AWS Backup

Developer Guide

AWS Backup: Developer Guide

Table of Contents

What Is AWS Backup?

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

AWS Backup provides a fully managed backup service and a policy-based backup solution that simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Supported Resources

The following are AWS resources that you can back up and restore using AWS Backup.

Supported Service	Supported Resource
Amazon Elastic File System (Amazon EFS)	Amazon EFS file systems
Amazon DynamoDB	DynamoDB tables
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon EC2 instances*
Amazon Elastic Block Store (Amazon EBS)	Amazon EBS volumes
Amazon Relational Database Service (Amazon RDS)	Amazon RDS databases**
Amazon Aurora	Aurora clusters
AWS Storage Gateway (Volume Gateway)	AWS Storage Gateway volumes

*AWS Backup does not support Amazon EC2 instance store-backed instances.

**AWS Backup currently supports all Amazon RDS database engines, including Amazon Aurora.

AWS Backup Overview

AWS Backup provides the following features and capabilities.

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.

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.

Cross-Account Management

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.

Before you can use the cross-account management feature, 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.

For more information about cross-account management, see Managing AWS Backup Resources Across Multiple AWS Accounts (p. 44).

Policy-Based Backup Solutions

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.

Tag-Based Backup Policies

You can use AWS Backup to apply backup plans to your AWS resources by 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.

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 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.

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.

Currently only Amazon EFS file system backups can be transitioned to cold storage. The cold storage expression is ignored for the backups of Amazon EBS, Amazon RDS, Amazon Aurora, Amazon DynamoDB, and AWS Storage Gateway.

Backup Access Policies

AWS Backup offers resource-based access policies for your backup vaults to 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, helping you meet your compliance requirements.

Getting Started

To learn more about AWS Backup, we recommend that you start with the following sections:

- AWS Backup: How It Works (p. 4)
- Getting Started with AWS Backup (p. 12) AWS Backup Developer GuideAPI_Operations.html

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 Other AWS Services

Many AWS services offer backup features that help you protect your data. These features include Amazon Elastic Block Store (Amazon EBS) snapshots, Amazon Relational Database Service (Amazon RDS) snapshots, Amazon DynamoDB backups, and AWS Storage Gateway snapshots.

AWS Backup implements its backup features using the existing capabilities of other services.

Topics

Configuring Services to Work 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

1. Open the AWS Backup console at https://console.aws.amazon.com/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.

AWS Backup uses existing backup capabilities of AWS services to implement its centralized features. For example, when you create a backup plan, AWS Backup uses the EBS snapshot capabilities when creating backups on your behalf according to your backup plan.

All per-service backup capabilities continue to be available. For example, you can make snapshots of your EBS volumes using the Amazon Elastic Compute Cloud (Amazon EC2) API. AWS Backup provides a common way to manage backups across AWS services both in the AWS Cloud and on premises. AWS Backup provides a centralized backup console that offers backup scheduling, retention management, and backup monitoring.

> **Note**
> Backups created with AWS Backup cannot be deleted with APIs belonging to the backed-up resource. For information about deleting recovery points using the AWS Backup API, see DeleteRecoveryPoint (p. 110).

For more information about how AWS Backup works with other AWS services, see the following:

- 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
- Backing Up Your Volumes in AWS Storage Gateway

Working with Amazon EC2

Using AWS Backup, you can schedule or perform on-demand backup jobs that include entire EC2 instances, along with associated configuration data. This limits the need for you to interact with the storage (Amazon EBS) layer. Similarly, you can restore an entire Amazon EC2 instance from a single recovery point. A 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.

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 AMI (Amazon Machine Image).

AWS Backup will 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.

Restoring Amazon EC2 Resources

You can restore Amazon EC2 resources using the AWS Backup console, AWS Command Line Interface (AWS CLI), or API.

The console provides an interactive user interface for restoring resources, but its functionality is limited. Currently, you can't use the AWS Backup console to configure the following restore parameters.

```
NetworkInterfaces = [{
 "AssociatePublicIpAddress": true,
 "DeleteOnTermination": false,
 "Description": "test network interface",
 "DeviceIndex": 1,
 "Groups": ["your nic_groups_id"],
 "Ipv6AddressCount": 1,
 "Ipv6Addresses": [{
  "Ipv6Address1": "ipv6_address2"
 }],
 "NetworkInterfaceId": "your nic_interface_id",
 "PrivateIpAddress": "your private_ip_address",
 "PrivateIpAddresses": [{
  "Primary": true,
  "PrivateIpAddress": "private_ip_address_1"
 }, {
  "Primary": false,
  "PrivateIpAddress": "private_ip_address_2"
 }],
 "SecondaryPrivateIpAddressCount": 1,
 "SubnetId": "nic_subnet_id",
 "InterfaceType": "interface"
}],
```

```
ElasticGpuSpecification = [{
 "Type": "test_elastic_gpu_type"
}],
```

```
CapacityReservationSpecification = {
 "CapacityReservationPreference": "none"
},
```

```
InstanceMarketOptions = {
 "MarketType": "spot",
 "SpotOptions": {
  "MaxPrice": "test_spot_price_value",
  "SpotInstanceType": "persistent",
  "BlockDurationMinutes": 20,
  "ValidUntil": "2019-12-16T12:34:56.000Z",
  "InstanceInterruptionBehavior": "hibernate"
 }
},
```

```
LicenseSpecifications = [{
 "LicenseConfigurationArn": "your_license_configuration_arn"
}],
```

However, you can use the AWS CLI and the API to perform a full restore. For more information about restore parameters, see run-instances.

All the restore configurations for an EC2 instance should be provided as restore metadata, which is a map of key-value pairs. The key is the name of the configuration, and value as is a JSON serialized string.

> **Note**
> When restoring a backup, AWS Backup doesn't allow mutation of the SSH key pair, so you can only restore using a backed-up key pair.
> AWS Backup doesn't allow you to modify the instance profile to prevent the possibility of privilege escalations. You can choose not to apply this from AWS Backup, but if you want to change it, you can apply it from 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.

> **Note**
> When you are restoring from AWS Backup, all quotas and restrictions of the configuration that can be used to launch an instance from an EC2 run instance API apply.

Working with Amazon EFS

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

For information, see Getting Started with Amazon Elastic File System in the *Amazon Elastic File System User Guide*.

Working with Amazon DynamoDB

AWS Backup currently supports Amazon DynamoDB (DynamoDB).

For information, see Getting Started with DynamoDB in the *Amazon DynamoDB Developer Guide*.

Working with Amazon EBS

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

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

For information about Amazon EBS, see Amazon Elastic Block Store (Amazon EBS).

Working with Amazon RDS and Amazon Aurora

AWS Backup currently supports Amazon RDS database engines and Aurora clusters.

For information on Amazon RDS, see Getting Started with Amazon RDS in the *Amazon RDS User Guide*.

For information about backing up and restoring Aurora clusters, see Overview of Backing Up and Restoring an Aurora DB Cluster in the *Amazon Aurora User Guide*.

Working with AWS Storage Gateway

Amazon EBS snapshots can be restored as AWS Storage Gateway volumes. For information about restoring resources, see Working with Backups (p. 32).

Cross-Region Backups

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.

You can use the AWS Backup console, the AWS Command Line Interface (AWS CLI), or the AWS Backup API to copy your backups for the following resources, defining different backup lifecycles in different Regions as appropriate:

- Amazon Elastic File System (Amazon EFS) file systems

  Note
  Copy rules are at the plan level. If you want to apply a different copy rule to a subset of file systems, you should create a new plan.
- Amazon Elastic Block Store (Amazon EBS) volumes
- Amazon Relational Database Service (Amazon RDS) databases and Amazon Aurora clusters
- AWS Storage Gateway volumes

You can also recover from backups stored in different Regions. For information about creating copies, see Creating a Backup Copy (p. 34).

Cross-Region backups are available in all AWS Regions that are available in AWS Backup except Asia Pacific (Hong Kong) and Middle East (Bahrain).

Important
To avoid additional charges, we recommend against setting aggressive backup, copy, and retention policies. Aggressive backup, copy, and retention policies can incur additional costs when a process experiences delays. For example, such delays might cause the backup in the destination region to be lifecycled before incremental backups of the source are taken. This would cause you to incur full backup copy and storage costs. We highly recommend a retention policy that is not more frequent than a weekly cadence, because of the potential occurrences described above. Contact your technical account manager or solutions architect for specific guidance.

How Cross-Account Management Works

Using AWS Backup, you can manage your backups across all your AWS accounts within AWS Organizations. With cross-account management, you can use backup policies to automatically apply backup plans across your accounts. You can also create a backup policy that uses tag-based resource selections, and apply it to all the accounts in your organization, or to individual accounts to protect their local resources.

To manage your protected resources across AWS accounts, you need a master account in AWS Organizations. For information about how AWS Organizations works, see AWS Organizations terminology and concepts in the *AWS Organizations User Guide*. An *organizational unit* (OU) is a layer of hierarchy that organizes member accounts in the organization. You can also invite existing AWS accounts

to join your organization. You can create a backup policy that uses tag-based resource selections and apply it to all the accounts in your organization. You can also apply it to individual accounts to protect their local resources using this policy.

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 correspondent 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 one effective 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 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, Policies Syntax, and Policy Inheritance (p. 48) in the *AWS Organizations User Guide*. For more information about cross-account management, see Managing AWS Backup Resources Across Multiple AWS Accounts (p. 44).

Metering Backup and Pricing Usage

Backup usage for existing backup capabilities (except Amazon EFS) will continue to be metered and billed by their respective service, and the pricing remains unchanged. There is no additional charge to use the AWS Backup centralized backup features beyond the existing backup storage pricing charged by AWS services, such as Amazon EBS snapshot storage fees. There is no additional charge for Amazon EC2 instance backups.

For services that introduce backup capabilities on AWS Backup, such as Amazon EFS, backup usage is metered and billed by AWS Backup. For more information, see AWS Backup pricing.

Important
To avoid additional charges, we recommend against setting aggressive backup, copy, and retention policies. Aggressive backup, copy, and retention policies can incur additional costs when a process experiences delays. For example, such delays might cause the backup in the destination region to be lifecycled before incremental backups of the source are taken. This would cause you to incur full backup copy and storage costs. We highly recommend a retention policy that is not more frequent than a weekly cadence, because of the potential occurrences described above. Contact your technical account manager or solutions architect for specific guidance.

AWS Backup Blogs, Videos, and Other Resources

For more information about AWS Backup, including benefits, use cases, blogs, and videos, see the following:

- Video: AWS Backup
- Blog: Protecting your data with AWS Backup

Setting Up

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

1. Sign up for AWS (p. 10)
2. Create an IAM User (p. 10)

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 are a new AWS customer, you can get started with AWS Backup for free. For more information, see AWS Free Usage Tier.

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

1. Open https://portal.aws.amazon.com/billing/signup.
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 administrator 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.

Note
We strongly recommend that you adhere to the best practice of using the **`Administrator`** IAM user below 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.

Getting Started with AWS Backup

This tutorial shows you how to perform the tasks necessary to back up and restore your resources using AWS Backup.

Topics

Prerequisites

Before you begin, ensure that you have the following:

- An AWS account. For more information, see Setting Up (p. 10).
- An Amazon Elastic Block Store (Amazon EBS) volume. For more information, see Creating an Amazon EBS Volume in the *Amazon EC2 User Guide for Linux Instances*.

