an IAM role (p. 18)

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.

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 for yourself and add the user to an administrators group (console)

1. Sign in to the IAM console as the account owner by choosing Root user and entering your AWS account email address. On the next page, enter your password.
Create an IAM user

Note
We strongly recommend that you adhere to the best practice of using the Administrator IAM user that follows and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.

2. In the navigation pane, choose Users and then choose Add user.
3. For User name, enter Administrator.
4. Select the check box next to AWS Management Console access. Then select Custom password, and then enter your new password in the text box.
5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to User must create a new password at next sign-in to allow the new user to reset their password after they sign in.
6. Choose Next: Permissions.
7. Under Set permissions, choose Add user to group.
8. Choose Create group.
9. In the Create group dialog box, for Group name enter Administrators.
10. Choose Filter policies, and then select AWS managed - job function to filter the table contents.
11. In the policy list, select the check box for AdministratorAccess. Then choose Create group.

Note
You must activate IAM user and role access to Billing before you can use the AdministratorAccess permissions to access the AWS Billing and Cost Management console. To do this, follow the instructions in step 1 of the tutorial about delegating access to the billing console.

12. Back in the list of groups, select the check box for your new group. Choose Refresh if necessary to see the group in the list.
13. Choose Next: Tags.
14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see Tagging IAM entities in the IAM User Guide.
15. Choose Next: Review to see the list of group memberships to be added to the new user. When you are ready to proceed, choose Create user.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see Access management and Example policies.

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 Proceed.
4. On the Attach permissions policies page, paste 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: Overview.
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
- Cross-Region and cross-account backups for Amazon FSx using AWS Backup

Topics

- Prerequisites (p. 19)
- Getting started 1: Service Opt-in (p. 20)
- Getting started 2: Create an on-demand backup (p. 20)
- Getting started 3: Create a scheduled backup (p. 22)
- Getting started 4: Create Amazon EFS automatic backups (p. 24)
- Getting started 5: View your backup jobs and recovery points (p. 25)
- Getting started 6: Restore a backup (p. 26)
- Getting started 7: Create an audit report (p. 27)
- Getting started 8: Clean up resources (p. 29)

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. 16).
- 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. 24). 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. 16).

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. 20).

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, only persistent deployment type is 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. 68).
   - 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 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. 67).

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. 22).

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. 19).

Topics
- Step 1: Create a backup plan by modifying an existing one (p. 22)
- Step 2: Assign resources to a backup plan (p. 23)
- Step 3: Create a backup vault (p. 23)
- Next steps (p. 24)

Step 1: Create a backup plan by modifying 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. 31).

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. 38).

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 Working with backup vaults (p. 49).

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 resources types that support AWS
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. 24).

**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**

1. Open the Amazon EFS console at https://console.aws.amazon.com/efs.
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. 210).

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 in the Amazon Elastic File System User Guide.

**Next steps**

To view the backups that you've created, proceed to Getting started 5: View your backup jobs and recovery points (p. 25).
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. 25)
• View all backups in a vault (p. 25)
• View details of protected resources (p. 25)
• Next steps (p. 26)

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. 26).

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**. 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. 81).

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. 27).

**Getting started 7: Create an audit report**

In **Getting started 5: View your backup jobs and recovery points** (p. 25), 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-0bc877ae77800000",
    "backupRuleId": "ab88bfb8-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. 29).

Getting started 8: Clean up resources

After you perform all the tasks in Getting started with AWS Backup (p. 19), you might want to clean up what you have created to avoid incurring any unnecessary charges.

Topics
- Step 1: Delete restored AWS resources (p. 29)
- Step 2: Delete the backup plan (p. 29)
- Step 3: Delete the recovery points (p. 30)
- Step 4: Delete the backup vault (p. 30)
- Step 5: Delete the report plan (p. 30)
- Step 6: Delete the reports (p. 30)

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. 31)
- Assigning resources to a backup plan (p. 38)
- Deleting a backup plan (p. 48)
- Updating a backup plan (p. 48)

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. 31)
- Creating backup plans using a JSON document and the AWS Backup CLI (p. 32)
- Backup plan options and configuration (p. 32)
- AWS CloudFormation templates for backup plans (p. 36)

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.

  For step-by-step instructions, see Step 1: Create a backup plan by modifying an existing one (p. 22) in the Getting Started section.
• Build a new plan from scratch — You can create a new backup plan by specifying each of the backup configuration details described in the following sections. You can choose from the recommended default configurations.

If you try to create a backup plan that is identical to an existing plan, you get an AlreadyExistsException error.

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.

```json
{
    "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.

```bash
aws backup create-backup-plan --cli-input-json file:///PATH-TO-FILE/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 and Amazon FSx cannot start backups 4 hours before or during their maintenance window or automatic backup window. 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>

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.

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 “expire after days” 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. 23).

**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 https://docs.aws.amazon.com/aws-backup/latest/devguide/recovery-point-create-a-copy.html#create-cross-account-backup.

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.

**Expense** 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. 67).
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:
            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"
      AdvancedBackupSettings:
        - ResourceType: EC2
      BackupOptions:
        WindowsVSS: enabled
    BackupPlanRule:
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. 38)
- Assigning resources programmatically (p. 40)
- Assigning resources using AWS CloudFormation (p. 45)
- Quotas on resource assignment (p. 48)

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.

     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 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:

```
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 performs 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".

<table>
<thead>
<tr>
<th>Resource assignment</th>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select all resources in my account.</td>
<td><code>{ &quot;BackupSelection&quot;: { &quot;Resources&quot;: [ &quot;*&quot; ] } }</code></td>
</tr>
<tr>
<td>Select all resources in my account, but exclude EBS volumes.</td>
<td><code>{ &quot;BackupSelection&quot;: { &quot;Resources&quot;: [ &quot;*&quot; ], &quot;NotResources&quot;: [ &quot;arn:aws:ec2:*:*:volume/*&quot; ] } }</code></td>
</tr>
<tr>
<td>Select all resources tagged with &quot;backup&quot;: &quot;true&quot; in my account, but exclude EBS volumes.</td>
<td><code>{ &quot;BackupSelection&quot;: { &quot;Resources&quot;: [ &quot;*&quot; ], &quot;NotResources&quot;: [ &quot;arn:aws:ec2:*:*:volume/*&quot; ], &quot;Conditions&quot;: { } } }</code></td>
</tr>
</tbody>
</table>
### Resource Assignment

<table>
<thead>
<tr>
<th>JSON</th>
</tr>
</thead>
</table>
| ```json
"StringEquals":[
  {
    "ConditionKey":"aws:ResourceTag/backup",
    "ConditionValue":"true"
  }
]
``` |

Select all RDS instances and EBS volumes resources tagged with both "backup":"true" and "stage":"prod".

<table>
<thead>
<tr>
<th>JSON</th>
</tr>
</thead>
</table>
| ```json
{"BackupSelection":{
  "Resources":[
    "arn:aws:rds:*:*:db:*",
    "arn:aws:ec2:*:*:volume/*",
  ],
  "Conditions":{
    "StringEquals":[
      {
        "ConditionKey":"aws:ResourceTag/backup",
        "ConditionValue":"true"
      },
      {
        "ConditionKey":"aws:ResourceTag/stage",
        "ConditionValue":"prod"
      }
    ]
  }
}
``` |

Note that 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.
### Resource assignment

<table>
<thead>
<tr>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select all RDS instances and EBS volumes tagged with &quot;backup&quot;: &quot;true&quot; but not &quot;stage&quot;: &quot;test&quot;.</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;BackupSelection&quot;: {</td>
</tr>
<tr>
<td>&quot;Resources&quot;: [</td>
</tr>
<tr>
<td>&quot;arn:aws:rds:<em>:</em>:db:*&quot;,</td>
</tr>
<tr>
<td>&quot;arn:aws:ec2:<em>:</em>:volume/*&quot;</td>
</tr>
<tr>
<td>],</td>
</tr>
<tr>
<td>&quot;Conditions&quot;: {</td>
</tr>
<tr>
<td>&quot;StringEquals&quot;: [</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;ConditionKey&quot;: &quot;aws:ResourceTag/backup&quot;,</td>
</tr>
<tr>
<td>&quot;ConditionValue&quot;: &quot;true&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>],</td>
</tr>
<tr>
<td>&quot;StringNotEquals&quot;: [</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;ConditionKey&quot;: &quot;aws:ResourceTag/stage&quot;,</td>
</tr>
<tr>
<td>&quot;ConditionValue&quot;: &quot;test&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select all resources tagged with &quot;key1&quot; and a value which begins with &quot;include&quot; but not with &quot;key2&quot; and value that contains the word &quot;exclude&quot;.</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;BackupSelection&quot;: {</td>
</tr>
<tr>
<td>&quot;Resources&quot;: [</td>
</tr>
<tr>
<td>&quot;*&quot;</td>
</tr>
<tr>
<td>],</td>
</tr>
<tr>
<td>&quot;Conditions&quot;: {</td>
</tr>
<tr>
<td>&quot;StringLike&quot;: [</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;ConditionKey&quot;: &quot;aws:ResourceTag/key1&quot;,</td>
</tr>
<tr>
<td>&quot;ConditionValue&quot;: &quot;include*&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>],</td>
</tr>
<tr>
<td>&quot;StringNotLike&quot;: [</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;ConditionKey&quot;: &quot;aws:ResourceTag/key2&quot;,</td>
</tr>
<tr>
<td>&quot;ConditionValue&quot;: &quot;<em>exclude</em>&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>

Note the use of the wildcard character (*) in include* and *exclude*.
<table>
<thead>
<tr>
<th>Resource assignment</th>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select all resources tagged with “backup”: “true” except RDS and FSx resources.</td>
<td>{  &quot;BackupSelection&quot;:{    &quot;Resources&quot;: [      &quot;<em>&quot;    ],    &quot;NotResources&quot;: [      &quot;arn:aws:rds:</em>&quot;,      &quot;arn:aws:fsx:*&quot;    ],    &quot;Conditions&quot;: {      &quot;StringEquals&quot;: [        {          &quot;ConditionKey&quot;: &quot;aws:ResourceTag/backup&quot;,          &quot;ConditionValue&quot;: &quot;true&quot;        }      ]    }  }</td>
</tr>
<tr>
<td>Items in NotResources are combined using the Boolean OR.</td>
<td></td>
</tr>
<tr>
<td>Select all resources tagged with a tag “backup” and any value</td>
<td>{  &quot;BackupSelection&quot;:{    &quot;Resources&quot;: [      &quot;<em>&quot;    ],    &quot;Conditions&quot;: {      &quot;StringLike&quot;: [        {          &quot;ConditionKey&quot;: &quot;aws:ResourceTag/backup&quot;,          &quot;ConditionValue&quot;: &quot;</em>&quot;        }      ]    }  }</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Resource assignment</th>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select all RDS instances, the Aurora cluster “my-aurora-cluster”, and all resources tagged with “backup”: “true”, except for those resources tagged with “stage”: “test”.</td>
<td>{  &quot;BackupSelection&quot;:{  &quot;Resources&quot;: [  &quot;arn:aws:rds:<em>:</em>:db:<em>&quot;,  &quot;arn:aws:rds:</em>:*:db-cluster:my-aurora-cluster&quot; ],  &quot;ListOfTags&quot;: [  {  &quot;ConditionType&quot;: &quot;StringEquals&quot;,  &quot;ConditionKey&quot;: &quot;backup&quot;,  &quot;ConditionValue&quot;: &quot;true&quot; } ],  &quot;Conditions&quot;: [  {  &quot;StringNotEquals&quot;: [  {  &quot;ConditionKey&quot;: &quot;aws:ResourceTag/stage&quot;,  &quot;ConditionValue&quot;: &quot;test&quot; } ] } ] } }</td>
</tr>
<tr>
<td>Resource assignment</td>
<td>JSON</td>
</tr>
<tr>
<td>---------------------</td>
<td>------</td>
</tr>
<tr>
<td>Select all resources tagged with tag &quot;backup&quot;: &quot;true&quot; except for RDS instances tagged with &quot;stage&quot;: &quot;test&quot;.</td>
<td>Use two CLI commands to create two selections to select this group of resources. The first selection applies to all resources except RDS instances. The second selection applies to RDS instances.</td>
</tr>
</tbody>
</table>
| | \{
| |   "BackupSelection":{
| |     "Resources": [
| |     "*
| |     ],
| |     "NotResources": [
| |     "arn:aws:rds:*:*:db:*"
| |     ],
| |     "Conditions": {
| |     "StringEquals": [
| |     { "ConditionKey": "aws:ResourceTag/backup", "ConditionValue": "true"
| |     }
| |     ]
| |   }
| | }
| | \{
| |   "BackupSelection":{
| |     "Resources": [
| |     "arn:aws:rds:*:*:db:*"
| |     ],
| |     "Conditions": {
| |     "StringEquals": [
| |     { "ConditionKey": "aws:ResourceTag/backup", "ConditionValue": "true"
| |     }
| |     ],
| |     "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.
• 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 Amazon RDS resource.
  • 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
```

46
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::IAM::RoleName}/AWSBackupServiceRolePolicyForBackup"

BasicBackupSelection:
  Type: 'AWS::Backup::BackupSelection'
  Properties:
    BackupPlanId: !Ref BasicBackupPlan
    BackupSelection:
      SelectionName: !Ref BackupSelectionName
      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 tags
- 30 conditions

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.
Working with backup vaults

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

• Creating a backup vault (p. 49)
• Setting access policies on backup vaults (p. 50)
• AWS Backup Vault Lock (p. 53)
• Deleting a backup vault (p. 56)

Creating 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. 23) 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.

You can create a new encryption key by following the 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. 139) 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.

Setting 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 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. 144) 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. 51)
- Deny access to a backup vault (p. 51)
- Deny access to delete recovery points in a backup vault (p. 52)
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": {
            "AWS": "arn:aws:iam::Account ID:role/MyRole"
         },
         "Action": [
            "backup:DescribeBackupVault",
            "backup:DeleteBackupVault",
            "backup:PutBackupVaultAccessPolicy",
            "backup:DeleteBackupVaultAccessPolicy",
            "backup:GetBackupVaultAccessPolicy",
            "backup:StartBackupJob",
            "backup:GetBackupVaultNotifications",
            "backup:PutBackupVaultNotifications",
            "backup:DeleteBackupVaultNotifications",
            "backup:GetBackupPointsByBackupVault"
         ],
      }
   ]
}
```
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:",
                        "BBBBBBBBBBBBBBBBBBBB:",
                        "112233445566"
                    ]
                }
            }
        }
    ]
}
```

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"
                    ]
                }
            }
        }
    ]
}
```
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 yet to receive a third-party assessment for SEC 17a-4(f) and CFTC. Do not confuse AWS Backup Vault Lock with S3 Glacier Vault Lock, which is a different feature for a different AWS service.

AWS Backup Vault Lock enforces a write-once, read-many (WORM) setting for all the backups you store and create in a backup vault.

With AWS Backup Vault Lock, you can add an additional layer of defense that protects backups (recovery points) in your backup vaults from inadvertent or malicious:

- Delete operations and
- Updates that shorten or otherwise alter their retention period

AWS Backup Vault Lock helps you can enforce retention periods, prevent early deletions by privileged users (including the AWS account root user), and meet your organization's data protection policies and procedures.

Note
You can configure AWS Backup Vault Lock using the AWS Backup API, CLI, or SDK. Currently, you cannot configure AWS Backup Vault Lock using the AWS Backup console.

Important
AWS Backup Vault Lock takes effect immediately. It gives you a minimum three-day (72-hour) cooling-off period to delete or update its configuration before it permanently locks your vault. You can optionally extend the duration of this cooling-off period. Use this cooling-off period to test AWS Backup Vault Lock against your workloads and use cases. After your cooling-off period expires, you cannot delete or otherwise alter AWS Backup Vault Lock using the AWS Backup console, API, CLI, or SDK.

Topics
- Locking a backup vault (p. 54)
- Reviewing a backup vault for its AWS Backup Vault Lock configuration (p. 55)
- Deleting AWS Backup Vault Lock during the cooling-off period (p. 55)
• Achieving defense in depth with AWS Backup Vault Lock and other AWS Backup security features (p. 56)

Locking a backup vault

To configure AWS Backup Vault Lock, use `PutBackupVaultLockConfiguration` like this CLI example:

```
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
```

You can configure four options:

1. **BackupVaultName** (required)
   
   The name of the vault to lock.

2. **ChangeableForDays** (optional)
   
   The cooling-off period in days before AWS Backup Vault Lock cannot be deleted. 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.

   You must set `ChangeableForDays` to 3 or greater because AWS Backup enforces a minimum 72-hour cooling-off period before AWS Backup Vault Lock takes effect and becomes immutable.

   Before the lock date, you can delete AWS Backup Vault Lock from the vault using `DeleteBackupVaultLockConfiguration` or change the AWS Backup Vault Lock configuration using `PutBackupVaultLockConfiguration`. On and after the lock date, AWS Backup Vault Lock becomes immutable and cannot be changed or deleted.

   If not specified, you can use `DeleteBackupVaultLockConfiguration` or `PutBackupVaultLockConfiguration` any time.

3. **MaxRetentionDays** (optional)
   
   The maximum retention period that the vault retains its recovery points. This setting can be useful if, for example, you must destroy certain data after retaining it for four years (1460 days).

   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 AWS Backup Vault Lock are not affected.

4. **MinRetentionDays** (optional)
   
   The minimum retention period that the vault retains its recovery points. This setting can be useful if, for example, you must retain certain data for at least seven years (2555 days).

   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.
Reviewing a backup vault for its AWS Backup Vault Lock configuration

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

To determine whether you applied AWS Backup 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.

```
{
    "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 period).
2. **LockDate** is the UTC date and time when your cooling-off period ends. After this time, you cannot delete or change your AWS Backup Vault Lock on this vault. Use any publicly-available time converters to convert this string to your local time.
3. **MaxRetentionDays** and **MinRetentionDays** are previously described.

If "Locked":false, like the following example, you have not applied Vault Lock (or deleted it).

```
{
    "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": 3,
    "Locked": false
}
```

Deleting AWS Backup Vault Lock during the cooling-off period

To delete your AWS Backup Vault Lock during your cooling-off period (and before your **LockDate**), use `DeleteBackupVaultLockConfiguration` like this CLI example:
Achieving defense in depth with AWS Backup Vault
Lock and other AWS Backup security features

AWS Backup Vault Lock adds an additional layer of security to your data protection defense in depth. Additional layers that you can use to strengthen your security posture include:

- AWS Backup itself, since the content within its recovery points are immutable,
- 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.

Deleting 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 policy 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 following table contains examples of AWS Backup-supported resource types and their corresponding recovery point ID.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Backup name</th>
<th>Recovery point ID example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon FSx file system</td>
<td>Amazon FSx backup</td>
<td>backup/backup-0edcf967356c809c7</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2) instance</td>
<td>Amazon EC2 backup</td>
<td>image/ami-0edcf967356c809c7</td>
</tr>
<tr>
<td>Amazon EBS volume</td>
<td>Amazon EBS snapshot</td>
<td>snap/snap-05f426fd8kdjb4224</td>
</tr>
<tr>
<td>Amazon RDS database</td>
<td>Amazon RDS snapshot</td>
<td>awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453</td>
</tr>
<tr>
<td>Amazon Aurora DB cluster</td>
<td>Aurora clusters</td>
<td>awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453</td>
</tr>
<tr>
<td>Amazon EFS file system</td>
<td>Amazon EFS backup</td>
<td>d99699e7-e183-477e-bfcd-ccb1c6e5455e</td>
</tr>
<tr>
<td>DynamoDB table</td>
<td>DynamoDB backup without</td>
<td>table/MyDynamoDBTable/backup/01547087347000-c8b62d3</td>
</tr>
<tr>
<td></td>
<td>Advanced DynamoDB backup (p. 63)</td>
<td></td>
</tr>
<tr>
<td>DynamoDB table</td>
<td>DynamoDB backup with</td>
<td>12a34a56-7bb8-901c-cd23-4567d8e9ef01</td>
</tr>
<tr>
<td></td>
<td>Advanced DynamoDB backup (p. 63)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>Storage Gateway volume</td>
<td>Amazon EBS snapshot*</td>
<td>snapshot/snap-0d40e49137e31d9e0</td>
</tr>
</tbody>
</table>

*When you back up an Storage Gateway volume, an Amazon EBS snapshot is created. This snapshot can then be restored either as an Amazon EBS volume or as an Storage Gateway volume.

