AWS Resource Access Manager

User Guide

AWS Resource Access Manager: User Guide

The AWS Documentation website is getting a new look!

Try it now and let us know what you think. Switch to the new look >>

You can return to the original look by selecting English in the language selector above.

Table of Contents

What Is AWS RAM?

AWS Resource Access Manager (AWS RAM) lets you share your resources with any AWS account or through AWS Organizations. If you have multiple AWS accounts, you can create resources centrally and use AWS RAM to share those resources with other accounts.

Contents

Benefits

AWS RAM offers the following benefits:

- **Reduces operational overhead**—Create resources centrally and use AWS RAM to share those resources with other accounts. This eliminates the need to provision duplicate resources in every account, which reduces operational overhead.
- **Provides security and consistency**—Govern consumption of shared resources using existing policies and permissions, to achieve security and control. AWS RAM offers a consistent experience for sharing different types of AWS resources.
- **Provides visibility and auditability**—View usage details for shared resources through integration with Amazon CloudWatch and AWS CloudTrail. AWS RAM provides comprehensive visibility into shared resources and accounts.

How Resource Sharing Works

When you share a resource with another account, then that account is granted access to the resource. Any policies and permissions in that account apply to the shared resource.

Sharing Your Resources

You can share resources that you own by creating a resource share. When you create a resource share, you specify a name, the resources to share, and the principals with whom to share. Principals can be AWS accounts, organizational units, or an entire organization from AWS Organizations. Your account retains full ownership of the resources that you share.

Using Shared Resources

When the owner of a resource shares it with your account, you can access the shared resource just as you would if it was owned by your account. You can access the resource using the respective service's console, AWS CLI, and API. The actions that users are allowed to perform vary depending on the resource type. All

IAM policies and service control policies configured in your account apply, which enables you to leverage your existing investments in security and governance controls.

Service Limits

Your AWS account has the following limits related to AWS RAM. You can request an increase for some of these limits. To request a limit increase, contact AWS Support.

Resource	Default limit
Maximum number of resource shares per account	5000
Maximum number of shared resources per account	5000
Maximum number of pending invitations per account	20

Accessing AWS RAM

You can work with AWS RAM in any of the following ways:

AWS RAM Console

AWS RAM provides a web-based user interface, the AWS RAM console. If you've signed up for an AWS account, you can access the AWS RAM console by signing into the AWS Management Console and selecting AWS RAM from the console home page.

AWS Command Line Interface (AWS CLI)

The AWS CLI provides direct access to the AWS RAM public API operations. It is supported on Windows, macOS, and Linux. For more information about getting started, see the AWS Command Line Interface User Guide. For more information about the commands for AWS RAM, see the AWS CLI Command Reference.

AWS Tools for Windows PowerShell

AWS provides commands for a broad set of AWS products for those who script in the PowerShell environment. For more information about getting started, see the AWS Tools for Windows PowerShell User Guide. For more information about the cmdlets for AWS RAM, see the AWS Tools for Windows PowerShell Cmdlet Reference.

Query API

The AWS RAM HTTPS Query API gives you programmatic access to AWS RAM and AWS. The AWS RAM API lets you issue HTTPS requests directly to the service. When you use the AWS RAM API, you must include code to digitally sign requests using your credentials. For more information, see the AWS RAM API Reference.

Pricing

There are no additional charges for creating resource shares and sharing your resources across accounts. Resource usage charges vary depending on the resource type. For more information about about how shareable resources are billed, refer to the respective service's documentation.

Shareable Resources

AWS RAM lets you share resources that are provisioned and managed in other AWS services. AWS RAM does not let you manage resources, but it does provide the features that let you make resources available across AWS accounts.

The following sections list the services that integrate with AWS RAM, and the resources that support sharing.

Services

Amazon EC2

You can share the following Amazon EC2 resources using AWS RAM.

