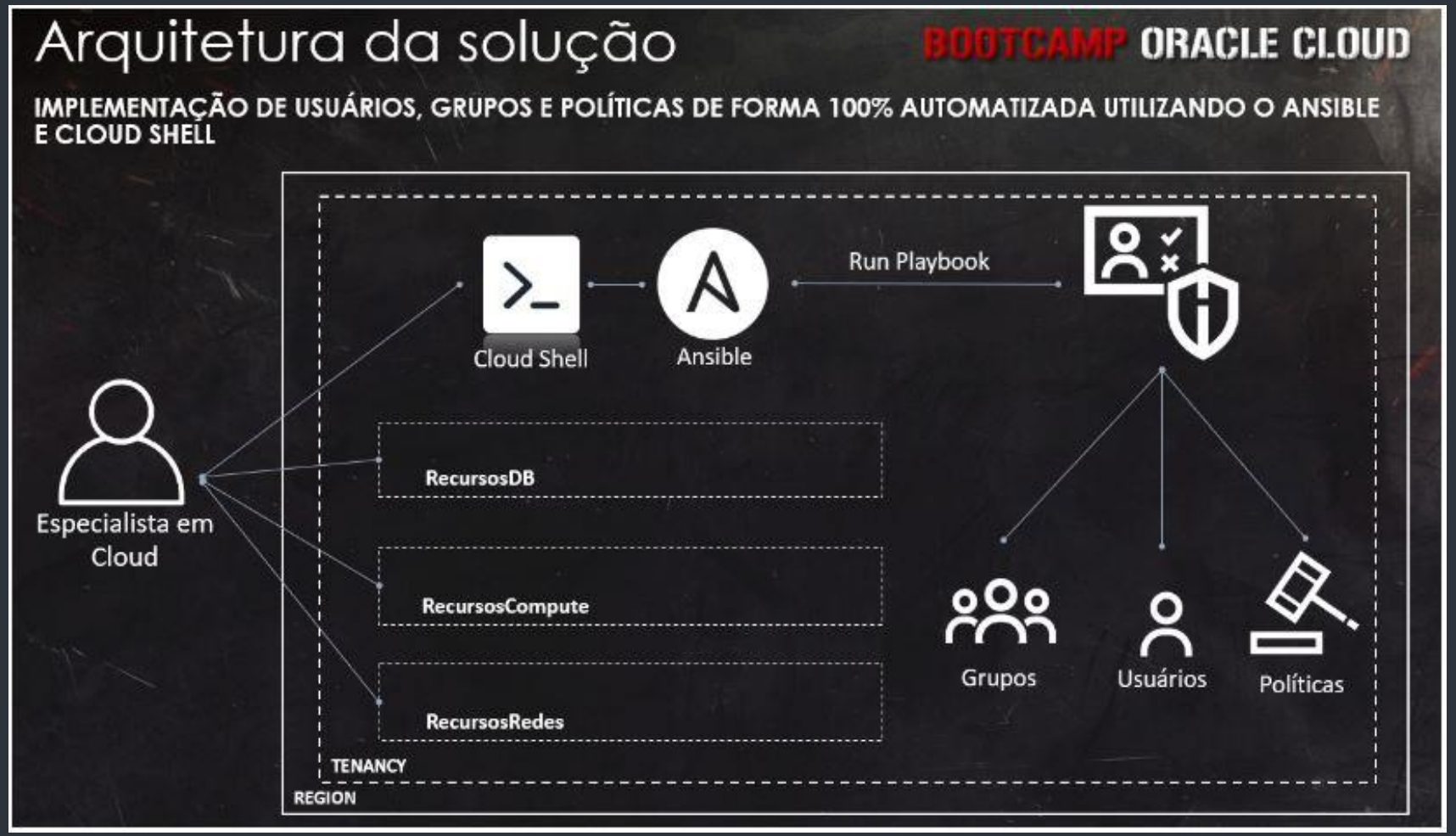
#pracima

Hands on – IAM

1

Implementação de usuários, grupos e políticas de forma 100% automatizada utilizando o Ansible e Cloud Shell.