Important
To avoid additional charges, configure your retention policy with a warm storage duration of at least one week.
AWS Backup calculates your lifecycle from the start of your backup job, not its completion. For example, assume that 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 will implement your retention period of one day and remove your backup from warm storage when your backup job completes. The next day, AWS Backup cannot create an incremental backup because there's 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.

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

Topics
- Creating a backup (p. 58)
- Copy a backup (p. 69)
- Viewing a list of backups (p. 79)
- Editing a backup (p. 79)
- Deleting backups (p. 80)
- Restoring a backup (p. 81)

Creating a backup

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

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. 31).

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. 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 created, pending, running, aborting, aborted, completed, failed, and expired.

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 its lifecycle limit 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 enable that.

For more information about creating backup plans, see Creating a backup plan (p. 31).

Topics
- Creating an on-demand backup (p. 59)
- Restoring to a specified time using point-in-time recovery (p. 60)
- Advanced DynamoDB backup (p. 63)
- Creating Windows VSS backups (p. 67)
- Amazon EBS multi-volume, crash-consistent backups (p. 68)
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.

**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. If you're working with a service that does not support **Transition to cold storage**, the value is marked **N/A**. Otherwise, you can specify when to transition this backup 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.
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. 67)**.
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**

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). Compare that with snapshot backups, which you can only take as frequently as every hour. You can also store snapshot backups for a maximum of 100 years. Because continuous and snapshot backups offer different advantages, we recommend that you protect your resources with both continuous and snapshot backup rules.

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 enable 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**.
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**

AWS Backup supports continuous backups and point-in-time recovery for the following services and applications. This section describes resource-specific advantages, limitations, and best practices for using PITR in AWS Backup.

**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.

**Note**

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

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](https://docs.aws.amazon.com/AmazonRDS/latest/ApressGuide/gdbinstance.html).
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.

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

- **Restoring recent activity** — You might not be able to restore the most recent 5 minutes of activity due to how Amazon RDS handles its transaction logs.
- **Creating copies of Amazon RDS continuous backups** — You can't create copies of Amazon RDS continuous backups because Amazon RDS does not allow copying transaction logs.

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 your instance details page in the Amazon RDS console, choose **Maintenance and backup**, and find the **Automated backup** field.

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:DescribeDBInstanceAutomatedBackupsAPI`. In the AWS Backup console, you must have the `rds:DescribeDBInstanceAutomatedBackupsAPI` 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

• Call the StartRestoreJob API operation with the RestoreTime parameter, as in the following example.

  "RestoreTime":"2011-09-07T23:45:00Z"

You must express RestoreTime in Universal Coordinated Time (UTC). For more information, see RestoreTime.

Stopping continuous backups

If you want to stop continuous backups, you must delete the continuous backup rule from your backup plan. 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.

Making copies of 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, copies that snapshot to the destination vault, and then deletes the source snapshot. To learn more about copying your recovery points across accounts and Regions, see Copying a backup.

AWS Backup does not support on-demand copies of continuous backups. AWS Backup does not support copies of Amazon RDS continuous backups because Amazon RDS does not allow copies of its transaction logs.
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.

Advanced DynamoDB backup

**Note**

Advanced DynamoDB backup is not available in China Regions.

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.

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. 148).

**Topics**
- Enabling advanced DynamoDB backup using the console (p. 64)
- Enabling advanced DynamoDB backup programmatically (p. 65)
- Editing an advanced DynamoDB backup (p. 65)
- Restoring an advanced DynamoDB backup (p. 66)
- Deleting an advanced DynamoDB backup (p. 66)
- Other benefits of full AWS Backup management when you enable advanced DynamoDB backup (p. 66)

### 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**.

   If it is not, choose **Opt-in** and enable DynamoDB as an AWS Backup supported service.
4. Under the **Advanced features for DynamoDB backups** section, choose **Enable**.
5. 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 programatically**

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 database (p. 88).

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. 80).

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. 139) 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. 143) 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. 13) for more information.

**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. Not all instance types or applications are supported for Windows VSS backups.

For more information, see Creating a VSS Application-Consistent Snapshot in the *Amazon EC2 User Guide for Windows Instances*.

To back up and restore VSS-enabled Windows resources running Amazon EC2, follow these steps:

- Complete the required prerequisite tasks. For instructions, see Before You Begin in the *Amazon EC2 User Guide for Windows Instances*.
- Download, install, and configure the VSS agent in AWS Systems Manager. This step is required. For instructions, see Update SSM Agent by using Run Command in the *AWS Systems Manager User Guide*.
- 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 in the *Amazon EC2 User Guide for Windows Instances*. For an example of the IAM policy, see Managed policies (p. 148).
- Enable VSS in AWS Backup.

**To enable Windows VSS backup in AWS Backup**

2. On the dashboard, choose the type of backup you want to create, either Create an on-demand backup or Manage Backup plans. 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 section, choose Windows VSS. This enables you to take application-consistent Windows VSS backups.
5. Create your backup.

**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.
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. It does not copy tags from your recovery points to your restored resources.

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. 146).
- 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 enable Advanced DynamoDB backup (p. 63) with AWS Backup.
- 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. You can also automate a sequence of cross-account and cross-Region copies for most supported resources, except for Amazon RDS, Amazon Aurora, Amazon DocumentDB, and Amazon Neptune. For those snapshots, AWS Backup only supports automating either cross-account or cross-Region copies due to how those services create their encryption keys.

Copies inherit their source configuration unless you specify otherwise. There is one exception: if you specify that your copy "Never" expire, your copy still inherits its source expiration date. Currently, if you want your backup copies to be permanent, 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 (p. 69)
- Creating backup copies across AWS accounts (p. 71)

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."

You can use AWS Backup to copy your backups for all supported, defining different backup plans in different Regions, subject to the following limitations:

- DynamoDB supports cross-Region backup after you enable Advanced DynamoDB backup (p. 63).
- Amazon RDS, Amazon Aurora, Amazon DocumentDB, and Amazon Neptune support cross-Region backup, or cross-account backup, but not both in the same backup plan. You can use a AWS Lambda script to accomplish both. Also, copying Amazon RDS custom option groups across AWS Regions is not supported.

69
- Amazon EFS supports cross-Region copy at the plan level. To apply a different copy rule to a subset of file systems, create a new plan.

Cross-Region backup is available in all AWS Regions where AWS Backup is available except for Asia Pacific (Hong Kong), Middle East (Bahrain), Europe (Milan), and Africa (Cape Town).

**Performing on-demand cross-Region backup**

**To copy an existing backup on-demand**

2. Choose **Backup vaults**.
3. Choose a vault and choose a recovery point from the vault.
4. Choose the **Copy** button.
5. Enter the following values:
   - **Destination Region**: Choose the destination AWS Region for the copy. You can add a new copy rule per copy to a new destination.
   - **(Advanced settings) Backup vault**: Choose the destination backup vault for the copy.
   - **(Advanced settings) 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.
   - **(Advanced settings) Lifecycle**: 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.
     - **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.
6. Choose **Create backup copy**.

**Scheduling cross-Region backup**

You can use a scheduled backup plan to copy backups across AWS Region.

**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**
   
   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.

10. Choose **Create plan**.

Creating backup copies across AWS accounts

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.

You can use AWS Backup to copy your backups for all supported resources, subject to the following limitations:

- DynamoDB supports cross-account backup after you enable Advanced DynamoDB backup (p. 63).
- For resource types that do not support full AWS Backup management (those that do not have a checkmark in the "Full AWS Backup management" section of the Feature availability by resource (p. 2) table), cross-account backup only supports customer managed keys. It does not support vaults that are encrypted using AWS keys, including default vaults, because AWS keys are not intended to be shared between accounts.

You must use vaults other than your default vaults to perform cross-account backup.
For resource types that support full AWS Backup management, you can perform cross-account backups using any AWS Backup backup vault because AWS Backup independently manages the encryption of those backups.

- Amazon RDS, Amazon Aurora, Amazon DocumentDB, and Amazon Neptune support cross-Region backup, or cross-account backup, but not both in the same backup plan. You can use a AWS Lambda script to accomplish both. Also, copying Amazon RDS custom option groups across AWS Regions is not supported.

- Amazon EC2 does not allow cross-account copies of AWS Marketplace AMIs. For more information, see Copying an AMI in the Amazon EC2 User Guide.

Cross-Region backup are available in all AWS Regions where AWS Backup is available except for China Regions, Asia Pacific (Hong Kong), Middle East (Bahrain), Europe (Milan), Africa (Cape Town), and Asia Pacific (Tokyo).

### 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 such as `ec2:ModifySnapshotAttribute`. For more information about both 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. 78).

  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. 75). To limit which accounts can receive the contents of other accounts' backup vaults, see Configuring your account as a destination account (p. 77).

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.

{
"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"
        }
    }
]

(Advanced settings) Transition to cold storage

Choose the options that you want for your Amazon EFS file system.

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 the backups of other resource types.

**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.

AWS Backup needs permissions to access the external (source) account. The wizard shows an example policy that provides this access. This policy is shown following.

```
{
  "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 resource types.

**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.

---

**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 Creating backup copies across AWS accounts (p. 71).
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 (p. 76)
- Share a destination backup vault an organizational unit in AWS Organizations (p. 76)
- Share a destination backup vault with an organization in AWS Organizations (p. 77)

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 1111222233333.

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
          "arn:aws:iam::4444555566666:root",
          "arn:aws:iam::1111222233333: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":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-aib2c3d4e5/r-f6g7h8i9j0example/ou-def0-awssbbbb",
            "o-aib2c3d4e5/r-f6g7h8i9j0example/ou-def0-awssbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```
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".

```
{
  "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 access controls in AWS Organizations to limit your destination accounts.

- Limit destination accounts using tags (p. 77)
- Limit destination accounts using account numbers and vault names (p. 78)
- Limit destination accounts using organizational units in AWS Organizations (p. 78)

Limit destination accounts using tags

The following policy limits destination accounts to accounts with backup vaults tagged DestinationBackupVault.

```
{
  "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

The following policy limits destination accounts to only two accounts. The first destination account is account 112233445566 with the backup vault name prefix cab. The second destination account is account 123456789012 in AWS Region us-west-1 with the 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

The following policy limits destination accounts to the accounts within certain organizational units. You must attach this policy to an AWS Organizations node that contains your source account.

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource": "*",
      "Condition":{
        "ForAllValues:StringNotLike":{
          "backup:CopyTargetOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbb/ou-jkl0-awssddd/*"
          ]
        }
      }
    }
  ]
}
```

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
There are two ways to view a list of your backups using the AWS Backup console. You can view the backups that are associated with a particular AWS resource. Or, you can view all the backups that are organized in a single backup vault, which can be across multiple AWS resources and different resource types.

Topics
- Listing backups by protected resource (p. 79)
- Listing backups by backup vault (p. 79)

Listing backups by protected resource

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 all the backups for the resource, even the ones that were not created by AWS Backup. From this view, you can also choose a backup and restore it.

Listing backups by backup vault

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 select a backup and edit it, delete it, or restore it.

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 the backups of other resource types.
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 whether to keep or delete your continuous backup data. Continuous backups only have a single recovery point.
   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

**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](#).

When you restore a backup in AWS Backup, it generally creates a new resource with the backup that you are restoring. For each restore, you must specify the restore parameters.

Restore parameters are specific to a resource type, such as the volume size when restoring an Amazon Elastic Block Store (Amazon EBS) snapshot. When you restore a backup using the AWS Backup console,
the service-specific restore parameters are presented automatically. For each restore, a restore job is created with a unique job ID—for example, 1323657E-2AA4-1D94-2C48-5D7A423E7394.

You can view the status of a restore job on the Jobs page of the AWS Backup console. Restore job statuses include created, pending, running, aborting, aborted, completed, failed, and expired.

For basic restore instructions and links to documentation for each service that uses the AWS Backup console, see Getting started 6: Restore a backup (p. 26) in the Getting Started section.

To restore a backup using the AWS Command Line Interface (AWS CLI), API, or SDK, pass configuration information for your resource to the StartRestoreJob (p. 411) API operation.

The configuration information that you need to restore your resource varies depending on the service that you want to restore. To get the configuration metadata that your backup was created with, you can call GetRecoveryPointRestoreMetadata (p. 351), but you might need more information to restore your resource. Each service requires different configuration values ("restore metadata") to restore is also available in the following topics.

Topics
- Restoring an Amazon FSx file system (p. 82)
- Using AWS Backup to restore an Amazon EBS volume (p. 85)
- Restoring an Amazon EFS file system (p. 86)
- Restoring an Amazon DynamoDB database (p. 88)
- Restoring an Amazon RDS database (p. 90)
- Restoring an Amazon Aurora cluster (p. 91)
- Restoring an Amazon EC2 instance (p. 93)
- Restoring an AWS Storage Gateway volume (p. 95)
- Restoring an Amazon DocumentDB cluster (p. 96)
- Restoring a Amazon Neptune cluster (p. 97)

Restoring an Amazon 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. 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. 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

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.

For more information about Microsoft Active Directory, see Working with Active Directory in Amazon FSx for Windows File Server in the FSx for Windows File Server User Guide.

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** in the **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. If you are restoring an FSx for Windows File Server file system, provide the **Windows authentication** information that is used to access the file system, or you can create a new one.

   For detailed information about Microsoft Active Directory, see **Working with Active Directory in Amazon FSx for Windows File Server** in the **FSx for Windows File Server User Guide**.

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 IAM role.

14. 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:

```plaintext
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStart Time
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
```

**FSx for Windows File Server restore metadata**

You can specify the following metadata during an FSx for Windows File Server restore:

```plaintext
ThroughputCapacity
PreferredSubnetId
ActiveDirectoryId
```
FSx for Lustre restore metadata

You can specify the following metadata during an FSx for Lustre restore:

- **PerUnitStorageThroughput**
- **DriveCacheType**

Example CLI restore command:

```bash
```

Example restore metadata:

```
"restoreMetadata":  "{\"StorageType\":\"SSD\",\"KmsKeyId\":\"arn:aws:kms:us-east-1:123456789012:key/1234567890abcdef-123b-123c-defg-1h2i2j3k4l5m6n7o8p9q0\",\"StorageCapacity\":\"1200\",\"VpcId\":\"vpc-0ab0979fa431ad326\",\"FileSystemType\":\"LUSTRE\",\"LustreConfiguration\":\"{\"WeeklyMaintenanceStartTime\":\"4:10:30\",\"DeploymentType\":\"PERSISTENT_1\",\"PreferredSubnetId\":\"subnet-1234\",\"PerUnitStorageThroughput\":\"50\",\"CopyTagsToBackups\":\"true\"},\"FileSystemId\":\"fs-0ca11fb3d18a35c2\",\"SubnetIds\":\"[\"subnet-0e66e94eb3295351\"]\"}"
```

Using AWS Backup to restore 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**.
   - 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.
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.

**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:

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the EBS volume being restored.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Whether the volume is encrypted.</td>
</tr>
<tr>
<td>kmsKey</td>
<td>The KMS key used to encrypt the volume.</td>
</tr>
<tr>
<td>availabilityZone</td>
<td>The availability zone of the volume.</td>
</tr>
</tbody>
</table>

**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/mynname/efs` and the file path is `user/home/mynname/efs/file1`, you enter `/file1`. Paths are case sensitive. Wildcard characters and regex strings are not supported.

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
   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. 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.

Restoring an Amazon DynamoDB database

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 key**, choose the key that AWS Backup will use to encrypt your restored table.
   - When you restore in the same Region as your original table, you must specify an encryption key for your restored table. The default encryption key is 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.

7. Choose **Restore**.

   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:

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>originalTableName</td>
<td>Table name of the original table</td>
</tr>
<tr>
<td>backupName</td>
<td>Name of the backup</td>
</tr>
<tr>
<td>backupArn</td>
<td>ARN of the backup</td>
</tr>
<tr>
<td>primaryPartitionKey</td>
<td>Primary partition key</td>
</tr>
<tr>
<td>sortKey</td>
<td>Sort key</td>
</tr>
<tr>
<td>provisionedRcu</td>
<td>Provisioned read capacity units</td>
</tr>
<tr>
<td>provisionedWcu</td>
<td>Provisioned write capacity units</td>
</tr>
<tr>
<td>encryptionType</td>
<td>Encryption type</td>
</tr>
<tr>
<td>kmsMasterKeyArn</td>
<td>ARN of the key used for encryption</td>
</tr>
<tr>
<td>autoScaling</td>
<td>Auto scaling</td>
</tr>
<tr>
<td>stream</td>
<td>Stream status</td>
</tr>
<tr>
<td>secondaryIndices</td>
<td>Secondary indices</td>
</tr>
<tr>
<td>indexName</td>
<td>Index name</td>
</tr>
<tr>
<td>indexType</td>
<td>Index type</td>
</tr>
<tr>
<td>projectedAttributes</td>
<td>Projected attributes</td>
</tr>
<tr>
<td>targetTableName</td>
<td>Name of the restored table</td>
</tr>
</tbody>
</table>

Example:

```json
"restoreMetadata": {"provisionedWriteCapacityUnits": "0", "autoScaling": "Disabled", "kmsMasterKeyArn": "Not Applicable", "encryptionType": "Default", "provisionedReadCapacityUnits": "0", "secondaryIndices": "[]", "backupArn": "arn:aws:dynamodb:us-east-1:234567890123:table/simcher-loadtest-ScenariosTable-C4B1Q3B9Z2DQ/backup/01616319501023-bc657c53", "sortKey": "-", "stream": "Disabled", "targetTableName": null, "originalTableName": "simcher-loadtest-ScenariosTable-C4B1Q3B9Z2DQ", "backupName": "simcher-loadtest-ScenariosTable-C4B1Q3B9Z2DQ-AwsBackup-2021-03-21T09.15.00Z-D2A6E00C-F3F8-AD99-A47D-8AA26EA38F01", "primaryPartitionKey": "testId"}
```
Restoring an Amazon 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 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, accept the defaults or specify the options for the Encryption and KMS key settings.
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:

```java
String dBInstanceIdentifier;
String engine;
String licenseModel;
String dBInstanceClass;
String availabilityZone;
Boolean multiAZ;
Boolean publiclyAccessible;
String storageType;
Integer port;
Integer iops;
```
Boolean autoMinorVersionUpgrade;
String dBParameterGroupName;
String optionGroupName;
List<String> vpcSecurityGroupIds;
String dBSecurityGroupName;
Boolean enableIAMDatabaseAuthentication;
Boolean deletionProtection;
String dBClusterName;
String tdeCredentialArn;
String domain;
String domainIAMRoleName;
Boolean copyTagsToSnapshot;
List<String> enableCloudwatchLogsExports;
List<ProcessorFeature> processorFeatures;

Example:

"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": false}"

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:]
Example:

```
```

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**

Userdata is not a parameter. It is not protected by the console, CLI, or SDK.