Resource	Use case
Capacity Reservations	Create and manage Capacity Reservations centrally, and share the reserved capacity with other AWS accounts. This lets multiple AWS accounts launch their Amazon EC2 instances into centrally-managed reserved capacity. For more information, see Working with Shared Capacity Reservations in the *Amazon EC2 User Guide for Linux Instances*.
Subnets	Create and manage subnets centrally, and share them with other AWS accounts. This lets multiple AWS accounts launch their application resources into centrally-managed VPCs. These resources include Amazon EC2 instances, Amazon Relational Database Service (RDS) databases, Amazon Redshift clusters, and AWS Lambda functions. For more information, see Working with VPC Sharing in the *Amazon VPC User Guide*.
Traffic mirror targets	Create and manage traffic mirror targets centrally, and share them with other AWS accounts. This lets multiple AWS accounts send mirrored network traffic from traffic mirror sources in their accounts to a shared, centrally-managed traffic mirror target. For more information, see Cross-Account Traffic Mirroring Targets in the *Traffic Mirroring Guide*.
Transit gateways	Create and manage transit gateways centrally, and share them with other AWS accounts. This lets multiple AWS accounts route traffic between their VPCs and on-premises networks through a shared, centrally-managed transit gateway. For

Resource	Use case
	more information, see Sharing a Transit Gateway in the *Transit Gateways Guide*.

AWS License Manager

You can share the following AWS License Manager resources using AWS RAM.

Resource	Use case
License configurations	Create and manage license configurations centrally, and share them with other AWS accounts. This lets you enforce centrally-managed licensing rules that are based on the terms of your enterprise agreements across multiple AWS accounts. For more information, see Using License Configurations in the *AWS License Manager User Guide*.

Amazon Aurora

You can share the following Amazon Aurora resources using AWS RAM.

Resource	Use case
DB clusters	Create and manage a DB cluster centrally, and share it with other AWS accounts. This lets multiple AWS accounts clone a shared, centrally-managed DB cluster. For more information, see Cross-Account Aurora DB Cluster Cloning in the *Amazon Aurora User Guide*.

Amazon Route 53

You can share the following Amazon Route 53 resources using AWS RAM.

Resource	Use case
Forwarding rules	Create and manage forwarding rules centrally, and share them with other AWS accounts. This lets multiple AWS accounts forward DNS queries from their VPCs to the target IP addresses defined in shared, centrally-managed resolver rules. For more information, see Sharing Forwarding Rules with Other AWS Accounts and Using Shared Rules in the *Amazon Route 53 Developer Guide*.

Getting Started with AWS RAM

With AWS RAM, you can share resources that you own with individual AWS accounts or through AWS Organizations, and you can use resources that were shared with you by other AWS accounts or through AWS Organizations.

Topics

Sharing Your Resources

To start sharing a resource that you own using AWS RAM, do the following:

- Enable Sharing with AWS Organizations (p. 5)
- Create a Resource Share (p. 6)

> **Note**
> Some resources have special considerations and prerequisites for sharing. For more information, see Shareable Resources (p. 3).

Enable Sharing with AWS Organizations

If you would like to share resources with your organization or organizational units, then you must use the AWS RAM console or CLI command to enable sharing with AWS Organizations.

When you share resources within your organization, AWS RAM does not send invitations to principals. Principals in your organization get access to shared resources without exchanging invitations.

> **Important**
> If you do not enable sharing with AWS Organizations, you cannot share resources with your organization or organizational units within your organization. However, you can still share resources with individual AWS accounts in your organization. In this case, the accounts are treated as external principals. They receive an invitation to join the resource share, and they must accept the invitation to get access to the shared resources.

Requirements

- Only the master account can enable sharing with AWS Organizations.
- The organization must be enabled for all features. For more information, see Enabling All Features in Your Organization in the *AWS Organizations User Guide*.

To enable sharing with AWS Organizations (Console)

1. Open the **Settings** page of AWS RAM console at https://console.aws.amazon.com/ram/home#Settings.
2. Choose **Enable sharing with AWS Organizations**.

To enable sharing with AWS Organizations (AWS CLI)

Use the enable-sharing-with-aws-organization command.

This command can be used in any region, and it enables sharing with AWS Organizations in all regions in which AWS RAM is supported.

Create a Resource Share

To share resources that you own, create a resource share, add the resources to share, and specify the principals with whom they are to be shared.