  For information about Amazon EBS, see Amazon Elastic Block Store (Amazon EBS).
- You should be familiar with the services and resources that you are backing up.

  AWS Backup currently supports the following services:
  - Amazon Elastic Compute Cloud (Amazon EC2)

    For information, see Getting Started with Amazon EC2 Windows Instances in the *Amazon EC2 User Guide for Windows Instances* or Getting Started with Amazon EC2 Linux Instances in the *Amazon EC2 User Guide for Linux Instances*.
  - Amazon Elastic File System (Amazon EFS)

    For information, see Getting Started with Amazon Elastic File System in the *Amazon Elastic File System User Guide*.
  - Amazon DynamoDB

    For information, see Getting Started with DynamoDB in the *Amazon DynamoDB Developer Guide*.
  - Amazon Relational Database Service (Amazon RDS) and Amazon Aurora

    For information on Amazon RDS, see Getting Started with Amazon RDS in the *Amazon RDS User Guide*.

    For information on Amazon Aurora, see Overview of Backing Up and Restoring an Aurora DB Cluster in the *Amazon Aurora User Guide*.
  - AWS Storage Gateway

    For information, see Creating a Volume Gateway in the *AWS Storage Gateway User Guide*.

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

To configure the services used with AWS Backup

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/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 used with AWS Backup. Choose **Confirm** when your services are configured.

   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 Option 3: Create Automatic Backups (p. 17). To disable automatic backups, use the Amazon EFS console or API.

- AWS resources that you're backing up should be in the Region that you're using for this tutorial. Your resources must all be in the same AWS Region. This tutorial uses the US East (N. Virginia) Region (us-east-1).

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 (p. 10).

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.

Option 1: 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

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
2. From the dashboard, choose **Create on-demand backup**. Or, 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; 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. Specify a transition to cold storage value (if appropriate) and an expire value.

   Note

   - Only Amazon EFS backups support transition to cold storage. All other resource types are saved to warm storage. 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 24 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
   When creating a tag-based backup plan, if you choose a role other than **Default role**, make sure that it has the necessary permissions to back up all tagged resources. AWS Backup tries to process all resources with the selected tags. If it encounters a resource that it doesn't have permission to access, the backup plan fails.
10. Choose **Create on-demand backup**. This takes you to the **Jobs** page, where you will see a list of jobs.
11. Choose the **Backup job ID** for the resource that you chose to back up to see the details of that job.

Next Steps

To verify the status and monitor the details of your backup activity, proceed to Option 2: Create a Scheduled Backup (p. 14).

Option 2: 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. 12).

Topics

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. 23).

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

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
2. From the dashboard, choose **Manage Backup plans**. Or, using the navigation pane, choose **Backup plans**.
3. 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 radio button for the backup rule and then choose **Edit**. 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.
5. For the backup vault, choose **Default**.
6. When you have finished editing the rule, choose **Save**.

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

Step 2: Assign Resources to a Backup Plan

To apply backup plans to your AWS resources, you choose a backup plan and assign resources to it by using tags or listing the resource IDs directly. For more information about resources, see Assigning Resources to a Backup Plan (p. 26).

Note
If you are protecting more than 100 resources in a plan, we recommend that you use tag-based management.

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. You can create multiple resources from several or all of the supported services. These resources can include the following:

- DynamoDB tables
- Amazon EBS volumes
- Amazon EC2 instances
- Amazon EFS file systems
- Amazon RDS instances and Amazon Aurora clusters
- AWS Storage Gateway volumes

Note
To assign resources by tags, you must apply tags to your resources. For example, you might want to tag all of the resources for this exercise with the key-value pair of `BackupPlan:MissionCritical`.

To assign resources to a backup plan

1. On the AWS Backup console dashboard, choose **Manage Backup plans**. Or, using the navigation pane, choose **Backup plans**.
2. Choose a plan from the list; for example, `Daily-Monthly-1yr-Retention`.

3. On the plan summary page, choose **Assign resources**.
4. In the **Resource assignment name** field, choose a name for the resource assignment.

   For example, you can name your resource selection, **`ApplicationFoo`**. You can then assign all the AWS resources used for this application, which might be a mix of Amazon EBS volumes, Amazon EFS file systems, and Amazon RDS tables.
5. 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.
   If you choose a role other than **Default role**, the role name must include either the string **AwsBackup** or **AWSBackup**. Role names without one of those strings don't have sufficient permissions to perform the operation. Also, make sure that your custom role has the necessary permissions to back up all tagged resources. For more information, see Assigning Resources to a Backup Plan (p. 26).
6. In the **Assign resources** section, ensure that the **Assign by** control displays **Tags**. Enter a key and value that your resources are tagged with; for example, **`BackupPlan:MissionCritical`**. Choose **Add assignment** to add all resources that are tagged with your chosen key-value pair.

   Note
   When creating a tag-based backup plan, if you choose a role other than **Default role**, make sure that it has the necessary permissions to back up all tagged resources. AWS Backup tries to process all resources with the selected tags. If it encounters a resource that it doesn't have permission to access, the backup plan fails.

   Any supported resource in the selected Region that is tagged with this key-value pair is automatically assigned to this backup plan.
7. When a new **Assign by** control appears below your first resource assignment, change the value to **`Resource ID`**.
8. Choose the resource type that you want to add to your selection, for example, **EBS**. Place your cursor in the **Volume ID** field, and the available resources for this type will appear.
9. Choose a resource from the list, and then choose **Add assignment**.
10. When you have finished adding resources, choose **Assign resources**.

You then return to the plan summary page, which contains information about your backup plan, your backup rules, your resource assignments, and any backup plan tags.

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. 28).

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 KMS key. You can use either a key that you already created, or select the default AWS Backup master key.

   Note
   The AWS KMS key that is specified here applies only to backups of services that support AWS Backup encryption. Currently only Amazon Elastic File System (Amazon EFS) is supported.
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 verify the status and monitor the details of your backup activity, proceed to Monitor Your Backup Jobs and Verify That Your Resources Are Protected (p. 17).

Option 3: Create 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, select the file system that you want to turn automatic backups on for.
3. Choose **Edit** in the General settings panel.
4. To turn automatic backups on, select **Enable automatic backups**.

   Note
   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.

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 Service-Linked Roles for AWS Backup (p. 67).

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*.

Monitor Your Backup Jobs and Verify That Your Resources Are Protected

AWS Backup enables you to 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

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

To view backup job status

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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.

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

After monitoring and verifying the backups for your resource, proceed to Restore a Backup (p. 19).

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

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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.

   Amazon Elastic Block Store (Amazon EBS)

   For example, if you are restoring an Amazon EBS snapshot, you can choose to restore the snapshot as an EBS volume or as an AWS Storage Gateway volume. This is because AWS Backup integrates with both services, and any Amazon EBS snapshot can be restored to either an EBS volume or an AWS Storage Gateway volume.

   For more information about restoring with Amazon EBS, see Replacing an Amazon EBS volume using a previous snapshot in the *Amazon EC2 User Guide for Linux Instances*.

   Amazon Elastic File System (Amazon EFS)

   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 an **Item-level restore**.

   For more information, including restoring an Amazon EFS recovery point to a different directory in case of a disaster recovery situation, see the *Restore a Recovery Point* section in Using AWS Backup with Amazon EFS.

   Full restore

   To perform a full restore, follow the instructions at Using AWS Backup with Amazon EFS in the *Amazon EFS User Guide*.

   Item-level restore

   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, wildcards, and regex strings.

   For more information, see the *Restore a Recovery Point* section in Using AWS Backup with Amazon EFS.

AWS Storage Gateway

To restore a Storage Gateway volume using AWS Backup, see Backing Up Your Volumes in the *AWS Storage Gateway User Guide*.

Amazon RDS and Amazon Aurora

To restore an Amazon RDS database using AWS Backup, see Backing Up and Restoring an Amazon RDS DB Instance in the *Amazon RDS User Guide*.

To restore an Aurora cluster using AWS Backup, see Overview of Backing Up and Restoring an Aurora DB Cluster in the *Amazon Aurora User Guide*.

DynamoDB

To restore a DynamoDB table, see Restoring a DynamoDB Table from a Backup in the *Amazon DynamoDB Developer Guide*.

Amazon Elastic Compute Cloud (Amazon EC2)

To restore an Amazon EC2 instance, see Replacing an Amazon EBS volume using a previous snapshot in the *Amazon EC2 User Guide for Windows Instances*.

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 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 a specific resource, see Restoring a Backup Using the Console (p. 36).

For detailed information about restore, see Restoring a Backup (p. 35).

Next Steps

After you verify your restore results, we recommend that you delete any AWS resources that you don't need to keep, so as not to incur unnecessary charges. For more information, see Clean Up Resources (p. 21).

Clean Up Resources

After you perform all the tasks in Getting Started with AWS Backup (p. 12), you might want to clean up what you have created to avoid incurring any unnecessary charges.

Topics

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 refers to restored resources, not 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. You must delete all resource assignments for a backup plan before the plan can be deleted.

Follow these steps to delete a backup plan:

To delete a backup plan

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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. Choose the recovery points and delete them one by one.

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**.

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.

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

Topics

Creating a Backup Plan

When you create a backup plan, it is added to the set of plans in your account. You can also use the AWS CloudFormation template to create a backup plan. For information, see AWS Backup Resource Type Reference in the *AWS CloudFormation User Guide*.

Topics

Creating Backup Plans Using the AWS Management Console

AWS Backup provides two 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. Be aware that backup plans created by AWS Backup are based on backup 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. 14) 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, as described in the next section. You can choose from the recommended default configurations.

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

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.

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

Backup Rules

Backup plans are composed of one or more backup rules. Each backup rule consists of the following elements.

Backup Rule Name

Backup rule names are case sensitive. They must contain from 1 to 63 alphanumeric characters or hyphens.

Backup Frequency

The backup frequency determines how often a backup is created. You can choose a frequency of every 12 hours, daily, weekly, or monthly. When selecting weekly, you can specify which days of the week you want backups to be taken. When selecting monthly, you can choose a specific day of the month.

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. For more information about cron expressions, see Schedule Expressions for Rules in the *Amazon CloudWatch Events User Guide*.

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

- Currently only Amazon EFS file system backups can be transitioned to cold storage. The cold storage expression is ignored for the backups of Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB, and AWS Storage Gateway.
- 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 24 hours. This 24-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. 16).

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 Cross-Region Backups (p. 8).

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

Destination Region

The destination Region for the backup copy.

(Advanced Settings) Backup Vault

The destination backup vault for the copy.

(Advanced Settings) IAM Role

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

(Advanced Settings) Lifecycle

Specifies when to transition the backup copy to cold storage and when to expire (delete) the copy. Backups transitioned to cold storage must be stored in cold storage for a minimum of 90 days. You can't change this value after a copy has transitioned to cold storage.

Expire specifies the number of days after creation that the copy is deleted. This must be greater than 90 days beyond the **Transition to cold storage** value.

Note
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 24 hours. This 24-hour window helps ensure consistent performance for deletion.

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.

Assigning Resources to a Backup Plan

When you assign a resource to a backup plan, that resource is backed up automatically according to the backup plan. The backups for that resource are managed according to the backup plan. You can assign resources using tags or resource IDs.

> **Note**
> If you are protecting more than 100 resources in a plan, we recommend that you use tag-based management.

