



Explore, organize, and manage access to your AWS resources

Fabian Labat

Senior Solutions Architect

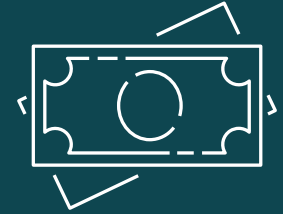
Why organize your AWS resources?



Security boundaries



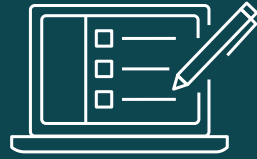
Relationships



Identification



Automation



Cost allocation

Break down cost by multiple dimensions

- Cost center
- Business unit
- Customer
- Project
- Application
- Environment



AWS tagging



What are tags?

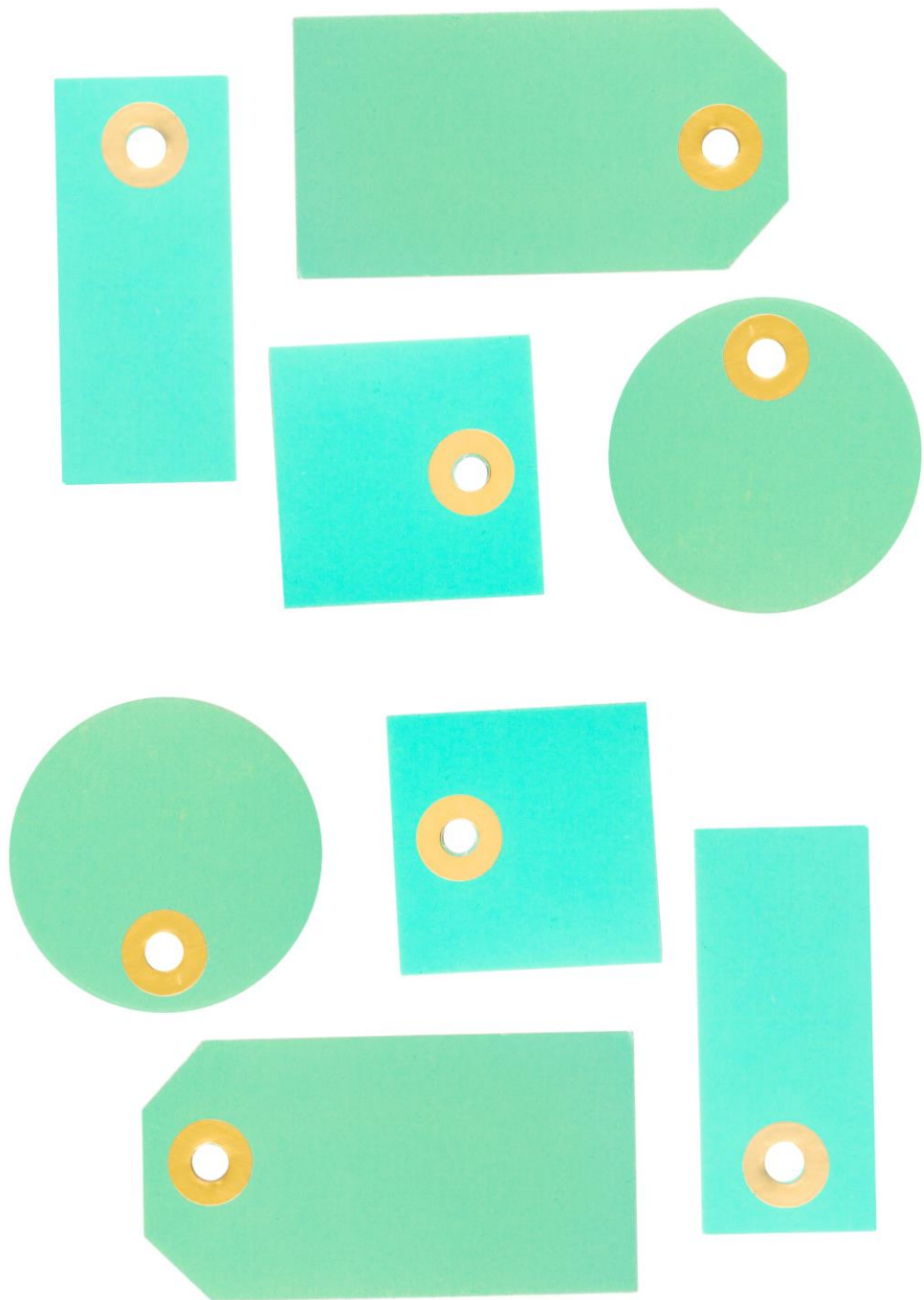
AWS Resources



AWS Tags

Tag key	Tag value
cost-center	193384
environment	PRODUCTION
project	hermes
application-id	xyz456





