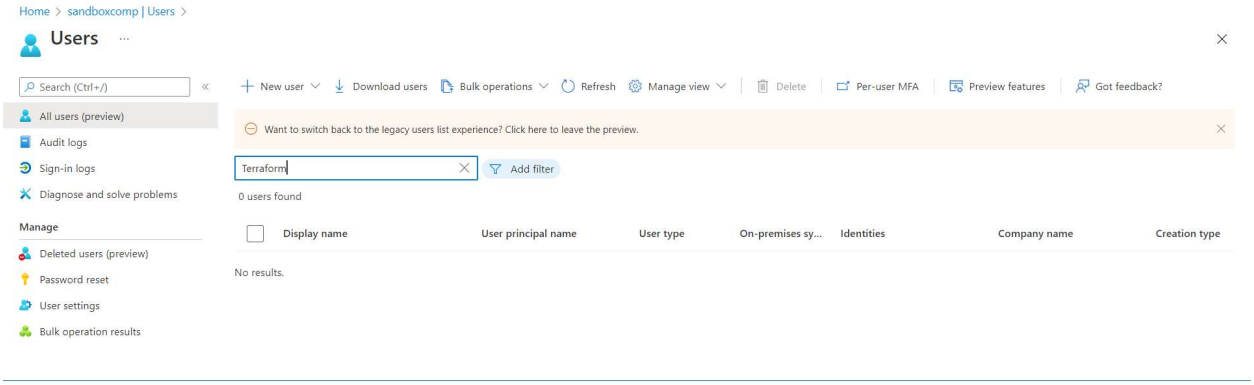
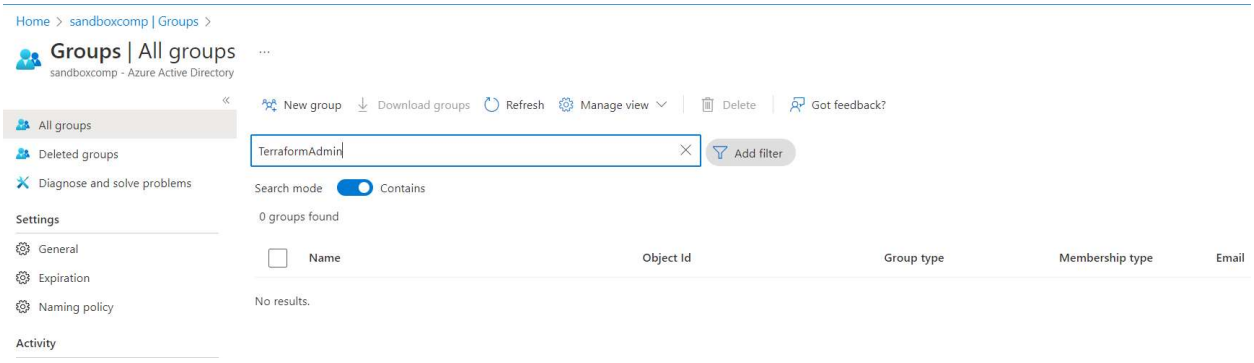
Terraform Multi-cloud Sample: AWS IAM and Azure AD

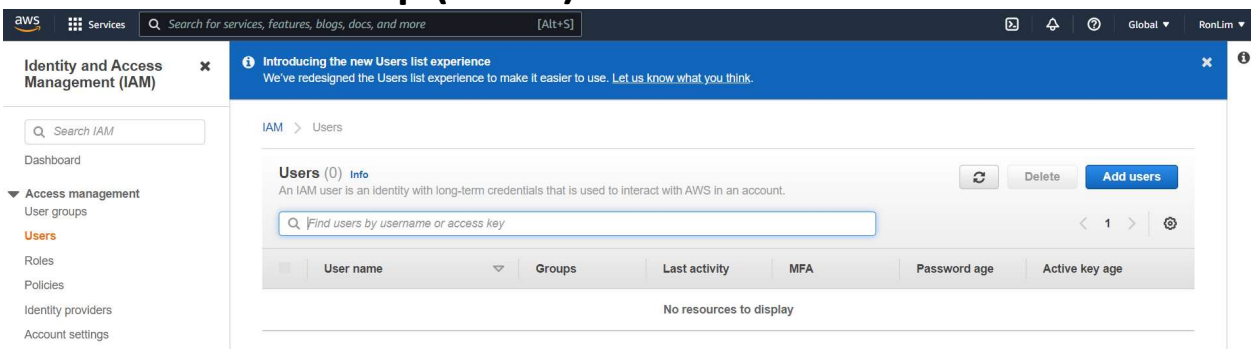
By Ronald Stewart Lim

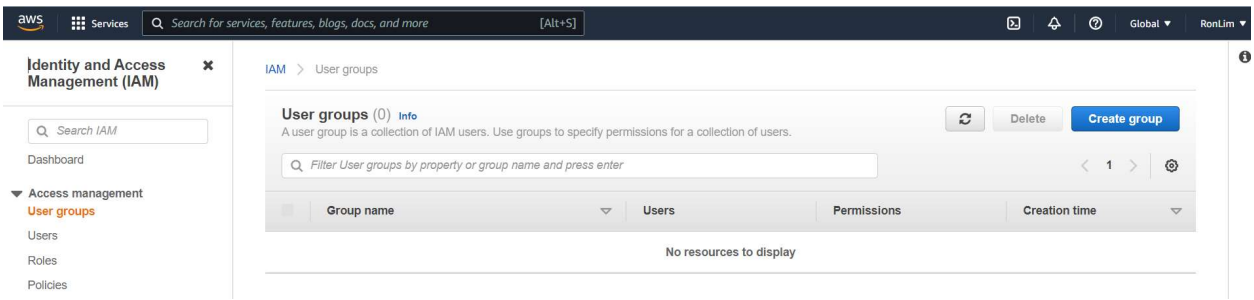
Azure User and Group (Initial)