Using tags to assign resources is a simple and scalable way to back up multiple resources. Any resources with the tags that you specify in the resource assignment are assigned to the backup plan. For example, if you include the tag values "`July`" and "`August`," your backup will include all resources tagged with the selected months.

For example, you can define a backup plan that meets your backup requirements for mission critical data and create a resource assignment with the tag key "`Classification`" and tag value "`MissionCritical`." Then any of your resources with that tag are automatically assigned to your mission critical backup plan.

> **Note**
> When creating a tag-based backup plan, if you choose a role other than **Default role**, make sure that it has the necessary permissions to back up all tagged resources. AWS Backup tries to process all resources with the selected tags. If it encounters a resource that it doesn't have permission to access, the backup plan fails.

For step-by-step instructions for assigning resources to a backup plan, see Step 2: Assign Resources to a Backup Plan (p. 15) in the Getting Started section.

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.

To delete a backup plan using the AWS Backup console

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
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

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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 you organize your backups in. 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. If you require different encryption keys or access policies for different groups of backups, you can optionally create multiple backup vaults. Otherwise, you can have all your backups organized in the default backup vault.

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

Topics

Creating a Backup Vault

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

For step-by-step instructions for creating a backup vault, see Step 3: Create a Backup Vault (p. 16) in the Getting Started guide.

When creating a backup vault, you can define the following elements.

Backup Vault Name

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

KMS Encryption Master Key

The AWS KMS encryption master key is used to protect your backups in this backup vault. By default, AWS Backup creates a master 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 master encryption key by going to the **Encryption keys** section of the AWS Identity and Access Management (IAM) console. For more information, see Creating Keys in the *AWS Key Management Service Developer Guide*.

After you create a backup vault and set the AWS KMS encryption master 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 (p. 50) 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 and Recovery Points

With AWS Backup, you can assign a policy to a role, user, or group that restricts access 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 use the following example policies as a guide to limit access to resources when you are working with AWS Backup vaults.

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. 54) for resource-specific recovery point ARNs.

Note
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

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

```
{
    "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",
                "backup:DescribeRecoveryPoint"
            ],
            "Resource": ["arn:aws:ec2:Region::snapshot/*"]
        }
    ]
}
```

Note
This access policy only controls 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 in order to fully control the access to backups.

Deny Access to a Backup Vault

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

```
{
    "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:ListRecoveryPointsByBackupVault"
            ],
            "Resource": "arn:aws:backup:Region:Account ID:backup-vault:backup vault name"
        }
    ]
}
```

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

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
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*, *Account ID*, and principal type (*role/MyRole*) with values for your environment.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "statement ID",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "aws:userId": [
                        "arn:aws:iam::Account ID:role/MyRole""
                    ]
                }
            }
        }
    ]
}
```

For information about getting a unique ID for an IAM entity, see Getting the Unique ID.

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:

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

5. Choose **Attach policy**.

Deleting a Backup Vault

You can delete a backup vault in AWS Backup only after all associated backups have been deleted.

To delete a backup vault using the AWS Backup console

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
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, and then choose **Delete**.

Note
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.

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.

In AWS Backup, recovery points are saved 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 2016. 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 the AWS resource types that AWS Backup supports and examples of their corresponding recovery point ID.

Resource Type	Backup Name	Recovery Point ID Example
Amazon Elastic Compute Cloud (Amazon EC2) instance	Amazon EC2 backup	`image/ami-0ecdf967356c809c7`
Amazon EBS volume	Amazon EBS snapshot	`snapshot/snap-05f426fd8kdjb4224`
Amazon RDS database	Amazon RDS snapshot	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Amazon Aurora DB cluster	Aurora clusters	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Amazon EFS file system	Amazon EFS backup	`d99699e7-e183-477e-bfcd-ccb1c6e5455e`
DynamoDB table	DynamoDB backup	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`
AWS Storage Gateway volume	Amazon EBS snapshot*	`snapshot/snap-0d40e49137e31d9e0`

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

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

Topics

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. 23).

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. 23).

Topics

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

1. Open the AWS Backup console at https://console.aws.amazon.com/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 using Amazon EBS, DynamoDB, Amazon RDS, or Amazon Aurora the **Transition to cold storage** value is marked **N/A** because these resource types cannot be saved to cold storage.

   If you're using Amazon EFS, choose the desired value to specify when this backup is transitioned to cold storage.
7. Choose an **Expire** value.

   Note
   When backups expire and are marked for deletion as part of your lifecycle policy, AWS Backup deletes the backups at a randomly chosen point over the following 24 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
    Adding tags to a backup using AWS Backup console is only supported for backups of Amazon Elastic File System (Amazon EFS) file systems. You can edit the tags of other backups using the service's console or API.
11. Choose **Create on-demand backup**. This takes you to the **Jobs** page, where you will see a list of jobs.
12. Choose the **Backup job ID** for the resource that you chose to back up to see the job details.

Copying Tags onto Backups

The tags that are assigned to your resources can be associated with your recovery points that are stored in backup vaults. Tags are automatically assigned to your backups with the following exceptions:

- DynamoDB does not support assigning tags to backups.
- 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. Tags that are assigned during backup have priority, and both sets of tags are selected in alphabetical order.
- 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. 56).

If you copy your backup to another AWS Region, AWS Backup copies all tags of the original backup to the destination AWS Region.

Creating a Backup Copy

You can copy backups to multiple AWS Regions on demand or automatically as part of a scheduled backup plan. For more information about backup plans, see Creating a Backup Plan (p. 23).

Note
AWS Backup doesn't support option groups when you are copying Amazon RDS databases.

To copy an existing backup on-demand

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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.

Note
Copying Amazon DynamoDB tables across AWS Regions is not supported.

(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.

Currently only Amazon EFS file system backups can be transitioned to cold storage. The cold storage expression is ignored for the backups of Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB, and AWS Storage Gateway.

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 24 hours. This window helps ensure consistent performance.

6. Choose **Create backup copy**.

For information about applying tags to your backup copy, see Copying Tags onto Backups (p. 34).

When you copy a backup to a new AWS Region for the first time, AWS Backup copies the backup in full. If a service supports incremental backups, subsequent copies of that backup in the same AWS Region will be incremental.

Note
Backup copies are automatically be encrypted for all supported resources.

Restoring a Backup

When you restore a backup in AWS Backup, a new resource is created based on 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 Restore a Backup (p. 19) in the Getting Started section.

For step-by step restore instructions for each service when using the AWS Backup console, see Restoring a Backup Using the Console (p. 36).

Topics

Restoring a Backup Using the Console

After a resource has been backed up at least once, it is considered protected and is available to be restored using AWS Backup. The restore parameters you use are specific to the resource type that is backed up. You can restore any of the resources AWS Backup supports.

Topics

Restoring an Amazon EBS Volume

If you are restoring an Amazon Elastic Block Store (Amazon EBS) snapshot, you can choose to restore the snapshot as an EBS volume or as an AWS Storage Gateway volume. This is because AWS Backup integrates with both services, and any Amazon EBS snapshot can be restored to either an EBS volume or an AWS Storage Gateway volume.

To restore an Amazon EBS volume

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
2. In the navigation pane, choose **Protected resources** and then 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 the **Gateway** you want to restore to and enter the **iSCSI target name**.
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.

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.

Item-Level Restore

When you perform an item-level restore, AWS Backup restores a specific file or directory. You must specify the relative path related to the mount point. For example, if the file system is mounted to `/user/home/myname/efs` and the file path is `user/home/myname/efs/file1`, you enter **`/file1`**. Paths are case sensitive. Wildcards and regex strings are not supported.

You can restore those items to either a new or 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 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.

To restore an Amazon EFS file system

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
2. In the navigation pane, choose **Protected resources** and the EFS 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.

   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 filesystem 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, wildcards, 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 Elastic File System.

5. For **Restore location**

   - Choose the **Restore to directory in source file system** option, if you want to restore to the source file system.
   - Choose the **Restore to a new file system** option, if you want to restore to a different file system.
     - (Recommended) For **Performance**, choose **General purpose**.
     - Choose **Enable encryption**, if you want to encrypt your file system. Master key ID's and aliases appear in the list after they have been created using the AWS Key Management Service (AWS KMS) console.
     - In the **Master key** text box, choose the key you want to use from the list.

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
   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.

Restoring an Amazon DynamoDB Database

To restore a DynamoDB database

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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 **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.

6. 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.

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*.

To restore an Amazon RDS database

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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.
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 **Master 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.

Restoring an Amazon Aurora Cluster

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

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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 (VPN)**, **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.

Restoring an Amazon EC2 instance

Restoring an Amazon EC2 instance requires that you specify multiple restore options. For information about these options, see What is Amazon EC2? in the *Amazon EC2 User Guide for Windows Instances*.

You can also select the **Info** link next to a restore option to display help information including links to specific pages in the *Amazon EC2 User Guide for Windows Instances*.

To restore an Amazon EC2 instance

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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 when creating and managing backups on your behalf.
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.

Restoring a Backup Using the AWS CLI or the AWS Backup API

To restore a backup using the AWS Command Line Interface (AWS CLI) or the AWS Backup API, you typically pass configuration information for your resource to the StartRestoreJob (p. 196) 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. 152), but you might need more information to restore your resource. Each service requires different configuration values to restore a recovery point.

Amazon EFS Restore Metadata

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`.
- `ItemsToRestore` — A serialized list 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.
- `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. For more information about restoring to a new or existing file system, see the note in the previous section, Restoring a Backup Using the Console (p. 36).

For more information about Amazon EFS configuration values, see create-file-system.

Amazon EC2 Restore Options

You can restore an Amazon EC2 instance using the AWS Backup console, the SDK, or the AWS CLI.

When using the console, you have the following two options:

Restore with default settings

This is the recommended option. This option restores an Amazon EC2 instance with the parameters and settings that can be customized on the console. These parameters include the following:

- Instance type
- Amazon VPC
- Subnet
- Security groups
- IAM role
- Shutdown behavior
- Stop–hibernate behavior
- Termination protection
- T2/T3 unlimited
- Placement group name
- EBS-optimized instance

- Tenancy
- RAM disk ID
- Kernel ID
- User data
- Deletion on termination

These parameters are prefilled to match the original backup. You can change them before restoring the instance. AWS Backup identifies parameters with values that might not be valid or that might result in an invalid restore.

Major restore

This option restores all 38 parameters, including the 22 parameters that are not customizable on the console. This is suitable if you require all 38 parameters and are comfortable restoring parameters without validation or customization.

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.

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 abort a backup job using the AWS Backup console

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
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**.

Viewing a List of Backups

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

Follow these steps to view a list of backups of a particular resource on the AWS Backup console.

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
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.

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
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.

Currently only Amazon EFS file system backups can be transitioned to cold storage. The cold storage expression is ignored for the backups of Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB, and AWS Storage Gateway.

> **Note**
> Editing the tags of a backup using AWS Backup is only supported for backups of Amazon Elastic File System (Amazon EFS) file systems. You can still edit the tags of other services' backups using the service's console or API.

Backups that are transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, the "expire after days" setting must be 90 days greater than the "transition to cold after days" setting. When you update the "transition to cold after days" setting, the value must be a minimum of the backup's age plus one day. The "transition to cold after days" setting cannot be changed after a backup has been transitioned to cold.

The following is an example of how to update the lifecycle of a backup.

To edit the lifecycle of a backup

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.
2. In the navigation pane, choose **Backup vaults**.
3. In the **Backups** section, choose a backup.
4. On the backup details page, choose **Edit**.
5. Configure the lifecycle settings, and then choose **Save**.

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 master 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 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 do this from the AWS Backup console or the AWS Command Line Interface (AWS CLI). 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 master account.

The cross-account management feature is not available in the following AWS Regions:

- Middle East (Bahrain)
- Asia Pacific (Hong Kong)
- AWS GovCloud
- China (Beijing)
- China (Ningxia)

To use cross-account management, you must follow these steps:

1. Create a master account in AWS Organizations and add accounts under the master account.
2. Enable the cross-account management feature in AWS Backup.
3. Create a backup policy to apply to all AWS accounts under your master account.

   Note
   For backup plans that are managed by Organizations, the resource opt-in settings in the master account overrides the settings in a member account.
4. Manage backup, restore, and copy jobs in all your AWS accounts.

Topics

Creating a Master Account in Organizations

First, you need to create your organization and configure it with AWS member accounts in AWS Organizations.

To create a master 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

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.

   You can only do this from the master 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 master account.

Creating a Backup Policy

After you enable cross-account management, create a policy that allows you to manage resources across multiple accounts at the same time from your master 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 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. AWS Backup assumes this role in each account and has permissions to perform backup and copy jobs. This role is also used for lifecycle deletions.

   Note
   AWS Backup doesn't validate that the role exists or if the role can be assumed.
   Backup plans created by cross-account management,AWS Backup will use the opt-in settings from the master account and overrides the settings specific accounts.
   For each account you want to add backup policies, you need to create the vaults and IAM roles yourself.
9. Add tags to the backup plan, if desired. 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 creating a backup plan.