Tag naming and limits

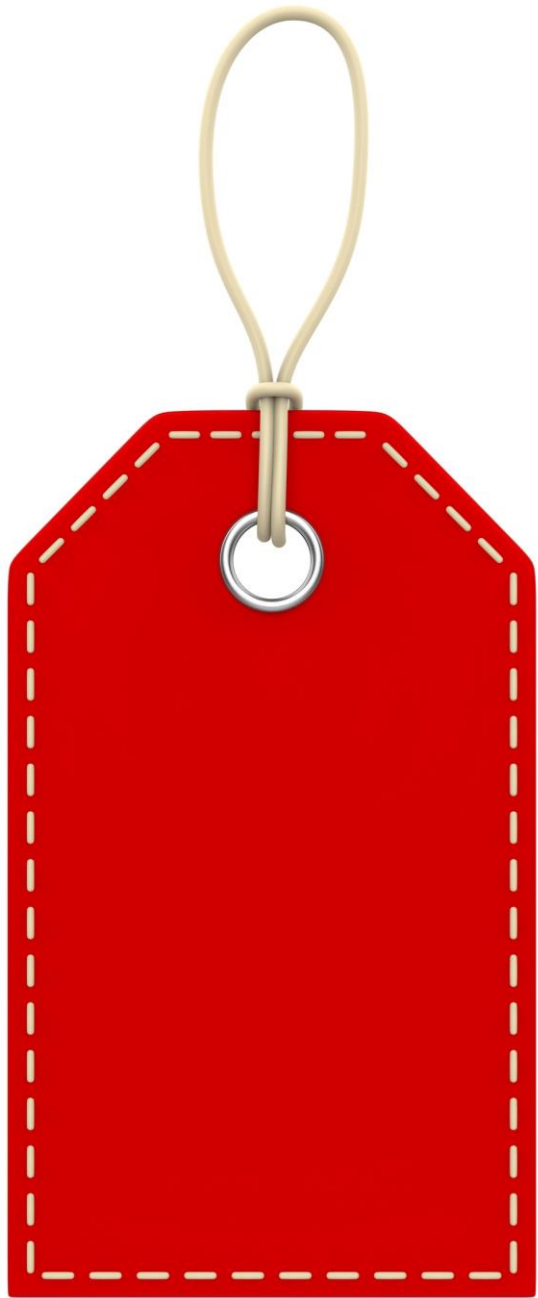
Each resource can have a maximum of 50 tags

System created tags that begin with **aws:** are reserved

For each resource, a Tag key must be unique

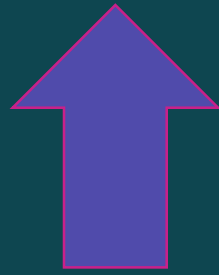
Each tag key can have only one value



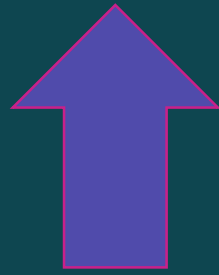


Tag naming and limits

Tag key	Tag value
song-name	supercalifragilisticexpialidocious



1-128 UTF-8 chars



0-256 UTF-8 chars

Letters, numbers, spaces representable in UTF-8, and the following characters:

_ . : / = + - @



CostCenter

#

costCenter

#

Costcenter

#

costcenter

Tag naming and limits

Tag keys and values are
case sensitive

Use the same convention for all tags company-wide

Tagging use cases



Tags for cost allocation



app=foo-bar cost-center=851274

cost-center=761015

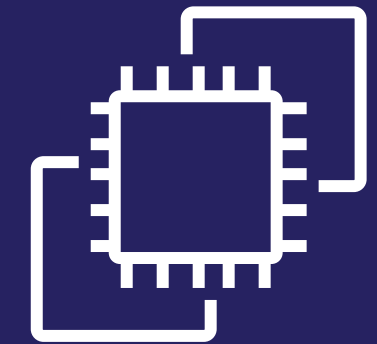
env=PROD

Cost Center	\$
761015	1839.44
851274	373.85

Application	\$
foo-bar	132.43

Environment	\$
PROD	4362.43

Tags for automation



EC2 Instance

Key	Value
auto-shutdown	TRUE
env	DEV
schedule	weekdays



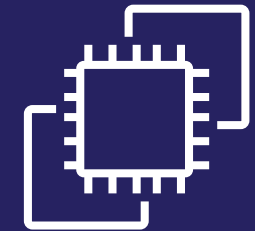
Automated Start-Shutdown

Tags for access control

```
{
  "Action": [
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}"
    }
  }
}
```

