Terraform ECR Repository Module

Provider: AWS (`hashicorp/aws`)

1. Overview

This Terraform configuration creates an **Amazon Elastic Container Registry (ECR)** repository with:

- Configurable image tag mutability (`MUTABLE`/`IMMUTABLE`)
- Automated vulnerability scanning on push
- Custom tags for resource tracking

---

2. Resource: `aws_ecr_repository`

Configuration

Parameter	Description	Default/Value
`name`	Name of the ECR repository	*Required* (`var.ecr_name`)
`image_tag_mutability`	Tag immutability setting	`"MUTABLE"`
`scan_on_push`	Enable scan-on-push for vulnerabilities	`true`
`tags`	Custom tags (e.g., `Environment=prod`)	*Required* (`var.tags`)

Example Usage

```hcl
Copy
module "ecr" {
  source = "./path/to/module"

  ecr_name         = "my-app-ecr"
  img_tag_mutability = "IMMUTABLE"  # Prevent tag overwrites
  scan_on_push     = true
  tags             = { Environment = "prod" }
}
```

3. Variables (`variables.tf`)

Variable	Type	Default	Description
`ecr_name`	`string`	*Required*	Name of the ECR repository
`img_tag_mutability`	`string`	`"MUTABLE"`	`MUTABLE` or `IMMUTABLE`
`scan_on_push`	`bool`	`true`	Enable automatic image scanning
`tags`	`map(string)`	*Required*	Tags (e.g., `{ Team = "DevOps" }`)
`user_region`	`string`	`"us-east-1"`	AWS region (unused in resource)

4. Outputs (`outputs.tf`)

Output	Description	Example Value
`ecr_name`	Repository name	`"my-app-ecr"`
`ecr_id`	Registry ID (AWS account ID)	`"123456789012"`
`ecr_uri`	Repository URL	`"123456789012.dkr.ecr.us-east-1.amazonaws.com/my-app-ecr"`
`ecr_region`	**Note**: Outputs ARN, not region (fix recommended)	`"arn:aws:ecr:us-east-1:123456789012:repository/my-app-ecr"`

5. Security Recommendations

1. **Immutable Tags**: Set `img_tag_mutability = "IMMUTABLE"` in production to prevent image tampering.
2. **Scanning**: Keep `scan_on_push = true` for CVE detection.
3. **IAM Policies**: Restrict push/pull access using IAM policies.

6. Fix for `ecr_region` Output

The current `ecr_region` output returns the ARN, not the region. To fix:

hcl

output "ecr_region" {

  value = var.user_region # Or parse from ARN: split(":", aws_ecr_repository.aws_ecr.arn)[3]

}

Dependencies

- **AWS Provider**: Requires `hashicorp/aws` configured with proper credentials.