```
{
  "plans": {
    "PiiMasterBackupPlan": {
      "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": "2"
            },
            "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": "28"
                },
                "move_to_cold_storage_after_days": {
                  "@@assign": "180"
                }
              }
            }
          }
        }
      },
      "selections": {
        "tags": {
          "SelectionDataType": {
            "iam_role_arn": {
              "@@assign": "arn:aws:iam::$account:role/MyIamRole"
            },
            "tag_key": {
              "@@assign": "dataType"
            },
            "tag_value": {
              "@@assign": [
                "PII",
                "RED"
              ]
            }
          }
        }
      },
      "backup_plan_tags": {
        "stage": {
          "tag_key": {
            "@@assign": "Stage"
          },
          "tag_value": {
            "@@assign": "Beta"
          }
        }
      }
    }
  }
}
```

10. 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
    You should validate your policy and make sure 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 doesn't provide policy validation for AWS Organizations SDK and JSON.
    If policies that are applied to the master account and a member account conflict, both policies will be executed without issues (that is, the policies will independently execute for each account). For example, if the master 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 execute.

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 master 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 master account. After you opt in, all the jobs across your organization that were created after the opt-in are visible. When you opt out, AWS Backup keeps the jobs in the aggregated view for 30 days (from reaching a terminus state). Created jobs after the opt-out are not visible and do not show any newly created backup jobs. For opt-in instructions, see Enabling Cross-Account Management (p. 45).

To monitor multiple accounts

1. Sign in to the AWS Management Console, and open the AWS Backup console at https://console.aws.amazon.com/backup.

   You can only do this from the master 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 master 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.

Defining Policies, Policies 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.

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 is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

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

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

All backups in AWS are encrypted using AWS KMS managed keys (SSE-KMS). 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.

Resource Type	How to Configure Encryption	Independent Backup Encryption
Amazon Elastic Block Store (Amazon EBS)	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.	Not supported
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

Resource Type	How to Configure Encryption	Independent Backup Encryption
Amazon Elastic File System (Amazon EFS)	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.	Supported
Amazon DynamoDB	DynamoDB backups are always encrypted. 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.	Not supported
AWS Storage Gateway	AWS Storage Gateway snapshots are automatically encrypted with the same encryption key that was used to encrypt the source AWS Storage Gateway volume. Snapshots of unencrypted AWS Storage Gateway volumes are also unencrypted. **Note** You don't need to use a customer master key (CMK) across all services to enable AWS Storage Gateway. You only need to copy the Storage Gateway backup to a vault that configured a CMK. This is because Storage Gateway does not have a service-specific AWS KMS managed key.	Not supported

Encryption for Backup Copies

AWS Backup encrypts backup copies by default whenever possible, even if the original backup is unencrypted.

You have two options for encrypting backup copies:

- Use the default AWS managed CMK for the destination backup vault. The default key is different for each service and is managed by AWS.
- Designate a customer managed CMK across all services to be used by the copy job. This is the only supported option for AWS Storage Gateway backups.

For more information about AWS KMS, see What is AWS Key Management Service?

To learn more about backup encryption for each of the services that AWS Backup supports, see the following topics:

- Encrypting Your Data Using AWS Key Management Service in the *AWS Storage Gateway User Guide*.
- Encrypting Amazon RDS Resources in the *Amazon RDS User Guide*

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 EBS volume. 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.

Topics

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 administrator 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

- Access Policies (p. 56)
- Managed Policies (p. 57)

Resources and Operations

A resource is an object that exists within a service. AWS Backup resources include backup plans, backup vaults, and backups. *Backup* is a general term that refers to the various types of backup resources that exist in AWS. For example, Amazon EBS snapshots, Amazon Relational Database Service (Amazon RDS) snapshots, and Amazon DynamoDB backups are all types of backup resources.

In AWS Backup, backups are also referred to as *recovery points*. When using AWS Backup, you also work with the resources from other AWS services that you are trying to protect, such as Amazon EBS volumes or DynamoDB tables. These resources have unique Amazon Resource Names (ARNs) associated with them. ARNs uniquely identify AWS resources. You must have an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies or API calls.

The following table lists resources, subresources, and ARN format.

AWS Backup Resource ARNs

Resource Type	ARN Format
Backup plan	`arn:aws:backup:region:account-id:backup-plan:*`
Backup vault	`arn:aws:backup:region:account-id:backup-vault:*`
Recovery point for Amazon EBS	`arn:aws:ec2:region::snapshot/*`
Recovery point for Amazon EFS	`arn:aws:backup:region:account-id:recovery-point:*`
Recovery point for Amazon RDS	`arn:aws:rds:region:account-id:snapshot:awsbackup:*`
Recovery point for Amazon Aurora	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`
Recovery point for AWS Storage Gateway	`arn:aws:ec2:region::snapshot/*`
Recovery point for DynamoDB	`arn:aws:dynamodb:region:account-id::table/*/backup/*`

AWS Backup provides a set of operations to work with AWS Backup resources. For a list of available operations, see AWS Backup Actions (p. 88).

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. 54)), the service defines a set of API operations (see Actions (p. 88)). 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. 54).
- 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 AWS Backup API Permissions: Actions, Resources, and Conditions Reference (p. 55).

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.

AWS Backup API Permissions: Actions, Resources, and Conditions Reference

When you are setting up Access Control (p. 53) and writing a permissions policy that you can attach to an IAM identity (identity-based policies), you can use the following list as a reference. The list includes

each AWS Backup API operation, the corresponding actions for which you can grant permissions to perform the action, and the AWS resource for which you can grant the permissions. You specify the actions in the policy's `Action` field, and you specify the resource value in the policy's `Resource` field.

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*.

To save metadata tags on resources that are stored in a backup vault, the following permissions are required for the specified resource types.

Permissions Required to Assign Tags to Backups

Resource Type	Required Permission
Amazon EFS file system	`elasticfilesystem:DescribeTags`
Amazon EBS volume	`ec2:DescribeTags`
Amazon RDS database and Amazon Aurora cluster	`rds:ListTagsForResource`
AWS Storage Gateway volume	`storagegateway:ListTagsForResource`

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. 57).

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 and Recovery Points (p. 29).

Managed Policies

Managed policies are standalone identity-based policies that you can attach to multiple users, groups, and roles in your AWS account. You can use AWS managed policies or customer managed policies to control access to backups in AWS Backup.

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.

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. These policies are predefined with the appropriate permissions that AWS Backup requires to perform backup operations on your behalf.

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.

Policy Name	IAM Managed Policy Name	Description
Backup Administrator IAM Policy	AWSBackupFullAccess (AWSBackupAdminPolicy is deprecated)	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.
Backup Operator IAM Policy	AWSBackupOperatorAccess (AWSBackupOperatorPolicy is deprecated)	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

Policy Name	IAM Managed Policy Name	Description
		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.
Backup Administrator AWS Organizations Policy	AWSBackupOrganizationAdminAccess	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.
Default Service Role Policy for Backups	AWSBackupServiceRolePolicyForBackups	Provides AWS Backup permissions to create backups of all supported resource types on your behalf.
Default Service Role Policy for Restores	AWSBackupServiceRolePolicyForRestores	Provides AWS Backup permissions to restore backups of all supported resource types on your behalf.

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 Services

Service Backup Policy	Service Restore Policy
DynamoDB Backup Policy	DynamoDB Restore Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:CreateBackup"
            ],
            "Resource":
 "arn:aws:dynamodb:*:*:table/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "dynamodb:DescribeBackup",
                "dynamodb:DeleteBackup"
            ],
            "Resource":
 "arn:aws:dynamodb:*:*:table/*/backup/*",
            "Effect": "Allow"
        },
        {
            "Effect": "Allow",
            "Action": [

 "backup:DescribeBackupVault",

 "backup:CopyIntoBackupVault"
            ],
            "Resource":
 "arn:aws:backup:*:*:backup-vault:*"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "dynamodb:DescribeBackup",
                "dynamodb:DescribeTable",

 "dynamodb:RestoreTableFromBackup",
                "dynamodb:Scan",
                "dynamodb:Query",
                "dynamodb:UpdateItem",
                "dynamodb:PutItem",
                "dynamodb:GetItem",
                "dynamodb:DeleteItem",
                "dynamodb:BatchWriteItem"
            ],
            "Resource":
 "arn:aws:dynamodb:*:*:table/*",
            "Effect": "Allow"
        },
        {
            "Action": [

 "dynamodb:RestoreTableFromBackup"
            ],
            "Resource":
 "arn:aws:dynamodb:*:*:table/*/backup/*",
            "Effect": "Allow"
        }
    ]
}
```

Amazon EBS Backup Policy	Amazon EBS Restore Policy

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

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

Service Backup Policy

```
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot"
            ],
            "Resource": [
                "arn:aws:ec2:*::snapshot/
*",
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Effect": "Allow",
            "Action": [

 "backup:DescribeBackupVault",

 "backup:CopyIntoBackupVault"
            ],
            "Resource":
 "arn:aws:backup:*:*:backup-vault:*"
        }
    ]
}
```

Service Restore Policy

```
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes"
            ],
            "Resource": "*"
        }
    ]
}
```

Service Backup Policy	Service Restore Policy
Amazon EFS Backup Policy	Amazon EFS Restore Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticfilesystem:Backup"
            ],
            "Resource":
 "arn:aws:elasticfilesystem:*:*:file-
system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Effect": "Allow",
            "Action": [

 "backup:DescribeBackupVault",

 "backup:CopyIntoBackupVault"
            ],
            "Resource":
 "arn:aws:backup:*:*:backup-vault:*"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:Restore",