- Imagine que você está atuando como Especialista em Cloud e foi requisitado(a) realizar a criação de usuários, grupos e políticas na Oracle Cloud Infrastructure. Foi recomendado ter o pensamento em escala e fazer o uso de uma ferramenta poderosa chamada Ansible, visando criar de maneira rápida, simples e 100% automatizada todos os recursos do IAM.
- Implementando esta solução utilizando infrastructure as code, no futuro ao surgir uma demanda de criação de novos usuários na OCI, terá a possibilidade de otimizar muito o tempo com solução da demanda, sendo necessário apenas indicar os recursos que se deseja criar.

- Para solução deste hands-on foram criados três compartments na OCI, recursos de compute engine, data base e networks.

RecursosCompute	Active	...lsnn5q	Yes	Not Enabled	0	Tue, Sep 28, 2021, 01:05:12 UTC
RecursosDB	Active	...rrclua	Yes	Not Enabled	0	Tue, Sep 28, 2021, 01:05:29 UTC
RecursosRedes	Active	...oaql3a	Yes	Not Enabled	0	Tue, Sep 28, 2021, 01:04:35 UTC

- Criando as variáveis de ambiente na console da OCI.

```
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ export PARENT_COMPARTMENT_OCID=ocid1.tenancy.oc1..aaaaaaaakaewj2arow5qhoxw62cvtxauau7gewp5thrgq2t7hucw41tjvu2q
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ export COMPUTE_COMPARTMENT_OCID=ocid1.compartment.oc1..aaaaaaaasmiji6mkcmks25rkajk3jjpe3j3ikmwrzipxgc1fnbvp4rlsnn5q
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ export REDES_COMPARTMENT_OCID=ocid1.compartment.oc1..aaaaaaaargxqaqe5zynv4hzsuq5hf3bgy7jxovecfn7zrpe3n7ddx6oaql3a
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ export DB_COMPARTMENT_OCID=ocid1.compartment.oc1..aaaaaaaagc5xcr5awnyuljext2b5rksgmxvbt3iczrstfcwrjtqtz3rrclua
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$
```

- Configuração e download dos playbook Ansible.

```
leniel1@cloudshell:~ (us-phoenix-1)$ mkdir tcb-bmc-iam
leniel1@cloudshell:~ (us-phoenix-1)$ cd tcb-bmc-iam/
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ wget https://objectstorage.us-ashburn-1.oraclecloud.com/p/JwXwD1vHS3yOm79o1LQUctIXMw9ZryXR5BQ9o6fLbv2zhpyDvIVkGiw6tQItN3Vn/n/idqfa2z2mift/b/bootcamp-oci/o/oci-f-handson-modul
o-iam.zip
--2021-09-28 01:11:53--  https://objectstorage.us-ashburn-1.oraclecloud.com/p/JwXwD1vHS3yOm79o1LQUctIXMw9ZryXR5BQ9o6fLbv2zhpyDvIVkGiw6tQItN3Vn/n/idqfa2z2mift/b/bootcamp-oci/o/oci-f-handson-modulo-iam.zip
Resolving objectstorage.us-ashburn-1.oraclecloud.com (objectstorage.us-ashburn-1.oraclecloud.com)... 134.70.32.1, 134.70.28.1, 134.70.24.1
Connecting to objectstorage.us-ashburn-1.oraclecloud.com (objectstorage.us-ashburn-1.oraclecloud.com)|134.70.32.1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7815 (7.6K) [application/zip]
Saving to: ‘oci-f-handson-modulo-iam.zip’

100%[=============================================================================================================================================================>] 7,815       --.-K/s   in 0s

2021-09-28 01:11:54 (78.5 MB/s) - ‘oci-f-handson-modulo-iam.zip’ saved [7815/7815]

leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ unzip oci-f-handson-modulo-iam.zip
Archive:  oci-f-handson-modulo-iam.zip
  inflating: tcb-bmc-iam-cria-usuarios.yaml
   creating: __MACOSX/
  inflating: __MACOSX/._tcb-bmc-iam-cria-usuarios.yaml
  inflating: tcb-bmc-iam-cria-usuarios-compute-admin.yaml
  inflating: __MACOSX/._tcb-bmc-iam-cria-usuarios-compute-admin.yaml
  inflating: tcb-bmc-iam-cria-usuarios-dba-admin.yaml
  inflating: __MACOSX/._tcb-bmc-iam-cria-usuarios-dba-admin.yaml
  inflating: tcb-bmc-iam-cria-usuarios-redes-admin.yaml
  inflating: __MACOSX/._tcb-bmc-iam-cria-usuarios-redes-admin.yaml
  inflating: tcb-bmc-iam-cria-grupos-e-politicas.yaml
  inflating: tcb-bmc-iam-cria-usuarios-cloud-admin.yaml
  inflating: __MACOSX/._tcb-bmc-iam-cria-usuarios-cloud-admin.yaml
  inflating: tcb-bmc-iam-cria-usuarios-operadores.yaml
  inflating: __MACOSX/._tcb-bmc-iam-cria-usuarios-operadores.yaml
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ ls
__MACOSX                    tcb-bmc-iam-cria-grupos-e-politicas.yaml    tcb-bmc-iam-cria-usuarios-compute-admin.yaml  tcb-bmc-iam-cria-usuarios-operadores.yaml   tcb-bmc-iam-cria-usuarios.yaml
```