Considerations

- You can share a resource only if you own it. You can't share a resource that is shared with you.
- If you are part of an organization in AWS Organizations and sharing within your organization is enabled, principals in your organization are automatically granted access to the shared resources. Otherwise, principals receive an invitation to join the resource share and are granted access to the shared resources after accepting the invitation.
- After you add an organization to a resource share, changes to the OU or organization affect the resource share. For example, if you add a new account to the organization, it has access to the shared resources.
- You can't add the following to a resource share as principals: IAM users, IAM roles, or OUs or organizations outside your organization in AWS Organizations.

To create a resource share (Console)

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. If you are new to AWS RAM, choose **Create a resource share** from the home page. Otherwise, choose **Create resource share** from the **Resource shares** page.
3. Under **Description**, for **Name**, type a descriptive name for the resource share.
4. (Optional) Under **Resources**, select resources to add to the resource share as follows:

   a. For **Select resource type**, select the type of resource. This filters the list of shareable resources to resources of the selected type.

   b. Select the check boxes next to the resources. The selected resources are moved under **Selected resources**.

   If you are sharing zonal resources, using the Availability Zone ID (AZ ID) helps you determine the relative location of these resources across accounts. For more information, see AZ IDs for Your Resources (p. 14).
5. (Optional) Under **Principals**, do the following:

   a. By default, you can share resources with any AWS account. To restrict resource sharing to your organization in AWS Organizations, clear **Allow external accounts**.

   b. For each principal, specify its ID and choose **Add**:

   - To add an AWS account, type the 12-digit account ID. For example, `123456789012`.
   - To add an OU, type the ID of the OU. For example, `ou-abcd1234-mnop5678qrst9098uv76`.
   - To add your entire organization, type the ID of the organization. For example, `o-abcd1234efgh5678`.
6. (Optional) Under **Tags**, type a tag key and tag value. To add another tag, choose **Add tag** and type a tag key and tag value pair. These tags are not applied to the resources included in the resource share.
7. Choose **Create resource share**.

It can take a few minutes for the resource and principal associations to complete. Allow this process to complete before attempting to use the resource share.

8. You can add and remove resources and principals or apply custom tags to your resource share at any time. You can delete your resource share when you no longer want to share the resources. For more information, see Sharing Resources Owned by You (p. 8).

To create a resource share (AWS CLI)

Use the create-resource-share command.

Using Shared Resources

To start using shared resources, do the following:

- Respond to the Resource Share Invitation (p. 7)
- Use the Resources that are Shared with You (p. 7)

Respond to the Resource Share Invitation

If you receive an invitation to join a resource share, you must accept it to gain access to the shared resources. If you are part of an organization in AWS Organizations and sharing within your organization is enabled, principals in your organization are automatically granted access to the shared resources and do not receive these invitations.

To respond to invitations

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared with me**, **Resource shares**.
3. Review the list of resource shares to which you have been added.

   The **Status** column indicates your current participation status for the resource share. The `Pending` status indicates that you have been added to a resource share, but you have not yet accepted or rejected the invitation.
4. To respond to the resource share invitation, select the resource share ID and choose **Accept resource share** to accept the invitation, or **Reject resource share** to decline the invitation. If you reject the invitation, you do not get access to the resources. If you accept the invitation, you gain access to the resources.

Use the Resources that are Shared with You

After you accept the invitation to join a resource share, you gain the ability to perform specific actions on the shared resources. These actions vary by resource type. For more information, see Shareable Resources (p. 3).

Working with Shared Resources

You can share AWS resources that you own and access AWS resources that are shared with you.

Contents

Sharing Resources Owned by You

AWS RAM enables you to share the resources that you specify with the principals that you specify. At any time, you can modify resource shares that you have created and delete them when they are no longer needed.

Contents

Creating a Resource Share

To share resources that you own, create a resource share, add the resources to share, and specify the principals with whom they are to be shared.

To create a resource share, follow the directions in Sharing Your Resources (p. 5).

Updating a Resource Share

You can update a resource share at any time. You can add principals, resources, or tags to a resource share that you created. You can revoke access to shared resources by removing principals or resources from a resource share. If you revoke access, principals no longer have access to the shared resources.