AWS User and Group (Initial)





Terraform Multi-cloud Sample: AWS IAM and Azure AD

By Ronald Stewart Lim

Terraform Multicloud Implementation

- AWS Access Key already configured
- Authenticated in Azure using az login

Terraform implementation Output

```
D:\Terraform\terraform_multicloud>az login --allow-no-subscriptions
A web browser has been opened at
https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue the login in
the web browser. If no web browser is available or if the web browser fails to open, use device code
flow with `az login --use-device-code`.
The following tenants don't contain accessible subscriptions. Use 'az login --allow-no-subscriptions' to
have tenant level access.
c4ec77fe-bffb-47f2-9d98-d2d8266e17e7 'sandboxcomp'
[
 {
  "cloudName": "AzureCloud",
  "id": "<confidential>",
  "isDefault": true,
  "name": "N/A(tenant level account)",
  "state": "Enabled",
  "tenantId": "<confidential>",
  "user": {
   "name": "ron_lim_ms@sandboxcomp.onmicrosoft.com",
   "type": "user"
  }
 }
]

D:\Terraform\terraform_multicloud>aws configure
AWS Access Key ID [****************46RW]:
AWS Secret Access Key [****************gxlW]:
Default region name [us-east-1]:
Default output format [None]:

D:\Terraform\terraform_multicloud>cd AWS_IAM_Azure_AD

D:\Terraform\terraform_multicloud\AWS_IAM_Azure_AD>terraform init

Initializing the backend...

Initializing provider plugins...
- Finding latest version of hashicorp/azuread...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/azuread v2.28.1...
- Installed hashicorp/azuread v2.28.1 (signed by HashiCorp)
```

- Installing hashicorp/aws v4.29.0...
- Installed hashicorp/aws v4.29.0 (signed by HashiCorp)

Terraform has created a lock file .terraform.lock.hcl to record the provider selections it made above. Include this file in your version control repository so that Terraform can guarantee to make the same selections by default when you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see any changes that are required for your infrastructure. All Terraform commands should now work.

If you ever set or change modules or backend configuration for Terraform, rerun this command to reinitialize your working directory. If you forget, other commands will detect it and remind you to do so if necessary.

D:\Terraform\terraform_multicloud\AWS_IAM_Azure_AD>terraform validate
Success! The configuration is valid.

D:\Terraform\terraform_multicloud\AWS_IAM_Azure_AD>terraform apply

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
  + create

Terraform will perform the following actions:

