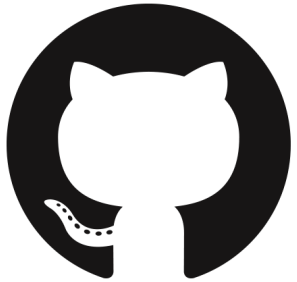
Using Terraform Safely

Martez Reed

Martez Reed

martezreed
Linkedin

@greenreedtech
Twitter



Martezr
Github

Infrastructure as Code (IaC)

Declaring and creating infrastructure resources through code

- AWS Cloudformation
- Azure ARM Templates
- Pulumi
- HashiCorp Terraform

HashiCorp Terraform

- Written in Golang
- Resource declaration in HCL
- Terraform providers for resource interation

```
resource "aws_instance" "web" {
  ami           = "${data.aws_ami.ubuntu.id}"
  instance_type = "t2.micro"

  tags = {
    Name = "HelloWorld"
  }
}
```

Terraform Modules

A container for multiple resources used together.

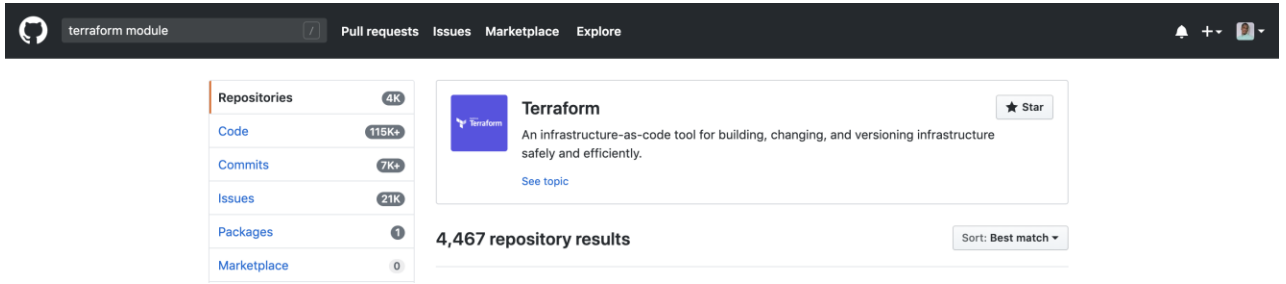
- Corporate EC2 Instance
- Application Stack
- AWS Network Stack

Public Terraform Modules

Terraform Registry: 109 Terraform Modules

https://registry.terraform.io/

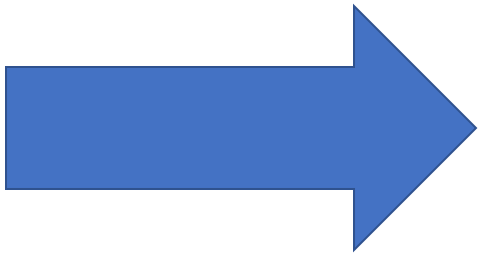
GitHub: 4,467 Terraform Modules



https://github.com/search?q=terraform+module

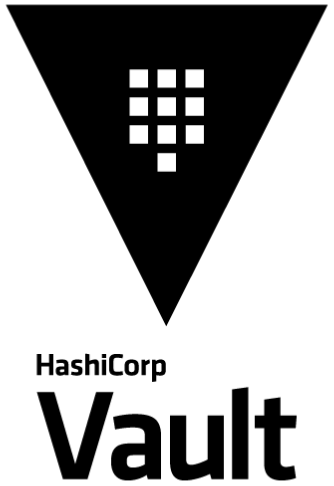
Public Terraform Modules

Speed (Agility)