**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**
Restoring an EC2 instance

- 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.

```json
"restoreMetadata": {
  "HibernationOptions": {"Configured":false},
  "InstanceInitiatedShutdownBehavior": "stop",
  "CpuOptions": {"CoreCount":1,"ThreadsPerCore":2},
  "SubnetId": "subnet-b35676f9",
  "SecurityGroupIds": ["sg-09e1b3a3f2f1ec0ba"],
  "EbsOptimized": false,
  "KeyName": "ec2CanaryKeyPair",
  "DisableApiTermination": false,
  "VpcId": "vpc-4853f372",
  "Placement": {"AvailabilityZone": "us-east-1"},
  "GroupName": ",",
  "Tenancy": "default",
  "NetworkInterfaces": [
    {"AssociatePublicIpAddress":true,"DeleteOnTermination":true,"DeviceIndex":0,"Groups": ["sg-09e1b3a3f2f1ec0ba"],
     "Ipv6AddressCount": 0,
     "Ipv6Addresses": [],
     "NetworkInterfaceId": "eni-024f43c22193155e3",
     "PrivateIpAddress": "172.31.24.10",
     "PrivateIpAddresses": ["172.31.24.10"],
     "Primary": true,
     "PrivateIpAddress": "172.31.24.10"},
    {"SecondaryPrivateIpAddressCount": 0,
     "SubnetId": "subnet-b35676f9",
     "InterfaceType": "interface",
     "InstanceType": "t3.nano",
     "CapacityReservationSpecification": "unlimited open",
     "Monitoring": false,"State": "disabled"}
  ]
}
```

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 an AWS Storage Gateway volume**

If you are restoring an AWS Storage Gateway volume snapshot, you can choose to restore the snapshot as an 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 an 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.
   - 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**.
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.
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**.
Restoring a Amazon 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.
5. In the Network & Security pane, accept the defaults or specify the options for the Virtual Private Cloud (VPC), Subnet group, and VPC security groups settings.
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:

  ```bash
  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 Amazon 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 Network & Security pane, accept the defaults or specify the Availability zone.
7. In the Database options pane, accept the defaults or specify the options for Database port and DB cluster parameter group.
8. In the Encryption pane, accept the default or specify the options for the Enable encryption or Disable encryption settings.
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 Restore role pane, choose the IAM role that AWS Backup will assume for this restore.
11. 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.
12. After your restore finishes, attach your restored Neptune cluster to an Amazon RDS instance.

Using the AWS CLI:

- For Linux, macOS, or Unix:

```
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:

```
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
```
Audit backups and create reports with AWS Backup Audit Manager

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. 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. 99)
- Working with audit reports (p. 112)
- Using AWS Backup Audit Manager with AWS CloudFormation (p. 121)
- Using AWS Backup Audit Manager with AWS Audit Manager (p. 126)
- AWS Backup Audit Manager controls and remediation (p. 127)
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.

Topics

- Choosing your controls (p. 99)
- Turning on resource tracking (p. 100)
- Creating frameworks using the AWS Backup console (p. 105)
- Creating frameworks using the AWS Backup API (p. 106)
- Viewing framework compliance status (p. 110)
- Finding non-compliant resources (p. 111)
- Updating audit frameworks (p. 111)
- Deleting audit frameworks (p. 112)

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 protected by 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 minimum frequency and minimum retention</td>
<td>Evaluates if backup frequency is at least [1 day] and retention period is at least [35 days].</td>
<td>Backup frequency; retention period</td>
<td>AWS Backup: backup plans</td>
</tr>
<tr>
<td>Backup prevent recovery point manual deletion</td>
<td>Evaluates if backup vaults do not allow manual deletion of recovery points</td>
<td>Up to 5 IAM roles that allow manual deletion of recovery points</td>
<td>AWS Backup: backup vaults</td>
</tr>
</tbody>
</table>
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.

For detailed information about these controls, see AWS Backup Audit Manager controls and remediation (p. 127).

### Topics
- Turning on resource tracking using the console (p. 100)
- Turning on resource tracking using the AWS Command Line Interface (AWS CLI) (p. 101)
- Turning on resource tracking using a AWS CloudFormation template (p. 105)

### 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.

   ```bash
   # aws configservice describe-configuration-recorders
   ```

   a. If your **ConfigurationRecorders** list is empty like this:

      ```json
      
      {  
        "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:

      ```json
      
      {  
        "ConfigurationRecorders":[  
          
          "recordingGroup":{  
            "allSupported":true,  
            "resourceTypes":[]  
          },
        ]
      }
      ```
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.

2. Create a AWS Config recorder with the AWS Backup Audit Manager resource types

```
# 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.

```
# 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/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",
                "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`.

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:GetBucketAcl",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketExistenceCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:ListBucket",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketDelivery",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

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.

$ 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":{}
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"35"
        },
        {
          "ParameterName":"requiredFrequencyValue",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{}
    },
    {
      "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
      "ControlInputParameters":[
      ],
      "ControlScope":{}
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters":[
      ],
      "ControlScope":{}
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
      "ControlInputParameters":[
      ],
      "ControlScope":{}
    }
  ]
}
```
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. Choose either AWS Backup framework (recommended) or Custom framework, and then choose Create framework.
   - If you choose AWS Backup framework (recommended), AWS Backup Audit Manager creates a framework with all available controls, as described in AWS Backup Audit Manager controls and remediation. After AWS Backup Audit Manager creates the framework, you are finished with this procedure.
   - If you choose Custom framework, you can customize which controls will be part of your framework and the parameters for those controls. The rest of this procedure assumes that you chose Custom framework.
7. Customize your controls. To include or remove each control from your framework, use the slider. The default is to include all controls in your framework with the default parameters that are shown in the brackets ([ ]). The list of AWS Backup Audit Manager controls describes the customization options for each control.
8. (Optional) Tag your framework by choosing Add new tag. You can use tags to search and filter your frameworks or track your costs.

AWS Backup Audit Manager might take several minutes to create the framework.
# Creating frameworks using the AWS Backup API

The following table contains sample API requests to `CreateFramework` (p. 269) for each control, along with sample API responses to the corresponding `DescribeFramework` (p. 307) 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>
</table>
| Backup resources protected by backup plan    | <pre>"FrameworkName": "Control1",
"FrameworkDescription": "This is a test framework",
"FrameworkControls": [
  {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
   "ControlInputParameters": [],
   "ControlScope":
   {"ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances
  }
],
"IdempotencyToken": "Control1",
"FrameworkTags": {"key1": "foo"}</pre> | <pre>{"FrameworkName": "Control1",
"FrameworkArn": "arn:aws:backup:us-east-1:1123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642",
"FrameworkDescription": "This is a test framework",
"FrameworkControls": [
  {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
   "ControlInputParameters": [],
   "ControlScope":
   {"ComplianceResourceTypes": ["RDS"]
  }
],
"CreationTime": 1516925490,
"DeploymentStatus": "Active",
"FrameworkStatus": "Completed",
"IdempotencyToken": "Control1",
"FrameworkTags": {"key1": "foo"}</pre> |
| Backup plan min frequency and retention check | <pre>"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"},
     ];
],
"IdempotencyToken": "Control2",
"FrameworkTags": {}</pre> | <pre>{"FrameworkName": "Control2",
"FrameworkArn": 
"arn:aws:backup:us-east-1:1123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d",
"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"},
     ];
],
"CreationTime": 1516925490,
"DeploymentStatus": "Active",
"FrameworkStatus": "Completed",
"IdempotencyToken": "Control2",
"FrameworkTags": {}</pre> |
### CreateFramework request

```json
{
  "Control": {
    "CreateFramework": {
      "request": {
        "ParameterValue": "35",
        "ParameterValue": "24"
      }
    }
  },
  "ControlScope": {
    "Tags": {
      "key1": "prod"
    } // Evaluate backup plans that tagged with "key1": "prod".
  }
},
"IdempotencyToken": "Control2",
"FrameworkTags": {
  "key1": "foo"
}
```

### DescribeFramework response

```json
{
  "ParameterValue": {
    "ParameterValue": "35",
    "ParameterValue": "24"
  }
},
"ControlScope": {
  "Tags": {
    "key1": "prod"
  }
},
"CreationTime": 1516925490,
"DeploymentStatus": "Active",
"FrameworkStatus": "Completed",
"IdempotencyToken": "Control2",
"FrameworkTags": {
  "key1": "foo"
}
```
<table>
<thead>
<tr>
<th>Control</th>
<th>CreateFramework request</th>
<th>DescribeFramework response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>CreateFramework request</td>
<td>DescribeFramework response</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Backup recovery point minimum retention check</td>
<td><code>{ &quot;FrameworkName&quot;: &quot;Control4&quot;, &quot;FrameworkDescription&quot;: &quot;This is a test framework&quot;, &quot;FrameworkControls&quot;: [ { &quot;ControlName&quot;: &quot;BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK&quot;, &quot;ControlInputParameters&quot;: [ { &quot;ParameterName&quot;: &quot;requiredRetentionDays&quot;, &quot;ParameterValue&quot;: &quot;35&quot; } ], &quot;ControlScope&quot;: {} // Default scope (no scope input) sets scope to all recovery points. } ], &quot;IdempotencyToken&quot;: &quot;Control4&quot;, &quot;FrameworkTags&quot;: { &quot;key1&quot;: &quot;foo&quot; } }</code></td>
<td><code>{ &quot;FrameworkName&quot;: &quot;Control4&quot;, &quot;FrameworkArn&quot;: &quot;arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c1&quot;, &quot;FrameworkDescription&quot;: &quot;This is a test framework&quot;, &quot;FrameworkControls&quot;: [ { &quot;ControlName&quot;: &quot;BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK&quot;, &quot;ControlInputParameters&quot;: [ { &quot;ParameterName&quot;: &quot;requiredRetentionDays&quot;, &quot;ParameterValue&quot;: &quot;35&quot; } ], &quot;ControlScope&quot;: {} }, { &quot;ParameterName&quot;: &quot;requiredRetentionDays&quot;, &quot;ParameterValue&quot;: &quot;35&quot; } ], &quot;ControlScope&quot;: {} }, { &quot;CreationTime&quot;: 1516925490, &quot;DeploymentStatus&quot;: &quot;Active&quot;, &quot;FrameworkStatus&quot;: &quot;Completed&quot;, &quot;IdempotencyToken&quot;: &quot;Control4&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.
- 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 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

AWS Backup Audit Manager delivers a daily report in CSV, JSON, or both formats to your Amazon S3 bucket. 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.

You can have a maximum of 20 report plans per AWS account.

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. 112)
- Creating report plans using the AWS Backup console (p. 117)
- Creating report plans using the AWS Backup API (p. 118)
- Creating on-demand reports (p. 119)
- Viewing audit reports (p. 120)
- Updating report plans (p. 120)
- Deleting report plans (p. 120)

Choosing your report template

A report template defines the information that your report plan includes in your report. AWS Backup Audit Manager 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>
<tbody>
<tr>
<td>BACKUP_JOB_REPORT</td>
<td>{</td>
</tr>
</tbody>
</table>
### 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;2021-07-14T00:00:00Z -</td>
</tr>
<tr>
<td></td>
<td>&quot;2021-07-15T00:00:00Z&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;backupJobId&quot;: &quot;FCCB040A-9426-2A49-2EA9-5EAFFAC656AC&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;jobStatus&quot;: &quot;COMPLETED&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-0bc877aee7782ba75&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupRuleId&quot;: &quot;ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcb&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;creationDate&quot;: &quot;2021-07-14T23:53:47.229Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;completionDate&quot;: &quot;2021-07-15T00:16:07.282Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;recoveryPointArn&quot;: &quot;arn:aws:ec2:us-west-2::image/ami-030caf9b9e5a6dcd&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;jobRunTime&quot;: &quot;00:22:20&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupSizeInBytes&quot;: 8589934592,</td>
</tr>
<tr>
<td></td>
<td>&quot;backupVaultName&quot;: &quot;Default&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  Sample report in JSON format

COPY_JOB_REPORT

```json
{
  "reportItems": [
    {
      "accountId": "112233445566",
      "region": "us-west-2",
      "copyJobId": "E0AD48A9-0560-B668-3EFO-941FDC0AD6B1",
      "jobStatus": "RUNNING",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877ae6f7e72ba75",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",
      "creationDate": "2021-07-15T15:42:04.771Z",
      "backupSizeInBytes": 8589934592,
      "sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-007b3819f225697299",
      "destinationRecoveryPointArn": "arn:aws:ec2:us-east-2::image/ami-0eba2199a0bece3c",
      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
    }
  ]
}
```
Choosing your report template

Backup report template

**RESTORE_JOB_REPORT**

```json
{
    "reportItems": [
        {
            "accountId": "11223445566",
            "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::11223445566: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></td>
</tr>
</tbody>
</table>

```json
{
    "reportItems": [
        {
            "accountId": "11223445566",
            "region": "me-south-1",
            "frameworkName": "TestFramework7",
            "frameworkDescription": "A test framework",
            "controlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
            "percentDone": "0.00%",
            "frameworkDescription": "A test framework",
            "frameworkName": "TestFramework7",
            "controlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN"
        }
    ]
}
```
<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;2021-08-17T03:21:56.002Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;numResourcesCompliant&quot;: 91, &quot;numResourcesNonCompliant&quot;: 205, &quot;controlFrequency&quot;: &quot;Twelve_Hours&quot;,</td>
</tr>
<tr>
<td></td>
<td>&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;11223445566&quot;, &quot;region&quot;: &quot;me-south-1&quot;, &quot;frameworkName&quot;: &quot;TestFramework7&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;frameworkDescription&quot;: &quot;A test framework&quot;, &quot;controlName&quot;: &quot;BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;controlComplianceStatus&quot;: &quot;NON_COMPLIANT&quot;, &quot;lastEvaluationTime&quot;: &quot;2021-08-17T03:21:19.995Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;numResourcesCompliant&quot;: 0, &quot;numResourcesNonCompliant&quot;: 25, &quot;controlScope&quot;: &quot;{(ComplianceResourceTypes: []),}&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;controlParameters&quot;: &quot;{&quot;requiredFrequencyValue&quot;:&quot;1&quot;, &quot;requiredRetentionDays&quot;:&quot;35&quot;, &quot;requiredFrequencyUnit&quot;:&quot;hours&quot;}&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
Creating report plans using the AWS Backup console

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 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. Choose the File format of your report. You can choose CSV (default), JSON, or both to receive your report in both formats.

10. Choose your S3 bucket name using the dropdown list.

11. (Optional) Enter a bucket prefix. AWS Backup delivers your reports to s3://your-bucket-name/prefix/Backup/us-west-2/year/month/day/report-name.

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.

**To view and apply this access policy to your S3 bucket**

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. 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**

```
{
    "Version":"2012-10-17",
    "Statement":[
    {
        "Effect":"Allow",
        "Principal":{
            "AWS":"arn:aws:iam::11111111: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. Use the following syntax to call CreateReportPlan (p. 273).
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.

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.

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, select the report you want to view by choosing its Completion time.
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.

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. 105)
- Deploy default controls (p. 125)
- Exempt IAM roles from control evaluation (p. 125)
- Create a report plan (p. 126)

**Turn on resource tracking**

The following template turns on resource tracking as described in Turning on resource tracking.

```yaml
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config
Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
    - Label: default: Recorder Configuration
      Parameters:
      - AllSupported
      - IncludeGlobalResourceTypes
      - ResourceTypes
    - Label: 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
```
Turn on resource tracking

### Description
Indicates whether to record all supported resource types.

**AllowedValues:**
- True
- False

### IncludedGlobalResourceTypes
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:
1 hour : One_Hour
3 hours : Three_Hours
6 hours : Six_Hours
12 hours : Twelve_Hours
24 hours : 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
        Action: s3:PutObject
        Resource:
          - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/${AWS::AccountId}/*"
      - Sid: AWSConfigBucketSecureTransport
        Effect: Deny
        Resource:
          - !Sub "arn:${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

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

ConfigRecorder:
  Type: AWS::Config::ConfigurationRecorder
  DependsOn:
    - ConfigBucketPolicy
  Properties:
    RoleARN: !GetAtt ConfigRecorderRole.Arn
    RecordingGroup:
      AllSupported: !Ref AllSupported
      IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
    ResourceTypes: !If
    - IsAllSupported
    - !Ref AWS::NoValue
    - !Ref ResourceTypes

ConfigDeliveryChannel:
  Type: AWS::Config::DeliveryChannel
  DependsOn:
    - ConfigBucketPolicy
  Properties:
    Name: !If
    - IsGeneratedDeliveryChannelName
      - !Ref AWS::NoValue
      - !Ref DeliveryChannelName
    ConfigSnapshotDeliveryProperties:
      DeliveryFrequency: !FindInMap
      - Settings
      - FrequencyMap
      - !Ref Frequency
    S3BucketName: !Ref ConfigBucket
SnsTopicARN: !If
  - CreateTopic
  - !Ref ConfigTopic
  - !Ref TopicArn

## Deploy default controls

The following template creates a framework with the first five 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: requiredRetentionDays
            ParameterValue: '35'
          - ParameterName: requiredFrequencyUnit
            ParameterValue: 'hours'
          - ParameterName: requiredFrequencyValue
            ParameterValue: '24'
      - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.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_RECOVERYPOINT_MANUALDELETIONDISABLED
        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.