To update a resource share using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared by me**, **Resource shares**.
3. Select the resource share and choose **Modify**.
4. (Optional) To change the name of the resource share, edit **Name**.
5. (Optional) To add a resource to the resource share, under **Resources**, select the type of resource and select the check box next to the resource.
6. (Optional) To remove a resource, locate the resource in the **Selected resources** panel and choose **X**.
7. (Optional) To add a principal, type the ID of the AWS account OU, or organization and choose **Add**.
8. (Optional) To remove a principal, locate it in the **Selected principals** panel and choose **X**.
9. (Optional) To add a tag to the resource share, under **Tags**, choose **Add tag** and type a tag key and tag value pair.
10. To remove a tag from the resource share, locate it and choose **Remove tag**.
11. Choose **Save changes**.

To update a resource share using the AWS CLI

Use the following commands:

- associate-resource-share
- disassociate-resource-share
- tag-resource
- update-resource-share

Viewing a Resource Share

You can view a list of all the resource shares that you have created. You can see which resources you are sharing and the principals with whom they are shared.

To view your resource shares using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared by me**, **Resource shares**.
3. Apply a filter to find specific resource shares. You can apply multiple filters to narrow your search.
4. Choose the resource share to review. The following information is available:

   - **Summary**—Lists information about the resource share, such as its name, ID, owner, Amazon Resource Name (ARN), creation date, and current status.
   - **Shared resources**—Lists the resources that are included in the resource share. Choose the ID of a resource to view it in its service console.
   - **Shared principals**—Lists the principals with whom the resources are shared.

- **Tags**—Lists the tag key-value pairs for the resource share.

To view your resource shares using the AWS CLI

Use the get-resource-shares command.

Viewing Your Shared Resources

You can view the resources that are shared by your account, across all resource shares. This enables you to determine which resources you are currently sharing, the number of resource shares they are included in, and the number of principals that have access to them.

To view the resources that you're sharing using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared by me**, **Shared resources**.
3. For each shared resource, the following information is available:

   - **Resource ID**—The ID of the resource. Choose the ID of a resource to view it in its service console.
   - **Resource type**—The type of resource.
   - **Last share date**—The date on which the resource was last shared.
   - **Resource shares**—The number of resource shares in which the resource is included. Choose the value to list the resource shares.
   - **Principals**—The number of principals with whom the resource is shared. Choose the value to view the principals.

To view the resources that you're sharing using the AWS CLI

Use the list-resources command.

Viewing the Principals with Whom You're Sharing

You can view the principals with whom you are sharing your resources, across all resource shares. Viewing the principals with whom you are sharing enables you to determine who has access to your shared resources.

To view the principals with whom you're sharing using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared by me**, **Principals**.
3. For each principal, the following information is available:

   - **Principal ID**—The ID of the principal.
   - **Resource shares**—The number of resource shares you shared with the principal. Choose the value to view the resource shares.
   - **Resources**—The number of resources you shared with the principal. Choose the value to view the shared resources.

To view the principals with whom you're sharing using the AWS CLI

Use the list-principals command.

Deleting a Resource Share

You can delete a resource share at any time. When you delete a resource share, all principals that were associated with the resource share lose access to the shared resources. Deleting a resource share does not delete the shared resources.

The deleted resource share remains visible in the console for a short period after deletion, but its status changes to `Deleted`.

To delete a resource share using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared by me**, **Resource shares**.
3. Select the resource share. Be sure to select the correct resource share. You can't recover a resource share after you delete it.
4. Choose **Delete**, type the confirmation message, and choose **Delete**.

To delete a resource share using the AWS CLI

Use the delete-resource-share command.

Supported Actions on Shared Resources

You can use the AWS CLI to view the actions that principals can perform on shared resources. For more information, see the get-resource-policies command.

Accessing Resources Shared With You

AWS RAM enables you to view the resource shares to which you have been added, the shared resources that you can access, and the accounts that have shared resources with you. You can also leave a resource share when you no longer require access to the shared resources.

Contents

Accepting and Rejecting Invitations

To access shared resources, a principal must add you to a resource share.

If you were added to the resource share by an account in your organization in AWS Organizations, and sharing within your organization is enabled, you are automatically get access to the shared resources.

