YCIT 018 - Cloud Networking & Security

Lab project

Instructor: Patrick Lécuyer & Nicolas Bédard

McGill | School of Continuing Studies

Overview

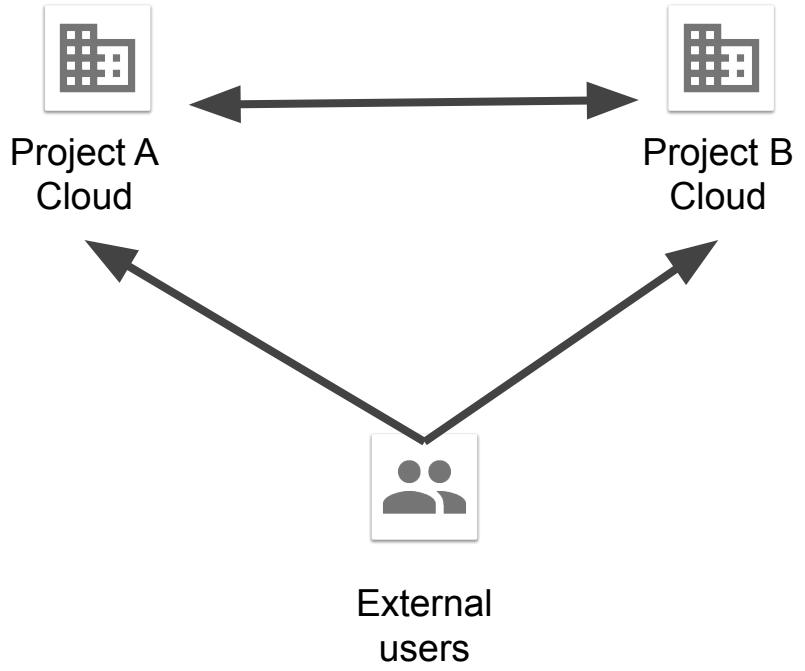
Build a complete Cloud solution to demonstrate networking and cybersecurity learning outcomes covered during the course. Students will need to build a replica of 2 typical architectures in the Cloud, then enable connectivity and security to access services between them and to external users according to provided requirements.

Hand-on topics covered by Lab Project:

- Project structure & permission
- VPC & Networking segmentation
- IAM
- VPN
- Firewalls
- Routing

Evaluation:

- 60% on Cloud configuration
- 30% on Documentation
- 10% on Extra functionality



GCP Credits

- You will be asked for a name and email address, which needs to match the domain. A confirmation email will be sent to you with a coupon code.
- You can request a coupon from the URL and redeem it until: 6/2/2021
- Coupon valid through: 2/2/2022
- You can only request ONE code per unique email address.

Configuration (60%)

- Organization, Project, IAM
- Compute Instances
- Network, Router & VPN
- Firewall

