Configure Secure RDP using a Windows Bastion Host

GSP303

Google Cloud Self-Paced Labs

Overview

In a challenge lab you're given a scenario and a set of tasks. Instead of following step-by-step instructions, you will use the skills learned from the labs in the quest to figure out how to complete the tasks on your own! An automated scoring system (shown on this page) will provide feedback on whether you have completed your tasks correctly.

When you take a challenge lab, you will not be taught new Google Cloud concepts. You are expected to extend your learned skills, like changing default values and reading and researching error messages to fix your own mistakes.

To score 100% you must successfully complete all tasks within the time period!

This lab is only recommended for students who have Compute Engine skills. Are you up for the challenge?

Topics tested

- Create a new VPC to host secure production Windows services.
- Create a Windows host connected to a subnet in the new VPC with an internal only network interface.
- Create a Windows bastion host (jump box) in with an externally accessible network interface.
- Configure firewalls rules to enable management of the secure Windows host from the Internet using the bastion host as a jump box.

Setup

Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This Qwiklabs hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

What you need

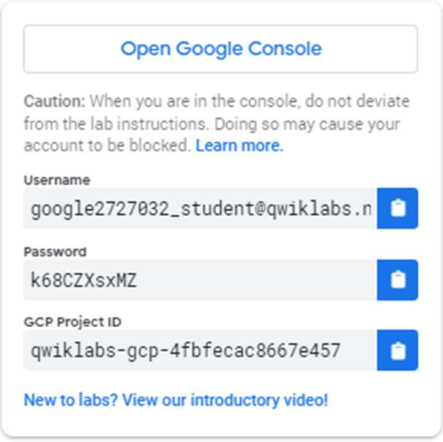
To complete this lab, you need:

- Access to a standard internet browser (Chrome browser recommended).
- Time to complete the lab.
  Note: If you already have your own personal Google Cloud account or project, do not use it for this lab.

Note: If you are using a Pixelbook, open an Incognito window to run this lab.

How to start your lab and sign in to the Google Cloud Console

1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is a panel populated with the temporary credentials that you must use for this lab.



Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

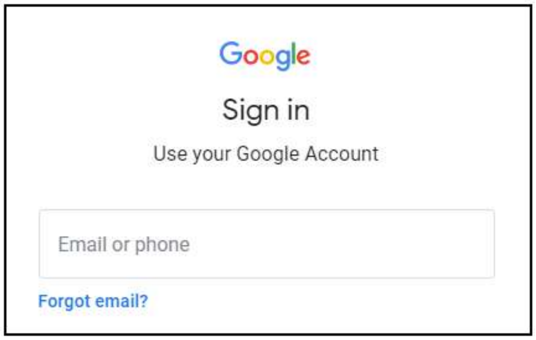
Username
google2727032_student@qwiklabs.n

Password
k68CZXsxMZ

GCP Project ID
qwiklabs-gcp-4fbfecac8667e457

New to labs? View our introductory video!

2. Copy the username, and then click **Open Google Console**. The lab spins up resources, and then opens another tab that shows the **Sign in** page.



Google

Sign in

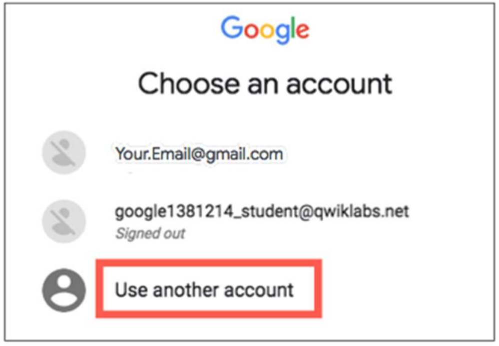
Use your Google Account

Email or phone

Forgot email?

Tip: Open the tabs in separate windows, side-by-side.

If you see the **Choose an account** page, click **Use Another Account**.



Google

Choose an account

Your.Email@gmail.com

google1381214_student@qwiklabs.net
Signed out

Use another account

3. In the **Sign in** page, paste the username that you copied from the Connection Details panel. Then copy and paste the password.

