Kiki's Secret Delivery Service over AF_VSOCK

Florian Maury

Terraform

Infrastructure as Code (IaC) command line tool

Declarative syntax

```
resource "outscale_net" "net01" {
    ip_range = "10.10.0.0/16"
    tenancy  = "default"
}
```

Metadata and data persisted within a state

State stored in cleartext

Ephemeral resources

Introduced in Terraform v1.10

New lifecycle: created and destroyed/closed with each run

- no trace in state

Allows secret handling and temporary infrastructure

Secret Deployment

Secret Manager

Contains all the secrets

Gives access to secrets on the need-to-know basis

Requires authentication

Go back to start, do not collect $200: requires a secret to authenticate!

Secret Deployment

Cloud-init: extremely difficult to secure

Ignition: not built for that

SSH delivery/Ansible:

- problem converter from confidentiality to integrity/authentication
- what is the SSH host public key?

Virtual Infrastructure Solution

Hypervisor network

AF_VSOCK:

- allows communications between hypervisor and guest
- no IP address; uses a Context ID (CID) assigned by the hypervisor

Systemd-ssh-generator:

- detects being run in a guest VM
- generates a .socket unit to listen on AF_VSOCK

ssh2vsock Terraform Provider

- https://registry.terraform.io/providers/X-Cli/ssh2vsock/latest/docs
- implements:
    - a data source to do a ssh-keyscan over AF_VSOCK
    - an ephemeral resource to build a SSH tunnel over AF_VSOCK
- allows skipping the host public key verification by leveraging implicit trust in the hypervisor