Lab Project architecture - Project & IAM

Project A Cloud

Accounts

Role covered in Lab

1. Project Owner
2. Compute Admin
3. Security Admin
4. Network Management Admin

Project B Cloud

Accounts

Role covered in Lab

1. Project Owner
2. Compute Admin
3. Security Admin
4. Network Management Admin

Requirement 1.1 - Create 2 Projects

1. Only 1 Organisation is required for IAM simplicity

Requirement 1.2 - Assign IAM roles to accounts

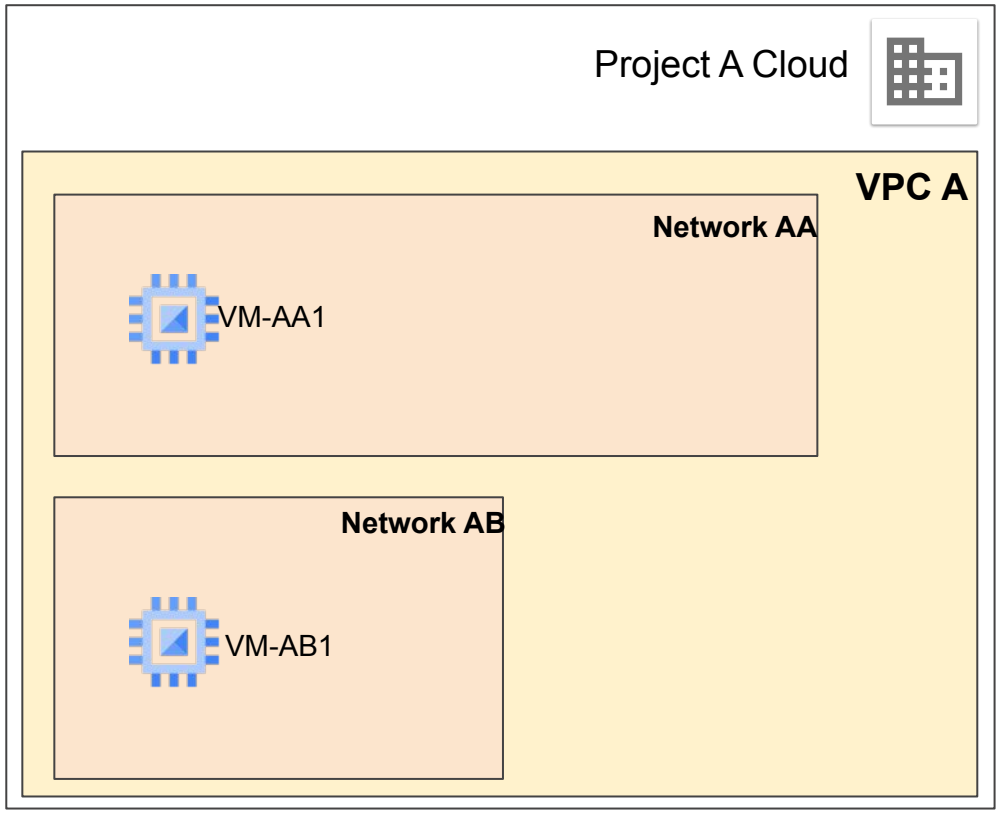
1. Your main account (used for evaluation) should remain intact
2. Assign the 4 roles covered in the diagram. Extra points for more advanced roles
3. Describe your role assignments and the expected results in your Lab documents for each account

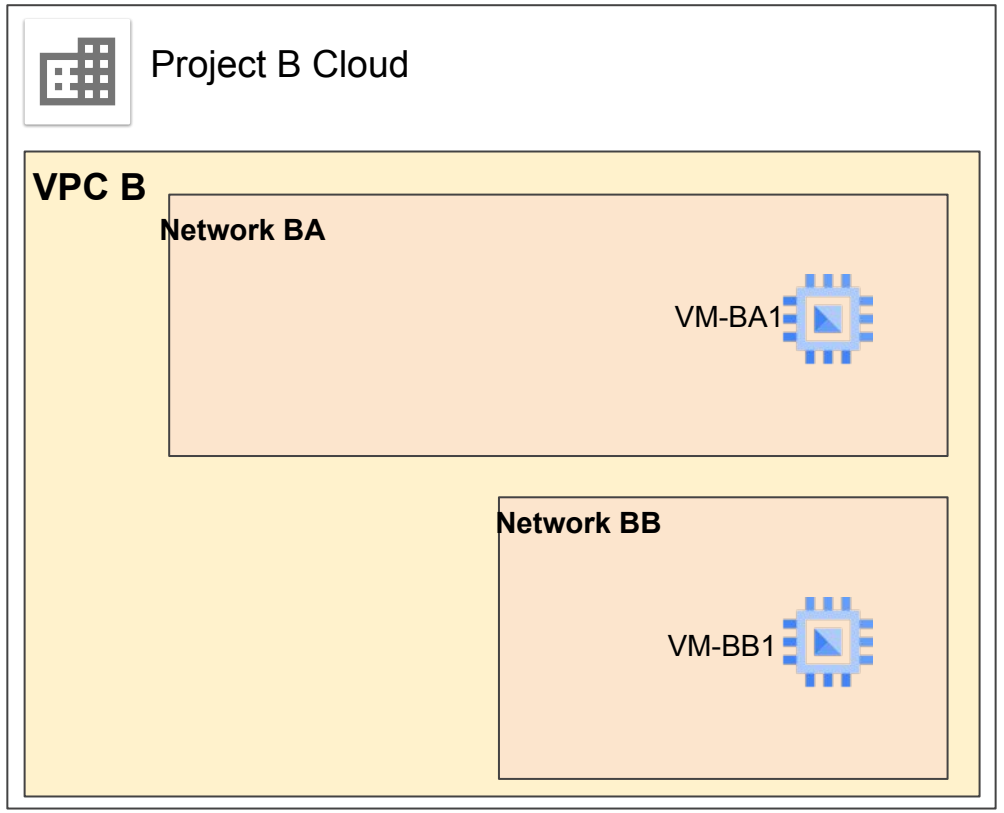
TIPS: To achieve role assignment, student can:

1. Create its own accounts list (extra-points!)
2. Use service-accounts (with no emails)
3. Use provided test account list (GCP only):
   sansareed.832206@gmail.com
   theonfrey.636475@gmail.com
   jonfrey.601857@gmail.com
   petyrmormont.422614@gmail.com
   daenerysbolton.360042@gmail.com
   rickonstone.911790@gmail.com
   catelynsand.630972@gmail.com

McGill | School of Continuing Studies

Lab Project architecture - Compute Instances





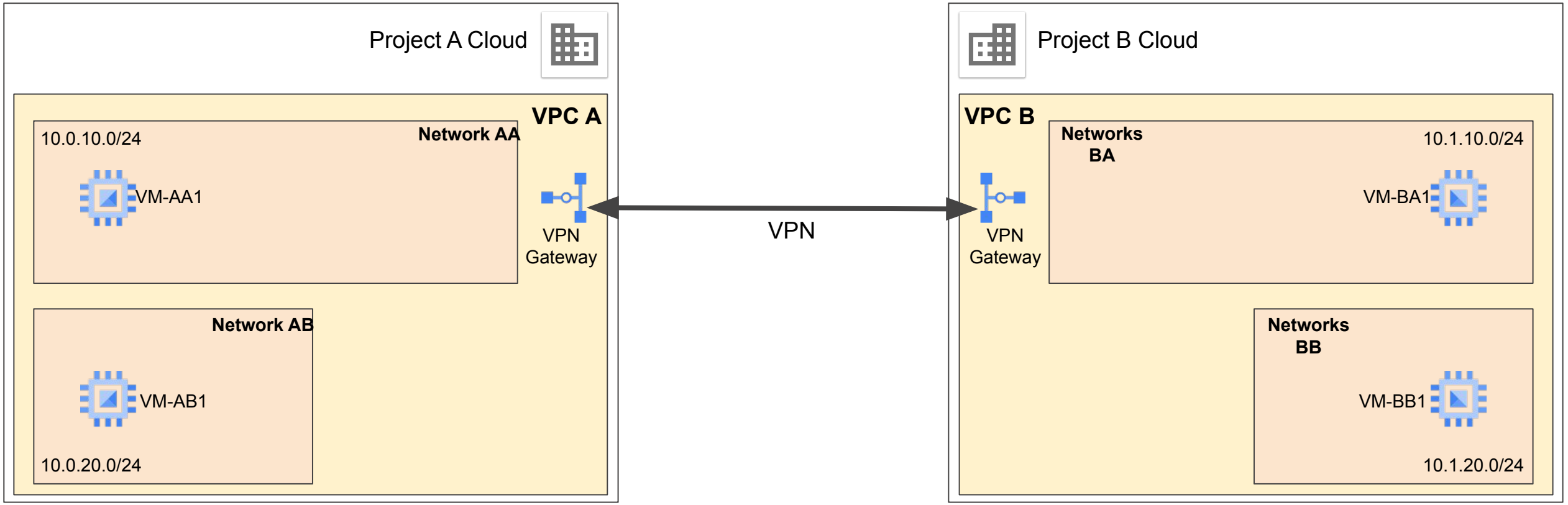
Requirement 2.1 - Create 2 distinct virtual Cloud using Projects

