**Terraform supported manipulation**

既然手動直接 vim 下去不是一個好方法，我們先來看 [terraform 官方支援的 state 操作](https://www.terraform.io/docs/cli/state/index.html)

state

* list
* show
* mv
* rm
* refresh
* taint/untaint
* import

**list**

terraform state list 上堂課已經說明過，放在這邊做範例

cd azure/foundation/compute\_network

terragrunt state list

module.network.data.azurerm\_resource\_group.network

module.network.azurerm\_subnet.subnet[0]

module.network.azurerm\_subnet.subnet[1]

module.network.azurerm\_subnet.subnet[2]

module.network.azurerm\_virtual\_network.vnet

另外一個用例是，有時我們在 web console 上看到 azure cloud 上的 remote resource，例如：在 azure web console 上看到一個 subnet，我們想要

* 根據 subnet 在 web consoel 上的資訊查詢對應的 .tf resource {} 在哪以便更改
* 根據我們對 terraform 的理解，實際的 subnet 需要透過 state 查詢，才能對應到 .tf resource
* 然而在一個複雜的 module 中 state list 出來的 resource 可能很多
* 直接閱讀 .tf 也會十分花時間，複雜的 terraform module 的 directory 也會十分複雜，可能會在引用外部 module，例如：azure/modules/compute\_network 內又引用 Azure/network/azurerm

terraform 提供了 state filter by id 的方式

* 在 web console 查到實際物件的 id
* 直接在 state list 中 filter by id 就可以快速查到 state
* 也可以根據 resource address 輕鬆找到 .tf resource

terraform state list -id /subscriptions/6fce7237-7e8e-4053-8e7d-ecf8a7c392ce/resourceGroups/terraform-30-days/providers/Microsoft.Network/virtualNetworks/acctvnet/subnets/dev-1

module.network.azurerm\_subnet.subnet[0]

**show**

這時我們可以進一步 show 出 state 的內容

terragrunt state show module.network.azurerm\_virtual\_network.vnet

resource "azurerm\_virtual\_network" "vnet" {

address\_space = [

"10.2.0.0/16",

]

dns\_servers = []

guid = "5e5fb9de-600b-4085-a59d-0792c567c3a3"

id = "/subscriptions/6fce7237-7e8e-4053-8e7d-ecf8a7c392ce/resourceGroups/terraform-30-days/providers/Microsoft.Network/virtualNetworks/acctvnet"

location = "southeastasia"

name = "acctvnet"

resource\_group\_name = "terraform-30-days"

subnet = [

{

address\_prefix = "10.2.1.0/24"

id = "/subscriptions/6fce7237-7e8e-4053-8e7d-ecf8a7c392ce/resourceGroups/terraform-30-days/providers/Microsoft.Network/virtualNetworks/acctvnet/subnets/dev-1"

name = "dev-1"

security\_group = ""

},

{

address\_prefix = "10.2.2.0/24"

id = "/subscriptions/6fce7237-7e8e-4053-8e7d-ecf8a7c392ce/resourceGroups/terraform-30-days/providers/Microsoft.Network/virtualNetworks/acctvnet/subnets/dev-2"

name = "dev-2"

security\_group = ""

},

{

address\_prefix = "10.2.3.0/24"

id = "/subscriptions/6fce7237-7e8e-4053-8e7d-ecf8a7c392ce/resourceGroups/terraform-30-days/providers/Microsoft.Network/virtualNetworks/acctvnet/subnets/dev-3"

name = "dev-3"

security\_group = ""

},

]

tags = {

"environment" = "foundation"

}

vm\_protection\_enabled = false

}

基本上所有 terraform 中設定 / 產生的資料，state 裡面都有

* 設定的 resource argument 參數
* apply 之後，API 回傳的實際 id / guid，對應遠端的 resource

在看另外一個

* [] 是 bash 的特殊字元，再進到 terraform 前，就被 bash 判定語法有誤
* 記得要使用 double / single quote

terragrunt state show module.network.azurerm\_subnet.subnet[0]

zsh: no matches found: module.network.azurerm\_subnet.subnet[0]

terragrunt state show 'module.network.azurerm\_subnet.subnet[0]'

resource "azurerm\_subnet" "subnet" {

address\_prefix = "10.2.1.0/24"

address\_prefixes = [

"10.2.1.0/24",

]

enforce\_private\_link\_endpoint\_network\_policies = false

enforce\_private\_link\_service\_network\_policies = false

id = "/subscriptions/6fce7237-7e8e-4053-8e7d-ecf8a7c392ce/resourceGroups/terraform-30-days/providers/Microsoft.Network/virtualNetworks/acctvnet/subnets/dev-1"

name = "dev-1"

resource\_group\_name = "terraform-30-days"

service\_endpoint\_policy\_ids = []

service\_endpoints = []

virtual\_network\_name = "acctvnet"

}

**Sensitive**

對資安敏感的人，可能看到 state show 已經覺得不太舒服

* 怎麼所有的參數都列出來啊
* 這邊的範例還沒有使用 sensitive variable，例如 password / secret 內容，state 中這些參數也是明碼儲存的

terraform state 其實是有一定的敏感性，官方文件也有建議要好好保管 terraform state 檔案

* 裡頭含有敏感資料，整個就要試做是敏感資料處理，應該加密儲存
* 並在 storage account 加上帳號群線控管
* 這課程的範例我們都沒做，所以 tfsec 掃描會一直報警 ;)
* state 落到有心人士手上，可以做很多事情，請妥善保管
* 這也是為何不建議 commit state 到版本控制系統中的原因之一