```
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
  ReportPlanTags:
    - Key: "a"
      Value: "1"
    - Key: "b"
      Value: "2"

Outputs:
  ReportPlanArn:
```

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 Compliance checks for resource configurations from 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 programmatically 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 specify a Tagged resources scope with a single tag key and optional value.
  - You can specify Resources by type by choosing one or more AWS Backup-supported services.
  - You can specify an individual resource using the Individual resources dropdown list.
- Remediation steps to bring applicable resources into compliance.

Backup resources protected by backup plan

Description: Evaluates if resources are protected by a backup plan.

Resource: AWS Backup: backup selection

Parameters: None

Scope:

- All resources (default)
- Tagged resources
- Resources by type
- Individual resources

Note

This control does not support Storage Gateway resources, regardless of scope.

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:

- All resources (default)
- Tagged resources
- Individual resources

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.

Backup prevent recovery point manual deletion

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:

- All resources (default)
- Tagged resources
- Individual resources

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.

Backup recovery point encrypted

Description: Evaluates if recovery points are encrypted.

Resource: AWS Backup: recovery points

Parameters: None

Scope:

- All resources (default)
- 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.

Backup recovery point minimum retention

**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:**
- All resources (default)
- Tagged resources

**Remediation:** Change the retention periods of your recovery points. For more information, see Editing a backup.
Managing AWS Backup resources across multiple AWS accounts

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. AWS Organizations quotas apply.

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. 135) 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.

The cross-account management feature is not available in the following AWS Regions: AWS GovCloud (US), China Regions, Middle East (Bahrain) Region, and Asia Pacific (Hong Kong) Region.

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.

**Topics**
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.

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.
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. 67).
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": "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"]
}
}
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*](#).

**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](#).
Using AWS CloudFormation to provision AWS Backup resources

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. 147).

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. 45).

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. 138)
- Identity and access management in AWS Backup (p. 142)
- Compliance validation for AWS Backup (p. 215)
- Resilience in AWS Backup (p. 215)
- Infrastructure security in AWS Backup (p. 216)

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

The way to configure encryption differs depending on the resource type. Certain resource types support the ability to encrypt your backups using a separate encryption key from the key used to encrypt the source resource. This capability adds another layer of protection for your backups.

The following table lists each supported resource type, how encryption is configured for backups, and whether independent encryption for backups is supported.

<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 DynamoDB after enabling Advanced DynamoDB backup (p. 63)</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>Not supported</td>
</tr>
<tr>
<td>Amazon DynamoDB without enabling Advanced DynamoDB backup (p. 63)</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.</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

**Note**
In order for AWS Backup to create a backup of an encrypted DynamoDB table, you must add the permissions `kms:Decrypt` and `kms:GenerateDataKey`. 
<table>
<thead>
<tr>
<th>Resource type</th>
<th>How to configure encryption</th>
<th>Independent AWS Backup encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon Elastic File System (Amazon EFS)</strong></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><strong>Amazon Elastic Block Store (Amazon EBS)</strong></td>
<td>Amazon EBS snapshots are automatically encrypted with the same encryption key that was used to encrypt the source EBS volume. Snapshots of unencrypted EBS volumes are also unencrypted.</td>
<td>Not supported</td>
</tr>
<tr>
<td><strong>Amazon Elastic Compute Cloud (Amazon EC2) AMIs</strong></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>
</tbody>
</table>
| **Amazon Relational Database Service (Amazon RDS)**| 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.  
**Note**  
AWS Backup currently supports all Amazon RDS database engines, including Amazon Aurora. | Not supported                      |
| **Amazon Aurora**                                 | 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.          | Not supported                      |
Encryption for backups in AWS Backup

<table>
<thead>
<tr>
<th>Resource type</th>
<th>How to configure encryption</th>
<th>Independent AWS Backup encryption</th>
</tr>
</thead>
<tbody>
<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></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></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>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>

**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.
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, to give you additional access controls to your backups, recovery points for some AWS Backup-supported services cannot be deleted using the source service when they support full AWS Backup management, as listed in the Feature availability by resource (p. 2) table. 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 can no 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. 142)
- Access control (p. 143)
- IAM service roles (p. 147)
- Managed policies for AWS Backup (p. 148)
- Using service-linked roles for AWS Backup (p. 210)
- Cross-service confused deputy prevention (p. 214)

**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. 144)
- Resource ownership (p. 144)
- Specifying policy elements: actions, effects, and principals (p. 145)
- Specifying conditions in a policy (p. 145)
- API permissions: actions, resources, and conditions reference (p. 145)
- Copy tags permissions (p. 146)
- Access policies (p. 147)
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 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 want 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 examples of resources, subresources, and ARN formats.

**AWS Backup resource ARNs**

<table>
<thead>
<tr>
<th>Resource type</th>
<th>ARN format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup vault</td>
<td>arn:aws:backup:region:account-id:backup-vault:*</td>
</tr>
<tr>
<td>Recovery point for Amazon EBS</td>
<td>arn:aws:ec2:region::snapshot/*</td>
</tr>
<tr>
<td>Recovery point for Amazon EFS</td>
<td>arn:aws:backup:region:account-id:recovery-point:*</td>
</tr>
<tr>
<td>Recovery point for Amazon RDS</td>
<td>arn:aws:rds:region:account-id:snapshot:awsbackup:*</td>
</tr>
<tr>
<td>Recovery point for Amazon Aurora</td>
<td>arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*</td>
</tr>
<tr>
<td>Recovery point for Storage Gateway</td>
<td>arn:aws:ec2:region::snapshot/*</td>
</tr>
<tr>
<td>Recovery point for DynamoDB without Advanced DynamoDB backup (p. 63)</td>
<td>arn:aws:dynamodb:region:account-id:table/<em>/backup/</em></td>
</tr>
<tr>
<td>Recovery point for DynamoDB with Advanced DynamoDB backup (p. 63) enabled</td>
<td>arn:aws:backup:region:account-id:recovery-point:12a34a56-7bb8-901c-cd23-4567d8e9ef01</td>
</tr>
</tbody>
</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. 257).

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 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. 144)), the service defines a set of API operations (see Actions (p. 257)). 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. 144).
• 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. 145).

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. 143) 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
Access control

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.

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.
- 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 supports assigning tags to backups after you enable Advanced DynamoDB backup (p. 63).

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. 148).

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 Setting access policies on backup vaults (p. 50).

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. 148).

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
You must create the default role using the AWS Management Console. You cannot create the default role using the AWS Command Line Interface (AWS CLI).

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 table at the end of Managed Policies.

The default service role created by AWS Backup manages creating and restoring backups. It has two managed policies, AWSBackupServiceRolePolicyForBackup and AWSBackupServiceRolePolicyForRestores.

To restore an Amazon EC2 instance, you must launch a new instance. To do so, you must manually include "Action":"iam:PassRole" in your role.

AWS Backup default service role for backups

This role includes an IAM policy that grants AWS Backup permissions to describe the resource being backed up, the ability to create, delete, or describe a backup, and the ability to add tags to the backup. This IAM policy includes the necessary permissions for all the resource types that AWS Backup supports.

AWS Backup Default service role for restores

This role includes an IAM policy that grants AWS Backup permissions to create, delete, or describe the new resource being created from a backup. 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.

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.
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 services. 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 services

<table>
<thead>
<tr>
<th>Service</th>
<th>Backup policy</th>
<th>Restore policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>DynamoDB</td>
<td>Backup Policy (with or without Advanced DynamoDB backup (p. 63))</td>
<td>Restore Policy (with or without Advanced DynamoDB backup (p. 63))</td>
</tr>
</tbody>
</table>

```json
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:RestoreTableFromAwsBackup"
      ]
    }
  ]
}
```
Service

وبة

backup

policy

"dynamodb:DescribeBackup",

"dynamodb:DescribeTable",

"dynamodb:CreateBackup",

"Resource":"arn:aws:dynamodb:*:*:table/*",

"Effect":"Allow",

"dynamodb:Scan",

"dynamodb:UpdateItem",

"dynamodb:PutItem",

"tag:GetResources"
Service
backup
policy

"Resource": "*",
"dynamodb:DeleteItem",

"Effect": "Allow"

dynamodb:BatchWriteItem

[
]

"Action":
[
"Resource": "arn:aws:dynamodb:*:*:table/*",

dynamodb:RestoreTableFromBackup",

],

dynamodb:DeleteBackup

"Action":
[
"Resource": "arn:aws:dynamodb:*:*:table/*",

dynamodb:RestoreTableFromBackup",

]
Service
backup
policy

"Effect":"Allow"
"dynamodb:DeleteBackup"
,
,

"dynamodb:DeleteBackup"

"Action":
[

"Effect":"Allow"

}
{
backup:DescribeBackupVault",
}

"backup:CopyIntoBackupVault"

],

"Resource":"arn:aws:backup:*:*:backup-vault:*"
Service backup policy

Amazon EBS Backup Policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "ec2:CreateVolume",
    },
    {
      "ec2:DeleteVolume"
      "Effect": "Allow",
    },
    "Action": [
      "Resource": []
    ]
  ]
}

Amazon EBS Restore Policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource": []
    }
  ]
}

Service

Policy

"ec2:CreateSnapshot",
"arn:aws:ec2:*::snapshot/*",

"ec2:DeleteSnapshot"

"arn:aws:ec2:*:*:volume/*",


"Resource":
[
},

{

"arn:aws:ec2:*::snapshot/*",

"Effect":"Allow",

"ArnName":ec2:*::volume/*

}

"ec2:DescribeSnapshots",
},

{

"ec2:DescribeVolumes"
Service

backup

policy

"Effect":"Allow",

"Action":
["ec2:DescribeVolumes",
"ec2:DescribeSnapshots",
"ec2:CopySnapshot",
"ec2:DescribeTags",
"Resource":""]
}
Service backup policy

"Action": [
    "tag:GetResources",
],

"Resource": "*",

"Effect": "Allow",

"Action": [
    "tag:GetResources",
],

"Resource": "*",

"Effect": "Allow",

"Action": ["tag:GetResources"]
Service
backup policy

"backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"

"Resource":"arn:aws:backup:*::*:backup-vault:*"

}]
}
}
Service back up policy

Amazon EFS Backup Policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
    }
  ]
}

Amazon EFS Restore Policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["elasticfilesystem:Restore", "elasticfilesystem:CreateFilesystem", "elasticfilesystem:DescribeFilesystems"]
    }
  ]
}
Service backup policy

{
,

{

"Resource":"arn:aws:elasticfilesystem:::file-system/*"

}

}

"tag:GetResources"

,

"Resource":"*",

"Effect":"Allow"

,

{

"Effect":"Allow",

"Action":

[
Managed policies

Service

backup policy

"backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"

"Resource":"arn:aws:backup:*:*:backup-vault:*"
AWS Backup Developer Guide
Managed policies

Service backup policy
Amazon RDS Backup Policy

{"Version":"2012-10-17",
 "Statement": [

 {
 "Effect":"Allow",
 "Action": [

 "rds:AddTagsToResource",

 "rds:DescribeDBSnapshots",

 "rds:CreateDBSnapshot",

 "rds:DescribeDBInstances",

 "rds:DescribeDBSnapshots",

 "rds:ListTagsForResource",

 "rds:RestoreDBInstanceFromDBSnapshot",

 "rds:RestoreDBInstanceFromDBSnapshotFromDBSnapshot",

 "rds:RestoreDBInstanceFromDBSnapshotFromDBSnapshot"
 ]
 ]
}
Service
backup
policy

"rds:CreateDBClusterSnapshot",

"rds:DeleteDBInstance",

"rds:AddTagsToResource",

"rds::DescribeDBInstances",

"rds::CreateDBClusterSnapshot",

"rds::DescribeDBClusters",

"rds::DescribeDBClusterSnapshots",

"rds::CopyDBClusterSnapshot"

"Resource":**

}
Service backup policy

"Effect": "Allow",

"Action": [ "rds:DeleteDBSnapshot",
            "rds:ModifyDBSnapshotAttribute"
          ],

"Resource": [ "arn:aws:rds:*:*:snapshot:awsbackup:*" ]

Service
backup
policy

"Effect":
"Allow",

"Action":
[
"rds:DeleteDBClusterSnapshot",

"rds:ModifyDBClusterSnapshotAttribute"
],

"Resource":
[

"arn:aws:rds:*:*:cluster-
snapshot:awsbackup:*"]

},

},

{

"Action":
[

"tag:GetResources"
Service backup policy

},

"Resource":"*",

"Effect":"Allow"

},

{

"Effect":"Allow",

"Action": ["backup:DescribeBackupVault",

"backup:CopyIntoBackupVault"

],}
Service
backup
policy

"Resource":"arn:aws:backup:*::*:backup-vault:*"

,

{

"Action":"kms:DescribeKey",

"Effect":"Allow",

"Resource":"

}

]}
}
Service
backup
policy
Amazon
Aurora
Backup
Policy

{
"Version":"2012-10-17",
"Statement":
[

{
"Effect":"Allow",

"Action":
[
"rds:DeleteDBClusterSnapshot",

"rds:DescribeDBClusters",

"rds:DescribeDBClusterSnapshots",

"rds:AddTagsToResource",

"rds:DeleteDBCluster",

"rds:RestoreDBClusterFromSnapshot",

"rds:ListTagsForResource",

"rds:AddTagsToResource"
]
}
}
Service
backup
policy

"rds:AddTagsToResource",

],
"rds:CopyDBClusterSnapshot"

"Resource":"*

],
}
}
}  
"Resource":"*

],
}
}

"Effect":"Allow",

"Action":
[

"rds:DeleteDBClusterSnapshot"
Service
backup policy

},

"resource":

[{

 "arn:aws:rds:*:*:cluster-snapshot:awsbackup::*

}]

},

{

 "action":

 ["tag:GetResources"

 }],

 "resource":"

}
```json
{
    "Effect": "Allow",
    "Action": [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
    ],
    "Resource": "arn:aws:backup::backup-vault::*"
}
```
Managed policies

```json
Service backup policy

{

"Action":"kms:DescribeKey",

"Effect":"Allow",

"Resource":"**"

}

}

}
Service
backup policy

Storage Gateway Backup Policy

{
  "Version":"2012-10-17",
  "Statement":
  [
    {
      "Effect":"Allow",
      "Action":
      [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource":"arn:aws:storagegateway:*:*:gateway/*
      volume/*
    }
  ],
  "storagegateway:DeleteVolume",
  "storagegateway:DescribeCachediSCSIVolumes",
  "storagegateway:DescribeCachediSCSIVolumes"
},
"storagegateway:DescribeCachediSCSIVolumes"

"Resource":"arn:aws:storagegateway:*:*:gateway/*
  volume/*"
Service

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"

}
Managed policies

Service backup policy

"Resource": "*",

"Effect": "Allow",

"Action": [
  "backup:DescribeBackupVault",
  "backup:CopyIntoBackupVault"
],

"Resource": "arn:aws:backup::*:backup-vault:*"
Service backup policy
Service
backup
policy
Amazon
FSx
Backup
Policy

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:*:backup/"
        },
        {
            "Action": "fsx:CreateFileSystemFromBackup"
        }
    ]
}

"Action": "EffectCreateBackup",
"Allow",

"Effect": "Deny"
**Service backup policy**

```json
"Resource": [

"arn:aws:fsx:*:*:filesystem/*",

"arn:aws:fsx:*:*:backup/*",

"arn:aws:fsx:*:*:backup/*"
]
]
],

{

"Action": "fsx:DescribeFileSystems",
"Action": "fsx:DescribeFileSystems",

"Effect": "Allow",
"Effect": "Allow",

"Resource": "arn:aws:fsx:*:*:filesystem/"
```
Service
backup
policy

"Source":
"arn:aws:fsx:*:*:file-system/
**
",
",
{

{
"Action":
"fsx:ListTagsForResource",

"Action":
"fsx:DescribeBackups",
"Effect":
"Allow",

"Effect":
"Allow",
"Resource":
"arn:aws:fsx:*:*:file-system/
**

"Resource":
"arn:aws:fsx:*:*:backup/
**

",

{
"Action":
"fsx:DeleteBackup",

"Effect":
"Allow",

["Resource":
"arn:aws:fsx:*:*:backup/*"]}]}
**Service backup policy**

```json
"arn:aws:fsx:*:*:backup/*"

,"fsx:DeleteFileSystem",
{

"Effect":
"Allow",

"fsx:ListTagsForResource",

"Resource":
"arn:aws:fsx:*:*:file-system/*",

"fsx:ManageBackupPrincipalAssociations",

"Condition":

"fsx:CopyBackup",

{"null":

"fsx:TagResource"

"Null":
```
Service

backup

policy

]

{

"Resource":
"arn:aws:fsx:*:*:backup/
**

}aws:ResourceTag/
aws:backup:source-
#source":
"false"

}

}

}

{

"Action":
"ds:DescribeDirectories",

"Effect":
"Allow",}
Service
backup
policy

"Resource":
  "*

}
Service backup policy

Amazon EC2 Backup Policy

Service

Managed policies

},

"arn:aws:ec2::*:snapshot/
*t,

"Effect":"Allow",
"arn:aws:ec2::*:volume/
*",

"Action":
[
]
},
"ec2:CreateImage",
{

"Effect":"

c2:DeregisterImage"

"Action":
[

"Resource":"

"ec2:DescribeSnapshots",
},

{

"ec2:DescribeVolumes"

"Effect":"

"Service

backup

policy
Service
backups
policy

"Action":
[

"Resource":"*"
],
"ec2:CopyImage",

"ec2:CopySnapshot"
"Effect":"Allow",

"Action":
[

"Resource":"*"
],
"ec2:DescribeImages",

"ec2:DescribeInstances"
"Effect":"Allow",

"Action":
[

"Resource":"*"
]
Service
backup
policy

},
"ec2:CreateTags"

{

},

"Action":
[
"Resource":"arn:aws:ec2::*:*:image/*"
}
"ec2:RunInstances"

{

},

"Effect":"Allow",

"Action":
[
"Resource":"
},
"ec2:DescribeSnapshots",

{

"Action":
["ec2:DescribeTags",

["ec2:DescribeImages",

"Action":
["ec2:CreateTags"
Service
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":**
Service
backup
policy

},

{

"Effect": "Allow",

"Action": [

"ec2:CreateSnapshot",

"ec2:DeleteSnapshot",

"ec2:DescribeVolumes",

"ec2:DescribeSnapshots"

],

}
Service backup policy

"Resource": [
  
  "arn:aws:ec2:*::snapshot/**",

  "arn:aws:ec2:*:*:volume/**"
]

},

{

  "Action": [

  "tag:GetResources"
  

  ]
  

  },

  

  }
Service
backup
policy

"Resource": "*",

"Effect": "Allow",

"Action": [
  "backup:DescribeBackupVault",
  "backup:CopyIntoBackupVault"
],

"Resource": "arn:aws:backup:*:*:backup-vault:*"
Service backup policy


Service backup policy

Windows VSS (Volume Shadow Copy Service) Backup Policy

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ]
    }
  ]
}
Service
backup
policy

"Resource": "arn:aws:ec2:*::snapshot/*",

"Effect": "Allow",

"Action": [
    "ec2:CreateImage",
    "ec2:DeregisterImage"
],

"Resource": "*"
"Effect":"Allow",

"Action": [ "ec2:CopyImage", "ec2:CopySnapshot" ],

"Resource":"*",

{ "Effect":"Allow",

"Action": [ ] }
Managed policies

Service backup policy

"ec2:CreateTags"

"Resource":"arn:aws:ec2:*::*:image/ *"

"Effect":"Allow",

"Action":
[
"ec2:DescribeSnapshots",
"ec2:DescribeTags",
]
Service
backup
policy

"ec2:DescribeImages",

"ec2:DescribeInstances",

"ec2:Describe InstanceAttribute",

"ec2:DescribeInstanceCreditSpecifications",

"ec2:DescribeNetworkInterfaces",

"ec2:DescribeElasticGpus",

"ec2:DescribeSpotInstanceRequests"
Service backup policy

"Resource":"**"

},

{

"Effect":"Allow",

"Action": [

"ec2:CreateSnapshot",

"ec2:DeleteSnapshot",

"ec2:DescribeVolumes",

"ec2:DescribeSnapshots"
]
Service
    backup
    policy

},

"Resource":
[

  "arn:aws:ec2:*::snapshot/ **",

  "arn:aws:ec2:*:*:volume/ **

]

},

{

"Action":
[

  "tag:GetResources"

]
Service
backup
policy

"Resource": "*",

"Effect": "Allow",

"Action": [
"backup:DescribeBackupVault",
"backup:CopyIntoBackupVault"
],
Service backup policy

"Resource": "arn:aws:backup:*::*:backup-vault:*"

},

{

"Effect": "Allow",

"Action": [

"ssm:CancelCommand",

"ssm:GetCommandInvocation"