1. Project are named Org_A & Org_B
2. Each project has 1 VPC
3. Each VPC has 2 Networks as per Network & VPN requirements
4. Each VPC has 1 router & VPN gateway as per Network & VPN requirements
5. Each Network had 1 compute instance
6. All resources in same Region & Zones for simplicity

Requirement 2.2 - VM instance

1. 1 Linux VM per Network (smallest VM available - f1-micro)
2. Default configuration (storage)
3. Network configuration as per requirements
4. Firewall configuration as per requirements

Lab Project architecture - Network & VPN



Requirement 3.1 - Create 4 Network

1. Network AA - 10.0.10.0/24
2. Network AB - 10.0.20.0/24
3. Network BA - 10.1.10.0/24
4. Network BB - 10.1.20.0/24

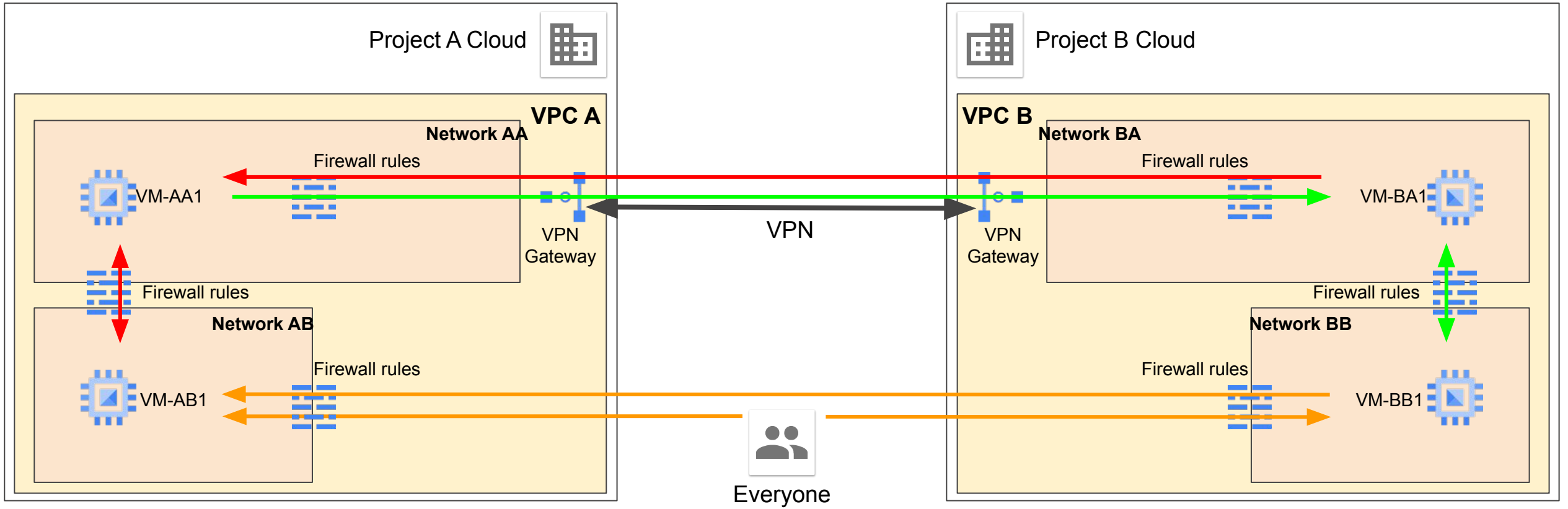
Requirement 3.2 - VM address assignments

1. All VM has Ephemeral addresses
2. VM-AA1 in Network AA (internal only)
3. VM-AB1 in Network AB
4. VM-BA1 in Network BA (internal only)
5. VM-BB1 in Network BB