 "elasticfilesystem:CreateFilesystem",

 "elasticfilesystem:DescribeFilesystems",

 "elasticfilesystem:DeleteFilesystem"
            ],
            "Resource":
 "arn:aws:elasticfilesystem:*:*:file-system/
*"
        }
    ]
}
```

Service Backup Policy	Service Restore Policy
Amazon RDS Backup Policy	Amazon RDS Restore Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds:AddTagsToResource",
                "rds:ListTagsForResource",
                "rds:DescribeDBSnapshots",
                "rds:CreateDBSnapshot",
                "rds:CopyDBSnapshot",
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:DeleteDBSnapshot"
            ],
            "Resource": [

 "arn:aws:rds:*:*:snapshot:awsbackup:*"
            ]
        },
        {
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Effect": "Allow",
            "Action": [

 "backup:DescribeBackupVault",

 "backup:CopyIntoBackupVault"
            ],
            "Resource":
 "arn:aws:backup:*:*:backup-vault:*"
        },
        {
            "Action": "kms:DescribeKey",
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
                "rds:DescribeDBSnapshots",
                "rds:ListTagsForResource",

 "rds:RestoreDBInstanceFromDBSnapshot",
                "rds:DeleteDBInstance",
                "rds:AddTagsToResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Service Backup Policy	Service Restore Policy
Amazon Aurora Backup Policy	Amazon Aurora Restore Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [

 "rds:CreateDBClusterSnapshot",
                "rds:DescribeDBClusters",

 "rds:DescribeDBClusterSnapshots",
                "rds:ListTagsForResource",
                "rds:AddTagsToResource",
                "rds:CopyDBClusterSnapshot"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [

 "rds:DeleteDBClusterSnapshot"
            ],
            "Resource": [
                "arn:aws:rds:*:*:cluster-
snapshot:awsbackup:*"
            ]
        },
        {
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
       },
        {
            "Effect": "Allow",
            "Action": [

 "backup:DescribeBackupVault",

 "backup:CopyIntoBackupVault"
            ],
            "Resource":
 "arn:aws:backup:*:*:backup-vault:*"
        },
        {
            "Action": "kms:DescribeKey",
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds:DeleteDBCluster",
                "rds:DescribeDBClusters",

 "rds:RestoreDBClusterFromSnapshot",
                "rds:ListTagsForResource",
                "rds:AddTagsToResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Service Backup Policy	Service Restore Policy
AWS Storage Gateway Backup Policy	AWS Storage Gateway Restore Policy

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [

 "storagegateway:CreateSnapshot"
            ],
            "Resource":
 "arn:aws:storagegateway:*:*:gateway/*/
volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteSnapshot"
            ],
            "Resource":
 "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Effect": "Allow",
            "Action": [

 "backup:DescribeBackupVault",

 "backup:CopyIntoBackupVault"
            ],
            "Resource":
 "arn:aws:backup:*:*:backup-vault:*"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [

 "storagegateway:DeleteVolume",

 "storagegateway:DescribeCachediSCSIVolumes",

 "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource":
 "arn:aws:storagegateway:*:*:gateway/*/
volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [

 "storagegateway:DescribeGatewayInformation",

 "storagegateway:CreateStorediSCSIVolume",

 "storagegateway:CreateCachediSCSIVolume"
            ],
            "Resource":
 "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListVolumes"
            ],
            "Resource":
 "arn:aws:storagegateway:*:*:*"
        }
    ]
}
```

Service Backup Policy	Service Restore Policy
Amazon EC2 Backup Policy	Amazon EC2 Restore Policy

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateTags",
            "ec2:DeleteSnapshot"
         ],

 "Resource":"arn:aws:ec2:*::snapshot/*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateImage",
            "ec2:DeregisterImage"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateTags"
         ],
         "Resource":"arn:aws:ec2:*:*:image/
*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:DescribeSnapshots",
            "ec2:DescribeTags",
            "ec2:DescribeImages",
            "ec2:DescribeInstances",

 "ec2:DescribeInstanceAttribute",

 "ec2:DescribeInstanceCreditSpecifications",

 "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeElasticGpus",

 "ec2:DescribeSpotInstanceRequests"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshot",
            "ec2:DeleteSnapshot",
            "ec2:DescribeVolumes",
            "ec2:DescribeSnapshots"
         ],
         "Resource":[
            "arn:aws:ec2:*::snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ]
      },
```

```
 {
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateVolume",
            "ec2:DeleteVolume"
         ],
         "Resource":[
            "arn:aws:ec2:*::snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:DescribeSnapshots",
            "ec2:DescribeVolumes"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:DescribeImages",
            "ec2:DescribeInstances"
         ],
         "Resource":"*"
      },
      {
         "Action":[
            "ec2:RunInstances"
         ],
         "Effect":"Allow",
         "Resource":"*"
      },
      {
         "Action":[
            "ec2:TerminateInstances"
         ],
         "Effect":"Allow",

 "Resource":"arn:aws:ec2:*:*:instance/*"
      },
      {
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::<account-
id>:role/<role-name>",
         "Effect":"Allow"
      }
   ]
}
```

Service Backup Policy	Service Restore Policy

<pre>{
"Action":[
"tag:GetResources"
],
"Resource":"*",
"Effect":"Allow"
},
{
"Effect": "Allow",
"Action": [
 	
"backup:DescribeBackupVault",
 	
"backup:CopyIntoBackupVault"
],
"Resource":
"arn:aws:backup:*:*:backup-vault:*"
}
]
}</pre>	

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.

You pass a role to AWS Backup when restoring or creating a backup. You also specify a role when assigning your AWS resources to a backup plan. This is the role that AWS Backup assumes when creating and expiring backups on your behalf according to the backup plan that you assigned the resource to.

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. 57).

Default Service Role for AWS Backup

When using AWS Backup 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 requires to perform backup operations for all the AWS services that it supports. You should use the default role if you are okay with using the same

role for all of the resource types that you want to back up. If you prefer to use separate roles for different resource types for security reasons, you can also create your own roles to pass to AWS Backup rather than using the default roles.

> **Note**
> If you are a first-time user of AWS Backup, you must create the role, list the role, and pass the role permissions. After the role is created, only list role and pass role permissions are required.

The default service role created by AWS Backup manages creating and restoring backups.

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.

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.

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.

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 permission to create backups on your behalf across AWS services.

The Backup service-linked role trusts the following services to perform backups on your behalf:

- `backup.amazonaws.com`

The role permissions policy allows AWS Backup to complete the following actions on the specified resources:

- Actions: `"elasticfilesystem:Backup", "elasticfilesystem:DescribeTags"` on `arn:aws:elasticfilesystem:*:*:file-system/*`

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 select the check box to protect the resource by creating an 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. Also, if you were using the AWS Backup service before June 17, 2020, when it began supporting service-linked roles, then AWS Backup created the Backup role in your account. 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 re-create the role in your account. When you select the check box to protect the resource by creating an automatic backup, AWS Backup creates the service-linked role for you again.

You can also use the IAM console to create a service-linked role with the **AWS Backup** use case. In the AWS CLI or the AWS API, create a service-linked role with the `backup.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a Service-Linked Role for AWS Backup

AWS Backup does not allow you to edit the Backup 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

You can use the IAM console, the AWS CLI or the AWS API to manually delete the service-linked role. To do this, you must first use the Amazon EFS console or API to clear the **Automatic backup** checkbox to disable automatic backup of Amazon EFS file systems.

> **Note**
> If the AWS Backup service is using the service-linked role when you try to delete the resources, the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete the Backup service-linked role

1. Use the Amazon EFS console to clear the **Automatic backup** checkbox to disable the automatic backup of Amazon EFS file systems. Or use the Amazon EFS `PutBackupPolicy` API to disable automatic backups.

   When there are no more Amazon EFS file systems selected to be backed up automatically, you can delete the service-linked role.
2. Use the IAM console, the AWS CLI, or the AWS API to delete the Backup service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

   Once the service-linked role is deleted, AWS Backup will remove the backup selection for those resources.

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 Regions and Endpoints in the *AWS General Reference*.

Logging and Monitoring in AWS Backup

Monitoring is an important part of maintaining the reliability, availability, and performance of AWS Backup and your AWS solutions. You should collect monitoring data from all parts of your AWS solution so that you can more easily debug a multi-point failure if one occurs. AWS provides several tools for monitoring your AWS Backup resources and responding to potential incidents:

AWS CloudTrail Logs

CloudTrail provides a record of actions taken by a user, role, or an AWS service in AWS Backup. 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. For more information, see Logging AWS Backup API Calls with AWS CloudTrail (p. 77).

AWS Trusted Advisor

Trusted Advisor draws upon best practices learned from serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and then makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps. All AWS customers have access to five Trusted Advisor checks. Customers with a Business or Enterprise support plan can view all Trusted Advisor checks. For more information, see AWS Trusted Advisor.

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

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. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

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 when working with AWS Backup.

Resource	Quota
Number of backup vaults per account	100
Number of concurrent backup copies (per service) to a destination AWS Region per account	5*
Number of backup plans per account	100
Number of versions per backup plan	2,000
Number of concurrent backup jobs per resource	1
Number of resource assignments per backup plan	100**
Number of metadata tags per saved resource	50
Number of recovery points per backup vault	1,000,000

*AWS Backup supports up to 50 concurrent backup copies of Amazon EC2 AMIs to a destination AWS Region per account.

**This quota applies to the number of resource assignment documents associated with a backup plan. There is no quota for the number of resources referenced in the assignment document.

Note
For services other than Amazon EFS, you might also encounter quotas imposed by those services.

Using Amazon SNS to Track AWS Backup Events

AWS Backup is designed to take advantage of the robust notifications delivered by Amazon Simple Notification Service (Amazon SNS). You configure Amazon SNS to send notifications for AWS Backup events from the Amazon SNS console. For more information, see Getting Started with Amazon SNS in the *Amazon Simple Notification Service Developer Guide*.

Topics

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. 108) — Deletes event notifications for the specified backup vault.
- GetBackupVaultNotifications (p. 149) — Lists all event notifications for the specified backup vault.
- PutBackupVaultNotifications (p. 187) — Turns on notifications for the specified topic and events.

The following events are supported:

Backup jobs

- `BACKUP_JOB_STARTED`
- `BACKUP_JOB_COMPLETED`

Restore jobs

- `RESTORE_JOB_STARTED`
- `RESTORE_JOB_COMPLETED`

Recovery points

- `RECOVERY_POINT_MODIFIED`

Completed Events

`Completed` notifications include a `STATE` attribute indicating the specific type of completion.

Examples: Completed Events

```
{
    "Type" : "Notification",
    "MessageId" : "12345678-abcd-123a-def0-abcd1a234567",
    "TopicArn" : "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
    "Subject" : "Notification from AWS Backup",
    "Message" : "An AWS Backup job was completed successfully. Recovery point ARN:
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
    "Timestamp" : "2019-08-02T18:46:02.788Z",
    "MessageAttributes" : {
        "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
        "State" : {"Type":"String","Value":"COMPLETED"},
        "AccountId" : {"Type":"String","Value":"123456789012"},
        "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
        "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
    }
}
```

```
{
    "Type" : "Notification",
    "MessageId" : "12345678-abcd-123a-def0-abcd1a234567",
    "TopicArn" : "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
    "Subject" : "Notification from AWS Backup",
    "Message" : "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-
west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-f22c-4dab-5eb6-
bbc7890ed123",
    "Timestamp" : "2019-08-02T18:46:02.788Z",
    "MessageAttributes" : {
        "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
        "State" : {"Type":"String","Value":"FAILED"},
        "AccountId" : {"Type":"String","Value":"123456789012"},
        "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
        "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
    }
}
```

```
{
    "Type" : "Notification",
    "MessageId" : "12345678-abcd-123a-def0-abcd1a234567",
    "TopicArn" : "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
    "Subject" : "Notification from AWS Backup",
    "Message" : "An AWS Backup job failed to complete in time. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
    "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.

```
aws backup --endpoint-url https://backup.region.amazonaws.com put-backup-vault-
notifications
    --backup-vault-name  --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
    --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED RECOVERY_POINT_MODIFIED
```

Example Get Backup Vault Notification

The following command lists all events currently subscribed to an Amazon SNS topic for the specified backup vault.

```
aws backup --endpoint-url https://backup.region.amazonaws.com get-backup-vault-
notifications
           --backup-vault-name myVault
```

The sample output is as follows:

```
{
    "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
    "BackupVaultEvents": [
        "RESTORE_JOB_STARTED",
        "RESTORE_JOB_COMPLETED",
        "RECOVERY_POINT_MODIFIED"
    ],
    "BackupVaultName": "myVault",
    "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

Example Delete Backup Vault Notification

The following command unsubscribes from an Amazon SNS topic for the specified backup vault.