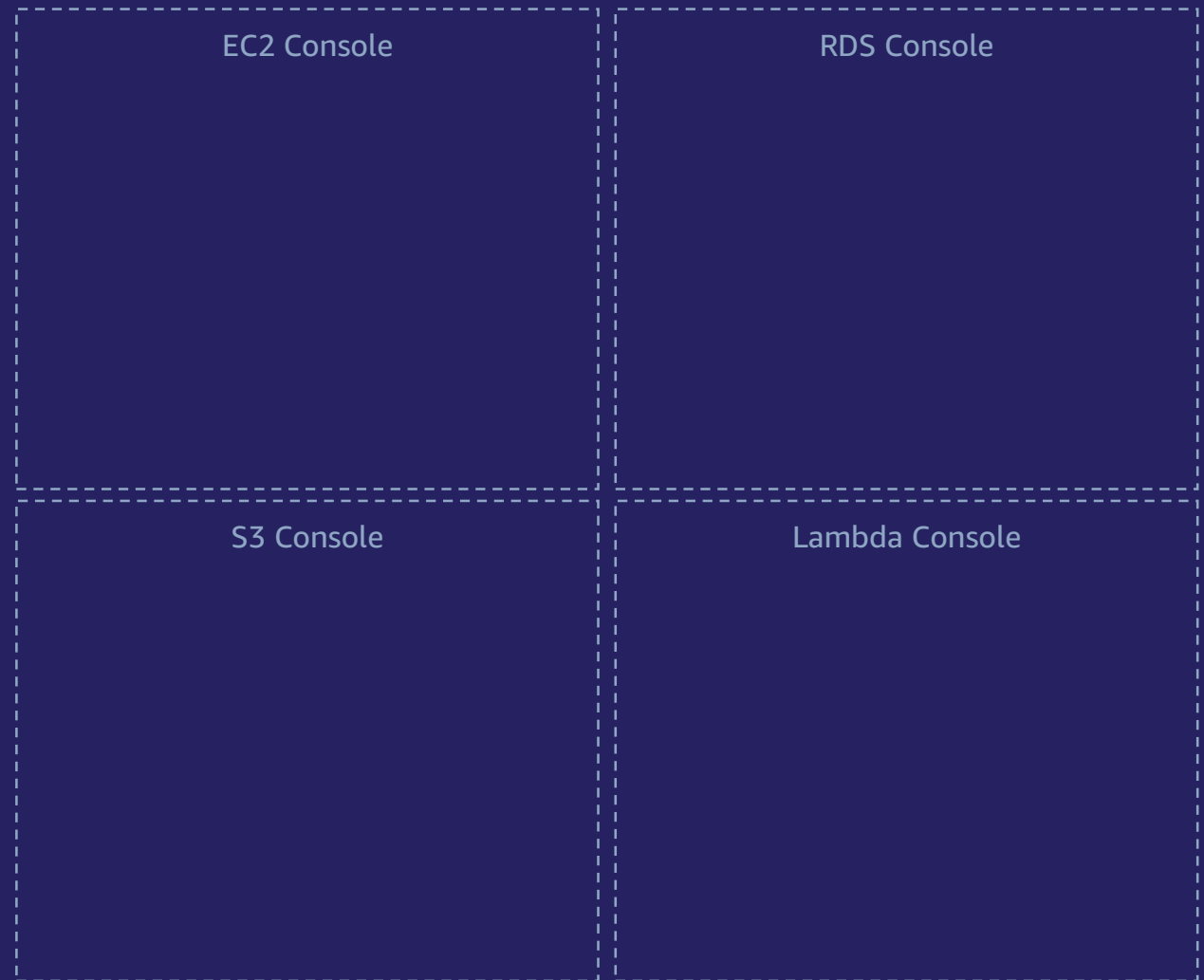


Key	Value
access-project	my-site

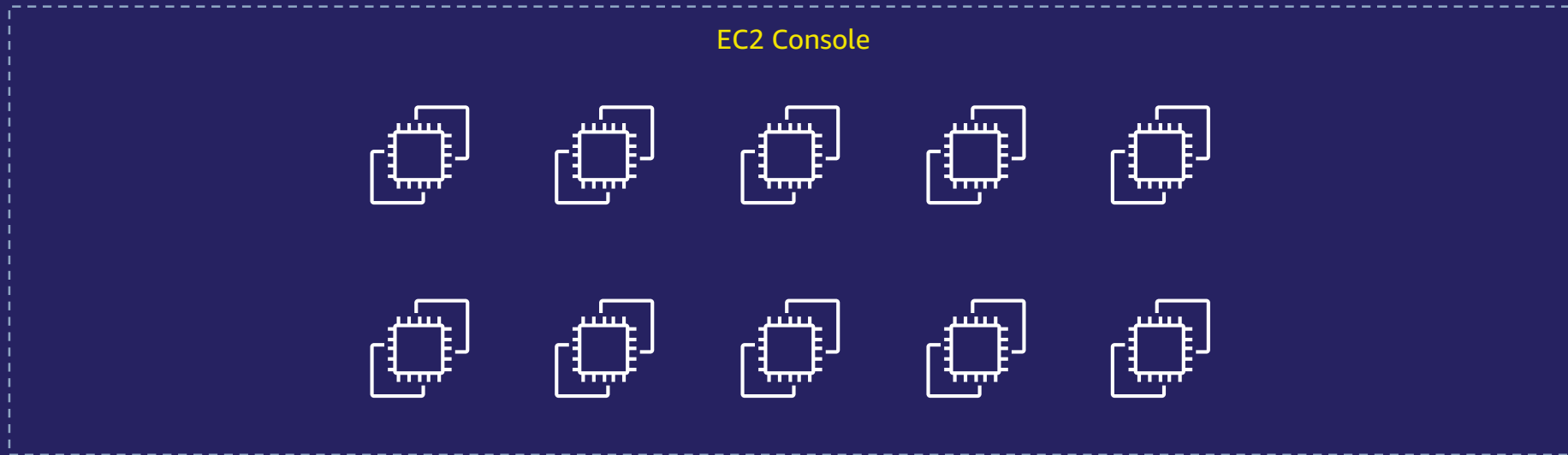


Key	Value
access-project	my-site

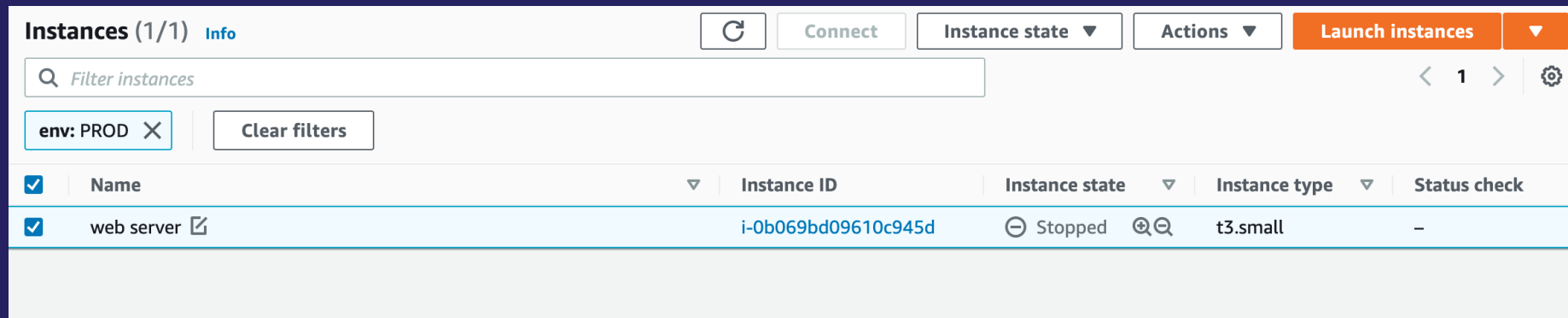
Tags for organizing



Organize resources



env=PROD



A screenshot of the AWS Management Console showing the EC2 Instances page. The page displays a table of instances with the following columns: Name, Instance ID, Instance state, Instance type, and Status check. The table shows one instance named "web server" with Instance ID "i-0b069bd09610c945d", Instance state "Stopped", Instance type "t3.small", and Status check "-". The filter "env: PROD" is applied to the table. The "Launch instances" button is visible in the top right corner.