Requirement 3.3 - Create 1 VPN Between VPC

1. Using Classic VPN mode
2. Using Network AA & AB
3. Using Reserved IP for the Gateway
4. Using IKE pre-shared key
5. Using static routes to reach destination in both directions

Lab Project architecture - Firewall



Requirement 4.1 - VM-AA1 & VM-BA1

1. Only use Private IP (Not directly accessible from Internet)
2. Communicate together using Router with static routes & VPN Gateway to encrypt communication.
3. VM-AA1 **CAN** ping VM-BA1 using Firewall rules
4. VM-BA1 **CANNOT** ping VM-AA1 using Firewall rules

Requirement 4.2 - VM-AA1 & VM-AB1

1. **CANNOT** ping in both direction using Firewall rules

Requirement 4.3 - VM-BA1 & VM-BB1-2

1. **CAN** ping in both direction using Firewall rules

Requirement 4.4 - Everyone on the Internet

1. **CAN** HTTP on port TCP-80 to VM-AB1 Public IP address.
2. **CANNOT** HTTP on port TCP-80 to VM-BB1 Public IP address.
3. **CAN** ping to VM-AB1 & VM-BB1 Public IP address.
4. **CANNOT** SSH to VM-AB1 & VM-BB1 Public IP address

Requirement 4.5 - VM-BB1 (using Public Internet)

1. **CANNOT** HTTP on port TCP-80 to VM-AB1 Public IP address.
2. **CAN** ping to VM-AB1 Public IP address.
3. **CAN** SSH to VM-AB1 Public IP address
4. **CANNOT** ping 8.8.8.8 (Google's Public DNS)

McGill | School of Continuing Studies

Documentation (30%)

McGill | School of Continuing Studies

Documentation

- 8-15 pages (including 1 front-page)
- Due date is April 5th @ 5:00 PM
- Recommended to send early if ready to accelerate correction
- Recommended document structure:
  - Section I - (60% of points)
    - High-level text explanation on how you achieved your configuration
    - Screenshot of your configuration for each requirements
  - Section II - (30 % of points)
    - Screenshot of your working configuration
      - Ping, Traceroute, Web request for each requirements
      - Logs in Cloud Web interface or console for each requirements
  - Section III - (10% of points)
    - Extra functionality (Screenshots & explanation)

Extra functionality (10%)

McGill | School of Continuing Studies

Be creative !

- Load-Balancer with Instance-Groups
- Service accounts firewall rules
- 2FA
- Certificates
- Encryption keys
- DNS
- NAT
- Network Tags
- Advanced IAM configuration
- Context-based access (Geo & Time)

GCP Credits & Tips

McGill | School of Continuing Studies

GCP Credits and Tips

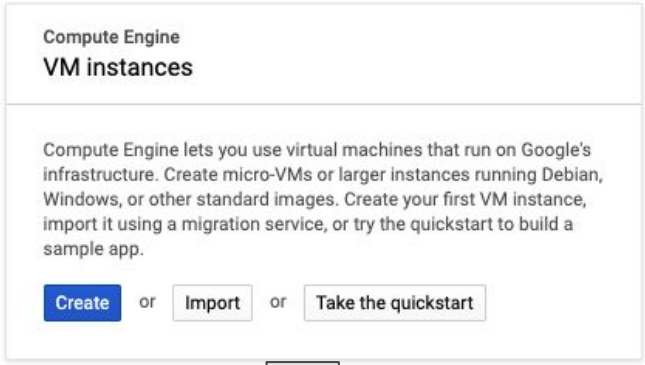
- Student can use any of the 3 main public cloud providers
  - Google Cloud Platform
  - AWS
  - Microsoft Azure
- We provide credit for Google Cloud Platform using your McGill email
- Tips
  - When not in use, stop your VM ! $$
  - Find configuration tips on Youtube if you are blocked !
  - Help your teammates on Slack

Web server set-up for requirement 4.4 & 4.5

Add the following commands under *Management--> Startup script* section when you create your VM-AB1 & VM-BB1 linux virtual machines