```
aws backup --endpoint-url https://backup.region.amazonaws.com delete-backup-vault-
notifications
           --backup-vault-name myVault
```

Specifying AWS Backup as a Service Principal

Note
To allow AWS Backup to publish SNS topics on your behalf, you must specify AWS Backup as a service principal.

Include the following JSON in the access policy of the Amazon SNS topic that you use to track AWS Backup events. You must specify the resource Amazon Resource Name (ARN) of your topic.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

The following sample JSON is an example of a basic Amazon SNS access policy that includes AWS Backup as a service principal. You must specify your own AWS account ID and the resource ARN of your topic.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:Publish",
        "SNS:RemovePermission",
        "SNS:SetTopicAttributes",
        "SNS:DeleteTopic",
        "SNS:ListSubscriptionsByTopic",
        "SNS:GetTopicAttributes",
        "SNS:Receive",
        "SNS:AddPermission",
        "SNS:Subscribe"
      ],
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Condition": {
        "StringEquals": {
          "AWS:SourceOwner": "account-id"
        }
      }
    },
    {
      "Sid": "__console_pub_0",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
    }
```

```
  ]
}
```

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*.

Logging AWS Backup API Calls with AWS 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

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. 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

All AWS Backup actions are logged by CloudTrail and are documented in AWS Backup API Actions (p. 88).

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.

- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding AWS Backup Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `StartBackupJob`, `StartRestoreJob`, and `DeleteRecoveryPoint` actions and also the `BackupJobCompleted` event.


```
    {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "account-id",
        "accessKeyId": aceess-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-00a422a05b9c6asd3",
        "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",
    "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-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
}
,
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "account-id",
        "accessKeyId": "access-key",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "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-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
}
,
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "account-id",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "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": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",
        "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:BackupVault",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/vol-06692095a6a421233",
        "creationDate": {
            "seconds": 1547101638,
            "nanos": 272000000
        },
        "backupSizeInBytes": 8589934592,
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "resourceType": "EBS"
    }
}
```


Logging Cross-Account Management Events

Using AWS Backup, you can manage your backups across all AWS accounts inside your AWS Organizations structure. AWS CloudTrail logs the following events for cross-account management.

- CreateOrganizationalBackupPlan
- UpdateOrganizationalBackupPlan
- DeleteOrganizationalBackupPlan

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.

Example: AWS Backup Log File Entries For Cross-Account Management

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

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


```
{
    "*eventVersion*": "1.05",
    "*userIdentity*": {
        "*accountId*": "account-id",
        "*invokedBy*": "backup.amazonaws.com"},
    "*eventTime*": "2020-06-02T00:34:00Z",
    "*eventSource*": "backup.amazonaws.com",
    "*eventName*": "CreateOrganizationalBackupPlan",
    "*awsRegion*": "ca-central-1",
    "*sourceIPAddress*": "backup.amazonaws.com",
    "*userAgent*": "backup.amazonaws.com",
    "*requestParameters*": null,
    "*responseElements*": null,
    "*eventID*": "f2642255-af77-4203-8c37-7ca19d898e84",
    "*readOnly*": false,
    "*eventType*": "AwsServiceEvent",
    "*recipientAccountId*": "account-id",
    "*serviceEventDetails*": {
        "*backupPlanId*": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "*backupPlanVersionId*": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "*backupPlanArn*": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "*backupPlanName*": "mybackupplan",
        "*backupRules*": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
\"name\":\"hourly\",\"description\":null,\"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault\",\"scheduleExpression
\":\"cron(0 0/1 ? * * *)\",\"startWindow\":\"PT1H\",\"completionWindow\":\"PT2H\",
\"lifecycle\":{\"moveToColdStorageAfterDays\":null,\"deleteAfterDays\":\"7\"},\"tags
\":null,\"copyActions\":[]}]",
        "*backupSelections*": "[{\"name\":\"selectiondatatype\",\"arn\":
\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
\"resources\":[],\"notResources\":[],\"conditions\":[{\"type\":\"STRINGEQUALS\",\"key\":
\"dataType\",\"value\":\"PII\"},{\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",\"value\":
\"RED\"}],\"creationDate\":\"2020-06-02T00:34:00.695Z\",\"creatorRequestId\":null}]",
        "*creationDate*": {
            "*seconds*": 1591058040,
            "*nanos*": 695000000
        },
        "*organizationId*": "org-id",
        "*accountId*": "account-id"
    }
}
```

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


```
{
    "*eventVersion*": "1.05",
    "*userIdentity*": {
        "*accountId*": "account-id",
        "*invokedBy*": "backup.amazonaws.com"
    },
    "*eventTime*": "2020-06-02T00:34:25Z",
    "*eventSource*": "backup.amazonaws.com",
    "*eventName*": "DeleteOrganizationalBackupPlan",
    "*awsRegion*": "ca-central-1",
    "*sourceIPAddress*": "backup.amazonaws.com",
    "*userAgent*": "backup.amazonaws.com",
    "*requestParameters*": null,
    "*responseElements*": null,
    "*eventID*": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
    "*readOnly*": false,
    "*eventType*": "AwsServiceEvent",
    "*recipientAccountId*": "account-id",
    "*serviceEventDetails*": {
        "*backupPlanId*": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "*backupPlanVersionId*": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "*backupPlanArn*": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "*backupPlanName*": "mybackupplan",
        "*deletionDate*": {
            "*seconds*": 1591058065,
            "*nanos*": 519000000
        },
        "*organizationId*": "org-id",
        "*accountId*": "account-id"
    }
}
```

Using AWS CloudFormation Templates with AWS Backup

The following information describes how to use AWS CloudFormation templates to simplify and automate tasks related to your backup plans, backup vaults, and resource selections.

Integrating AWS Backup with AWS CloudFormation

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 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 stack, you should consider the following:

- We recommend that you create separate templates for your backup plans and your backup vaults. Because backup vaults can be deleted only if they are empty, you can't delete a stack that includes backup vaults if they contain any recovery points.
- Be sure that 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 done this yet, the default service role is not available. You can also specify a custom role that you create. For more information about roles, see IAM Service Roles (p. 66).

Following is a sample template that creates a backup plan.

```
  Description: "Backup Plan template to back up all resources tagged with backup=daily
 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"
      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
```

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

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*.

Troubleshooting AWS Backup

When you use AWS Backup, you might encounter issues when working with backup plans, resources, and backup vaults. 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

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. For more information about access control using AWS Identity and Access Management (IAM) with AWS Backup, see Access Control (p. 53).

If you run into issues with backing up and restoring a particular resource type, it can be helpful to review the troubleshooting topic for that resource. For more information about troubleshooting other AWS services, see the following:

- Using AWS Backup with Amazon EFS in the *Amazon Elastic File System User Guide*
- On-Demand Backup and Restore for DynamoDB in the *Amazon DynamoDB Developer Guide*
- Amazon EBS Snapshots in the *Amazon EC2 User Guide for Linux Instances*
- Backing Up and Restoring Amazon RDS DB Instances in the *Amazon RDS User Guide*
- Overview of Backing Up and Restoring an Aurora DB Cluster in the *Amazon Aurora User Guide*.
- Backing Up Your Volumes in the *AWS Storage Gateway User Guide*

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 AWS CloudTrail (p. 77).

Troubleshooting Creating Resources

The following information can help you troubleshoot problems with creating 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:
  - Amazon RDS has a soft quota of 100 backups per AWS Region per account, and additional backups will 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.
  - If you initiate a backup either through a backup plan or by creating an on-demand backup, it will fail if it is scheduled 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*.
  - Backups that are initiated during a maintenance window will fail. For more information about Amazon RDS maintenance windows, see Maintaining a DB Instance in the *Amazon RDS User Guide*.

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. 53).

AWS Backup API

Actions

The following actions are supported:

- PutBackupVaultAccessPolicy (p. 185)
- PutBackupVaultNotifications (p. 187)
- StartBackupJob (p. 189)
- StartCopyJob (p. 193)
- StartRestoreJob (p. 196)
- StopBackupJob (p. 199)
- TagResource (p. 201)
- UntagResource (p. 203)
- UpdateBackupPlan (p. 205)
- UpdateRecoveryPointLifecycle (p. 208)
- UpdateRegionSettings (p. 211)

CreateBackupPlan

Backup plans are documents that contain information that AWS Backup uses to schedule tasks that create recovery points of resources.

If you call `CreateBackupPlan` with a plan that already exists, an `AlreadyExistsException` is returned.

Request Syntax

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number
                  }
               }
            ],
            "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. 90)

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

Type: BackupPlanInput (p. 218) object

Required: Yes

BackupPlanTags (p. 90)

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. 90)

Identifies the request and allows failed requests to be retried without the risk of executing the operation twice. If the request includes a `CreatorRequestId` that matches an existing backup plan, that plan is returned. This parameter is optional.

Type: String

Required: No

Response Syntax

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

{
   "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.

BackupPlanArn (p. 91)

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. 91)

Uniquely identifies a backup plan.

Type: String

CreationDate (p. 91)

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. 91)

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. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateBackupSelection

Creates a JSON document that specifies a set of resources to assign to a backup plan. Resources can be included by specifying patterns for a `ListOfTags` and selected `Resources`.

For example, consider the following patterns:

- `Resources: "arn:aws:ec2:region:account-id:volume/volume-id"`
- `ConditionKey:"department"`

  `ConditionValue:"finance"`

  `ConditionType:"StringEquals"`
- `ConditionKey:"importance"`

  `ConditionValue:"critical"`

  `ConditionType:"StringEquals"`

Using these patterns would back up all Amazon Elastic Block Store (Amazon EBS) volumes that are tagged as `"department=finance"`, `"importance=critical"`, in addition to an EBS volume with the specified volume Id.

Resources and conditions are additive in that all resources that match the pattern are selected. This shouldn't be confused with a logical AND, where all conditions must match. The matching patterns are logically 'put together using the OR operator. In other words, all patterns that match are selected for backup.

Request Syntax

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
   "BackupSelection": {
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreatorRequestId": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

backupPlanId (p. 93)

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. 93)

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

Type: BackupSelection (p. 226) object

Required: Yes

CreatorRequestId (p. 93)

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

Type: String

Required: No

Response Syntax

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

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupPlanId (p. 94)

Uniquely identifies a backup plan.