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check
<input checked="" type="checkbox"/>	web server 🔗	i-0b069bd09610c945d	⊖ Stopped 🔍	t3.small	-

```
$ aws ec2 describe-instances --filters Name=tag:env,Values=PROD
```

Resource groups



Resource groups

AWS service to organize resources

- Automate task on a large number of resources
- Applying updates or security patches
- Updating applications
- Opening or closing ports to network traffic
- Collecting specific log and monitoring data



Resource groups – Tag based

Group type and grouping criteria

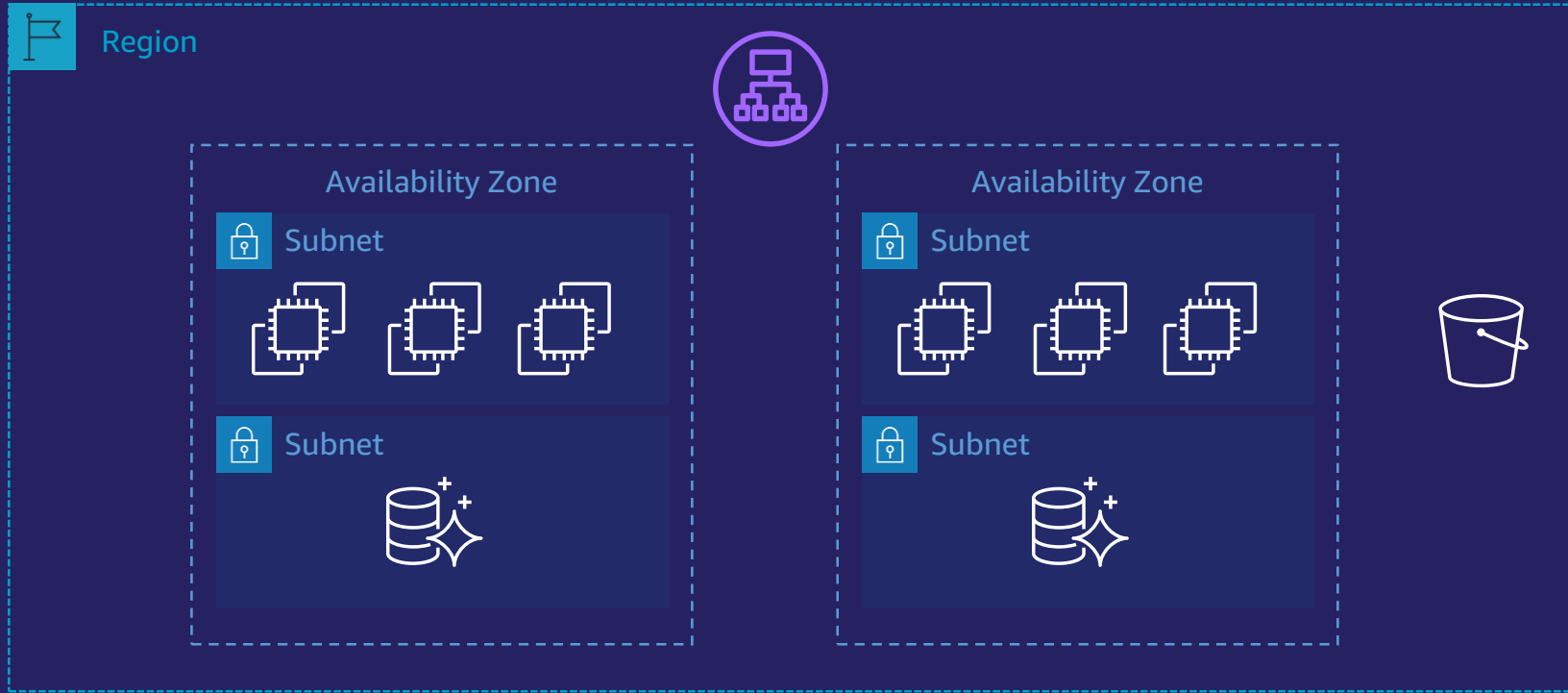
Tag based

All supported resource types

Tag

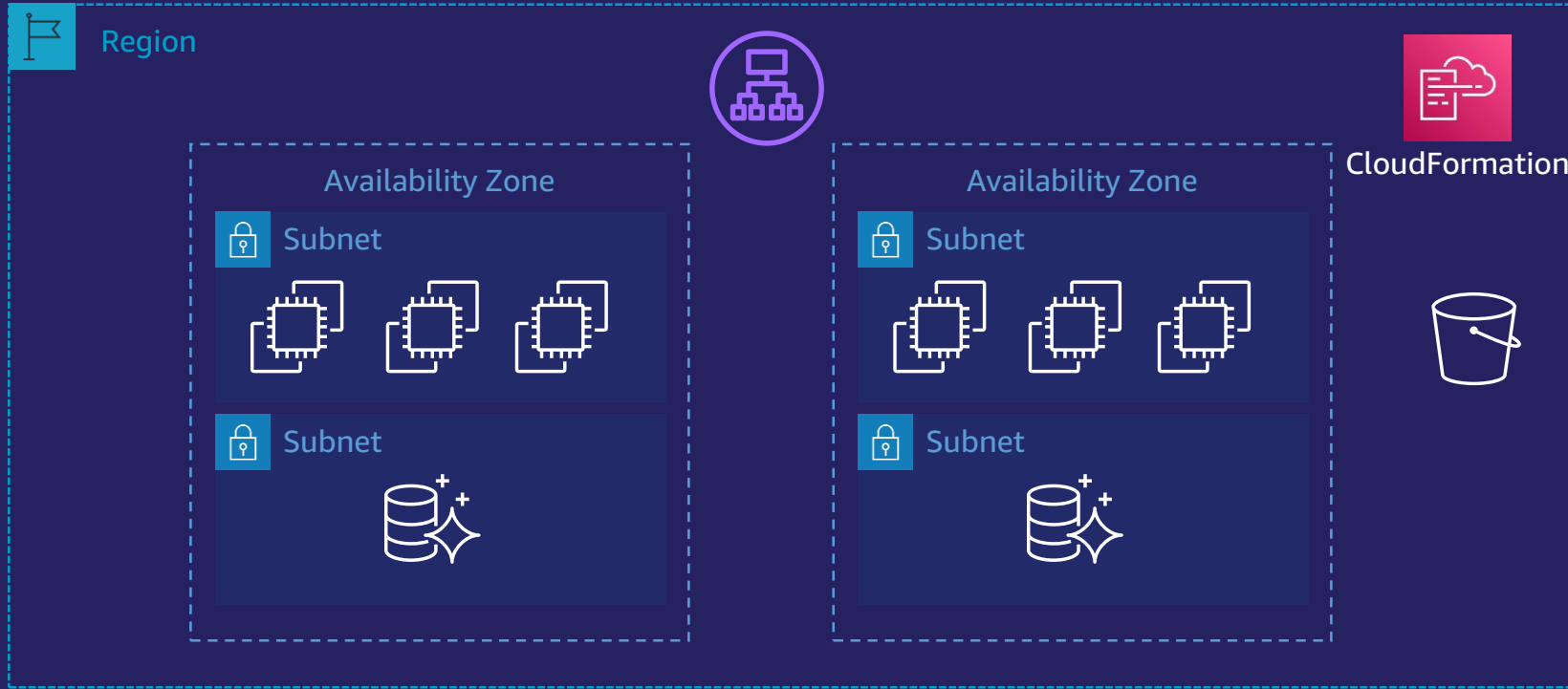
S:

env: PROD
app: MYAPP



Identifier	Tag: Name	Service	Type
i-0b069bd045d069	Webserver10	EC2	Instance
i-9610c90c9450c90	Webserver20	EC2	Instance
my-app-bucket	Production Data	S3	Bucket
database-1	My DB Cluster	RDS	DBCluster
...

Resource groups - CloudFormation



Group type and grouping criteria

CloudFormation stack based

All supported resource types

Stack:

my-site-prod

Identifier	Tag: Name	Service	Type
i-0b069bd045d069	Webserver10	EC2	Instance
i-9610c90c9450c90	Webserver20	EC2	Instance
my-app-bucket	Production Data	S3	Bucket
database-1	My DB Cluster	RDS	DBCluster
...

Resource groups integrations

Service	Integration details
CloudFormation	Provision and organize resources at the same time
CloudWatch	View metrics and alarms for a single resource group
DynamoDB	Create, edit, and delete groups of tables
EC2 dedicated host	Launch instances into resource groups
EC2 capacity reservations	Launch instances into resource groups with capacity reservations
License Manager	Manage licenses of your dedicated host groups
Resilience Hub	Discover applications defined using resource groups
Resource Access Manager	Share host resource groups across accounts
Service Catalog App Registry	Applications are automatically added to a resource group
Systems Manager	Gather insights and take bulk actions on resource groups
VPC Network Access Analyzer	Specify sources and destinations using resource groups

Resource groups demo



Create query-based group

Group type

Select a group type to define a group based on resource types and tags, or create a group based on your existing CloudFormation stack.

Tag based

Group resources by specifying tags that are shared by the resources.

CloudFormation stack based

Create a resource group based on an existing CloudFormation stack. The group will have the same logical structure as the stack.

Grouping criteria

Define a group based on resource types and tags.

Resource types

Select resource types

All supported resource types

Tags

Tag key

Optional tag value

Add

Preview group resources

Group resources

Export to CSV

Filter resources

< 1 > ⚙

Identifier

Tag: Name

Service

Type

Region

Tags

To see resources, click the Preview group resources button.