If you were added to a resource share by one of the following, you receive an invitation to join the resource share:

- An account outside of your organization in AWS Organizations

- An account inside your organization, if sharing with AWS Organizations is not enabled

If you receive an invitation to join a resource share, you must accept it to access to the shared resources. If you decline the invitation, you cannot access the shared resources.

You have seven days to accept an invitation to join a resource share. If you do not accept the invitation within seven days, it is automatically declined.

To respond to invitations

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared with me**, **Resource shares**.
3. Review the list of resource shares to which you have been added.

   The **Status** column indicates your current participation status for the resource share. The `Pending` status indicates that you have been added to a resource share, but you have not yet accepted or rejected the invitation.
4. To respond to the resource share invitation, select the resource share ID and choose **Accept resource share** to accept the invitation, or **Reject resource share** to decline the invitation. If you reject the invitation, you do not get access to the resources. If you accept the invitation, you gain access to the resources.

To respond to an invitation (AWS CLI)

Use the following commands:

- accept-resource-share-invitation
- reject-resource-share-invitation

Viewing Resource Shares

You can view the resource shares to which you have been added. You can see which principals are sharing resources with you and which resources they are sharing.

To view the resource shares using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared with me**, **Resource shares**.
3. Apply a filter to find specific resource shares. You can apply multiple filters to narrow your search.
4. The following information is available:

   - **Name**—The name of the resource share.
   - **ID**—The ID of the resource share. Choose the ID to view the resource share.
   - **Owner**—The ID of the AWS account that created the resource share.
   - **Status**—The current status of the resource share. Possible values include:
     - **Active**—The resource share is active and available for use.
     - **Deleted**—The resource share has been deleted and is no longer available for use.
     - **Pending**—An invitation to join the resource share is pending.

To view the resource shares using the AWS CLI

Use the get-resource-shares command.

Viewing Shared Resources

You can view the shared resources that you can access. You can see which principals are sharing resources and in which resource shares they are included.

To view shared resources using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared with me**, **Shared resources**.
3. Apply a filter to find specific shared resources. You can apply multiple filters to narrow your search.
4. The following information is available:

   - **Resource ID**—The ID of the resource. Choose the ID of the resource to view it in its service console.
   - **Resource type**—The type of resource.
   - **Last share date**—The date on which the resource was shared with you.
   - **Resource shares**—The number of resource shares in which the resource is included. Choose the value to view the resource shares.
   - **Owner ID**—The ID of the principal who owns the resource.

To view shared resources using the AWS CLI

Use the list-resources command.

Viewing Principals Sharing With You

You can view a list of all the principals that are sharing resources with you. You can see which resources and resource shares they have shared with you.

To view the principals that are sharing resources with you using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared with me**, **Principals**.
3. Apply a filter to find specific principals. You can apply multiple filters to narrow your search.
4. The following information is available:

   - **Principal ID**—The ID of the principal who is sharing with you.
   - **Resource shares**—The number of resource shares to which the principal has added you. Choose the value to view the resource shares.
   - **Resources**—The number of resources the principal is sharing with you. Choose the value to view the resources.

To view the principals that are sharing resources with you using the AWS CLI

Use the list-principals command.

Leaving a Resource Share

If you no longer need access to resources shared with you, you can leave a resource share at any time. When you leave a resource share, you lose access to the shared resources.

You cannot leave a resource share if you were added to it by an account inside your organization and sharing with AWS Organizations is enabled.

To leave a resource share using the console

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Shared with me**, **Resource shares**.
3. Select the resource share.
4. Choose **Leave resource share**, type the confirmation text, and choose **Leave resource share**.

To leave a resource share using the AWS CLI

Use the disassociate-resource-share command.

AZ IDs for Your Resources

To ensure that resources are distributed across the Availability Zones for a Region, we independently map Availability Zones to names for each account. For example, the Availability Zone `us-east-1a` for your AWS account might not have the same location as `us-east-1a` for another AWS account. For more information, see Regions and Availability Zones in the *Amazon EC2 User Guide*.

To identify the location of your resources relative to your accounts, you must use the *AZ ID*, which is a unique and consistent identifier for an Availability Zone. For example, `use1-az1` is an AZ ID for the `us-east-1` Region and it is the same location in every AWS account.