Type: String

CreationDate (p. 94)

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. 94)

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. 247).

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
- 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
Sensitive data, such as passport numbers, should not be included 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. 96)

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.

BackupVaultTags (p. 96)

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. 96)

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

Type: String

Required: No

EncryptionKeyArn (p. 96)

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. 97)

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. 97)

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. 97)

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. 247).

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
- 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. 99)

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. 99)

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. 99)

Uniquely identifies a backup plan.

Type: String

DeletionDate (p. 99)

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. 99)

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. 247).

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
- 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. 102)

Uniquely identifies a backup plan.

Required: Yes

selectionId (p. 102)

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. 247).

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
- 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. 104)

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. 247).

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
- 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. 106)

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. 247).

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
- 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. 108)

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. 247).

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
- 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.

Request Syntax

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 110)

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. 110)

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. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeBackupJob

Returns metadata associated with creating a backup of a resource.

Request Syntax

```
GET /backup-jobs/backupJobId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

backupJobId (p. 112)

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",
   "BackupSizeInBytes": number,
   "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. 112)

Returns the account ID that owns the backup job.

Type: String

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

BackupJobId (p. 112)

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

Type: String

BackupSizeInBytes (p. 112)

The size, in bytes, of a backup.

Type: Long

BackupVaultArn (p. 112)

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. 112)

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. 112)

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

Type: Long

CompletionDate (p. 112)

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. 112)

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. 244) object

CreationDate (p. 112)

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. 112)

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. 112)

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

Type: String

PercentDone (p. 112)

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

Type: String

RecoveryPointArn (p. 112)

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. 112)

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

Type: String

ResourceType (p. 112)

The type of AWS resource to be backed up; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database.

Type: String

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

StartBy (p. 112)

Specifies the time in Unix format and Coordinated Universal Time (UTC) when a backup job must be started before it is canceled. The value is calculated by adding the start window to the scheduled time. So if the scheduled time were 6:00 PM and the start window is 2 hours, the `StartBy` time would be 8:00 PM on the date specified. The value of `StartBy` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

State (p. 112)

The current state of a resource recovery point.

Type: String

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

StatusMessage (p. 112)

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

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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. 116)

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",
   "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. 116)

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. 116)

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. 116)

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. 116)

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

Type: String

EncryptionKeyArn (p. 116)

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

NumberOfRecoveryPoints (p. 116)

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. 247).

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
- 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. 119)

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. 119)

Contains detailed information about a copy job.

Type: CopyJob (p. 234) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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. 121)

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. 121)

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. 121)

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

Type: String

ResourceType (p. 121)

The type of AWS resource saved as a recovery point; for example, an 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. 247).

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
- 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. 123)

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. 123)

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",
   "Status": "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. 123)

The size, in bytes, of a backup.

Type: Long

BackupVaultArn (p. 123)

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

Type: String

BackupVaultName (p. 123)

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. 123)

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

Type: CalculatedLifecycle (p. 231) object

CompletionDate (p. 123)

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. 123)

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. 244) object

CreationDate (p. 123)

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. 123)

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. 123)

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

Type: String

IsEncrypted (p. 123)

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. 123)

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. 123)

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.

Type: Lifecycle (p. 237) object

RecoveryPointArn (p. 123)

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. 123)

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

Type: String

ResourceType (p. 123)

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}$`

Status (p. 123)

A status code specifying the state of the recovery point.

> **Note**
> A partial status indicates that the recovery point was not successfully re-created and must be retried.

Type: String

Valid Values: `COMPLETED | PARTIAL | DELETING | EXPIRED`

StorageClass (p. 123)

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. 247).

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

- 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 the service has a value set to `true`, AWS Backup attempts to protect that service's resources in this Region, when included in an on-demand backup or scheduled backup plan. If the value is set to `false` for a service, AWS Backup does not attempt 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

{
   "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.

ResourceTypeOptInPreference (p. 128)

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

Type: String to boolean map

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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. 130)

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. 130)

Returns the account ID that owns the restore job.

Type: String

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

BackupSizeInBytes (p. 130)

The size, in bytes, of the restored resource.

Type: Long

CompletionDate (p. 130)

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. 130)

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. 130)

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. 130)

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

Type: Long

IamRoleArn (p. 130)

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

Type: String

PercentDone (p. 130)

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

Type: String

RecoveryPointArn (p. 130)

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. 130)

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

Type: String

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

RestoreJobId (p. 130)

Uniquely identifies the job that restores a recovery point.

Type: String

Status (p. 130)

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. 130)

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. 247).

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
- 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. 134)

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. 134)

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. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetBackupPlan

Returns 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. 136)

Uniquely identifies a backup plan.

Required: Yes

VersionId (p. 136)

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

{
   "BackupPlan": {
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number
                  }
               }
            ],
            "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.

BackupPlan (p. 136)

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

Type: BackupPlan (p. 217) object

BackupPlanArn (p. 136)

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. 136)

Uniquely identifies a backup plan.

Type: String

CreationDate (p. 136)

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. 136)

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

Type: String

DeletionDate (p. 136)

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. 136)

The last time a job to back up resources was executed 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. 136)

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. 247).

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
- 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

```
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. 139)

A customer-supplied backup plan document in JSON format.

Type: String

Required: Yes

Response Syntax

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

{
   "BackupPlan": {
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number
                  }
               }
            ],
            "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. 139)

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

Type: BackupPlan (p. 217) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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. 142)

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": {
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number
                  }
               }
            ],
            "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. 142)

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. 217) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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. 144)

Uniquely identifies a backup plan.

Required: Yes

selectionId (p. 144)

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": {
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "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. 144)

Uniquely identifies a backup plan.

Type: String

BackupSelection (p. 144)

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

Type: BackupSelection (p. 226) object

CreationDate (p. 144)

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. 144)

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

Type: String

SelectionId (p. 144)

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. 247).

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
- 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. 147)

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. 147)

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. 147)

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. 147)

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. 247).

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
- 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. 149)

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. 149)

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. 149)

An array of events that indicate the status of jobs to back up resources to the backup vault.

Type: Array of strings

Valid Values: `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED`

BackupVaultName (p. 149)

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. 149)

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. 247).

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

- 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. 152)

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. 152)

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

BackupVaultArn (p. 152)

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

Type: String

RecoveryPointArn (p. 152)

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. 152)

The set of metadata key-value pairs that describes 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. 247).

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
- 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. 154)

Contains a string with the supported AWS resource types:

- `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
- `Storage Gateway` for AWS Storage Gateway

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. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupJobs

Returns metadata about your backup jobs.

Request Syntax

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&createdAfter=ByCreatedAfter&createdBefore=ByCre
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ByAccountId (p. 156)

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

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

ByBackupVaultName (p. 156)

Returns only backup jobs that will be stored in the specified backup vault. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

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

ByCreatedAfter (p. 156)

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

ByCreatedBefore (p. 156)

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

ByResourceArn (p. 156)

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

ByResourceType (p. 156)

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
- `Storage Gateway` for AWS Storage Gateway

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

ByState (p. 156)

Returns only backup jobs that are in the specified state.

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

MaxResults (p. 156)

The maximum number of items to be returned.

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

NextToken (p. 156)

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",
         "BackupSizeInBytes": number,
         "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. 157)

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

Type: Array of BackupJob (p. 214) objects

NextToken (p. 157)

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. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupPlans

Returns metadata of your saved backup plans, including 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. 159)

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

MaxResults (p. 159)

The maximum number of items to be returned.

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

NextToken (p. 159)

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": [
      {
         "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. 159)

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

Type: Array of BackupPlansListMember (p. 219) objects

NextToken (p. 159)

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. 247).

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
- 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. 161)

The maximum number of items to be returned.

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

NextToken (p. 161)

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. 161)

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

Type: Array of BackupPlanTemplatesListMember (p. 221) objects

NextToken (p. 161)

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. 247).

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
- 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. 163)

Uniquely identifies a backup plan.

Required: Yes

MaxResults (p. 163)

The maximum number of items to be returned.

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

NextToken (p. 163)

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": [
      {
         "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.

BackupPlanVersionsList (p. 163)

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

Type: Array of BackupPlansListMember (p. 219) objects

NextToken (p. 163)

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. 247).

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
- 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. 165)

Uniquely identifies a backup plan.

Required: Yes

MaxResults (p. 165)

The maximum number of items to be returned.

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

NextToken (p. 165)

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. 165)

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

Type: Array of BackupSelectionsListMember (p. 227) objects

NextToken (p. 165)

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. 247).

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
- 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. 167)

The maximum number of items to be returned.

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

NextToken (p. 167)

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",
         "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. 167)

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. 229) objects

NextToken (p. 167)

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. 247).

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
- 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=ByD
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ByAccountId (p. 169)

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

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

ByCreatedAfter (p. 169)

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

ByCreatedBefore (p. 169)

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

ByDestinationVaultArn (p. 169)

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. 169)

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

ByResourceType (p. 169)

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
- `Storage Gateway` for AWS Storage Gateway

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

ByState (p. 169)

Returns only copy jobs that are in the specified state.

Valid Values: `CREATED | RUNNING | COMPLETED | FAILED`

MaxResults (p. 169)

The maximum number of items to be returned.

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

NextToken (p. 169)

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. 170)

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

Type: Array of CopyJob (p. 234) objects

NextToken (p. 170)

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. 247).

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
- 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. 172)

The maximum number of items to be returned.

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

NextToken (p. 172)

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. 172)

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. 172)

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. 238) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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=ByBackupPlanId&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&maxResults=MaxRes
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

backupVaultName (p. 174)

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

ByBackupPlanId (p. 174)

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

ByCreatedAfter (p. 174)

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

ByCreatedBefore (p. 174)

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

ByResourceArn (p. 174)

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

ByResourceType (p. 174)

Returns only recovery points that match the specified resource type.

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

MaxResults (p. 174)

The maximum number of items to be returned.

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

NextToken (p. 174)

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",
         "Status": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 175)

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. 175)

An array of objects that contain detailed information about recovery points saved in a backup vault.

Type: Array of RecoveryPointByBackupVault (p. 239) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRecoveryPointsByResource

Returns detailed information about recovery points of the type specified by a resource Amazon Resource Name (ARN).

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. 177)

The maximum number of items to be returned.

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

NextToken (p. 177)

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. 177)

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"
      }
   ]
}
```

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. 177)

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. 177)

An array of objects that contain detailed information about recovery points of the specified resource type.

Type: Array of RecoveryPointByResource (p. 242) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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 metadata about the recovery process.

Request Syntax

```
GET /restore-jobs/?
accountId=ByAccountId&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&maxResults=MaxResults&n
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ByAccountId (p. 180)

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

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

ByCreatedAfter (p. 180)

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

ByCreatedBefore (p. 180)

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

ByStatus (p. 180)

Returns only restore jobs associated with the specified job status.

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

MaxResults (p. 180)

The maximum number of items to be returned.

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

NextToken (p. 180)

The next item following a partial list of returned items. For example, if a request is made to return `maxResults` number of items, `NextToken` allows you to return more items in your list starting at the location pointed to by the next token.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "NextToken": "string",
   "RestoreJobs": [
```

```
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 180)

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. 180)

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

Type: Array of RestoreJobsListMember (p. 245) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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.

Note
`ListTags` are currently only supported with Amazon EFS backups.