Group details

Group name

Type a name

Maximum 300 characters. Must contain only letters, numbers and hyphens.

Group description - optional

Type a description

Maximum 512 characters. It can only contain letters, numbers, hyphens, underscores, dots, and spaces.

Group tags - optional

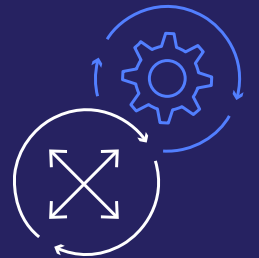
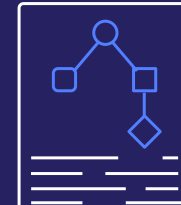
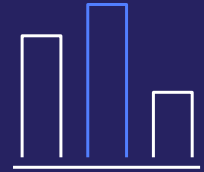
The tags specified here will not be applied to group resources, but only the resource group itself.

Tagging best practices



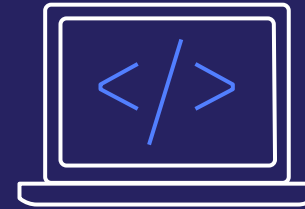
Tagging best practices

- Use tags consistently
- Define tag value proposition
- Focus on required tags
- Start small; less is more
- Adopt a standard for tag names
- Align tags with financial dimensions
- Avoid multi-valued tags
- Integrate with other data sources



Automate tagging

- CloudFormation
 - Resource tags
- Service Catalog
 - TagOption libraries
 - AutoTags
- Tagging solutions
 - Cloud Custodian
 - CloudTrail + Lambda



Tag governance process

- Impact analysis
- Tag request approval
 - Add, change, or deprecate tags
- Monitoring and remediation
 - Missing or incorrect tags
- Report tagging metrics and key process indicators



Tag Editor



Remediate untagged resources

Resource Groups Tagging API

```
$ aws resourcegroupstaggingapi tag-resources \  
  --resource-arn-list arn:aws:s3:::MyProductionBucket \  
  --tags Environment=Production,CostCenter=1234
```

AWS Config

`required-tags`

Tag Editor

Tag Editor

Find resources to tag
You can search for resources that you want to tag across regions. Then, you can add, remove, or edit tags for resources in your search results. [Learn more](#)

Regions
 ▼
 ×

Resource types
 ▼

Tags – Optional

Type the tag key and optional values shared by the resources you want to search for, and then choose Add or press Enter.

Tag Editor

- Find resources to tag
- View and edit tags for selected resources
- Export results to CSV



Tag Editor demo



- AWS Resource Groups
- Resources
 - Create Resource Group
 - Saved Resource Groups
- Tagging
 - Tag Editor
 - Tag Policies
- What's new

Tag Editor

Find resources to tag

You can search for resources that you want to tag across regions. Then, you can add, remove, or edit tags for resources in your search results. [Learn more](#)

Regions

Resource types

Tags - Optional

Type the tag key and optional values shared by the resources you want to search for, and then choose Add or press Enter.

Resource search results

Choose up to 500 resources for which you want to edit tags.

Identifier	Tag: Name	Service	Type	Region	Tags
------------	-----------	---------	------	--------	------

To see results, click the Search resources button.

Tag policies



Tag policies

“When tag key ‘env’ is attached to a resource, tag key must be lowercase and tag value must be PROD, TEST, or DEV”

```
{
  "tags": {
    "env": {
      "tag_key": {
        "@@assign": "env"
      },
      "tag_value": {
        "@@assign": [
          "PROD",
          "DEV",
          "TEST"
        ]
      }
    }
  }
}
```

Tag key	Tag value	Compliant
Env	PROD	NO
ENV	TEST	NO
env	prod	NO
env	PROD	YES

Tag policies



```
{
  "tags": {
    "env": {
      "tag_key": {
        "@@assign": "env"
      },
      "tag_value": {
        "@@assign": [
          "PROD",
          "DEV",
          "TEST"
        ]
      }
    }
  }
}
```



Attach tag policy to root, organizational unit, or account

Tag policies demo



AWS Organizations

- AWS accounts
- Services
- Policies**
- Settings
- Get started

Organization ID
o-79knhb8h5h

AWS Organizations > Policies

Policies

Policies in AWS Organizations enable you to manage different features of the AWS accounts in your organization. [Learn more](#)