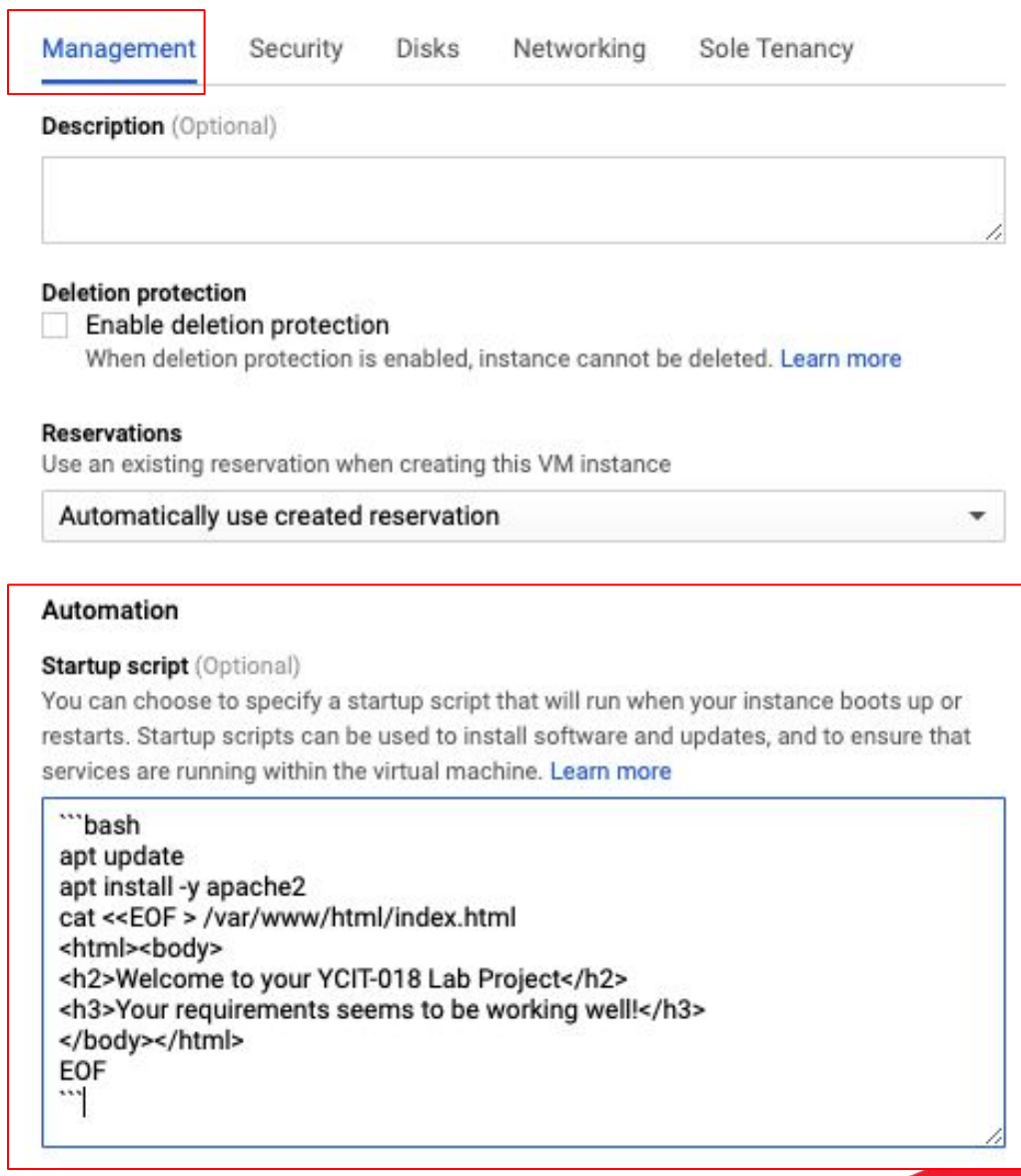
```bash
apt update
apt install -y apache2
cat <<EOF > /var/www/html/index.html
<html><body>
<h2>Welcome to your YCIT-018 Lab Project</h2>
<h3>Your requirements seems to be working well!</h3>
</body></html>
EOF
```

