Exploring GCE VMs Further

SSHing into Linux VMs - Options

In28 Minutes

- **Compute Engine Linux VMs** uses **key-based SSH** authentication
- **Two Options:**
  - **Metadata managed**: Manually create and configure individual SSH keys
  - **OS Login**: Manage SSH access without managing **individual** SSH keys!
    - Recommended for managing multiple users across instances or projects
    - Your Linux user account is linked to your Google identity
    - To enable: Set enable-oslogin to true in metadata
      - *gcloud compute* ***project-info/instances add-metadata --metadata enable-oslogin=TRUE***
    - (Advantage) Ability to import existing Linux accounts from on premises AD and LDAP
    - Users need to have roles : roles/compute.osLogin or roles/compute.osAdminLogin
- (Windows) **Windows** instances use **password** authentication(username and password)
  - Generate using console or gcloud (gcloud compute reset-windows-password)

SSHing into Linux VMs - Details

- **Option 1**: Console - SSH Button
  - Ephemeral SSH key pair is created by Compute Engine
- **Option 2**: Gcloud - *gcloud compute ssh*
  - A username and persistent SSH key pair are created by Compute Engine
  - SSH key pair reused for future interactions
- **Option 3**: Use customized SSH keys
  - (Metadata managed): Upload the public key to project metadata OR
  - (OS Login): Upload your public SSH key to your OS Login profile
    - *gcloud compute os-login ssh-keys add* OR
    - Use OS Login API : POST ***https://oslogin.googleapis.com/v1/users/ACCOUNT_EMAIL:importSshPublicKey***
- You can disable Project wide SSH keys on a specific compute instance
  - *gcloud compute* ***instances add-metadata [INSTANCE_NAME] --metadata block-project-ssh-keys=TRUE***

Executing Shutdown Script on a GCE VM

- **Execute commands** before a GCE VM is **stopped, terminated or restarted**
  - Perform **cleanup** or export of logs
  - Applicable for Preemptible and Non Preemptible GCE VMs
- Very **similar to startup script**
  - Run as:
    - `root` user in Linux VMs
    - `System` account in Windows VMs
  - **Stored as metadata**
    - --metadata-from-file shutdown-script=script.sh
    - You can store startup and shutdown scripts in cloud storage
      - --metadata shutdown-script-url=gs://bucket-in-cloud-storage/file
- Run on **best-effort basis**
  - Example: WON'T run if you use hard reset (instances.reset)
  - Example: WON'T run if you exceed grace period for preemptible instances

Startup Script Example

Deploy new application version to Compute Engine

```
# Setup logging agent
curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh
sudo bash install-logging-agent.sh

# Install GIT
apt-get update
apt-get install -yq git

# Clone Repo
git clone https://github.com/in28minutes/your-app.git /opt/app

# Build and Run app
//...
```

Troubleshooting VM startup and ...

In28 Minutes

- **Check 1**: Are there **Quota** errors?
- **Check 2**: Is **boot disk** full?
- **Check 3**: Check **serial port output**
  - Each VM instance has 4 virtual serial ports
  - Serial Port Output: OS, BIOS, and other system-level entities write output to serial ports
    - Useful for troubleshooting crashes, failed boots, startup, or shutdown issues
    - Accessible from Cloud Console, the gcloud tool, and the Compute Engine API
    - You can send serial port output to Cloud Logging:
      - gcloud compute project-info add-metadata --metadata serial-port-logging-enable=true
    - Interactive access to the serial console allows you to login and debug boot issues (without needing a full boot up)
      - gcloud compute instances get-serial-port-output
- **Check 4**: Does your disk have a **valid file system**?
  - Attach boot disk as a data disk to another VM and check the file system

Moving VM instances between Zones and Regions

In 28 Minutes

- VM instances can be **moved between zones in the same region:**
  - `gcloud compute instances move my-instance --zone us-central1-a --destination-zone us-central1-b`

- **Restrictions**: You cannot use move command for:
  - Instances that are part of a MIG
  - Instances attached with local SSDs
  - Instances in TERMINATED status
  - Moving instances across regions
  - Go for a **Manual Approach:**
    - Create snapshots of attached persistent disks
      - `gcloud compute disks snapshot my-disk-a --snapshot-names my-pd-snapshot --zone ZONE`
    - Create copies of persistent disks in destination zone (of new region)
      - `gcloud compute disks create my-disk-b --source-snapshot my-pd-snapshot --zone ZONE`
    - Create new instance in destination zone (of new region) and attach the persistent disks