Policy type	Status
AI services opt-out policies Artificial Intelligence (AI) services opt-out policies enable you to control whether AWS AI services can store and use your content. Learn more	Enabled
Backup policies Backup policies enable you to deploy organization-wide backup plans to help ensure compliance across your organization's accounts. Using policies helps ensure consistency in how you implement your backup plans. Learn more	Enabled
Service control policies Service control policies (SCPs) enable central administration over the permissions available within the accounts in your organization. This helps ensure that your accounts stay within your organization's access control guidelines. Learn more	Enabled
Tag policies Tag policies help you standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values. Learn more	Enabled

AWS Resource Access Manager



AWS Resource Access Manager

- Securely share resources across AWS accounts
- Share within AWS Organizations, IAM roles, and IAM users
- Reduce operational overhead
- Improve security and visibility
- Optimize costs





AWS Organizations

Infrastructure OU

Networking Account



Transit Gateway

Workloads OU

App A Account



App B Account



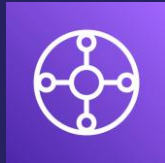
AWS Organizations

Infrastructure OU

Networking Account

Private subnet

Private subnet



Workloads OU

App A Account

App B Account

Resource Access Manager demo



- Resource Groups & Tag Editor
- Resource Access Manager**
 - Shared by me
 - Resource shares
 - Shared resources
 - Principals
 - Shared with me
 - Resource shares
 - Shared resources
 - Principals
 - Permissions library **New**
 - Settings

AWS Resource Access Manager

Share AWS resources with other AWS accounts.

Start sharing your AWS resources with other accounts

[Create a resource share](#)

Pricing

AWS RAM is offered at no additional charge. There are no setup fees or upfront commitments.

More resources

- [What is AWS Resource Access Manager?](#)
- [Getting started](#)
- [Documentation](#)

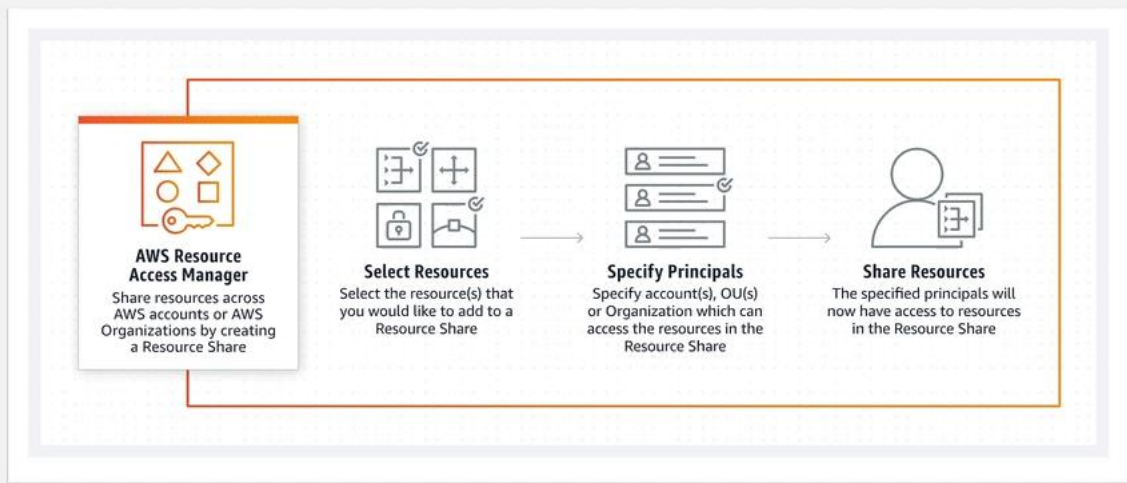
Your AZ ID

AZ IDs provides a consistent way of identifying the location of a resource across all your accounts. This makes it easier for you to provision resources centrally in a single account and share them across multiple accounts.

The following table shows you the AZ IDs for availability zones in this region

AZ Name	AZ ID
us-east-2a	use2-az1
us-east-2b	use2-az2
us-east-2c	use2-az3

How it works



Use cases

Manage resources centrally in a multi-account environment

Create resources centrally and use RAM to share them to benefit from a simplified resource management experience in a multi-account environment.

Increase efficiency, decrease costs

RAM enables you to efficiently use your resources across accounts in multiple parts of your company, improving utilization and driving costs down.

Stay compliant

You can use RAM to easily share standard building blocks to enable compliance and maintain consistency across accounts.

Benefits and features

Reduces operational overhead

Create resources centrally, and use RAM to share those resources with other accounts. This eliminates the need to provision duplicate resources in every account, which reduces operational overhead.

Visibility and auditability

Through integration with AWS CloudWatch and AWS CloudTrail, RAM provides comprehensive visibility into shared resources and accounts.



Thank you!