],

"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
• Attach this policy to your IAM role for restores:

```
{
    "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>Backup Audit IAM Policy</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 AWSBackupServiceRoleForBackupReports</td>
</tr>
</tbody>
</table>
## Managed policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>IAM-managed policy name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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><strong>AWSBackupFullAccess</strong></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></td>
<td>(AWSBackupAdminPolicy is deprecated)</td>
<td></td>
</tr>
<tr>
<td>Backup Operator IAM Policy</td>
<td><strong>AWSBackupOperatorAccess</strong></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></td>
<td>(AWSBackupOperatorPolicy is deprecated)</td>
<td></td>
</tr>
</tbody>
</table>
AWS Backup Developer Guide
Managed policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>IAM-managed policy name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Administrator AWS</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>Organizations Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Service Role Policy for</td>
<td>AWSBackupServiceRolePolicyForBackups</td>
<td>Provides AWS Backup permissions to create backups of all supported resource types on your behalf.</td>
</tr>
<tr>
<td>Backups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Service Role Policy for</td>
<td>AWSBackupServiceRolePolicyForRestores</td>
<td>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:</td>
</tr>
<tr>
<td>Restores</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Policy updates for AWS Backup

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies.

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>AWSBackupServiceLinkedRolePolicyForserviceName</td>
<td>Added permission to back up Amazon DynamoDB tables</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td>AWSBackupServiceRolePolicyForserviceName</td>
<td>Added permissions to back up Amazon DynamoDB tables</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td>AWSBackupServiceLinkedRolePolicyForserviceName</td>
<td>Added permissions to restore Amazon DynamoDB tables</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>AWSBackupOperatorAccess — Removed redundant actions</td>
<td>AWS Backup removed the existing actions <code>backup:GetRecoveryPointRestoreMetadata</code> and <code>rds:DescribeDBSnapshots</code> because they were redundant. AWS Backup did not need both <code>backup:GetRecoveryPointRestoreMetadata</code> and <code>backup:Get*</code> as part of the AWSBackupOperatorAccess AWS Managed Policy. Also, AWS Backup did not need both <code>rds:DescribeDBSnapshots</code> and <code>rds:describeDBSnapshots</code> as part of the AWSBackupOperatorAccess AWS Managed Policy.</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td>AWSBackupServiceLinkedRolePolicyForBackup — Added permissions to support fine-grained resource assignments to backup plans</td>
<td>AWS Backup added the new actions <code>elasticfilesystem:DescribeFileSystems</code>, <code>dynamodb:ListTables</code>, <code>storagegateway:ListVolumes</code>, <code>ec2:DescribeVolumes</code>, <code>ec2:DescribeInstances</code>, <code>rds:DescribeDBInstances</code>, <code>rds:DescribeDBClusters</code>, and <code>fsx:DescribeFileSystems</code> 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>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>AWSBackupAuditAccess</strong> —</td>
<td>AWS Backup added <strong>AWSBackupAuditAccess</strong> to grant the user permissions to use AWS Backup Audit Manager. Permissions include the ability to configure compliance frameworks and generate reports.</td>
<td>August 24, 2021</td>
</tr>
<tr>
<td>Added new policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AWSServiceRolePolicyForBackupReports</strong> —</td>
<td>AWS Backup added <strong>AWSServiceRolePolicyForBackupReports</strong> 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.</td>
<td>August 24, 2021</td>
</tr>
<tr>
<td>Added new policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AWSBackupFullAccess</strong> —</td>
<td>AWS Backup added <strong>iam:CreateServiceLinkedRole</strong> 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.</td>
<td>July 5, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>AWSBackupServiceLinkedRolePolicy</td>
<td>AWS Backup added the new action <code>dynamodb:DeleteBackup</code> to grant <code>DeleteRecoveryPoint</code> 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 <code>DeleteRecoveryPoint</code> API operation.</td>
<td>July 5, 2021</td>
</tr>
<tr>
<td>AWSBackupOperatorAccess</td>
<td>AWS Backup removed the existing actions <code>backup:GetRecoveryPointRestoreMetadata</code> and <code>rds:DescribeDBSnapshots</code> because they were redundant. AWS Backup did not need both <code>backup:GetRecoveryPointRestoreMetadata</code> and <code>backup:Get*</code> as part of the <code>AWSBackupOperatorAccess</code> AWS Managed Policy. Also, AWS Backup did not need both <code>rds:DescribeDBSnapshots</code> and <code>rds:describeDBSnapshots</code> as part of the <code>AWSBackupOperatorAccess</code> AWS Managed Policy.</td>
<td>May 25, 2021</td>
</tr>
<tr>
<td>AWSBackupOperatorPolicy</td>
<td>AWS Backup removed the existing actions <code>backup:GetRecoveryPointRestoreMetadata</code> and <code>rds:DescribeDBSnapshots</code> because they were redundant. AWS Backup did not need both <code>backup:GetRecoveryPointRestoreMetadata</code> and <code>backup:Get*</code> as part of the <code>AWSBackupOperatorPolicy</code> AWS Managed Policy. Also, AWS Backup did not need both <code>rds:DescribeDBSnapshots</code> and <code>rds:describeDBSnapshots</code> as part of the <code>AWSBackupOperatorPolicy</code> AWS Managed Policy.</td>
<td>May 25, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| **AWSBackupServiceRolePolicyForRestores**   | 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. | **May 24, 2021** |
| **AWSBackupServiceRolePolicyForRestores**   | 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. | **May 24, 2021** |
| **AWSBackupServiceRolePolicyForBackup**     | 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. | **April 12, 2021** |
| **AWSBackupServiceLinkedRolePolicyForBackup** | 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. | **April 12, 2021** |
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. 211)
- Using roles for AWS Backup Audit Manager (p. 212)
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 AWSServiceLinkedRolePolicyForBackup 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:

   ```bash
   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 AWSBackupServiceLinkedRolePolicyForBackup 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.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the calling service) calls another service (the called service). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions that AWS Backup gives another service to the resource. If
you use both global condition context keys, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

The value of `aws:SourceArn` must be a AWS Backup vault when using AWS Backup to publish Amazon SNS topics on your behalf.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcards (*) for the unknown portions of the ARN. For example, `arn:aws:servicename::123456789012:*`.

The following example policy shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in AWS Backup to prevent the confused deputy problem: Specifying AWS Backup as a service principal (p. 253).

### 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.
- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.
- **AWS Config** – This AWS service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

### 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) 1.0 or later. We recommend 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 Backup quotas

Following are the resource quotas that apply when working with AWS Backup.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of backup vaults per Region per account</td>
<td>100</td>
</tr>
<tr>
<td>Number of concurrent backup copies (per service) to a destination Region per account</td>
<td>5*</td>
</tr>
<tr>
<td>Number of backup plans per Region per account</td>
<td>100</td>
</tr>
<tr>
<td>Number of versions per backup plan</td>
<td>2,000</td>
</tr>
<tr>
<td>Number of active backup jobs per account</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Number of concurrent backup jobs per resource**</td>
<td>1</td>
</tr>
<tr>
<td>Number of metadata tags per saved resource</td>
<td>50</td>
</tr>
<tr>
<td>Number of recovery points per backup vault</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Number of frameworks per account per Region</td>
<td>10</td>
</tr>
<tr>
<td>Number of controls per account per Region</td>
<td>50</td>
</tr>
<tr>
<td>Number of report plans per account</td>
<td>20</td>
</tr>
<tr>
<td>Number of frameworks per report plan</td>
<td>1,000</td>
</tr>
</tbody>
</table>

*AWS Backup supports up to 100 concurrent backup copies of Amazon EC2 Amazon Machine Images (AMIs) to a destination AWS Region per account.

**The quota of one concurrent backup job per resource cannot be increased. This quota helps you maintain the performance of your workloads.

If you need an AWS Backup quota adjusted for a specific use case, you can ask if this is possible by contacting AWS Support.

AWS Backup allows you to assign an unlimited number of resources to a backup plan using tags. You can assign up to 100 unique resources to a backup plan using Amazon Resource Names (ARNs).

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.

**Note**
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
• Storage Gateway
• Amazon DynamoDB
• Amazon FSx for Lustre
• Amazon FSx for Windows File Server
• Amazon DocumentDB
• Amazon Neptune
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. 219) and Monitoring AWS Backup metrics with CloudWatch (p. 241).

- 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. 243).

- 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 Using Amazon SNS to track AWS Backup events (p. 249).

Monitoring AWS Backup events using EventBridge

**Topics**

- Monitor events using EventBridge (p. 219)
- Differences with the AWS Backup notification API (p. 240)

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, COMPLETED, FAILED,</td>
<td>accountId, resources: recoveryPointArn, details, backupJobId, backupSizeInBytes, backupVaultName, backupVaultArn, bytesTransferred, completionDate, expectedCompletionDate, iAmRoleArn, percentDone, EXPIRED, RUNNING, PENDING</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>Backup Job State Change</td>
<td>CREATED</td>
<td>accountld, resources: recoveryPointArn, details, backupJobId, state, creationDate</td>
</tr>
<tr>
<td>Copy Job State Change</td>
<td>COMPLETED, FAILED, RUNNING</td>
<td>accountld, resources: recoveryPointArn, details, backupSizeInBytes, completionDate, copyJobId, creationDate, destinationBackupVaultArn, destinationRestorationPointArn, iAmRoleArn, resourceArn, resourceType, state, statusMessage</td>
</tr>
<tr>
<td>Copy Job State Change</td>
<td>CREATED</td>
<td>accountld, resources: recoveryPointArn, details, state, creationDate, destinationBackupVaultArn</td>
</tr>
<tr>
<td>Restore Job State Change</td>
<td>CREATED, COMPLETED, FAILED, PENDING, RUNNING</td>
<td>accountld, resources: recoveryPointArn, details, state, creationDate, restoreJobId</td>
</tr>
<tr>
<td>Recovery Point State Change</td>
<td>COMPLETED, PARTIAL, EXPIRED</td>
<td>accountld, 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</td>
</tr>
</tbody>
</table>

**Monitor events using EventBridge**
Monitor events using EventBridge

<table>
<thead>
<tr>
<th>Event type</th>
<th>States</th>
<th>Event details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Job State Change</td>
<td>CREATED</td>
<td>accountId, resources: recoveryPointArn, details, state, creationDate, restoreJobId</td>
</tr>
<tr>
<td>Recovery Point State Change</td>
<td>FAILED, COMPLETED, RUNNING, ABORTED, PENDING</td>
<td>accountId, resources: recoveryPointArn, details, backupSizeInBytes, completionDate, createdResourceArn, creationDate, expectedCompletionTimeMinutes, iAmRoleArn, percentDone, restoreJobId, status, statusMessage</td>
</tr>
<tr>
<td>Recovery Point State Change</td>
<td>MODIFIED, DELETED</td>
<td>accountId, resources: recoveryPointArn, resources: backupVaultArn, details, lifecycle, calculatedLifecycle, state</td>
</tr>
<tr>
<td>Backup Vault State Change</td>
<td>CREATED, DELETED, MODIFIED</td>
<td>accountId, resources: backupVaultArn, details, backupVaultName, state</td>
</tr>
<tr>
<td>Region Settings State Change</td>
<td>MODIFIED</td>
<td>accountId, details, modifiedAt, state, resourceTypeOptInPreference</td>
</tr>
<tr>
<td>Recovery Point State Change</td>
<td>MODIFIED, DELETED</td>
<td>accountId, resources: RecoveryPointArn, resources: backupVaultArn, details, lifecycle, calculatedLifecycle, state</td>
</tr>
<tr>
<td>Backup Plan State Change</td>
<td>CREATED, DELETED, MODIFIED</td>
<td>accountId, resources: backupPlanArn, details, backupPlanId, versionId, creationDate, deletionDate</td>
</tr>
</tbody>
</table>

Use these sample JSON payloads if you would like to use these events programmatically.

<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Backup Job: FAILED | {
|                    | "version": "0",
|                    | "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
|                    | "detail-type": "Backup Job State Change",
|                    | "source": "aws.backup",
|                    | "account": "1112233445566",
|                    | "time": "2020-07-29T20:15:26Z",
|                    | "region": "us-east-1",
|                    | "resources": [],
|                    | "detail": {                                   |
### Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;backupJobId&quot;: &quot;34176239-e96d-4e1d-9fad-529dbb3c3556&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;2020-07-30T04:13:07.392Z&quot;,</td>
</tr>
<tr>
<td>&quot;iamRoleArn&quot;: &quot;arn:aws:iam::1112233445566: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-2:1112233445566: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>}</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>
Monitor events using EventBridge

Event state

Backup Job: COMPLETED

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;version&quot;: &quot;0&quot;,</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;dafac799-9b88-0134-26b7-fef4d5a134f&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;1112233445566&quot;,</td>
</tr>
<tr>
<td>&quot;time&quot;: &quot;2020-07-15T21:41:17Z&quot;,</td>
</tr>
<tr>
<td>&quot;region&quot;: &quot;us-east-1&quot;,</td>
</tr>
<tr>
<td>&quot;resources&quot;: [</td>
</tr>
<tr>
<td>],</td>
</tr>
<tr>
<td>&quot;detail&quot;: {</td>
</tr>
<tr>
<td>&quot;backupJobId&quot;: &quot;a827233a-d405-4a86-a440-759fa94f34dd&quot;,</td>
</tr>
<tr>
<td>&quot;backupSizeInBytes&quot;: &quot;36048&quot;,</td>
</tr>
<tr>
<td>&quot;backupVaultName&quot;: &quot;9732c1b4-1091-472a-9d9f-52e0565ee39a_beta&quot;,</td>
</tr>
<tr>
<td>&quot;bytesTransferred&quot;: &quot;36048&quot;,</td>
</tr>
<tr>
<td>&quot;creationDate&quot;: &quot;2020-07-15T21:40:31.207Z&quot;,</td>
</tr>
<tr>
<td>&quot;iamRoleArn&quot;: &quot;arn:aws:iam::1112233445566:role/MockRCBackupIntegTestRole&quot;,</td>
</tr>
<tr>
<td>&quot;resourceType&quot;: &quot;CryoTestClient&quot;,</td>
</tr>
<tr>
<td>&quot;state&quot;: &quot;COMPLETED&quot;,</td>
</tr>
<tr>
<td>&quot;completionDate&quot;: &quot;2020-07-15T21:41:05.921Z&quot;,</td>
</tr>
<tr>
<td>&quot;startBy&quot;: &quot;2020-07-16T05:40:31.207Z&quot;,</td>
</tr>
<tr>
<td>&quot;percentDone&quot;: 100</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
**Event state**

**JSON payload**

<table>
<thead>
<tr>
<th>Backup Job: RUNNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{</td>
</tr>
</tbody>
</table>
|   "version": "0",
|   "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
|   "detail-type": "Backup Job State Change",
|   "source": "aws.backup",
|   "account": "1112233445566",
|   "region": "us-east-1",
|   "resources": [],
|   "detail": { |
|     "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
|     "backupSizeInBytes": "3221225472",
|     "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15_beta",
|     "bytesTransferred": "0",
|     "creationDate": "2020-07-15T21:38:31.152Z",
|     "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupIntegTestRole",
|     "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
|     "resourceType": "EBS",
|     "state": "RUNNING",
|     "startBy": "2020-07-16T05:00:00Z",
|     "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
|     "percentDone": 99,
|     "createdBy": { |
|       "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
|       "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5_beta",
|       "backupPlanVersion": "YTkszNmUMnUtwMWRNS00Y2RklThmZGUtNjA5NTc4NGM1YTYc5",
|       "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
<p>|     } |
|   } |
| } |
| } |</p>
<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Job: ABORTED</td>
<td></td>
</tr>
</tbody>
</table>

```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": "f59bffdcd-2538-4bbe-8343-1c60da27c27_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.",
    "completionDate": "2020-07-15T21:33:01.621Z",
    "startBy": "2020-07-16T05:33:00.803Z",
    "percentDone": 0
  }
}
```
### Event state

Backup Job: EXPIRED

```json
{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "111233445566",
  "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::111233445566: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,
    "creatorId": {
      "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00NjhlLTIzMTExNWRjOWYyYmZiNzVj",
      "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2"
    }
  }
}
```
### Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup Job: PENDING</strong></td>
</tr>
</tbody>
</table>

```json
{
    "version": "0",
    "id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
    "detail-type": "Backup Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-07-29T20:03:30Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "backupJobId": "2cffdb68-d6ed-485f-9f9b-8b530749f1c2",
        "backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975_beta",
        "bytesTransferred": "0",
        "creationDate": "2020-07-29T20:01:06.224Z",
        "iamRoleArn": "arn:aws:iam::111223345566:role/MockRCBackupIntegTestRole",
        "resourceType": "CryoTestClient",
        "state": "PENDING",
        "statusMessage": "",
        "startBy": "2020-07-30T04:01:06.224Z",
        "percentDone": 0
    }
}
```

| **Backup Job: CREATED** |

```json
{
    "version": "0",
    "id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
    "detail-type": "Backup Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-06-22T20:32:53Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
        "state": "CREATED",
        "creationDate": "2020-06-22T20:32:47.466Z"
    }
}
```
<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
## Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Job: <strong>RUNNING</strong></td>
</tr>
</tbody>
</table>

```json
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b9482d2c58e4",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:07:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3af9",
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4AC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceType": "EBS",
    "state": "RUNNING",
    "destinationRecoveryPointArn": {},
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWNQ4",
      "backupPlanRuleId": "70e356d3-1a11-4f61-8585-af5d6b9bb18"
    }
  }
}
```
Monitor events using EventBridge

<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Copy Job: COMPLETED | {
  "version": "0",
  "id": "47deb974-6473-aef1-56c2-52c3eadfceb",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:08:04Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541AACC84C85",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceType": "EBS",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T22:07:58.111Z",
    "destinationRecoveryPointArn": {
      "value": "arn:aws:ec2:us-west-2::snapshot/snap-0726fe70935546180"
    },
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
### Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copy Job: CREATED</strong></td>
</tr>
</tbody>
</table>

```json
{
    "version": "0",
    "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
    "detail-type": "Copy Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-06-22T21:06:32Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-west-2::image/ami-088b126e2170b98e"
    ],
    "detail": {
        "creationDate": "2020-06-22T21:06:25.754Z",
        "state": "CREATED",
        "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:ef09da5a-21a6-461f-a98f-857e9e621a17_beta"
    }
}
```
<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
</table>
| Restore Job: FAILED | {  
  "version": "0",  
  "id": "296805cc-6ad4-32f2-fb86-4e66c84abce7",  
  "detail-type": "Restore Job State Change",  
  "source": "aws.backup",  
  "account": "1112233445566",  
  "time": "2020-07-15T20:19:29Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ec2:us-west-2::image/ami-06b9894dfbf1f9cf48"  
  ],  
  "detail": {  
    "restoreJobId": "9B333A28-526B-01CD-4A77-9785A08922FD",  
    "backupSizeInBytes": "22548578304",  
    "creationDate": "2020-07-15T20:19:07.303Z",  
    "iamRoleArn": "arn:aws:iam:1112233445566: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."  
  }  
}  
}
## Monitor events using EventBridge

### Event state: Restore Job: RUNNING

<table>
<thead>
<tr>
<th>Event state</th>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Job: RUNNING</td>
<td></td>
</tr>
</tbody>
</table>

```
{
   "version": "0",
   "id": "6137a1f0-33f3-99ee-a01a-3d8b96fe2ad6",
   "detail-type": "Restore Job State Change",
   "source": "aws.backup",
   "account": "111223445566",
   "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::111223445566: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": "1112233445566",
  "time": "2020-07-15T03:14:58Z",
  "region": "us-east-1",
  "resources": [  
  ],
  "detail": {  
    "restoreJobId": "EF332640-02A5-5978-693F-987970F09961",
    "backupSizeInBytes": "0",
    "creationDate": "2020-07-15T03:10:01.742Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/CanaryAWSBackupRole",
    "percentDone": 0,
    "resourceType": "RDS",
    "status": "COMPLETED",
    "completionDate": "2020-07-15T03:14:53.128Z"
  }
}
### Event state

**Restore Job: PENDING**

```json
{
  "version": "0",
  "id": "0586085f-3079-cd79-10b7-908d3c3a2lea",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "restoreJobId": "EB9CE5CB-2B92-8B66-FD16-9829F4DDA0D7",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupIntegTestRole",
    "percentDone": 0,
    "resourceType": "CryoTestClient",
    "status": "PENDING"
  }
}
```

**Restore Job: CREATED**