To view the AZ IDs for the Availability Zones in your account

1. Open the AWS RAM console at https://console.aws.amazon.com/ram.
2. In the navigation pane, choose **Resource Access Manager**.
3. The AZ IDs for the current Region are under **Your AZ ID**.

Viewing AZ IDs enables you to determine the location of resources in one account relative to the resources in another account. For example, if you share a subnet in the Availability Zone with the AZ ID `use-az2` with another account, this subnet is available to that account in the Availability Zone whose AZ ID is also `use-az2`. The AZ ID for each virtual private cloud (VPC) and subnet is displayed in the Amazon VPC console.

To view AZ IDs using the AWS CLI

- describe-availability-zones
- DescribeAvailabilityZones

Authentication and Access Control

You can use IAM policies to control access to certain AWS RAM features and resource sharing capabilities. For more information about IAM policies, see Permissions and Policies in the *IAM User Guide*. For more information about managing and creating custom IAM policies, see Managing IAM Policies.

Contents

IAM Policies for AWS RAM

By default, IAM users don't have permission to create or modify AWS RAM resources. To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant permission to use specific resources and API actions. You then attach those policies to the IAM users or groups that require those permissions.

An IAM policy is a JSON document that includes the following statements: Effect, Action, Resource, and Condition. An IAM policy typically takes the following form:

```
{
    "Statement":[{
        "Effect":"effect",
        "Action":"action",
        "Resource":"arn",
        "Condition":{
            "condition":{
                "key":"value"
            }
        }
    }]
}
```

Effect

The *Effect* statement indicates whether the policy allows or denies a user permission to perform an action. The possible values include: `Allow` and `Deny`.

Action

The *Action* statement specifies the AWS RAM API actions for which the policy is allowing or denying permission. For a complete list of the allowed actions, see Actions Defined by AWS Resource Access Manager in the *IAM User Guide*.

Resource

The *Resource* statement specifies the AWS RAM resources that are affected by the policy. To specify a resource in the statement, you need to use its unique Amazon Resource Name (ARN). For a complete list of the allowed resources, see Resources Defined by AWS Resource Access Manager in the *IAM User Guide*.

Condition

Condition statements are optional. They can be used to further refine the conditions under which the policy applies. AWS RAM supports the following condition keys:

- `aws:RequestTag/${TagKey}` — Specifies a tag key and value pair that must be used when creating or tagging a resource share.
- `aws:ResourceTag/${TagKey}` — Indicates that the action can be performed only on resources that have the specified tag key and value pair.
- `aws:TagKeys` — Specifies the tag keys that can be used when creating or tagging a resource share.
- `ram:AllowsExternalPrincipals` — Indicates that the action can be performed only on resource shares that allow or deny sharing with external principals. An external principal is an AWS account outside of your AWS organization
- `ram:Principal` — Indicates that the action can be performed only on the specified principal.
- `ram:RequestedResourceType` — Indicates that the action can be performed only on the specified resource type. Resource types must be specified in the following format:
  - `ec2:CapacityReservation`
  - `ec2:Subnet`
  - `ec2:TrafficMirrorTarget`
  - `ec2:TransitGateway`
  - `license-manager:LicenseConfiguration`
  - `rds:Cluster`
  - `route53resolver:ResolverRule`
- `ram:ResourceArn` — Indicates that the action can be performed only on a resource with the specified ARN.
- `ram:ResourceShareName` — Indicates that the action can be performed only on a resource share with the specified name.
- `ram:ShareOwnerAccountId` — Indicates that the action can be performed only on resource shares owned by a specific account.

Example IAM Policies

Examples

Example 1: Allow Sharing of Specific Resources

You can use an IAM policy to restrict principals to associating only specific resources with resource shares.

For example, the following policy limits principals to sharing only the resolver rule with the specified Amazon Resource Name (ARN).

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
```

```
        "Condition": {
            "StringEquals": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

Example 2: Allow Sharing of Specific Resource Types

You can use an IAM policy to limit principals to associating only specific resource types with resource shares.