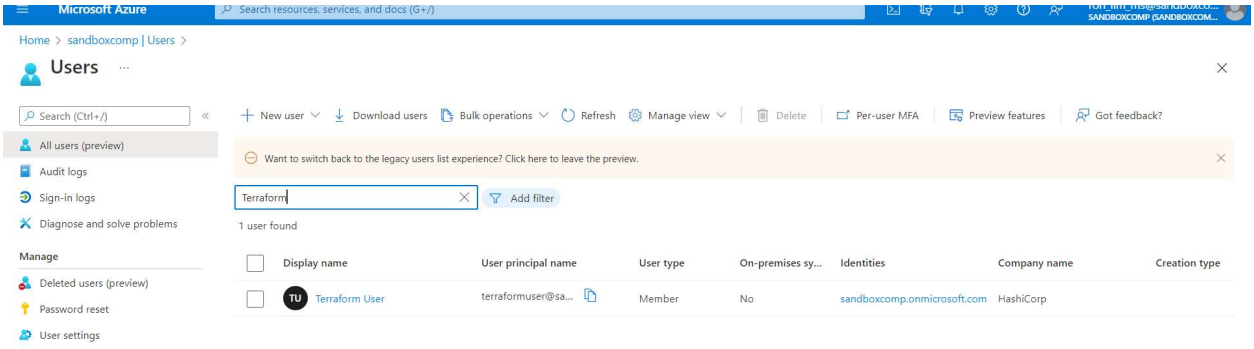
```
  # aws_iam_group.admingroup will be created
  + resource "aws_iam_group" "admingroup" {
      + arn       = (known after apply)
      + id        = (known after apply)
      + name      = "admingroup"
      + path      = "/"
      + unique_id = (known after apply)
    }

  # aws_iam_group_membership.adminteam will be created
  + resource "aws_iam_group_membership" "adminteam" {
      + group = "admingroup"
      + id    = (known after apply)
      + name  = "tf-testing-group-membership"
      + users = [
          + "admin1",
          + "admin2",
```

```
    ]
 }

# aws_iam_user.testadminuser1 will be created
+ resource "aws_iam_user" "testadminuser1" {
   + arn          = (known after apply)
   + force_destroy = false
   + id           = (known after apply)
   + name         = "admin1"
   + path         = "/"
   + tags_all     = (known after apply)
   + unique_id    = (known after apply)
 }

# aws_iam_user.testadminuser2 will be created
+ resource "aws_iam_user" "testadminuser2" {
   + arn          = (known after apply)
   + force_destroy = false
   + id           = (known after apply)
   + name         = "admin2"
   + path         = "/"
   + tags_all     = (known after apply)
   + unique_id    = (known after apply)
 }

# azuread_group.group will be created
+ resource "azuread_group" "group" {
   + auto_subscribe_new_members     = (known after apply)
   + display_name                   = "TerraformAdmin"
   + external_senders_allowed       = (known after apply)
   + hide_from_address_lists        = (known after apply)
   + hide_from_outlook_clients      = (known after apply)
   + id                             = (known after apply)
   + mail                           = (known after apply)
   + mail_nickname                  = (known after apply)
   + members                        = (known after apply)
   + object_id                      = (known after apply)
   + onpremises_domain_name         = (known after apply)
   + onpremises_netbios_name        = (known after apply)
   + onpremises_sam_account_name    = (known after apply)
   + onpremises_security_identifier = (known after apply)
   + onpremises_sync_enabled        = (known after apply)
   + owners                         = (known after apply)
   + preferred_language             = (known after apply)
   + prevent_duplicate_names        = false
   + proxy_addresses                = (known after apply)
   + security_enabled               = true
```

```
    + visibility                = (known after apply)
  }

 # azuread_group_member.groupmember will be created
 + resource "azuread_group_member" "groupmember" {
    + group_object_id  = (known after apply)
    + id               = (known after apply)
    + member_object_id = (known after apply)