```json
{
  "version": "0",
  "id": "af32977e-378f-2122-f985-fca4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T18:50:49Z",
  "region": "us-east-1",
  "resources": [
  ],
  "detail": {
    "restoreJobId": "267EA62F-C125-EFES-7099-9D98FC0E422A",
    "creationDate": "2020-06-22T18:50:49Z",
    "state": "CREATED"
  }
}
```
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-4aaf-a642-dd0f1c95b0f0",
|   "detail-type": "Recovery Point Change",
|   "source": "aws.backup",
|   "account": "1112233455556",
|   "time": "2020-07-15T21:39:07Z",
|   "region": "us-east-1",
|   "resources": [ |
|     "arn:aws:rds:us-west-2:1112233455556:cluster-backup:snapshot:awsbackup:job-4ece7121-d60e-00c2-5c3b-49960142d03b"
|   ],
|   "detail": { |
|     "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15_beta",
|     "creationDate": "2020-07-15T21:38:31.152Z",
|     "iamRoleArn": "arn:aws:iam::1112233455556:role/FullBackupIntegTestRole",
|     "resourceType": "Aurora",
|     "resourceArn": "arn:aws:rds:us-west-2:1112233455556:cluster:cryo-aurora-14029f40-b0b6-4a61-9fd2-9886f2771add",
|     "status": "COMPLETED",
|     "isEncrypted": "false",
|     "storageClass": "WARM",
|     "completionDate": "2020-07-15T21:39:05.689Z",
|     "createdBy": { |
|       "backupPlanId": "bde0f455-4e24-4668-4932a97f5cc5",
|       "backupPlanArn": "arn:aws:backup:us-west-2:1112233455556:backup-plan:bde0f455-4e24-4668-4932a97f5cc5",
|       "backupPlanVersion": "YTkzNmM0M0M0UtMWMrHNS00Y2RlThmZGUtNjA5NTc4NGM1Y2t5",
|       "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
|     },
|     "lifecycle": { |
|       "deleteAfterDays": 100
|     },
|     "calculatedLifeCycle": { |
|       "deleteAt": "2020-10-23T21:38:31.152Z"
|     }
|   }
|} |
### Event state

<table>
<thead>
<tr>
<th>JSON payload</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recovery Point: DELETED</strong></td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;version&quot;: &quot;0&quot;,</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;6089ee76-d856-0d7c-ceed7-0a431cd43343&quot;,</td>
</tr>
<tr>
<td>&quot;detail-type&quot;: &quot;Recovery Point Change&quot;,</td>
</tr>
<tr>
<td>&quot;source&quot;: &quot;aws.backup&quot;,</td>
</tr>
<tr>
<td>&quot;account&quot;: &quot;1112233445566&quot;,</td>
</tr>
<tr>
<td>&quot;time&quot;: &quot;2020-07-29T22:38:49Z&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;arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-01d4d0a-32d1-4d54-bd70-bced933ef107&quot; ]</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>&quot;detail&quot;: {</td>
</tr>
<tr>
<td>&quot;state&quot;: &quot;DELETED&quot;,</td>
</tr>
<tr>
<td>&quot;lifecycle&quot;: {</td>
</tr>
<tr>
<td>&quot;deleteAfterDays&quot;: 300</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>&quot;calculatedLifeCycle&quot;: {</td>
</tr>
<tr>
<td>&quot;deletedAt&quot;: &quot;2021-05-25T22:29:02.452Z&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td><strong>Recovery Point: MODIFIED</strong></td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;version&quot;: &quot;0&quot;,</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;14365bb1-ade-00-1-le3-8fac188d7996&quot;,</td>
</tr>
<tr>
<td>&quot;detail-type&quot;: &quot;Recovery Point Change&quot;,</td>
</tr>
<tr>
<td>&quot;source&quot;: &quot;aws.backup&quot;,</td>
</tr>
<tr>
<td>&quot;account&quot;: &quot;1112233445566&quot;,</td>
</tr>
<tr>
<td>&quot;time&quot;: &quot;2020-07-02T23:33:57Z&quot;,</td>
</tr>
<tr>
<td>&quot;region&quot;: &quot;us-east-1&quot;,</td>
</tr>
<tr>
<td>&quot;resources&quot;: [</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>&quot;detail&quot;: {</td>
</tr>
<tr>
<td>&quot;calculatedLifeCycle&quot;: {</td>
</tr>
<tr>
<td>&quot;toColdStorageAfterDays&quot;: &quot;Fri Dec 04 22:55:11 UTC 2020&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>&quot;state&quot;: &quot;MODIFIED&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>
### Event state

<table>
<thead>
<tr>
<th>Event Description</th>
<th>JSON Payload</th>
</tr>
</thead>
</table>
## Event state

### Backup Plan: MODIFIED

```
{
    "version": "0",
    "id": "2895ae3f-bdd4a-0a23-6071-2652adb92c3f",
    "detail-type": "Backup Plan State Change",
    "source": "aws.backup",
    "account": "1122343
5566",
    "time": "2020-06-24T23:18:25Z",
    "region": "us-east-1",
    "resources": [
    ],
    "detail": {
        "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
        "versionId": "NjIwNDEtMjJmLTMzLzE0M2JmLMS2NzNzQyNzIxNDk0",
        "modifiedAt": "2020-06-24T23:18:19.168Z",
        "state": "MODIFIED"
    }
}
```

### Backup Plan: DELETED

```
{
    "version": "0",
    "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
    "detail-type": "Backup Plan State Change",
    "source": "aws.backup",
    "account": "11223435566",
    "time": "2020-06-24T23:18:25Z",
    "region": "us-east-1",
    "resources": [
    ],
    "detail": {
        "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
        "versionId": "NjIwNDEtMjJmLTMzLzE0M2JmLMS2NzNzQyNzIxNDk0",
        "deletionDate": "2020-06-24T23:18:19.411Z",
        "state": "DELETED"
    }
}
```
### Event state

#### JSON payload

**Backup Plan: CREATED**

```
{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bd0d4bdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-d3afa4c84f59_beta"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
    "versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYy0zMjViYy0zMjY5",
    "creationDate": "2020-06-24T23:18:15.318Z",
    "state": "CREATED"
  }
}
```

**Region Setting: MODIFIED**

```
{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dbab9c68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "modifiedAt": "2020-06-24T22:54:57.161Z",
    "ResourceTypeOptInPreference": { "Aurora": true },
    "state": "MODIFIED"
  }
}
```

### 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.
Monitoring AWS Backup metrics with CloudWatch

Topics

- Monitor metrics with CloudWatch (p. 241)
- Differences with the AWS Backup dashboard (p. 243)

Monitor metrics with CloudWatch

You can use CloudWatch to monitor AWS Backup metrics. The 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. Different job types have different available states.</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 an email or SMS using Amazon SNS or open a ticket to the engineering team to investigate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reporting criteria: There is a nonzero value</td>
<td></td>
</tr>
<tr>
<td></td>
<td></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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reporting criteria: There is a nonzero value</td>
<td></td>
</tr>
<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></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>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 that AWS Backup scheduled but did not start. Often caused by scheduling a backup job during or 4 hours before a database resource or Amazon FSx maintenance window or automated backup window and not using AWS Backup to perform continuous backup for point-in-time restores. See Point-in-Time Recovery 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>
<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>
</tbody>
</table>
## Differences with the AWS Backup dashboard

The AWS Backup console has its own dashboard, which you can view by choosing **Dashboard** in the navigation pane. This dashboard shows metrics for the last 24 hours. The CloudWatch dashboard shows metrics over a longer period of time. For specifics, see What is the retention period of all metrics? in the CloudWatch FAQ.

The AWS Backup dashboard also shows you metrics at a point in time. CloudWatch shows you metrics over a period of time. For example, suppose that you have nine jobs completed and one job in progress over the last 4 hours. The AWS Backup dashboard would show you nine jobs completed and one job in progress. CloudWatch would show you 10 jobs in progress if you view running jobs metrics during the last 4 hours.

We recommend that you use the dashboard that enables you to most easily detect potential issues.

## 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.

**Topics**

- [AWS Backup information in CloudTrail](#)
- [Understanding AWS Backup log file entries](#)
- [Logging cross-account management events](#)
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
- 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 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.

For an ongoing record of events in your AWS account, including events for AWS Backup, create a trail. A trail 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
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

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.

```json
{
  "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.metal1.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-00a422a05b9c6a3d",
    "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
    "startWindowMinutes": 60
  },
  "responseElements": {
    "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
    "creationDate": "Jan 10, 2019 1:45:24 PM"
  },
  "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
  "eventId": "fe8146a5-7812-4a95-90ad-074498be1234",
  "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",
  "creditsUsed": "W/doc-843a0-00ac198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12 java/1.8.0_192",
  "requestParameters": {
    "restorePointId": "backupJobId_='8a3c2a87-b23e-4d56-b045-fa9e88ede4e6'",
    "backupVaultName": "Default",
    "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/vol-00a422a05b9c6a3d",
    "iamRoleArn": "arn:aws:iam::123456789012:role/AWSStateManager",
    "startTime": "2019-01-10T13:45:24Z",
    "endTime": "2019-01-10T13:49:50Z"
  },
  "responseElements": {
    "restoreJobId": "8a3c2a87-b23eb-4d56-b045-fa9e88ede4e6",
    "creationDate": "Jan 10, 2019 2:49:50 PM"
  },
  "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
  "eventId": "fe8146a5-7812-4a95-90ad-074498be1234",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-id"
}
```
"userAgent": "aws-internal/3 aws-sdk-java/1.11.465
Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
"requestParameters": {
  "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bd9c9d99",
  "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": "783dddde-6d7e-4539-8fab-376aa9668543",
"eventID": "ff35ddea-7577-4aee-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",
  "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.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
  "requestParameters": {
    "backupVaultName": "Default",
    "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
  },
  "responseElements": null,
  "requestID": "f1f1b33a-48a-436c-917b-754f1ab5fd7",
  "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-id"
},
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "account-id",
    "invokedBy": "backup.amazonaws.com"
  },
  "eventTime": "2019-01-10T14:52:42Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "DeleteRecoveryPoint",
  "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.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
  "requestParameters": {
    "backupVaultName": "Default",
    "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
  },
  "responseElements": null,
  "requestID": "f1f1b33a-48a-436c-917b-754f1ab5fd7",
  "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-id"
},
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountID": "account-id",
    "invokedBy": "backup.amazonaws.com"
  },
  "eventTime": "2019-01-10T14:52:42Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "DeleteRecoveryPoint",
  "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.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
  "requestParameters": {
    "backupVaultName": "Default",
    "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
  },
  "responseElements": null,
  "requestID": "f1f1b33a-48a-436c-917b-754f1ab5fd7",
  "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
  "eventType": "AwsApiCall",
  "recipientAccountId": "account-id"}
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.

```json
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "account-id",
    "invokedBy": "backup.amazonaws.com"},
  "eventTime": "2020-06-02T00:34:00Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "CreateOrganizationalBackupPlan",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "account-id",
  "serviceEventDetails": {
    "completionDate": {
      "seconds": 1547108091,
      "nanos": 906000000
    },
    "state": "COMPLETED",
    "percentDone": 100,
    "backupJobId": "8A8E73BB-A8C5-E058-8224-90FA323A3C0E",
    "backupVaultName": "BackupVault",
    "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c314d361233",
    "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/vol-06692095a6a4321233",
    "creationDate": {
      "seconds": 1547101638,
      "nanos": 272000000
    },
    "backupSizeInBytes": 8589934592,
    "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
    "resourceType": "EBS"
  }
}
```
The following example shows a CloudTrail log entry that demonstrates the DeleteOrganizationalBackupPlan action.

```json
{
  "@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": "ZTA1Y2ZjZDYtNjM0Yy00ZTA1LWIyNjAtM2M1NzQ4OTmMzRj",
    "@backupPlanName": "mybackupplan",
    "@backupRules": "[{"id":"745f00e5-7f57-3f35-8a0e-ed4b8c48a8e2","scheduleExpression":"cron(0 0/1 ? * * *)","startWindow":"PT1H","completionWindow":"PT2H","lifecycle":{"moveToObjectAfterDays":null,"deleteAfterDays":"7"},"tags":null,"copyActions":[]},
    "@backupSelections": "[{"name":"selectiondatatype","arn":"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-a075ea715686","resources":[]},
    "@creationDate": "2020-06-02T00:34:00.695Z",
    "@organizationId": "org-id",
    "@accountId": "account-id"
  }
}
```

The following example shows a CloudTrail log entry that demonstrates the DeleteOrganizationalBackupPlan action.

```json
{
  "@eventVersion": "1.05",
  "@userIdentity": {
    "@accountId": "account-id",
    "@invokedBy": "backup.amazonaws.com"
  },
  "@eventTime": "2020-06-02T00:34:25Z",
  "@eventSource": "backup.amazonaws.com",
  "@eventName": "DeleteOrganizationalBackupPlan",
  "@awsRegion": "ca-central-1",
  "@sourceIpAddress": "backup.amazonaws.com",
  "@userAgent": "backup.amazonaws.com",
  "@requestParameters": null,
  "@responseElements": null,
  "@readOnly": false,
  "@eventType": "AwsServiceEvent",
  "@recipientAccountId": "account-id",
  "@serviceEventDetails": {
    "@backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "@backupPlanVersionId": "ZTA1Y2ZjZDYtNjM0Yy00ZTA1LWIyNjAtM2M1NzQ4OTmMzRj",
    "@backupPlanName": "mybackupplan",
    "@deletionDate": 1591058040,
    "@creationDate": 1591058040,
    "@organizationId": "org-id",
    "@accountId": "account-id"
  }
}
```
Using Amazon SNS to track 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.

Topics
- Common use cases (p. 249)
- AWS Backup notification APIs (p. 249)
- Examples of events (p. 250)
- AWS Backup notification command examples (p. 252)
- Specifying AWS Backup as a service principal (p. 253)

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.

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. 288) — Deletes event notifications for the specified backup vault.
- GetBackupVaultNotifications (p. 348) — Lists all event notifications for the specified backup vault.
- PutBackupVaultNotifications (p. 398) — 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>
</tbody>
</table>

249
### Examples of events

<table>
<thead>
<tr>
<th>Event</th>
<th>Amazon SNS Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup job completed</strong></td>
<td>```json</td>
</tr>
</tbody>
</table>
  "Records": [{
    "EventSource": "aws: sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802a1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1234567",
      "Subject": "Notification from AWS Backup",
      ..."MessageAttributes": {
      "EventType": {
        "Type": "String", "Value": "BACKUP_JOB"},
      "State": {
        "Type": "String", "Value": "COMPLETED"},
      "AccountId": {
        "Type": "String", "Value": "123456789012"},
      "Id": {
        "Type": "String", "Value": "1b2345b2-f22c-4eb6-bbcd7890ed123"},
      "StartTime": {
        "Type": "String", "Value": "2019-09-02T13:48:52.226Z"}
      }
    }
  }|
  ``` |
| **Backup job failed** | ```json|
  "Records": [{
    "EventSource": "aws: sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802a1ed45",
  }|
  ``` |
### Examples of events

<table>
<thead>
<tr>
<th>Event</th>
<th>Amazon SNS Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;Sns&quot;: {</td>
</tr>
</tbody>
</table>
|       |   "Type": "Notification",
|       |   "MessageId": "12345678-
|       |     abcd-123a-def0-abc1a234567",
|       |   "TopicArn": "arn:aws:sns:us-
|       |     west-1:123456789012:backup-2sq-sns-topic",
|       |   "Subject": "Notification from AWS Backup",
|       |   "MessageAttributes": { |
|       |     "EventType": {       |
|       |       "Type": "String",
|       |       "Value": "BACKUP_JOB"},
|       |     "State": {          |
|       |       "Type": "String",
|       |       "Value": "FAILED"},
|       |     "AccountId": {      |
|       |       "Type": "String",
|       |       "Value": "123456789012"},
|       |     "Id": {             |
|       |       "Type": "String",
|       |       "Value": "1b2345b2-
|       |       f2cc-4dab-5eb6-bbc7890ed123"},
|       |     "StartTime": {      |
|       |       "Type": "String",
|       |       "Value": "2019-09-02T13:48:52.226Z"}   |
|       |   }                     |
|       | }                       |
### Event

<table>
<thead>
<tr>
<th>Event</th>
<th>Amazon SNS Notification</th>
</tr>
</thead>
</table>
| Backup job could not complete during the backup window | ```json
{
  "Records": [
    {
      "EventSource": "aws: sns",
      "EventVersion": "1.0",
      "EventSubscriptionArn": "arn:aws:sns:...-a3802ad1ed45",
      "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": "EXPIRED"
          },
          "AccountId": {
            "Type": "String",
            "Value": "123456789012"
          },
          "Id": {
            "Type": "String",
            "Value": "1b2345b2-f22c-4dab-5eb6-bbc7890ed123"
          },
          "StartTime": {
            "Type": "String",
            "Value": "2019-09-02T13:48:52.226Z"
          }
        }
      }
    }
  ]
}
``` |

### 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.

```bash
aws backup get-backup-vault-notifications
  --backup-vault-name myVault
```

The sample output is as follows:

```json
{
  "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.

```bash
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.

```json
{
  "Sid": "My-statement-id",
  "Effect": "Allow",
  "Principal": {
    "Service": "backup.amazonaws.com"
  },
  "Action": "SNS:Publish",
}
```

The following sample JSON is an example of a basic Amazon SNS access policy that includes AWS Backup as a service principal. This example allows for cross-account access.

```json
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
    }
  ]
}
```
"Principal": {
  "Service": "backup.amazonaws.com"
},
"Action": [
  "SNS:Publish",
  "SNS:RemovePermission",
  "SNS:SetTopicAttributes",
  "SNS:DeleteTopic",
  "SNS:ListSubscriptionsByTopic",
  "SNS:GetTopicAttributes",
  "SNS:Receive",
  "SNS:AddPermission",
  "SNS:Subscribe"
],
"Condition": {
  "ArnLike": {
  },
  "StringEquals": {
    "aws:SourceAccount": "account-id"
  }
},
"Sid": "__console_pub_0",
"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 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 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. 255)
• Troubleshooting creating resources (p. 255)
• Troubleshooting deleting resources (p. 256)

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. 143).

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. 243).

Troubleshooting creating resources

The following information can help you troubleshoot problems with creating backups.

• In general, AWS database services and Amazon FSx cannot start backups 4 hours before or during their maintenance window or automatic backup window. 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.

• When creating Amazon 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 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.

• You cannot specify RDS options when using AWS Backup to make a backup copy. If you get an error such as "The snapshot requires a target option group with the following options: Timezone..." you must remove the option or instead use the Amazon RDS console or API to initiate the copy.

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. 143).
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.