- Execução do playbook para criar automaticamente os group and policies na OCI.

```
leniell@cloudshell:tcb-bmc-iam (us-phoenix-1)$ ansible-playbook tcb-bmc-iam-cria-grupos-e-politicas.yaml
[DEPRECATION WARNING]: Ansible will require Python 3.8 or newer on the controller starting with Ansible 2.12. Current version: 3.6.8 (default, Mar  9 2021, 15:08:44) [GCC 4.8.5 20150623 (Red Hat 4.8.5-44.0.3)]. This
feature will be removed from ansible-core in version 2.12. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[WARNING]: No inventory was parsed, only implicit localhost is available
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [Criação de grupos e politicas na Oracle Cloud Infrastructure] ************************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************************************************
ok: [localhost]

TASK [Valida pre-requisitos] ***************************************************************************************************************************************************************************
skipping: [localhost] => (item=PARENT_COMPARTMENT_OCID)
skipping: [localhost] => (item=COMPUTE_COMPARTMENT_OCID)
skipping: [localhost] => (item=REDES_COMPARTMENT_OCID)
skipping: [localhost] => (item=DB_COMPARTMENT_OCID)

TASK [Criar um grupo para o gerenciamento dos recursos de Compute] *************************************************************************************************************************
changed: [localhost]

TASK [set_fact] ****************************************************************************************************************************************************************************************
ok: [localhost]

TASK [Criar um grupo para o gerenciamento dos recursos de Redes] ***************************************************************************************************************************
changed: [localhost]

TASK [set_fact] ****************************************************************************************************************************************************************************************
ok: [localhost]

TASK [Criar um grupo para o gerenciamento dos recursos de Database] ************************************************************************************************************************
changed: [localhost]

TASK [set_fact] ****************************************************************************************************************************************************************************************
ok: [localhost]

PLAY RECAP *********************************************************************************************************************************************************************************************
localhost                  : ok=21   changed=10   unreachable=0    failed=0    skipped=1    rescued=0    ignored=0

leniell@cloudshell:tcb-bmc-iam (us-phoenix-1)$
```

- Groups que foram criados na OCI utilizando infrastructure as code com Ansible.

Create Group | Delete

Name	Description	Created
Operadores	Grupo com responsabilidades de monitorar os recursos em execução na Tenancy	Tue, Sep 28, 2021, 01:37:57 UTC
TCBCloudAdmin	Grupo de Especialistas Cloud e Arquitetos de Soluções	Tue, Sep 28, 2021, 01:37:54 UTC
DBAsAdmin	Grupo permitido realizar o gerenciamento de todos os recursos de database que estão no compartimento RecursosDatabase	Tue, Sep 28, 2021, 01:37:50 UTC
RedesAdmin	Grupo permitido realizar o gerenciamento de todos os recursos de rede no compartimento RecursosRedes	Tue, Sep 28, 2021, 01:37:48 UTC
ComputeAdmin	Grupo permitido realizar o gerenciamento de todos r compartimento RecursosCompute	