  }

 # azuread_user.user will be created
 + resource "azuread_user" "user" {
    + about_me                    = (known after apply)
    + account_enabled             = true
    + business_phones             = (known after apply)
    + company_name                = "HashiCorp"
    + creation_type               = (known after apply)
    + department                  = "HashiCorp"
    + disable_password_expiration = false
    + disable_strong_password     = false
    + display_name                = "Terraform User"
    + external_user_state         = (known after apply)
    + force_password_change       = false
    + id                          = (known after apply)
    + im_addresses                = (known after apply)
    + mail                        = (known after apply)
    + mail_nickname               = "terraformuser"
    + object_id                   = (known after apply)
    + onpremises_distinguished_name  = (known after apply)
    + onpremises_domain_name      = (known after apply)
    + onpremises_immutable_id     = (known after apply)
    + onpremises_sam_account_name = (known after apply)
    + onpremises_security_identifier = (known after apply)
    + onpremises_sync_enabled     = (known after apply)
    + onpremises_user_principal_name = (known after apply)
    + password                    = (sensitive value)
    + proxy_addresses             = (known after apply)
    + show_in_address_list        = true
    + user_principal_name         = "terraformuser@sandboxcomp.onmicrosoft.com"
    + user_type                   = (known after apply)
  }

Plan: 7 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.
```

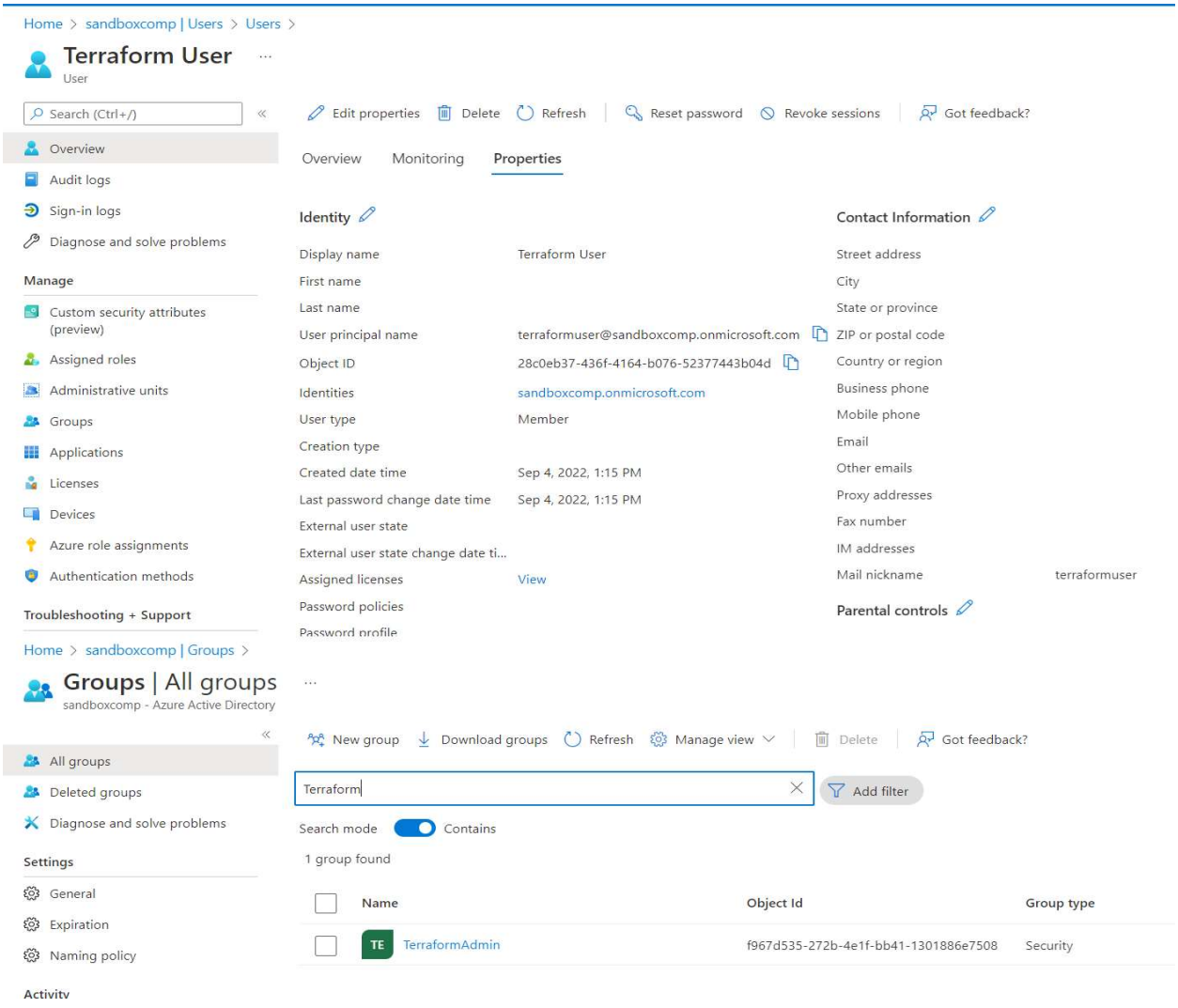
```
Enter a value: yes

azuread_group.group: Creating...
azuread_user.user: Creating...
aws_iam_group.admingroup: Creating...
aws_iam_user.testadminuser2: Creating...
aws_iam_user.testadminuser1: Creating...
azuread_user.user: Creation complete after 2s [id=28c0eb37-436f-4164-b076-52377443b04d]
aws_iam_group.admingroup: Creation complete after 1s [id=admingroup]
aws_iam_user.testadminuser1: Creation complete after 1s [id=admin1]
aws_iam_user.testadminuser2: Creation complete after 1s [id=admin2]
aws_iam_group_membership.adminteam: Creating...
aws_iam_group_membership.adminteam: Creation complete after 1s [id=tf-testing-group-membership]
azuread_group.group: Still creating... [10s elapsed]
azuread_group.group: Still creating... [20s elapsed]
azuread_group.group: Creation complete after 24s [id=f967d535-272b-4e1f-bb41-1301886e7508]
azuread_group_member.groupmember: Creating...
azuread_group_member.groupmember: Creation complete after 2s [id=f967d535-272b-4e1f-bb41-
1301886e7508/member/28c0eb37-436f-4164-b076-52377443b04d]

Apply complete! Resources: 7 added, 0 changed, 0 destroyed.
```