Security

Public Terraform Modules

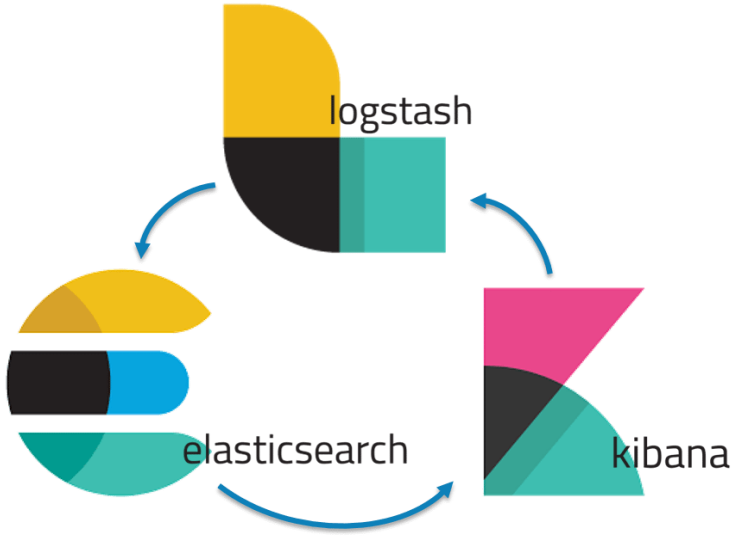



```
# !! WARNING !! These example AMIs are meant only convenience when initially testing this repo. Do NOT use these example
# AMIs in a production setting as those TLS certificate files are publicly available from the Module repo containing
# this code.


# To make testing easier, we allow requests from any IP address here but in a production deployment, we *strongly*
# recommend you limit this to the IP address ranges of known, trusted servers inside your VPC.

allowed_ssh_cidr_blocks             = ["0.0.0.0/0"]
allowed_inbound_cidr_blocks         = ["0.0.0.0/0"]
```

Public Terraform Modules



Public Terraform Modules

- Develop a formal module review process
- Understand the technology
- Update the module version accordingly

Terraform Secrets

```
resource "tls_private_key" "example" {
  algorithm = "ECDSA"
}

resource "tls_self_signed_cert" "example" {
  key_algorithm   = "${tls_private_key.example.algorithm}"
  private_key_pem = "${tls_private_key.example.private_key_pem}"
  validity_period_hours = 12
  allowed_uses = [
      "key_encipherment",
      "digital_signature",
      "server_auth",
  ]
  subject {
      common_name  = "example.com"
  }
}
```

https://www.terraform.io/docs/state/sensitive-data.html

Terraform Secrets

tls_private_key resource

Important Security Notice The private key generated by this resource will be stored *unencrypted* in your Terraform state file. **Use of this resource for production deployments is *not* recommended**. Instead, generate a private key file outside of Terraform and distribute it securely to the system where Terraform will be run.

https://www.terraform.io/docs/providers/tls/r/private_key.html

Terraform Secrets

Terraform Show Output

```
# tls_private_key.example:
resource "tls_private_key" "example" {
    algorithm       = "ECDSA"
    ecdsa_curve     = "P224"
    id              = "97bbb6dc1cfe44f5cf33976a2b94fba8671c422f"
    private_key_pem = "-----BEGIN EC PRIVATE KEY-----\nMGgCAQEEHIFodc48ovOxgeTFOhw039UcMC5glOZyI8NIcq2gBwYFK4EEACGhPAM6\nAAQ044dMB
tBC7BG4oeRiKYEBg+2PoyOqE1LNNXcAeURuKhQZGj9AL/jxAgKRMAn/\nJstJekojzTRQ7Q==\n-----END EC PRIVATE KEY-----\n"
    public_key_pem  = "-----BEGIN PUBLIC KEY-----\nME4wEAYHKoZIzj0CAQYFK4EEACEDOgAENOOHTAbQQuwRuKHkYimBAYPtj6MjqhNS\nzTV3AHlEbioUG
Ro/QC/48QICkTAJ/ybLSXpKI800UO0=\n-----END PUBLIC KEY-----\n"
    rsa_bits        = 2048
}
```

Terraform Secrets

Private key is visible in tfstate files #38

Open [redacted] opened this issue 21 days ago · 4 comments

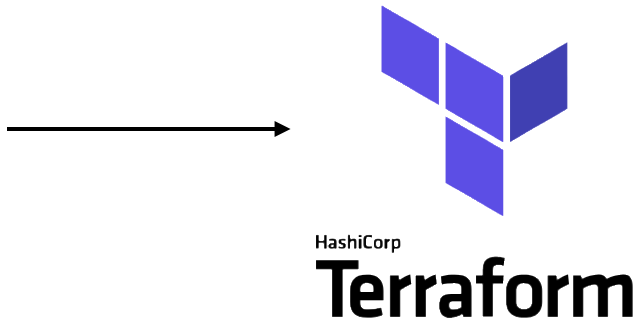
[redacted]

[redacted] commented 21 days ago

I can see private key in tfstate file..... isn't it a security breach..?