1- Create VM



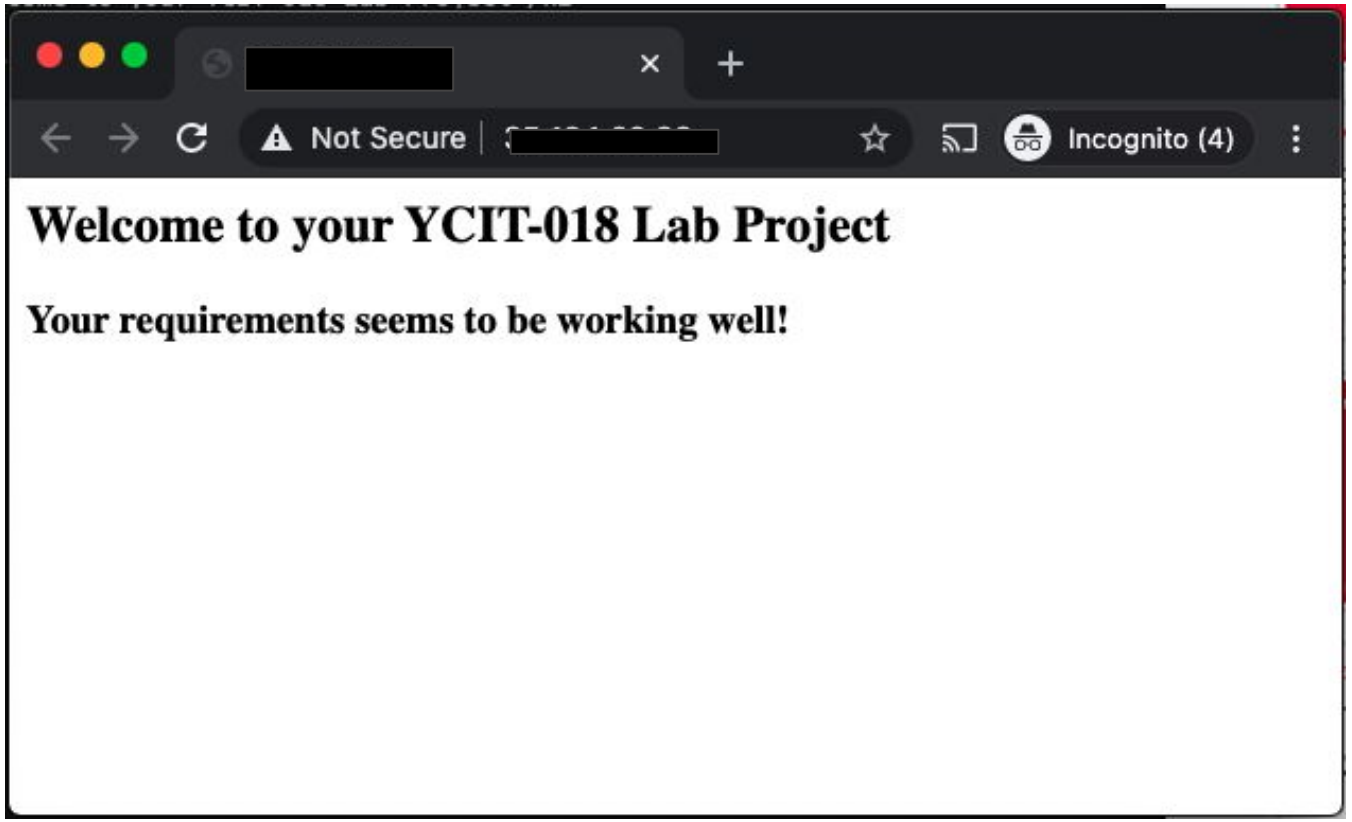
2- Expand menu

3- Input script



Web server set-up for requirement 4.4 & 4.5

You should see this Web page if your VM & Security is set-up properly



IMPORTANT: Suspend your VM when not in use ! Don't tempt the crypto-miners devil !