Service Name

AWS Resource Access Manager

Service Overview

AWS Resource Access Manager (RAM) is a service that enables secure sharing of AWS resources across accounts, organizations, and IAM roles and users for supported resource types. It reduces operational overhead by allowing the creation of a resource once and sharing it with other accounts, providing security and consistency by managing access through a single set of policies and permissions, and offering visibility and auditability through integration with Amazon CloudWatch and AWS CloudTrail. RAM simplifies cross-account access by allowing sharing with organizations, organizational units (OUs), and individual accounts without the need to enumerate every account ID. Shared resources appear as native resources in the receiving accounts, and the resource owners can see which principals have access to each resource.

Key Use Cases

- Multi-account resource sharing: Enable organizations to share AWS resources like Transit Gateways, subnets, and Route 53 Resolver rules across multiple AWS accounts without duplicating resources
- Centralized infrastructure management: Create resources once in a central account and share them with other accounts, reducing operational overhead and maintaining consistency across the organization
- Cross-account network connectivity: Share VPC resources, Transit Gateways, and networking components to establish secure connectivity between accounts while maintaining centralized control

Features

- **Resource Sharing**: Share AWS resources across accounts, organizations, organizational units, and IAM roles/users
- **Managed Permissions**: Control access with AWS managed permissions or create custom customer managed permissions
- **Resource-based Policies**: Automatically generate and manage resource-based policies for shared resources
- **Cross-account Visibility**: View shared resources as native resources in consuming accounts with full visibility of access grants
- **Organizations Integration**: Seamless integration with AWS Organizations for organization-wide resource sharing
- **Regional and Global Resources**: Support for sharing both regional and global AWS resources

- **Invitation Management**: Handle resource share invitations for accounts outside the organization
- **Audit and Monitoring**: Integration with CloudTrail and CloudWatch for logging and monitoring resource sharing activities

Value Proposition

AWS Resource Access Manager eliminates the need to provision and manage duplicate resources across multiple AWS accounts, significantly reducing operational overhead and costs. It provides centralized control and governance while maintaining security through managed permissions and resource-based policies:

- RAM simplifies multi-account architectures by enabling seamless resource sharing within AWS Organizations without complex cross-account configurations
- The service offers native integration with AWS services, ensuring shared resources appear and function as native resources in consuming accounts
- Key advantages include no additional charges for the service itself, compliance with major security standards (PCI DSS, FedRAMP, SOC, ISO), and comprehensive audit capabilities through CloudTrail integration

Service Integration

AWS Resource Access Manager integrates deeply with AWS Organizations for organization-wide resource sharing and automatic service-linked role creation. It works seamlessly with AWS Identity and Access Management (IAM) for permission management and access control:

- RAM integrates with Amazon CloudWatch and AWS CloudTrail for comprehensive monitoring, logging, and audit capabilities of all resource sharing activities
- The service supports sharing of resources from over 40 AWS services including Amazon VPC, AWS Transit Gateway, Amazon Route 53 Resolver, AWS License Manager, Amazon Aurora, AWS CodeBuild, Amazon S3, Amazon DynamoDB, and many others
- RAM also integrates with AWS Systems Manager, AWS Private Certificate Authority, AWS Network Firewall, and AWS Backup for specialized sharing scenarios

Onboarding and Offboarding

Getting started with AWS Resource Access Manager is straightforward through the AWS RAM console, AWS CLI, or AWS SDKs. Customers can create resource shares by specifying resources to share, selecting managed permissions for each resource type, and defining the principals (accounts, OUs, or IAM roles/users) to grant access:

- For organization-wide sharing, enable sharing within AWS Organizations first

- The service automatically creates necessary service-linked roles and resource-based policies
- Customers can view, update, and manage resource shares through the console or APIs
- For accounts outside the organization, recipients receive email invitations that must be accepted to gain access to shared resources

Getting Started Guide: https://docs.aws.amazon.com/ram/latest/userguide/getting-started.html

Data Removal

To offboard from AWS Resource Access Manager, customers can stop sharing resources by removing them from resource shares or deleting the resource shares entirely. When a resource share is deleted, all principals lose access to the shared resources immediately. Customers can leave resource shares they no longer need access to, which revokes their access to those shared resources. The resource owner retains full ownership and control of the original resources throughout the sharing process.

Backup/Restore and Disaster Recovery

AWS Resource Access Manager itself does not provide backup and disaster recovery capabilities as it is a resource sharing service. However, RAM can be used to share backup-related resources like AWS Backup vaults, Amazon Aurora clusters, and other resources that support backup functionality. The service enables sharing of disaster recovery resources across accounts, facilitating multi-account disaster recovery strategies.

Backup Capabilities

AWS Resource Access Manager does not have inherent backup capabilities as it is a resource sharing service. RAM does not work directly with AWS Backup for its own data, but it can be used to share AWS Backup resources such as backup vaults and recovery points across accounts, enabling centralized backup management strategies.

Disaster Recovery

AWS Resource Access Manager does not provide disaster recovery capabilities itself, nor does it work with AWS Elastic Disaster Recovery directly. However, RAM can facilitate disaster recovery strategies by enabling the sharing of disaster recovery resources across accounts and regions, supporting multi-account disaster recovery architectures.

Recovery Objectives

AWS Resource Access Manager can indirectly support RPO and RTO objectives by enabling efficient resource sharing across accounts for disaster recovery scenarios. By eliminating the need to duplicate resources across accounts, RAM can help maintain

consistent disaster recovery configurations and reduce recovery complexity, potentially improving RTO through simplified resource access patterns.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/ram/latest/userguide/service-quotas.html

FAQ: https://aws.amazon.com/ram/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/ram/latest/userguide/what-is.html

User Guide: https://docs.aws.amazon.com/ram/latest/userguide/

API Reference: https://docs.aws.amazon.com/ram/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/ram/faqs/

Cost Optimization

AWS Resource Access Manager provides significant cost optimization by eliminating the need to duplicate resources across multiple AWS accounts. The service itself incurs no additional charges, making it a cost-effective solution for multi-account resource sharing:

- Organizations can achieve substantial cost savings by provisioning expensive resources like Transit Gateways, dedicated hosts, or licensed software once and sharing them across accounts rather than provisioning multiple instances
- This approach reduces both infrastructure costs and operational overhead associated with managing duplicate resources
- RAM enables efficient resource utilization by allowing multiple accounts to share the same underlying infrastructure while maintaining security and access control

Savings Considerations

Primary cost savings with AWS Resource Access Manager come from resource consolidation and elimination of duplicate provisioning across accounts. Organizations can significantly reduce infrastructure costs by sharing expensive resources like AWS License Manager configurations, AWS Transit Gateways, and Amazon Aurora clusters instead of creating separate instances per account:

- Operational savings include reduced management overhead, simplified compliance management through centralized resource governance, and decreased complexity in multi-account architectures
- RAM enables better resource utilization rates and helps organizations avoid over-provisioning by sharing underutilized resources across accounts
- The service supports cost allocation through resource tagging and provides visibility into resource usage across shared accounts