Create Policy | Delete

Name	Description	Statements	Created
OperadoresPolicy	Permissão para visualizar inspecionando todos os recursos da Tenancy	1	Tue, Sep 28, 2021, 01:38:12 UTC
TCBCloudAdminPolicy	Permissão para gerenciar todos os recursos na tenancy	1	Tue, Sep 28, 2021, 01:38:10 UTC
DBAsAdminPolicy	Permissão para gerenciar os recursos de Database	1	Tue, Sep 28, 2021, 01:38:07 UTC
RedesAdminPolicy	Permissão para gerenciar os recursos de Redes	2	Tue, Sep 28, 2021, 01:38:04 UTC
ComputeAdminPolicy	Permissão para gerenciar os recursos de Compute	1	Tue, Sep 28, 2021, 01:38:00 UTC
PSM-root-policy	PSM managed compartment root policy	7	Tue, Sep 28, 2021, 01:33:19 UTC
Tenant Admin Policy	Tenant Admin Policy	1	Mon, Sep 27, 2021, 23:16:32 UTC

- Execução do playbook para criar os usuários do Cloud Admin na OCI.

```
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ ansible-playbook tcb-bmc-iam-cria-usuarios-cloud-admin.yaml
[DEPRECATION WARNING]: Ansible will require Python 3.8 or newer on the controller starting with Ansible 2.12. Current version: 3.6.8 (default, Mar  9 2021, 15:08:44) [GCC 4.8.5 20150623 (Red Hat 4.8.5-44.0.3)]. This
feature will be removed from ansible-core in version 2.12. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[WARNING]: No inventory was parsed, only implicit localhost is available
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [Criação de usuários Cloud Admin na Oracle Cloud Infrastructure] ***********************************************************************************

TASK [Gathering Facts] ***********************************************************************************************************************
ok: [localhost]

TASK [Valida pre-requisitos] *****************************************************************************************************************
skipping: [localhost] => (item=PARENT_COMPARTMENT_OCID)

TASK [Obtém ID do Grupo] *********************************************************************************************************************
ok: [localhost]

TASK [set_fact] ******************************************************************************************************************************
ok: [localhost]

TASK [Cria usuários, adiciona em grupo e define senha] ***************************************************************************************
included: /home/leniel1/tcb-bmc-iam/tcb-bmc-iam-cria-usuarios.yaml for localhost => (item=pedro.ribeiro)
included: /home/leniel1/tcb-bmc-iam/tcb-bmc-iam-cria-usuarios.yaml for localhost => (item=bruna.santos)

TASK [Cria usuário] ***************************************************************************************************************************
changed: [localhost]

TASK [set_fact] ******************************************************************************************************************************
ok: [localhost]

TASK [debug] *********************************************************************************************************************************
ok: [localhost] => {
    "msg": "Usuário pedro.ribeiro criado"
}
```

```
PLAY RECAP ************************************************************************************************************************************
localhost                  : ok=21   changed=6    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0

leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$
```

- Execução do playbook para criar os usuários de Data Base admin, network admin, compute admin and operators admin na OCI.

```
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ ansible-playbook tcb-bmc-iam-cria-usuarios-dba-admin.yaml
[DEPRECATION WARNING]: Ansible will require Python 3.8 or newer on the controller starting with Ansible 2.12. Current version: 3.6.8 (default, Mar  9 2021, 15:08:44) [GCC 4.8.5 20150623 (Red Hat 4.8.5-44.0.3)]. This
feature will be removed from ansible-core in version 2.12. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[WARNING]: No inventory was parsed, only implicit localhost is available
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [Criação de usuários DBAs Admin na Oracle Cloud Infrastructure] ***********************************************************************************************************************************

TASK [Gathering Fact
ok: [localhost]
```

```
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ ansible-playbook tcb-bmc-iam-cria-usuarios-redes-admin.yaml
[DEPRECATION WARNING]: Ansible will require Python 3.8 or newer on the controller starting with Ansible 2.12. Current version: 3.6.8 (default, Mar  9 2021, 15:08:44) [GCC 4.8.5 20150623 (Red Hat 4.8.5-44.0.3)]. This
feature will be removed from ansible-core in version 2.12. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[WARNING]: No inventory was parsed, only implicit localhost is available
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [Criação de usuários Redes Admin na Oracle Cloud Infrastructure] **********************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************************************************
ok: [localhost]

TASK [Valida pre-requisitos] ***************************************************************************************************************************************************************************
skipping: [localhost] => (item=PARENT_COMPARTMENT_OCID)
```