- Actions
- Data Types
- Common Errors

Actions

The following actions are supported:

- CreateBackupPlan (p. 259)
- CreateBackupSelection (p. 263)
- CreateBackupVault (p. 266)
- CreateFramework (p. 269)
- CreateReportPlan (p. 273)
- DeleteBackupPlan (p. 277)
- DeleteBackupSelection (p. 280)
- DeleteBackupVault (p. 282)
- DeleteBackupVaultAccessPolicy (p. 284)
- DeleteBackupVaultLockConfiguration (p. 286)
- DeleteBackupVaultNotifications (p. 288)
- DeleteFramework (p. 290)
- DeleteRecoveryPoint (p. 292)
- DeleteReportPlan (p. 294)
- DescribeBackupJob (p. 296)
- DescribeBackupVault (p. 301)
- DescribeCopyJob (p. 305)
- DescribeFramework (p. 307)
- DescribeGlobalSettings (p. 310)
- DescribeProtectedResource (p. 312)
- DescribeRecoveryPoint (p. 314)
- DescribeRegionSettings (p. 319)
- DescribeReportJob (p. 321)
- DescribeReportPlan (p. 323)
- DescribeRestoreJob (p. 325)
- DisassociateRecoveryPoint (p. 329)
- ExportBackupPlanTemplate (p. 331)
- GetBackupPlan (p. 333)
- GetBackupPlanFromJSON (p. 337)
- GetBackupPlanFromTemplate (p. 340)
• GetBackupSelection (p. 343)
• GetBackupVaultAccessPolicy (p. 346)
• GetBackupVaultNotifications (p. 348)
• GetRecoveryPointRestoreMetadata (p. 351)
• GetSupportedResourceTypes (p. 353)
• ListBackupJobs (p. 355)
• ListBackupPlans (p. 358)
• ListBackupPlanTemplates (p. 361)
• ListBackupPlan Versions (p. 363)
• ListBackupSelections (p. 366)
• ListBackupVaults (p. 368)
• ListCopyJobs (p. 370)
• ListFrameworks (p. 373)
• ListProtectedResources (p. 375)
• ListRecoveryPointsByBackupVault (p. 377)
• ListRecoveryPointsByResource (p. 380)
• ListReportJobs (p. 383)
• ListReportPlans (p. 386)
• ListRestoreJobs (p. 388)
• ListTags (p. 391)
• PutBackupVaultAccessPolicy (p. 393)
• PutBackupVaultLockConfiguration (p. 395)
• PutBackupVaultNotifications (p. 398)
• StartBackupJob (p. 401)
• StartCopyJob (p. 405)
• StartReportJob (p. 409)
• StartRestoreJob (p. 411)
• StopBackupJob (p. 414)
• TagResource (p. 416)
• UntagResource (p. 418)
• UpdateBackupPlan (p. 420)
• UpdateFramework (p. 423)
• UpdateGlobalSettings (p. 427)
• UpdateRecoveryPointLifecycle (p. 429)
• UpdateRegionSettings (p. 432)
• UpdateReportPlan (p. 434)
CreateBackupPlan

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. 259)

Specifies the body of a backup plan. Includes a BackupPlanName and one or more sets of Rules.

Type: BackupPlanInput (p. 444) object

Required: Yes

BackupPlanTags (p. 259)

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. 259)

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. 260)**

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. 438) objects

**BackupPlanArn (p. 260)**

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. 260)**

Uniquely identifies a backup plan.

Type: String

**CreationDate (p. 260)**

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. 260)**

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. 490).

**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

Create a JSON document that specifies a set of resources to assign to a backup plan. For examples, see Assigning resources programmatically.

Request Syntax

```
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. 263)
```

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. 263)

Specifies the body of a request to assign a set of resources to a backup plan.

Type: BackupSelection (p. 452) object

CreatorRequestId (p. 263)

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

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. 264)

Uniquely identifies a backup plan.

Type: String

CreationDate (p. 264)

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. 264)

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. 490).

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

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. 266)**

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. 266)**

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. 266)**

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. 266)

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. 267)

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. 267)

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. 267)

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. 490).

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

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. 269)**

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. 471) objects

Required: Yes

**FrameworkDescription (p. 269)**

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. 269)**

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. 269)**

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. 269)**

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. 270)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String
FrameworkName (p. 270)

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. 490).

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

LimitExceeded Exception

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

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": {
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "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. 273)

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. 273)

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. 481) object

Required: Yes

ReportPlanDescription  (p. 273)

An optional description of the report plan with a maximum of 1,024 characters.
CreateReportPlan

Type: String
Length Constraints: Minimum length of 0. Maximum length of 1024.
Pattern: .*\S.*
Required: No

ReportPlanName (p. 273)

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. 273)

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. 273)

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. 487) object
Required: Yes

Response Syntax

HTTP/1.1 200
Content-type: application/json

```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. 274)**

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. 274)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

**ReportPlanName (p. 274)**

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. 490).

**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

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. 277)

- 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. 277)

- 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. 277)

- Uniquely identifies a backup plan.
- Type: String
DeleteBackupPlan (p. 277)

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. 277)

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. 490).

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

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. 280)*
  - Uniquely identifies a backup plan.
  - Required: Yes

- **selectionId** *(p. 280)*
  - 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. 490).*

**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

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. 282)

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. 490).

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

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. 284)

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. 490).

*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

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. 286)

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. 490).

InvalidParameterValue

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

MissingParameterValue

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

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. 288)**

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. 490).

**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

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. 290)*

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. 490).*

**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

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.

Request Syntax

DELETE /backup-vaults/{backupVaultName}/recovery-points/{recoveryPointArn} HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 292)

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. 292)

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. 490).

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

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. 294)*
  - 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. 490).*

- **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

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. 296)

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

{
  "AccountId": "string",
  "BackupJobId": "string",
  "BackupOptions": {
    "string": "string"
  },
  "BackupSizeInBytes": number,
  "BackupType": "string",
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "BytesTransferred": number,
  "CompletionDate": number,
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": number,
  "ExpectedCompletionDate": number,
  "IamRoleArn": "string",
  "PercentDone": "string",
  "RecoveryPointArn": "string",
  "ResourceArn": "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.

**AccountId (p. 296)**

Returns the account ID that owns the backup job.

Type: String

Pattern: ^[0-9]{12}$

**BackupJobId (p. 296)**

Uniquely identifies a request to AWS Backup to back up a resource.

Type: String

**BackupOptions (p. 296)**

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. 296)**

The size, in bytes, of a backup.

Type: Long

**BackupType (p. 296)**

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. 296)**

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. 296)**

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. 296)**

The size in bytes transferred to a backup vault at the time that the job status was queried.
Type: Long

**CompletionDate (p. 296)**

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. 296)**

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. 480)` object

**CreationDate (p. 296)**

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. 296)**

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. 296)**

Specifies the IAM role ARN used to create the target recovery point; for example, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

**PercentDone (p. 296)**

Contains an estimated percentage that is complete of a job at the time the job status was queried.

Type: String

**RecoveryPointArn (p. 296)**

An ARN that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B48880D45`.

Type: String

**ResourceArn (p. 296)**

An ARN that uniquely identifies a saved resource. The format of the ARN depends on the resource type.

Type: String

**ResourceType (p. 296)**

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.
StartBy (p. 296)

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.

State (p. 296)

The current state of a resource recovery point.

StatusMessage (p. 296)

A detailed message explaining the status of the job to back up a resource.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

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

Returns metadata about a backup vault specified by its name.

Request Syntax

GET /backup-vaults/{backupVaultName} HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 301)

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
}

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. 301)

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. 301)*

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

**CreationDate** *(p. 301)*

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.

Type: Timestamp

**CreatorRequestId** *(p. 301)*

A unique string that identifies the request and allows failed requests to be retried without the risk of running the operation twice.

Type: String

**EncryptionKeyArn** *(p. 301)*

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

**LockDate** *(p. 301)*

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.

Type: Timestamp

**Locked** *(p. 301)*

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.

Type: Boolean

**MaxRetentionDays** *(p. 301)*

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. 301)

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. 301)

The number of recovery points that are stored in a backup vault.

Type: Long

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

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

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. 305)**

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,
    "CompletionDate": number,
    "CopyJobId": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
    },
    "CreationDate": number,
    "DestinationBackupVaultArn": "string",
    "DestinationRecoveryPointArn": "string",
    "IamRoleArn": "string",
    "ResourceArn": "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. 305)**

Contains detailed information about a copy job.

Type: CopyJob (p. 466) object

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 490).

**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

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. 307)
  
  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. 307)_

The date and time that a framework 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

_**DeploymentStatus** (p. 307)_

The deployment status of a framework. The statuses are:

- `CREATE_IN_PROGRESS`
- `UPDATE_IN_PROGRESS`
- `DELETE_IN_PROGRESS`
- `COMPLETED`
- `FAILED`

Type: String

_**FrameworkArn** (p. 307)_

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String

_**FrameworkControls** (p. 307)_

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. 471) objects

_**FrameworkDescription** (p. 307)_

An optional description of the framework.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*\S.*`

_**FrameworkName** (p. 307)_

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. 307)_

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. 307)**

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. 490).

**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

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. 310)

The status of the flag isCrossAccountBackupEnabled.

Type: String to string map

LastUpdateTime (p. 310)

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. 490).
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

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.

resourceArn (p. 312)

An Amazon Resource Name (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

HTTP/1.1 200
Content-type: application/json

{
    "LastBackupTime": number,
    "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.

LastBackupTime (p. 312)

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. 312)

An ARN that uniquely identifies a resource. The format of the ARN depends on the resource type.

Type: String
DescribeProtectedResource

ResourceType (p. 312)

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. 490).

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

Returns metadata associated with a recovery point, including ID, status, encryption, and lifecycle.

Request Syntax

GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 314)

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. 314)

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,
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": number,
  "EncryptionKeyArn": "string",
  "IamRoleArn": "string",
  "IsEncrypted": boolean,

"LastRestoreTime": number,
"Lifecycle": {
   "DeleteAfterDays": number,
   "MoveToColdStorageAfterDays": number
},
"RecoveryPointArn": "string",
"ResourceArn": "string",
"ResourceType": "string",
"SourceBackupVaultArn": "string",
"Status": "string",
"StatusMessage": "string",
"StorageClass": "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. 314)**

The size, in bytes, of a backup.

Type: Long

**BackupVaultArn (p. 314)**

An ARN that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

**BackupVaultName (p. 314)**

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. 314)**

A CalculatedLifecycle object containing DeleteAt and MoveToColdStorageAt timestamps.

Type: CalculatedLifecycle (p. 459) object

**CompletionDate (p. 314)**

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

**CreatedBy (p. 314)**

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. 480) object
CreationDate (p. 314)

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. 314)

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. 314)

Specifies the IAM role ARN used to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

IsEncrypted (p. 314)

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

LastRestoreTime (p. 314)

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. 314)

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 “expire after days” 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 472) object

RecoveryPointArn (p. 314)

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. 314)

An ARN that uniquely identifies a saved resource. The format of the ARN depends on the resource type.

Type: String
**ResourceType** (p. 314)

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. 314)

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. 314)

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.

Type: String

Valid Values: COMPLETED | PARTIAL | DELETING | EXPIRED

**StatusMessage** (p. 314)

A status message explaining the reason for the recovery point deletion failure.

Type: String

**StorageClass** (p. 314)

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. 490).

**InvalidParameterValueChanged**

Indicates that something is wrong with a parameter's value. For example, the value is out of range.

HTTP Status Code: 400

**MissingParameterValueChanged**

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

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. 319)**

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. 319)**

Returns a list of all services along with the opt-in preferences in the Region.
DescribeRegionSettings

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. 490).

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

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. 321)

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. 321)

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. 483) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

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

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. 323)

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": {
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": "number",
      "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. 323)**

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. 485) object

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 490).

**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

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. 325)

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. 325)

Returns the account ID that owns the restore job.

Type: String

Pattern: ^[0-9]{12}$
**BackupSizeInBytes (p. 325)**

The size, in bytes, of the restored resource.

Type: Long

**CompletionDate (p. 325)**

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. 325)**

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. 325)**

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. 325)**

The amount of time in minutes that a job restoring a recovery point is expected to take.

Type: Long

**IamRoleArn (p. 325)**

Specifies the IAM role ARN used to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

**PercentDone (p. 325)**

Contains an estimated percentage that is complete of a job at the time the job status was queried.

Type: String

**RecoveryPointArn (p. 325)**

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. 325)**

Returns metadata associated with a restore job listed by resource type.

Type: String

Pattern: ^[a-zA-Z0-9\-\_\.]{1,50}$

**RestoreJobId (p. 325)**

Uniquely identifies the job that restores a recovery point.

Type: String
Status (p. 325)

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. 325)

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. 490).

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

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. 329)

The unique name of an AWS Backup vault.

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

Required: Yes

`recoveryPointArn` (p. 329)

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. 490).

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
ExportBackupPlanTemplate

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. 331)
```

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. 331)
```

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. 490).

**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

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. 333)

- Uniquely identifies a backup plan.
- Required: Yes

**VersionId** (p. 333)

- 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",
"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"
]
},
"BackupPlanArn": "string",
"BackupPlanId": "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.

**AdvancedBackupSettings (p. 333)**

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. 438) objects

**BackupPlan (p. 333)**

Specifies the body of a backup plan. Includes a BackupPlanName and one or more sets of Rules.

Type: BackupPlan (p. 443) object

**BackupPlanArn (p. 333)**

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. 333)**

Uniquely identifies a backup plan.

Type: String
CreationDate (p. 333)

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. 333)

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. 333)

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. 333)

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. 333)

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. 490).

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

Returns a valid JSON document specifying a backup plan or an error.

Request Syntax

```plaintext
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. 337)

A customer-supplied backup plan document in JSON format.

Type: String

Required: Yes

Response Syntax

```plaintext
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": {
    "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. 337)

Specifies the body of a backup plan. Includes a **BackupPlanName** and one or more sets of **Rules**.

Type: **BackupPlan** (p. 443) object

Errors

For information about the errors that are common to all actions, see **Common Errors** (p. 490).

**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

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. 340)*

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

{  
  "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. 340)**

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. 443) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

**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

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. 343)

Uniquely identifies a backup plan.

Required: Yes

selectionId (p. 343)

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. 343)

Uniquely identifies a backup plan.

Type: String

BackupSelection (p. 343)

Specifies the body of a request to assign a set of resources to a backup plan.

Type: BackupSelection (p. 452) object

CreationDate (p. 343)

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. 343)

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. 343)

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. 490).
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

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. 346)

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",
  "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. 346)

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. 346)

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. 346)
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. 490).

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

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. 348)

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. 348)

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. 348)

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 | RESTORE_JOB_COMPLETED | RESTORE_JOB_EXPIRED | RESTORE_JOB_STARTED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED

BackupVaultName (p. 348)

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. 348)

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. 490).

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

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
HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**backupVaultName** (p. 351)

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. 351)

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example,

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. 351)

An ARN that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.
Type: String

**RecoveryPointArn (p. 351)**

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

**RestoreMetadata (p. 351)**

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. 490)](#).

**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**

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. 353)**

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. 490).
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

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&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&maxResults=MaxResults&nextToken=NextToken&resourceArn=ByResourceArn&resourceType=ByResourceType&state=ByState

HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

ByAccountId (p. 355)

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. 355)

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\-\_\.){1,50}$

ByCreatedAfter (p. 355)

Returns only backup jobs that were created after the specified date.

ByCreatedBefore (p. 355)

Returns only backup jobs that were created before the specified date.

ByResourceArn (p. 355)

Returns only backup jobs that match the specified resource Amazon Resource Name (ARN).

ByResourceType (p. 355)

Returns only backup jobs for the specified resources:
- DynamoDB for Amazon DynamoDB
- EBS for Amazon Elastic Block Store
- EC2 for Amazon Elastic Compute Cloud
- EFS for Amazon Elastic File System
- RDS for Amazon Relational Database Service
- Aurora for Amazon Aurora
- Storage Gateway for Storage Gateway

Pattern: ^(a-zA-Z0-9\-\_\.){1,50}$

ByState (p. 355)

Returns only backup jobs that are in the specified state.
Valid Values: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED

**MaxResults (p. 355)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 355)**

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

```
{
  "BackupJobs": [
    {
      "AccountId": "string",
      "BackupJobId": "string",
      "BackupOptions": {
        "string": "string"
      },
      "BackupSizeInBytes": number,
      "BackupType": "string",
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "BytesTransferred": number,
      "CompletionDate": number,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "ExpectedCompletionDate": number,
      "IamRoleArn": "string",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
      "ResourceArn": "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. 356)**

An array of structures containing metadata about your backup jobs returned in JSON format.

Type: Array of BackupJob (p. 439) objects

**NextToken (p. 356)**

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. 490).

**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

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. 358)

A Boolean value with a default value of FALSE that returns deleted backup plans when set to TRUE.

MaxResults (p. 358)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 358)

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"]
,
"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.

BackupPlansList (p. 358)

An array of backup plan list items containing metadata about your saved backup plans.

Type: Array of BackupPlansListMember (p. 445) objects

NextToken (p. 358)

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. 490).

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

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. 361)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 361)

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": [  
    {  
      "BackupPlanTemplateId": "string",  
      "BackupPlanTemplateName": "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.

BackupPlanTemplatesList (p. 361)

An array of template list items containing metadata about your saved templates.

Type: Array of BackupPlanTemplatesListMember (p. 447) objects
**NextToken (p. 361)**

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. 490).

**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

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. 363)

Uniquely identifies a backup plan.

Required: Yes

MaxResults (p. 363)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 363)

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

{
   "BackupPlanVersionsList": [
       {
           "AdvancedBackupSettings": [
               {
                   "BackupOptions": {
                       "string": "string"
                   },
                   "ResourceType": "string"
               }
           ],
           "BackupPlanArn": "string",
           "BackupPlanId": "string",
           "BackupPlanName": "string",
           "CreationDate": number,
           "CreatorRequestId": "string",
           "DeletionDate": number,
           "LastExecutionDate": number,
           "string": "string"
       }
   ]
}
"VersionId": "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.

**BackupPlanVersionsList (p. 363)**

An array of version list items containing metadata about your backup plans.

Type: Array of BackupPlansListMember (p. 445) objects

**NextToken (p. 363)**

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. 490)](#).

**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

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. 366)**

Uniquely identifies a backup plan.

Required: Yes

**MaxResults (p. 366)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 366)**

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. 366)**

An array of backup selection list items containing metadata about each resource in the list.

Type: Array of BackupSelectionsListMember (p. 454) objects

**NextToken (p. 366)**

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. 490).

**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

Returns a list of recovery point storage containers along with information about them.