Azure User and Group (After Terraform Apply) = Refresh browser if needed



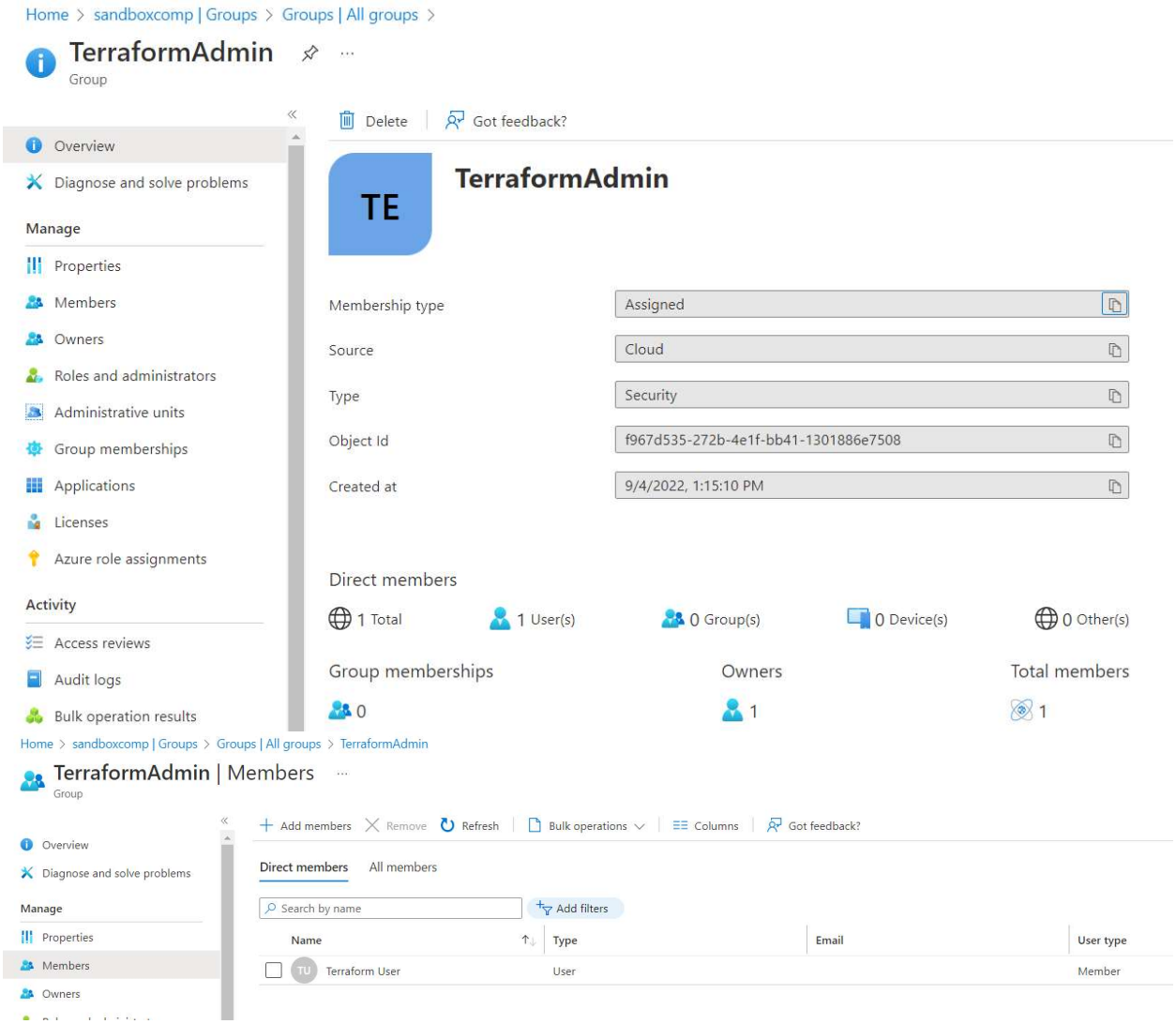
Terraform Multi-cloud Sample: AWS IAM and Azure AD