Request Syntax

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults (p. 183)

The maximum number of items to be returned.

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

NextToken (p. 183)

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. 183)

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. 183)

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. 183)

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. 247).

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
- 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. 185)

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. 185)

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. 247).

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
- 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

```
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. 187)

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. 187)

An array of events that indicate the status of jobs to back up resources to the backup vault.

Type: Array of strings

Valid Values: `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED`

Required: Yes

SNSTopicArn (p. 187)

The Amazon Resource Name (ARN) that specifies the topic for a backup vault's events; for example, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Type: String

Required: Yes

Response Syntax

```
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. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartBackupJob

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

Request Syntax

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

{
   "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.

BackupVaultName (p. 189)

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

CompleteWindowMinutes (p. 189)

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

IamRoleArn (p. 189)

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. 189)

A customer chosen string that can be used to distinguish between calls to `StartBackupJob`.

Type: String

Required: No

Lifecycle (p. 189)

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.

Type: Lifecycle (p. 237) object

Required: No

RecoveryPointTags (p. 189)

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. 189)

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

Type: String

Required: Yes

StartWindowMinutes (p. 189)

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

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. 190)

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

Type: String

CreationDate (p. 190)

The date and time that a backup job is started, 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. 190)

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. 247).

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
- 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.

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. 193)

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. 193)

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. 193)

A customer chosen string that can be used to distinguish between calls to `StartCopyJob`.

Type: String

Required: No

Lifecycle (p. 193)

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.

Type: Lifecycle (p. 237) object

Required: No

RecoveryPointArn (p. 193)

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. 193)

The name of a logical source container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

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

Required: Yes

Response Syntax

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

{
   "CopyJobId": "string",
   "CreationDate": number
}
```

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. 194)

Uniquely identifies a copy job.

Type: String

CreationDate (p. 194)

The date and time that a copy job is started, 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. 247).

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
- 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).

If the resource ARN is included in the request, then the last complete backup of that resource is recovered. If the ARN of a recovery point is supplied, then that recovery point is restored.

Request Syntax

```
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. 196)

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. 196)

A customer chosen string that can be used to distinguish between calls to `StartRestoreJob`.

Type: String

Required: No

Metadata (p. 196)

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`: 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.

Type: String to string map

Required: Yes

RecoveryPointArn (p. 196)

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. 196)

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
- `Storage Gateway` for AWS Storage Gateway

Type: String

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

Required: No

Response Syntax

```
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. 197)

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. 247).

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
- 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

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

URI Request Parameters

The request uses the following URI parameters.

backupJobId (p. 199)

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

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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. 201)

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. 201)

Key-value pairs that are used to help organize your resources. You can assign your own metadata to the resources you create.

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. 247).

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
- 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. 203)

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. 203)

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. 247).

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateBackupPlan

Replaces the body of a saved 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": {
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number
                  }
               }
            ],
            "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. 205)

Uniquely identifies a backup plan.

Required: Yes

Request Body

The request accepts the following data in JSON format.

BackupPlan (p. 205)

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

Type: BackupPlanInput (p. 218) object

Required: Yes

Response Syntax

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

{
   "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.

BackupPlanArn (p. 206)

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. 206)

Uniquely identifies a backup plan.

Type: String

CreationDate (p. 206)

The date and time a backup plan is updated, 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. 206)

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. 247).

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
- 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.

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. 208)

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. 208)

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 accepts the following data in JSON format.

Lifecycle (p. 208)

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. 237) 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. 209)

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

Type: String

CalculatedLifecycle (p. 209)

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

Type: CalculatedLifecycle (p. 231) object

Lifecycle (p. 209)

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. 237) object

RecoveryPointArn (p. 209)

An Amazon Resource Name (ARN) that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 247).

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
- 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 the service has a value set to `true`, AWS Backup attempts to protect that service's resources in this Region, when included in an on-demand backup or scheduled backup plan. If the value is set to `false` for a service, AWS Backup does not attempt to protect that service's resources in this Region.

Request Syntax

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "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.

ResourceTypeOptInPreference (p. 211)

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. 247).

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
- 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:

- RestoreJobsListMember (p. 245)

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

BackupSizeInBytes

The size, in bytes, of a backup.

Type: Long

Required: No

BackupVaultArn

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

Type: String

Required: No

BackupVaultName

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

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

Required: No

BytesTransferred

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

Type: Long

Required: No

CompletionDate

The date and time a job to create a backup job is completed, in Unix format and Coordinated Universal Time (UTC). The value of `CompletionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

CreatedBy

Contains identifying information about the creation of a backup job, including the `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion`, and `BackupRuleId` of the backup plan used to create it.

Type: RecoveryPointCreator (p. 244) object

Required: No

CreationDate

The date and time a backup job is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

ExpectedCompletionDate

The date and time a job to back up resources is expected to be completed, in Unix format and Coordinated Universal Time (UTC). The value of `ExpectedCompletionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

IamRoleArn

Specifies the IAM role ARN used to create the target recovery point; 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

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.

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
- 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

BackupPlanName

The display name of a backup plan.

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. 222) 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
- 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 and can back up a different selection of AWS resources.

Contents

BackupPlanName

The optional display name of a backup plan.

Type: String

Required: Yes

Rules

An array of `BackupRule` objects, each of which specifies a scheduled task that is used to back up a selection of resources.

Type: Array of BackupRuleInput (p. 224) 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
- AWS SDK for Ruby V3

BackupPlansListMember

Contains metadata about a backup plan.

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

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 executing the operation twice.

Type: String

Required: No

DeletionDate

The date and time a backup plan is deleted, in Unix format and Coordinated Universal Time (UTC). The value of `DeletionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

LastExecutionDate

The last time a job to back up resources was executed 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
- 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
- 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. 233) objects

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.

Type: Lifecycle (p. 237) object

Required: No

RecoveryPointTags

An array of key-value pair strings that are assigned to resources that are associated with this rule when restored from backup.

Type: String to string map

Required: No

RuleId

Uniquely identifies a rule that is used to schedule the backup of a selection of resources.

Type: String

Required: No

RuleName

An optional display name for a backup rule.

Type: String

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

Required: Yes

ScheduleExpression

A CRON expression 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
- 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. 233) objects

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.

Type: Lifecycle (p. 237) 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

An optional display name for a backup rule.

Type: String

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

Required: Yes

ScheduleExpression

A CRON expression 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
- AWS SDK for Ruby V3

BackupSelection

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

Contents

IamRoleArn

The ARN of the IAM role that AWS Backup uses to authenticate when backing up the target resource; for example, `arn:aws:iam::123456789012:role/S3Access`.

Type: String

Required: Yes

ListOfTags

An array of conditions used to specify a set of resources to assign to a backup plan; for example, `"StringEquals": {"ec2:ResourceTag/Department": "accounting"`.

Type: Array of Condition (p. 232) objects

Required: No

Resources

An array of strings that contain Amazon Resource Names (ARNs) of resources to assign to a backup plan.

Type: Array of strings

Required: No

SelectionName

The display name of a resource selection document.

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
- 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 executing the operation twice.

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
- 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, `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`.

Type: String

Required: No

BackupVaultName

The name of a logical container where backups are stored. Backup vaults are identified by names that are unique to the account used to create them and the AWS Region where they are created. They consist of lowercase letters, numbers, and hyphens.

Type: String

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

Required: No

CreationDate

The date and time a resource backup is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

CreatorRequestId

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

Type: String

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

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
- 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.

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
- 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. Conditions are used to filter resources in a selection that is assigned to a backup plan.

Contents

ConditionKey

The key in a key-value pair. For example, in `"ec2:ResourceTag/Department": "accounting"`, `"ec2:ResourceTag/Department"` is the key.

Type: String

Required: Yes

ConditionType

An operation, such as `StringEquals`, that is applied to a key-value pair used to filter resources in a selection.

Type: String

Valid Values: `STRINGEQUALS`

Required: Yes

ConditionValue

The value in a key-value pair. For example, in `"ec2:ResourceTag/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
- 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.

Type: Lifecycle (p. 237) 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
- 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. 244) 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`.

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
- 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.

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
- 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.

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
- 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\-\_]{2,50}$`

Required: No

CalculatedLifecycle

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

Type: CalculatedLifecycle (p. 231) 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. 244) 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.

Type: Lifecycle (p. 237) 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: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 saved 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}$`

Required: No

Status

A status code specifying the state of the recovery point.

Type: String

Valid Values: `COMPLETED | PARTIAL | DELETING | EXPIRED`

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
- 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

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
- 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
- AWS SDK for Ruby V3

RestoreJobsListMember

Contains metadata about a restore job.

Contents

AccountId

The account ID that owns the restore job.

Type: String

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

Required: No

BackupSizeInBytes

The size, in bytes, of the restored resource.

Type: Long

Required: No

CompletionDate

The date and time a job to restore a recovery point is completed, in Unix format and Coordinated Universal Time (UTC). The value of `CompletionDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

CreatedResourceArn

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

Type: String

Required: No

CreationDate

The date and time a restore job is created, in Unix format and Coordinated Universal Time (UTC). The value of `CreationDate` is accurate to milliseconds. For example, the value 1516925490.087 represents Friday, January 26, 2018 12:11:30.087 AM.

Type: Timestamp

Required: No

ExpectedCompletionTimeMinutes

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

Type: Long

Required: No

IamRoleArn

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

Type: String

Required: No

PercentDone

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

Type: String

Required: No

RecoveryPointArn

An ARN that uniquely identifies a recovery point; for example, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type: String

Required: No

ResourceType

The resource type of the listed restore jobs; for example, an Amazon Elastic Block Store (Amazon EBS) volume or an Amazon Relational Database Service (Amazon RDS) database.

Type: String

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

Required: No

RestoreJobId

Uniquely identifies the job that restores a recovery point.

Type: String

Required: No

Status

A status code specifying the state of the job initiated by AWS Backup to restore a recovery point.

Type: String

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

Required: No

StatusMessage

A detailed message explaining the status of the job to restore a recovery point.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java
- AWS SDK for Ruby V3

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

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:** 2019-01-15
- **Latest documentation update:** July 16, 2020

Change	Description	Date
Support for Amazon EFS Automatic Backup.	You can now use AWS Backup to automatically backup Amazon EFS file systems. For more information, see Option 3: Create Automatic Backups.	July 16, 2020
New AWS Region	AWS Backup is now available in the GovCloud Region. For more information, see AWS Backup endpoints and quotas in the *AWS General Reference*.	June 24, 2020
Support for managing backups across multiple AWS accounts.	You can now manage backups across multiple AWS accounts by using AWS Organizations. For more information, see How Cross-Account Management Works.	June 24, 2020
Support for Amazon Aurora added to AWS Backup.	You can now configure AWS Backup to backup resources for Amazon Aurora. For information, see Overview of Backing Up and Restoring an Aurora DB Cluster in the *Amazon Aurora User Guide*.	June 10, 2020
Support for configuring services to work with AWS Backup.	You can now configure AWS Backup to backup resources for specific AWS services. For more information, see Configuring Services to Work with AWS Backup.	May 20, 2020
Support for backing up Amazon EC2 instances and also adds support for Cross-Region backups.	You can now backup entire Amazon EC2 instances and also copy resources across AWS Regions. For more information, see Cross-Region Backups.	January 13, 2020
New guide	This is the first release of the *AWS Backup Developer Guide*.	January 15, 2019