Request Syntax

```
GET /backup-vaults/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**MaxResults (p. 368)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 368)**

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. 368)*

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. 456)* objects

**NextToken** *(p. 368)*

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. 490).*

**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

Returns metadata about your copy jobs.

Request Syntax

GET /copy-jobs/?
accountId=ByAccountId&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&
destinationVaultArn=ByDestinationVaultArn&
maxResults=MaxResults&nextToken=NextToken&
resourceArn=ByResourceArn&resourceType=ByResourceType&
state=ByState

URI Request Parameters

The request uses the following URI parameters.

ByAccountId (p. 370)

The account ID to list the jobs from. Returns only copy jobs associated with the specified account ID.

Pattern: ^[0-9]{12}$

ByCreatedAfter (p. 370)

Returns only copy jobs that were created after the specified date.

ByCreatedBefore (p. 370)

Returns only copy jobs that were created before the specified date.

ByDestinationVaultArn (p. 370)

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.

ByResourceArn (p. 370)

Returns only copy jobs that match the specified resource Amazon Resource Name (ARN).

ByResourceType (p. 370)

Returns only backup jobs for the specified resources:
- DynamoDB for Amazon DynamoDB
- EBS for Amazon Elastic Block Store
- EC2 for Amazon Elastic Compute Cloud
- EFS for Amazon Elastic File System
- RDS for Amazon Relational Database Service
- Aurora for Amazon Aurora
- Storage Gateway for Storage Gateway

Pattern: ^[a-zA-Z0-9\-\_\.]\{1,50}$

ByState (p. 370)

Returns only copy jobs that are in the specified state.

Valid Values: CREATED | RUNNING | COMPLETED | FAILED

MaxResults (p. 370)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.
**NextToken (p. 370)**

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

{
  "CopyJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "CompletionDate": number,
      "CopyJobId": "string",
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "ResourceArn": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "SourceRecoveryPointArn": "string",
      "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.

**CopyJobs (p. 371)**

An array of structures containing metadata about your copy jobs returned in JSON format.

Type: Array of CopyJob (p. 466) objects

**NextToken (p. 371)**

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. 490).

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

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. 373)**

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. 373)**

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. 373)**

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. 469) objects

**NextToken (p. 373)**

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. 490).

**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

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. 375)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 375)**

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",
      "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. 375)**

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. 375)

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. 473) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

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
ListRecoveryPointsByBackupVault

Returns detailed information about the recovery points stored in a backup vault.

Request Syntax

```
GET /backup-vaults/{backupVaultName}/recovery-points/?
backupPlanId={backupPlanId}&createdAfter={createdAfter}&createdBefore={createdBefore}&maxResults={maxResults}&nextToken={nextToken}&resourceArn={resourceArn}&resourceType={resourceType}
```

HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 377)

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.

**Note**

Backup vault name might not be available when a supported service creates the backup.

Pattern: `^[a-zA-Z0-9\-_\ ]{2,50}$`

Required: Yes

ByBackupPlanId (p. 377)

Returns only recovery points that match the specified backup plan ID.

ByCreatedAfter (p. 377)

Returns only recovery points that were created after the specified timestamp.

ByCreatedBefore (p. 377)

Returns only recovery points that were created before the specified timestamp.

ByResourceArn (p. 377)

Returns only recovery points that match the specified resource Amazon Resource Name (ARN).

ByResourceType (p. 377)

Returns only recovery points that match the specified resource type.

Pattern: `^[a-zA-Z0-9\-_\.]\{1,50}\$

MaxResults (p. 377)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 377)

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",
  "RecoveryPoints": [
    {
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CalculatedLifecycle": {
        "DeleteAt": number,
        "MoveToColdStorageAt": number
      },
      "CompletionDate": number,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "IamRoleArn": "string",
      "IsEncrypted": boolean,
      "LastRestoreTime": number,
      "Lifecycle": {
        "DeleteAfterDays": number,
        "MoveToColdStorageAfterDays": number
      },
      "RecoveryPointArn": "string",
      "ResourceArn": "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. 378)**

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. 378)**

An array of objects that contain detailed information about recovery points saved in a backup vault.
Type: Array of [RecoveryPointByBackupVault](p. 474) objects

**Errors**

For information about the errors that are common to all actions, see [Common Errors](p. 490).

**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
ListRecoveryPointsByResource

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**

```
GET /resources/resourceArn/recovery-points/?maxResults=MaxResults&nextToken=NextToken
HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**MaxResults (p. 380)**

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. 380)**

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. 380)**

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**

```
HTTP/1.1 200
Content-type: application/json
{
    "NextToken": "string",
    "RecoveryPoints": [
        {
            "BackupSizeBytes": number,
            "BackupVaultName": "string",
            "CreationDate": number,
            "EncryptionKeyArn": "string",
            "RecoveryPointArn": "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. 380)

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. 380)

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. 478) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

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

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. 383)

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. 383)

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. 383)

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. 383)

Returns only report jobs that are in the specified status. The statuses are:

CREATED | RUNNING | COMPLETED | FAILED

MaxResults (p. 383)

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. 383)

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
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. 383)

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. 383)

Details about your report jobs in JSON format.

Type: Array of **ReportJob** (p. 483) objects

Errors

For information about the errors that are common to all actions, see **Common Errors** (p. 490).

**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
ListReportPlans

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. 386)

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. 386)

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": {
        "FrameworkArns": [ "string" ],
        "NumberOfFrameworks": number,
        "ReportTemplate": "string"
      }
    }
  ]
}

386
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. 386)

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. 386)

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. 485) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

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

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&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. 388)**

The account ID to list the jobs from. Returns only restore jobs associated with the specified account ID.

Pattern: `^[0-9]{12}$`

**ByCreatedAfter (p. 388)**

Returns only restore jobs that were created after the specified date.

**ByCreatedBefore (p. 388)**

Returns only restore jobs that were created before the specified date.

**ByStatus (p. 388)**

Returns only restore jobs associated with the specified job status.

Valid Values: `PENDING` | `RUNNING` | `COMPLETED` | `ABORTED` | `FAILED`

**MaxResults (p. 388)**

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

**NextToken (p. 388)**

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": [
```

388
ListRestoreJobs

```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.

**NextToken (p. 388)**

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. 388)**

An array of objects that contain detailed information about jobs to restore saved resources.

Type: Array of `RestoreJobsListMember (p. 488)` objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

**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

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. 391)

The maximum number of items to be returned.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken (p. 391)

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. 391)

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. 391)**

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. 391)**

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. 490).

**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

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. 393)**

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. 393)**

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. 490).

**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

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 yet to receive a third-party assessment for SEC 17a-4(f) and CFTC.

**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. 395)**

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. 395)**

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.

Type: Long
Required: No

**MaxRetentionDays (p. 395)**

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. Recovery points already saved in the vault prior to Vault Lock are not affected.

Type: Long

Required: No

**MinRetentionDays (p. 395)**

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 that backup or copy job, and you should either modify your lifecycle settings or use a different vault. Recovery points already saved in the vault prior to Vault Lock are not affected.

Type: Long

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. 490).

**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

Turns on notifications on a backup vault for the specified topic and events.

Request Syntax

```plaintext
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. 398)

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. 398)

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`

**Note**

Ignore the list below because it includes deprecated events. Refer to the list above.

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`

Required: Yes
SNSTopicArn (p. 398)

The Amazon Resource Name (ARN) that specifies the topic for a backup vault's events; for example,

Type: String

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. 490).

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
**StartBackupJob**

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. 401)

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. 401)

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
StartBackupJob

Pattern: ^[a-zA-Z0-9\-\_]{2,50}$

Required: Yes

**CompleteWindowMinutes (p. 401)**

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.

Type: Long

Required: No

**IamRoleArn (p. 401)**

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. 401)**

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. 401)**

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 “expire after days” 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the “Full AWS Backup management” section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 472) object

Required: No

**RecoveryPointTags (p. 401)**

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. 401)**

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.
StartBackupJob

Type: String
Required: Yes

StartWindowMinutes (p. 401)
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.
Type: Long
Required: No

Response Syntax

HTTP/1.1 200
Content-type: application/json

{
    "BackupJobId": "string",
    "CreationDate": 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.

BackupJobId (p. 403)
Uniquely identifies a request to AWS Backup to back up a resource.
Type: String

CreationDate (p. 403)
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

RecoveryPointArn (p. 403)
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

Errors
For information about the errors that are common to all actions, see Common Errors (p. 490).

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

Starts a job to create a one-time copy of the specified resource.

Does not support continuous backups.

Request Syntax

```
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. 405)**

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. 405)**

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. 405)**

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. 405)**

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 "expire after days" 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: `Lifecycle (p. 472)` object

Required: No

**RecoveryPointArn (p. 405)**

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-108B488B0D45`.

Type: String

Required: Yes

**SourceBackupVaultName (p. 405)**

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**

```json
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "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.

**CopyJobId (p. 406)**

Uniquely identifies a copy job.
Type: String

**CreationDate (p. 406)**

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

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 490)](https://docs.aws.amazon.com/backup/latest/developerguide/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

**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

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. 409)*

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. 409)*

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. 409)**

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. 490).

**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

Recovers the saved resource identified by an Amazon Resource Name (ARN).

Request Syntax

```plaintext
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
  "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.

**IamRoleArn** (p. 411)

The Amazon Resource Name (ARN) of the IAM role that AWS Backup uses to create the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

Type: String

Required: Yes

**IdempotencyToken** (p. 411)

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. 411)

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. 411)**

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. 411)**

Starts a job to restore a recovery point for one of the following resources:

• **DynamoDB** for Amazon DynamoDB
• **EBS** for Amazon Elastic Block Store
• **EC2** for Amazon Elastic Compute Cloud
• **EFS** for Amazon Elastic File System
• **RDS** for Amazon Relational Database Service
• **Aurora** for Amazon Aurora
• **Storage Gateway** for Storage Gateway

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. 412)*

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. 490)](#).

**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
StopBackupJob

Attempts to cancel a job to create a one-time backup of a resource.

Request Syntax

```plaintext
POST /backup-jobs/backupJobId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

- `backupJobId` (p. 414)
  - 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

```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. 490).

- `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

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. 416)*

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. 416)*

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. 490).*
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

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. 418)

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. 418)

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. 490).

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

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. 420)*

Uniquely identifies a backup plan.

Required: Yes
Request Body

The request accepts the following data in JSON format.

BackupPlan (p. 420)

Specifies the body of a backup plan. Includes a BackupPlanName and one or more sets of Rules.

Type: BackupPlanInput (p. 444) 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. 421)

Contains a list of BackupOptions for each resource type.

Type: Array of AdvancedBackupSetting (p. 438) objects

BackupPlanArn (p. 421)

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. 421)

Uniquely identifies a backup plan.

Type: String

CreationDate (p. 421)

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.
VersionId (p. 421)

Unique, randomly generated, Unicode, UTF-8 encoded strings that are at most 1,024 bytes long. Version Ids cannot be edited.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 490).

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

Updates an existing framework identified by its `FrameworkName` with the input document in JSON format.

Request Syntax

```plaintext
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. 423)**

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. 423)**

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. 471)` objects
Required: No

FrameworkDescription (p. 423)

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. 423)

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

HTTP/1.1 200
Content-type: application/json

```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. 424)

The date and time that a framework 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

FrameworkArn (p. 424)

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.
Type: String

FrameworkName (p. 424)

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. 490).

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

InvalidArgumentException

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

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

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. 427)


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. 490).

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

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 “expire after days” 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the “Full AWS Backup management” 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.

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 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. 429)

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-108B4888B0D45.

Required: Yes

Request Body

The request accepts the following data in JSON format.

Lifecycle (p. 429)

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 “expire after days” 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. 472) 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. 430)

An ARN that uniquely identifies a backup vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.

Type: String

CalculatedLifecycle (p. 430)

A CalculatedLifecycle object containing DeleteAt and MoveToColdStorageAt timestamps.

Type: CalculatedLifecycle (p. 459) object

Lifecycle (p. 430)

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 “expire after days” 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 472) object
**RecoveryPointArn (p. 430)**

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B6E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 490).

**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

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. 432)

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. 432)

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. 490).

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

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": {
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "ReportTemplate": "string"
  }
}
```

URI Request Parameters

The request uses the following URI parameters.

**reportPlanName (p. 434)**

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. 434)**

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. 434)**

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: \texttt{ReportDeliveryChannel} (p. 481) object

Required: No

\textbf{ReportPlanDescription (p. 434)}

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: \texttt{.*\S.*}

Required: No

\textbf{ReportSetting (p. 434)}

Identifies the report template for the report. Reports are built using a report template. The report templates are:

\texttt{RESOURCE\_COMPLIANCE\_REPORT} | \texttt{CONTROL\_COMPLIANCE\_REPORT} | \texttt{BACKUP\_JOB\_REPORT} | \texttt{COPY\_JOB\_REPORT} | \texttt{RESTORE\_JOB\_REPORT}

If the report template is \texttt{RESOURCE\_COMPLIANCE\_REPORT} or \texttt{CONTROL\_COMPLIANCE\_REPORT}, this API resource also describes the report coverage by AWS Regions and frameworks.

Type: \texttt{ReportSetting} (p. 487) object

Required: No

\section*{Response Syntax}

\begin{verbatim}
HTTP/1.1 200
Content-type: application/json

{
    "CreationTime": \texttt{number},
    "ReportPlanArn": \texttt{"string"},
    "ReportPlanName": \texttt{"string"}
}
\end{verbatim}

\section*{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.

\textbf{CreationTime (p. 435)}

The date and time that a report plan is created, in Unix format and Coordinated Universal Time (UTC). The value of \texttt{CreationTime} is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

\textbf{ReportPlanArn (p. 435)}

An Amazon Resource Name (ARN) that uniquely identifies a resource. The format of the ARN depends on the resource type.
Type: String

**ReportPlanName (p. 435)**

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. 490).

**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
Data Types

The following data types are supported:

- AdvancedBackupSetting (p. 438)
- BackupJob (p. 439)
- BackupPlan (p. 443)
- BackupPlanInput (p. 444)
- BackupPlansListMember (p. 445)
- BackupPlanTemplatesListMember (p. 447)
- BackupRule (p. 448)
- BackupRuleInput (p. 450)
- BackupSelection (p. 452)
- BackupSelectionsListMember (p. 454)
- BackupVaultListMember (p. 456)
- CalculatedLifecycle (p. 459)
- Condition (p. 460)
- ConditionParameter (p. 461)
- Conditions (p. 462)
- ControlInputParameter (p. 463)
- ControlScope (p. 464)
- CopyAction (p. 465)
- CopyJob (p. 466)
- Framework (p. 469)
- FrameworkControl (p. 471)
- Lifecycle (p. 472)
- ProtectedResource (p. 473)
- RecoveryPointByBackupVault (p. 474)
- RecoveryPointByResource (p. 478)
- RecoveryPointCreator (p. 480)
- ReportDeliveryChannel (p. 481)
- ReportDestination (p. 482)
- ReportJob (p. 483)
- ReportPlan (p. 485)
- ReportSetting (p. 487)
- RestoreJobsListMember (p. 488)
AdvancedBackupSetting

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

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
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}$

BytesTransferred

The size in bytes transferred to a backup vault at the time that the job status was queried.

Type: Long

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

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. 480) object

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

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

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

**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

**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 resource recovery point.

Type: String

Valid Values: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED  
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

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

AdvancedBackupSettings

Contains a list of BackupOptions for each resource type.

Type: Array of AdvancedBackupSetting (p. 438) objects

Required: No

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 (p. 448) objects

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
BackupPlanInput

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

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 objects

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 objects

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
BackupPlansListMember

Contains metadata about a backup plan.

Contents

AdvancedBackupSettings

Contains a list of BackupOptions for a resource type.

Type: Array of AdvancedBackupSetting (p. 438) 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.
**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

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

Specifies a scheduled task used to back up a selection of resources.

Contents

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. 465) 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 "expire after days" 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 472) 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.
BackupRule

Type: String
Required: No

**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

**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.

Type: Long
Required: No

**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

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

Specifies a scheduled task used to back up a selection of resources.

Contents

**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. 465) 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 "expire after days" 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 472) 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

**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

**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.

Type: Long

Required: No

**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

**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

Used to specify a set of resources to a backup plan.

Contents

Conditions

A list of conditions that you define to assign resources to your backup plans using tags. For example, "StringEquals": "Department": "accounting". 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. 462) object

Required: No

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

ListOfTags

A list of conditions that you define to assign resources to your backup plans using tags. For example, "StringEquals": "Department": "accounting". 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. 460) objects

Required: No

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

**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

**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
BackupSelectionsListMember

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

Contains metadata about a backup vault.

Contents

BackupVaultArn

An Amazon Resource Name (ARN) that uniquely identifies a backup vault; for example,

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

The server-side encryption key that is used to protect your backups; for example,

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**

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 “expire after days” 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" 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

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**

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

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. 461)` 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. 461)` 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. 461)` 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. 461)` 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
ControlInputParameter

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
ControlScope

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++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
CopyAction
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 “expire after days” 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 472) 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

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

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

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. 480) object

Required: No

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

Required: No

DestinationBackupVaultArn

An Amazon Resource Name (ARN) that uniquely identifies a destination copy vault; for example, arn:aws:backup:us-east-1:123456789012:vault:aBackupVault.
CopyJob

Type: String
Required: No

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
Required: No

IamRoleArn

Specifies the IAM role ARN used to copy the target recovery point; for example, arn:aws:iam::123456789012:role/S3Access.

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

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
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
Framework

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 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 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

Contains detailed information about all of the controls of a framework. Each framework must contain at least one control.

Contents

ControlInputParameters

A list of ParameterName and ParameterValue pairs.

Type: Array of ControlInputParameter (p. 463) objects

Required: No

ControlName

The name of a control. This name is between 1 and 256 characters.

Type: String

Required: Yes

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. 464) 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
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 "expire after days" 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the "Full AWS Backup management" 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

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

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

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\-\_]\d+$`

Required: No

CalculatedLifecycle

A `CalculatedLifecycle` object containing `DeleteAt` and `MoveToColdStorageAt` timestamps.

Type: `CalculatedLifecycle (p. 459)` 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

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. 480)` 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, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type: String

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

**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

**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 “expire after days” 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.

Only resource types that support full AWS Backup management can transition their backups to cold storage. Those resource types are listed in the “Full AWS Backup management” section of the Feature availability by resource table. AWS Backup ignores this expression for other resource types.

Type: Lifecycle (p. 472) object

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:1EB3B6E7-9EB0-435A-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

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

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

**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-108B488B0D45.

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

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, 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

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
ReportDeliveryChannel

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

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

S3BucketName

The unique name of the S3 bucket that receives your reports.

Type: String

Required: Yes

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

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

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. 482) 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

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: 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 for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
ReportPlan

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. 481) 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
**ReportPlan**

**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:** .*

**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]*

**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. 487) 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
Contains detailed information about a report setting.

Contents

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

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

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
**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
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

InvalidParameterCombination
Parameters that must not be used together were used together.
HTTP Status Code: 400

InvalidParameterValue
An invalid or out-of-range value was supplied for the input parameter.
HTTP Status Code: 400

InvalidQueryParameter
The AWS query string is malformed or does not adhere to AWS standards.
HTTP Status Code: 400

MalformedQueryString
The query string contains a syntax error.
HTTP Status Code: 404

MissingAction
The request is missing an action or a required parameter.
HTTP Status Code: 400
**MissingAuthenticationToken**

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403
**MissingParameter**

A required parameter for the specified action is not supplied.

HTTP Status Code: 400
**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 General Reference.
Document history for AWS Backup

The following table describes the documentation for this release of AWS Backup.

- **API version:** 2021-11-23
- **Latest documentation update:** November 23, 2021

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch of AWS Backup advanced features for Amazon DynamoDB</td>
<td>Now, you can use AWS Backup to copy your backups across AWS Regions and accounts, tier those backups to cold storage, tag backups for cost management, and use other AWS Backup advanced features with your DynamoDB backups. For more information, see Working with Amazon DynamoDB (p. 10). This feature is not yet available in China Regions.</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 Assigning resources to a backup plan.</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 Assigning resources to a backup plan.</td>
<td>November 10, 2021</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 What is AWS Backup?</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 What is AWS Backup?</td>
<td>November 5, 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 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 AWS Backup Vault Lock.</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 vault. For more information, see AWS Backup Vault Lock.</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 Compliance report templates.</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 Backup audit and reports with AWS Backup Audit Manager.</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 Backup audit and reports with AWS Backup Audit Manager.</td>
<td>August 24, 2021</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>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</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 <code>fsx:CopyBackup</code> 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>FedRAMP High Authorization</td>
<td>AWS Backup is now authorized to support FedRAMP High workloads. For more information, see AWS Services in Scope by Compliance Program.</td>
<td>March 25, 2021</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</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="https://docs.aws.amazon.com/backup/latest/devguide/ref_endpoints.html">AWS Backup endpoints and quotas</a> in the <em>AWS General Reference</em>.</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="https://docs.aws.amazon.com/backup/latest/devguide/ref_backups.html">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="https://docs.aws.amazon.com/efs/latest/developerguide/restore.html">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="https://docs.aws.amazon.com/backup/latest/devguide/restore.html">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="https://docs.aws.amazon.com/backup/latest/devguide/monitoring.html">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="https://docs.aws.amazon.com/backup/latest/devguide/monitoring.html">Monitoring Events and Metrics with Amazon CloudWatch and Amazon EventBridge</a>.</td>
<td>February 3, 2021</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 <a href="https://docs.aws.amazon.com/backup/latest/devguide/share_backup.html">Creating backup copies across AWS accounts</a>.</td>
<td>November 18, 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 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>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 Opt in to managing services with AWS Backup.</td>
<td>May 20, 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 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>