By Ronald Stewart Lim

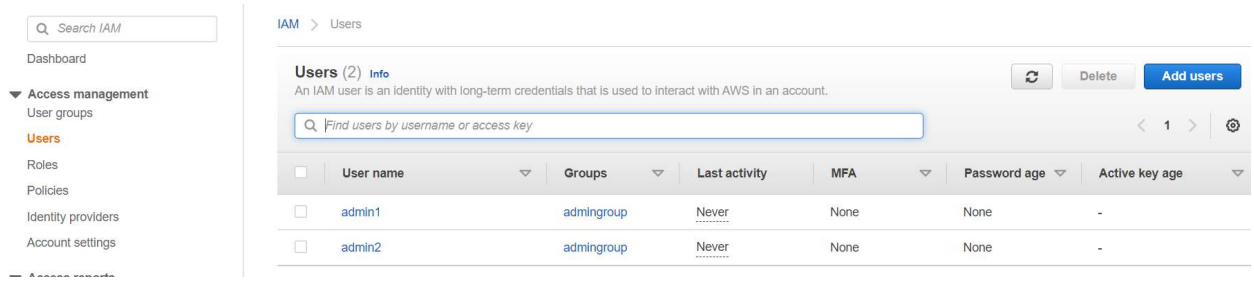


Terraform Multi-cloud Sample: AWS IAM and Azure AD

By Ronald Stewart Lim

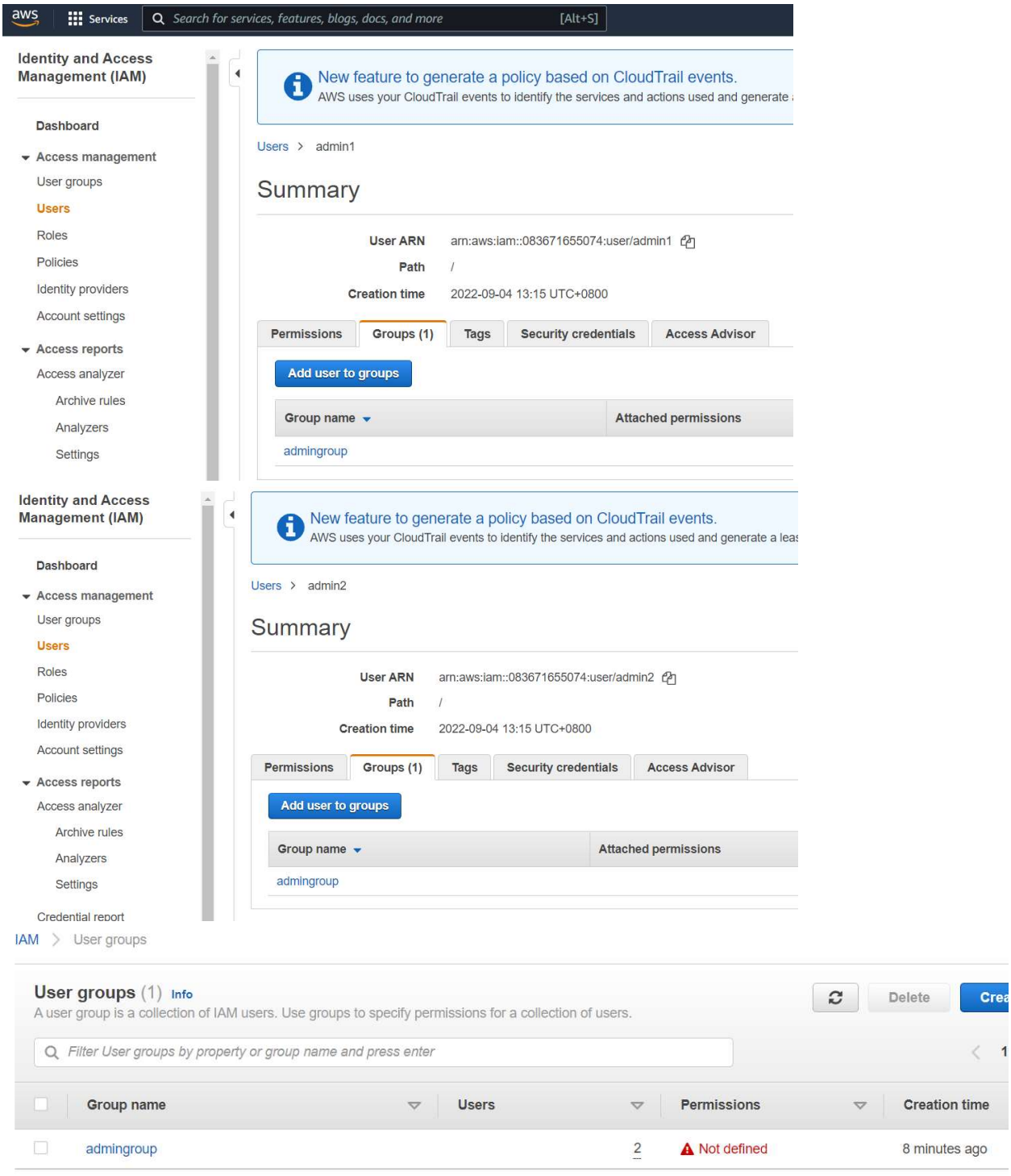


AWS IAM User and Group (After Terraform Apply) = Refresh browser if needed



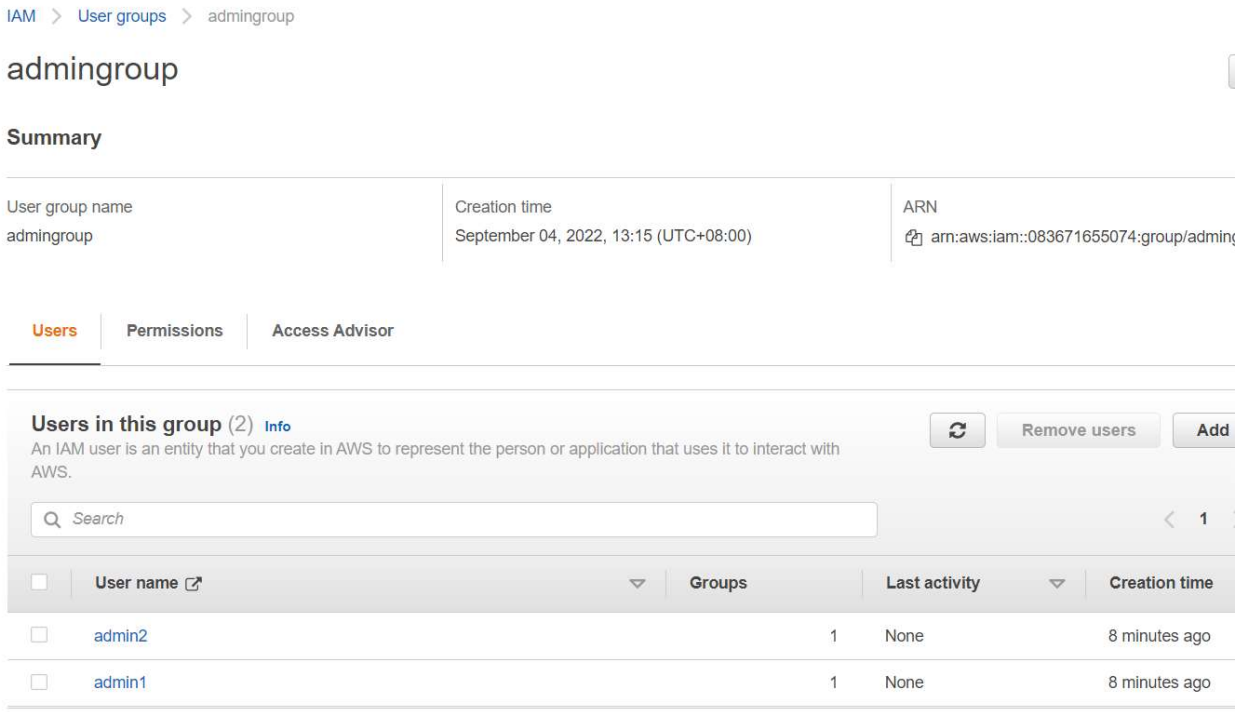
Terraform Multi-cloud Sample: AWS IAM and Azure AD