For example, the following policy limits principals to sharing only resolver rules.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    }]
}
```

Example 3: Restrict Sharing with External AWS Accounts

You can use an IAM policy to prevent principals from sharing resources with AWS accounts that are outside of its AWS organization.

For example, the following IAM policy prevents principals from adding external AWS accounts to resource shares.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ram:CreateResourceShare",
        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:AllowsExternalPrincipals": "false"
            }
        }
    }]
}
```

Disabling Sharing with AWS Organizations

If you previously enabled sharing with AWS Organizations and you no longer need to share resources with your entire organization or organizational units, you can disable sharing.

To disable sharing with AWS Organizations

1. Disable trusted access to AWS Organizations using the AWS Organizations disable-aws-service-access AWS CLI command.

```
$  aws organizations disable-aws-service-access --service-principal ram.amazonaws.com
```

   Important
   When you disable trusted access to AWS Organizations, principals within your organizations are removed from all resource shares and lose access to those shared resources.

2. Use the IAM console, the IAM AWS CLI, or the IAM API to delete the **AWSServiceRoleForResourceAccessManager** service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Monitoring AWS RAM

AWS RAM integrates with the following AWS services that offer monitoring and logging capabilities:

- **Amazon CloudWatch Events**—Delivers a near-real-time stream of system events that describe changes in AWS resources. CloudWatch Events enables automated event-driven computing, as you can write rules that watch for certain events and trigger automated actions in other AWS services when these events happen. For more information, see Monitoring with CloudWatch Events (p. 19).
- **AWS CloudTrail**—Captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see Logging AWS RAM API Calls with AWS CloudTrail (p. 19).

Monitoring with CloudWatch Events

Using Amazon CloudWatch Events, you can set up automatic notifications for specific events in AWS RAM. Events from AWS RAM are delivered to CloudWatch Events in near-real time. You can configure CloudWatch Events to monitor events and invoke targets in response to events that indicate changes to your resource shares. Changes to a resource share trigger events for both the owner of the resource share and the principals that were granted access to the resource share.

When you create an event pattern, the source is `aws.ram`.

For more information, see the Amazon CloudWatch Events User Guide.

Logging AWS RAM API Calls with AWS CloudTrail

AWS RAM is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS RAM. CloudTrail captures all API calls for AWS RAM as events. The calls captured include calls from the AWS RAM console and code calls to the AWS RAM API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS RAM. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Use the information collected by CloudTrail to determine the request that was made to AWS RAM, the requesting IP address, the requester, when it was made, and additional details.

For more information about CloudTrail, see the AWS CloudTrail User Guide.

AWS RAM Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS RAM, 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 RAM, 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 RAM actions are logged by CloudTrail and are documented in the AWS RAM API Reference. For example, calls to the `CreateResourceShare`, `AssociateResourceShare`, and `EnableSharingWithAwsOrganization` actions generate entries in the CloudTrail log files.

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 RAM 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 for the `CreateResourceShare` action.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
            "status": "ACTIVE"
        }
```

```
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Document History for AWS RAM User Guide

The following table describes the documentation updates for AWS RAM.

Change	Description	Date
Support for sharing On-Demand Capacity Reservations	Use AWS RAM to share On-Demand Capacity Reservations. For more information, see Shareable Resources (p. 3).	July 29, 2019
Support for sharing Aurora DB clusters	Use AWS RAM to share Aurora DB clusters. For more information, see Shareable Resources (p. 3).	July 02, 2019
Support for sharing Traffic Mirroring targets	Use AWS RAM to share Traffic Mirroring targets. For more information, see Shareable Resources (p. 3).	June 25, 2019
Support for sharing license configurations	Use AWS RAM to share AWS License Manager license configurations. For more information, see Shareable Resources (p. 3).	December 05, 2018
Support for sharing subnets	Use AWS RAM to share Amazon VPC subnets. For more information, see Shareable Resources (p. 3).	November 27, 2018
Support for sharing transit gateways	Use AWS RAM to share Amazon VPC transit gateways. For more information, see Shareable Resources (p. 3).	November 26, 2018
Support for sharing forwarding rules	Use AWS RAM to share Route 53 forwarding rules. For more information, see Shareable Resources (p. 3).	November 20, 2018
Initial release	This release introduces AWS Resource Access Manager.	November 20, 2018