Terraform Secrets

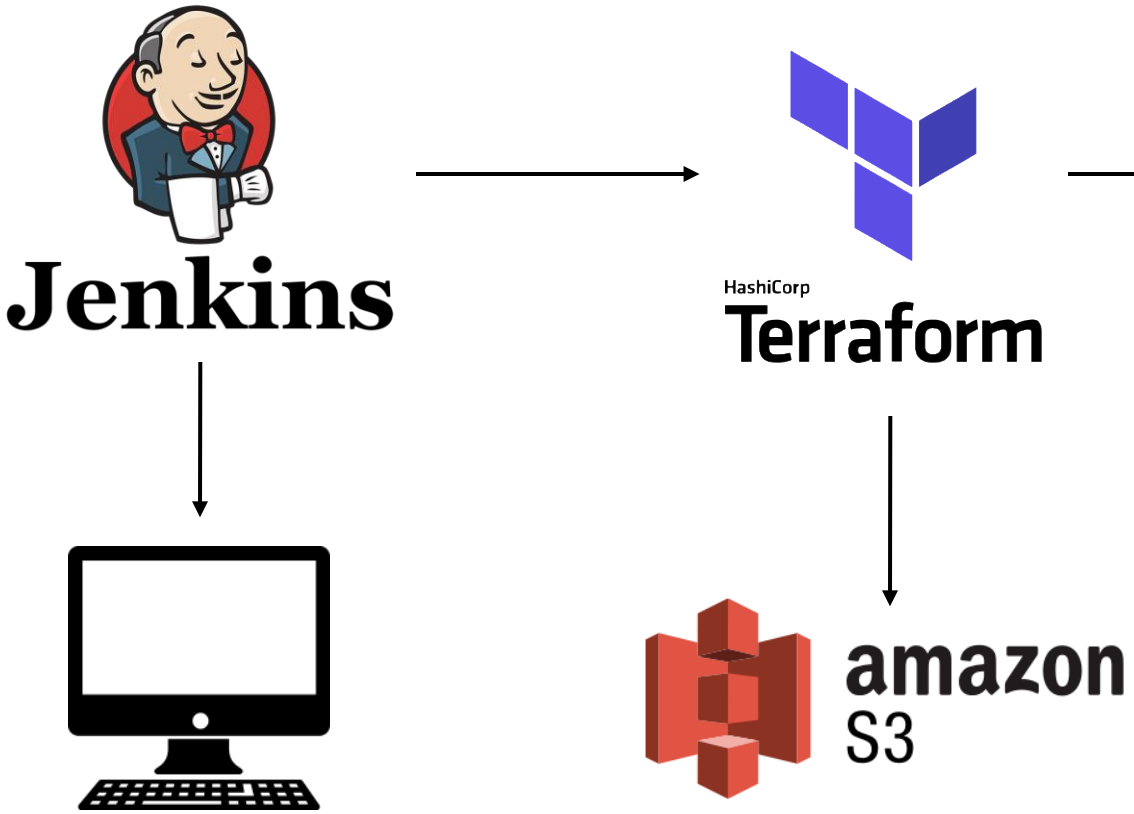
State Storage Encryption



DEVOPSDAYS CHICAGO 2019

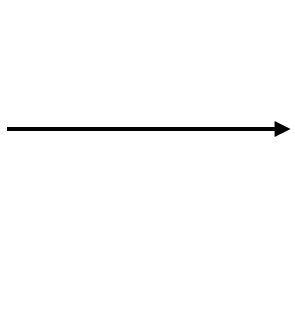
Terraform Secrets

Jenkins Console Output



Terraform Secrets

Jenkins Log File



Terraform Secrets

- Terrahelp: A tool written in GO that integrates with HashiCorp Vault to provide both file and inline encryption of Terraform state files.
- Terraformectomy: A shell script for redacting aws secrets from Terraform state files.
- Terraform IAM Redact Script: Another shell script for redacting AWS secrets from Terraform state files.

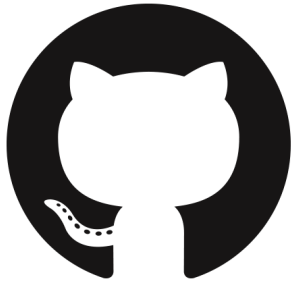
Terraform Secrets

There's no perfect solution but knowledge is power and knowing is half the battle

Martez Reed

martezreed
Linkedin

@greenreedtech
Twitter



Martezr
Github