By Ronald Stewart Lim



Terraform Multi-cloud Sample: AWS IAM and Azure AD

By Ronald Stewart Lim



Terraform Destroy Output

```
D:\Terraform\terraform_multicloud\AWS_IAM_Azure_AD>terraform destroy
aws_iam_group.admingroup: Refreshing state... [id=admingroup]
azuread_group.group: Refreshing state... [id=f967d535-272b-4e1f-bb41-1301886e7508]
azuread_user.user: Refreshing state... [id=28c0eb37-436f-4164-b076-52377443b04d]
aws_iam_user.testadminuser1: Refreshing state... [id=admin1]
aws_iam_user.testadminuser2: Refreshing state... [id=admin2]
azuread_group_member.groupmember: Refreshing state... [id=f967d535-272b-4e1f-bb41-
1301886e7508/member/28c0eb37-436f-4164-b076-52377443b04d]
aws_iam_group_membership.adminteam: Refreshing state... [id=tf-testing-group-membership]

Terraform used the selected providers to generate the following execution plan. Resource actions are
indicated with the following symbols:
  - destroy

Terraform will perform the following actions:

  # aws_iam_group.admingroup will be destroyed
  - resource "aws_iam_group" "admingroup" {
      - arn      = "arn:aws:iam::083671655074:group/admingroup" -> null
      - id       = "admingroup" -> null
      - name     = "admingroup" -> null
      - path     = "/" -> null
      - unique_id = "AGPARG6ZYEKRNCH7LNOEO" -> null
    }
```

```
# aws_iam_group_membership.adminteam will be destroyed
- resource "aws_iam_group_membership" "adminteam" {
   - group = "admingroup" -> null
   - id    = "tf-testing-group-membership" -> null
   - name  = "tf-testing-group-membership" -> null
   - users = [
      - "admin1",
      - "admin2",
     ] -> null
  }

# aws_iam_user.testadminuser1 will be destroyed
- resource "aws_iam_user" "testadminuser1" {
   - arn          = "arn:aws:iam::083671655074:user/admin1" -> null
   - force_destroy = false -> null
   - id           = "admin1" -> null
   - name         = "admin1" -> null
   - path         = "/" -> null
   - tags         = {} -> null
   - tags_all     = {} -> null
   - unique_id    = "AIDARG6ZYEKRJ34GEANZA" -> null
  }

# aws_iam_user.testadminuser2 will be destroyed
- resource "aws_iam_user" "testadminuser2" {
   - arn          = "arn:aws:iam::083671655074:user/admin2" -> null
   - force_destroy = false -> null
   - id           = "admin2" -> null
   - name         = "admin2" -> null
   - path         = "/" -> null
   - tags         = {} -> null
   - tags_all     = {} -> null
   - unique_id    = "AIDARG6ZYEKREFGPKC2IH" -> null
  }

# azuread_group.group will be destroyed
- resource "azuread_group" "group" {
   - assignable_to_role        = false -> null
   - auto_subscribe_new_members = false -> null
   - behaviors                 = [] -> null
   - display_name              = "TerraformAdmin" -> null
   - external_senders_allowed  = false -> null
   - hide_from_address_lists   = false -> null
   - hide_from_outlook_clients = false -> null
   - id                        = "f967d535-272b-4e1f-bb41-1301886e7508" -> null
   - mail_enabled              = false -> null
```

```
    - mail_nickname            = "f7e68be2-0" -> null
    - members                  = [
        - "28c0eb37-436f-4164-b076-52377443b04d",
      ] -> null
    - object_id                = "f967d535-272b-4e1f-bb41-1301886e7508" -> null
    - onpremises_sync_enabled  = false -> null
    - owners                   = [
        - "c1123682-92dd-4504-ba95-f21c642fd90c",
      ] -> null
    - prevent_duplicate_names  = false -> null
    - provisioning_options     = [] -> null
    - proxy_addresses          = [] -> null
    - security_enabled         = true -> null
    - types                    = [] -> null
  }

  # azuread_group_member.groupmember will be destroyed
  - resource "azuread_group_member" "groupmember" {
    - group_object_id  = "f967d535-272b-4e1f-bb41-1301886e7508" -> null
    - id               = "f967d535-272b-4e1f-bb41-1301886e7508/member/28c0eb37-436f-4164-b076-
52377443b04d" -> null
    - member_object_id = "28c0eb37-436f-4164-b076-52377443b04d" -> null
  }

  # azuread_user.user will be destroyed
  - resource "azuread_user" "user" {
    - account_enabled            = true -> null
    - business_phones            = [] -> null
    - company_name               = "HashiCorp" -> null
    - department                 = "HashiCorp" -> null
    - disable_password_expiration = false -> null
    - disable_strong_password    = false -> null
    - display_name               = "Terraform User" -> null
    - force_password_change      = false -> null
    - id                         = "28c0eb37-436f-4164-b076-52377443b04d" -> null
    - im_addresses               = [] -> null
    - mail_nickname              = "terraformuser" -> null
    - object_id                  = "28c0eb37-436f-4164-b076-52377443b04d" -> null
    - onpremises_sync_enabled    = false -> null
    - other_mails                = [] -> null
    - password                   = (sensitive value)
    - proxy_addresses            = [] -> null
    - show_in_address_list       = true -> null
    - user_principal_name        = "terraformuser@sandboxcomp.onmicrosoft.com" -> null
    - user_type                  = "Member" -> null
  }
```

Plan: 0 to add, 0 to change, 7 to destroy.

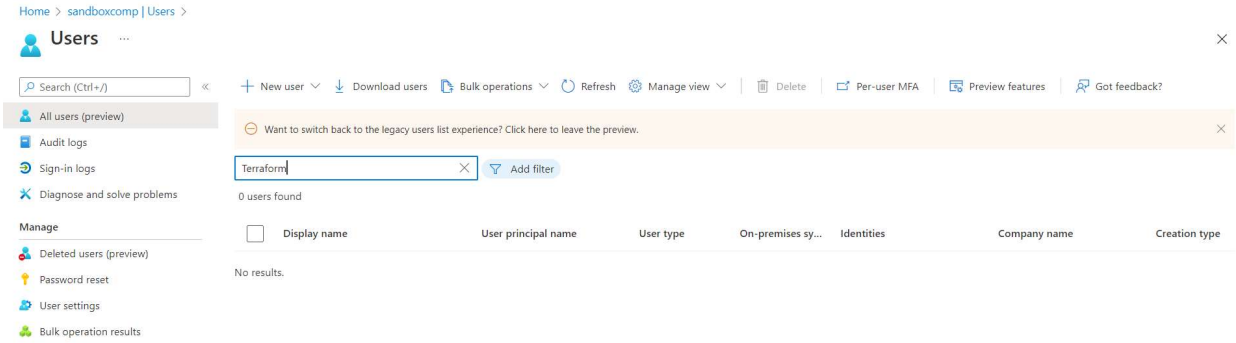
Do you really want to destroy all resources?
  Terraform will destroy all your managed infrastructure, as shown above.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value: yes