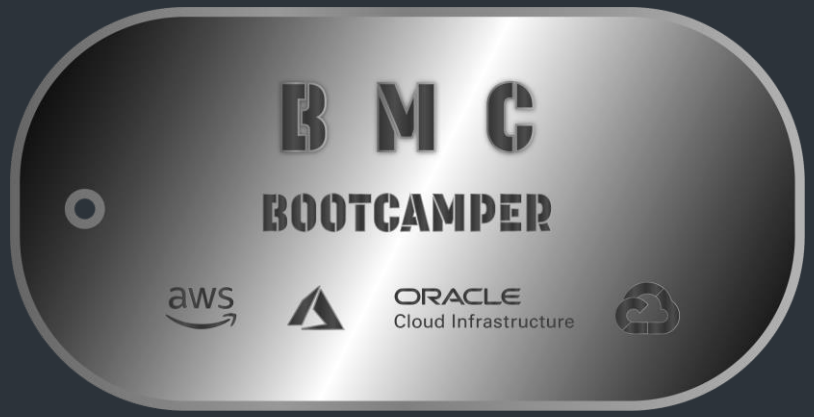
```
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ ansible-playbook tcb-bmc-iam-cria-usuarios-compute-admin.yaml
[DEPRECATION WARNING]: Ansible will require Python 3.8 or newer on the controller starting with Ansible 2.12. Current version: 3.6.8 (default, Mar  9 2021, 15:08:44) [GCC 4.8.5 20150623 (Red Hat 4.8.5-44.0.3)]. This
feature will be removed from ansible-core in version 2.12. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[WARNING]: No inventory was parsed, only implicit localhost is available
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [Criação de usuários Compute Admin na Oracle Cloud Infrastructure] ********************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************************************************
ok: [localhost]

TASK [Valida pre-requ
skipping: [localhost
```

```
leniel1@cloudshell:tcb-bmc-iam (us-phoenix-1)$ ansible-playbook tcb-bmc-iam-cria-usuarios-operadores.yaml
[DEPRECATION WARNING]: Ansible will require Python 3.8 or newer on the controller starting with Ansible 2.12. Current version: 3.6.8 (default, Mar  9 2021, 15:08:44) [GCC 4.8.5 20150623 (Red Hat 4.8.5-44.0.3)]. This
feature will be removed from ansible-core in version 2.12. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[WARNING]: No inventory was parsed, only implicit localhost is available
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [Criação de usuários Operadores na Oracle Cloud Infrastructure] ***********************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************************************************
ok: [localhost]

TASK [Valida pre-requisitos] ***************************************************************************************************************************************************************************
skipping: [localhost] => (item=PARENT_COMPARTMENT_OCID)
```

- Usuários que foram criados na OCI utilizando infrastructure as code com Ansible

Create User | Delete

Name	Status	Email	Federated	Created
victor.matos	Active	victor.matos@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 02:00:26 UTC
pedro.andrade	Active	pedro.andrade@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 02:00:16 UTC
thiago.francisco	Active	thiago.francisco@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 01:57:26 UTC
joao.roberto	Active	joao.roberto@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 01:57:15 UTC
joao.silveira	Active	joao.silveira@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 01:56:18 UTC
natalia.lima	Active	natalia.lima@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 01:56:08 UTC
zanon.brums	Active	zanon.brums@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 01:52:33 UTC
bruno.silva	Active	bruno.silva@thecloudbootcamp.com (Verification Pending)	No	Tue, Sep 28, 2021, 01:52:23 UTC



- Author: Leniel dos Santos
- Linkedin: https://www.linkedin.com/in/leniel-dos-santos-7813a924/