azuread_group_member.groupmember: Destroying... [id=f967d535-272b-4e1f-bb41-1301886e7508/member/28c0eb37-436f-4164-b076-52377443b04d]
aws_iam_group_membership.adminteam: Destroying... [id=tf-testing-group-membership]
aws_iam_group_membership.adminteam: Destruction complete after 2s
aws_iam_group.admingroup: Destroying... [id=admingroup]
aws_iam_user.testadminuser1: Destroying... [id=admin1]
aws_iam_user.testadminuser2: Destroying... [id=admin2]
aws_iam_group.admingroup: Destruction complete after 1s
aws_iam_user.testadminuser1: Destruction complete after 2s
aws_iam_user.testadminuser2: Destruction complete after 2s
azuread_group_member.groupmember: Still destroying... [id=f967d535-272b-4e1f-bb41-1301886e7508/member/28c0eb37-436f-4164-b076-52377443b04d, 10s elapsed]
azuread_group_member.groupmember: Still destroying... [id=f967d535-272b-4e1f-bb41-1301886e7508/member/28c0eb37-436f-4164-b076-52377443b04d, 20s elapsed]
azuread_group_member.groupmember: Destruction complete after 23s
azuread_group.group: Destroying... [id=f967d535-272b-4e1f-bb41-1301886e7508]
azuread_user.user: Destroying... [id=28c0eb37-436f-4164-b076-52377443b04d]
azuread_group.group: Still destroying... [id=f967d535-272b-4e1f-bb41-1301886e7508, 10s elapsed]
azuread_user.user: Still destroying... [id=28c0eb37-436f-4164-b076-52377443b04d, 10s elapsed]
azuread_user.user: Still destroying... [id=28c0eb37-436f-4164-b076-52377443b04d, 20s elapsed]
azuread_group.group: Still destroying... [id=f967d535-272b-4e1f-bb41-1301886e7508, 20s elapsed]
azuread_group.group: Destruction complete after 21s
azuread_user.user: Destruction complete after 22s

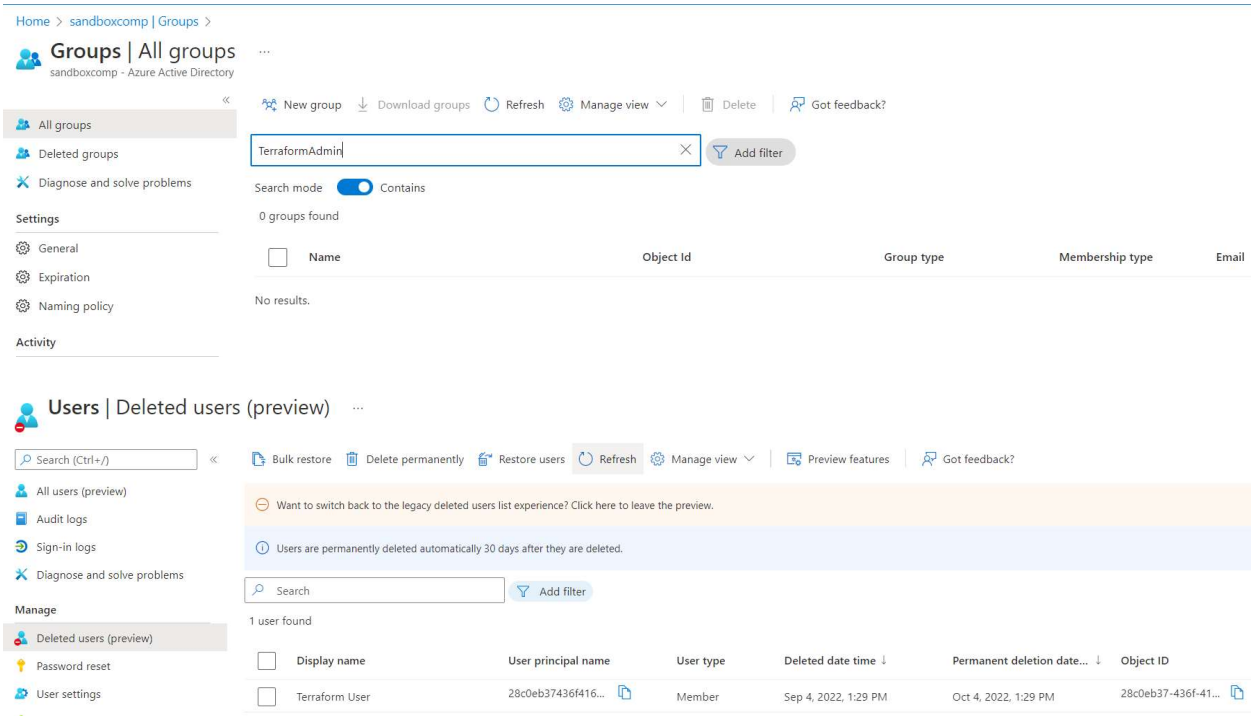
Destroy complete! Resources: 7 destroyed.

Azure User and Group After Terraform Destroy



Terraform Multi-cloud Sample: AWS IAM and Azure AD

By Ronald Stewart Lim



AWS User and Group After Terraform Destroy