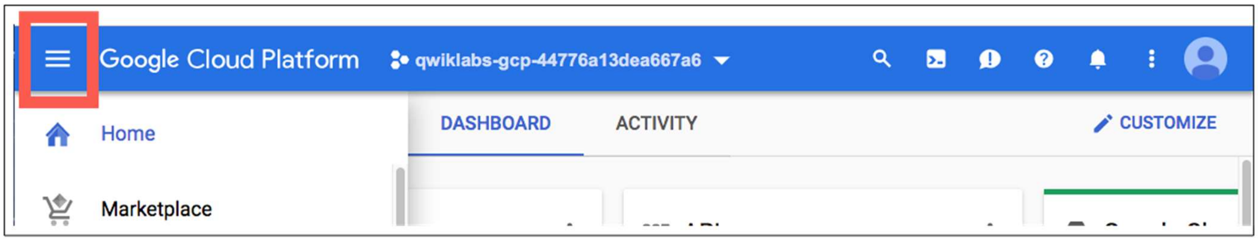
   Important: You must use the credentials from the Connection Details panel. Do not use your Qwiklabs credentials. If you have your own Google Cloud account, do not use it for this lab (avoids incurring charges).

4. Click through the subsequent pages:

   - Accept the terms and conditions.
   - Do not add recovery options or two-factor authentication (because this is a temporary account).
   - Do not sign up for free trials.

After a few moments, the Cloud Console opens in this tab.

Note: You can view the menu with a list of Google Cloud Products and Services by clicking the **Navigation menu** at the top-
left.



Challenge scenario

Your company has decided to deploy new application services in the cloud and your assignment is developing a secure framework for managing the Windows services that will be deployed. You will need to create a new VPC network environment for the secure production Windows servers.

Production servers must initially be completely isolated from external networks and cannot be directly accessible from, or be able to connect directly to, the internet. In order to configure and manage your first server in this environment, you will also need to deploy a bastion host, or jump box, that can be accessed from the internet using the Microsoft Remote Desktop Protocol (RDP). The bastion host should only be accessible via RDP from the internet, and should only be able to communicate with the other compute instances inside the VPC network using RDP.

Your company also has a monitoring system running from the default VPC network, so all compute instances must have a second network interface with an internal only connection to the default VPC network.

Your challenge

Deploy the secure Windows machine that is not configured for external communication inside a new VPC subnet, then deploy the Microsoft Internet Information Server on that secure machine.

Tasks:

The key tasks are listed below. Good luck!

- Create a new VPC network with a single subnet.
- Create a firewall rule that allows external RDP traffic to the bastion host system.
- Deploy two Windows servers that are connected to both the VPC network and the default network.
- Create a virtual machine that points to the startup script.
- Configure a firewall rule to allow HTTP access to the virtual machine.

Create the VPC Network

Create a new VPC network called `securenetwork`, then create a new VPC subnet inside `securenetwork`.

Once the network and subnet have been configured, configure a firewall rule that allows inbound RDP traffic (TCP port 3389) from the internet to the bastion host. This rule should be applied to the appropriate host using network tags.

Deploy your Windows instances and configure user passwords

Deploy a Windows 2016 server instance called `vm-securehost` with two network interfaces. Configure the first network interface with an internal only connection to the new VPC subnet, and the second network interface with an internal only connection to the default VPC network. This is the secure server.

Install a second Windows 2016 server instance called `vm-bastionhost` with two network interfaces. Configure the first network interface to connect to the new VPC subnet with an ephemeral public (external NAT) address, and the second network interface with an internal only connection to the default VPC network. This is the jump box or bastion host.

After your Windows instances have been created, create a user account and reset the Windows passwords in order to connect to each instance. The following `gcloud` command creates a new user called `app-admin` and resets the password for a host called `vm-bastionhost` located in the `us-central1-a` region:

```
gcloud compute reset-windows-password vm-bastionhost --user app_admin --zone us-central1-a
content_copy
```

Alternatively, you can force a password reset from the Compute Engine console. You will have to repeat this for the second host as the login credentials for that instance will be different.

Connect to the secure host and configure Internet Information Server

To connect to the secure host, you have to RDP into the bastion host first, and from there open a second RDP session to connect to the internal private network address of the secure host. A Windows Compute Instance with an external address can be connected to via RDP using the RDP button that appears next to Windows Compute instances in the Compute Instance summary page.

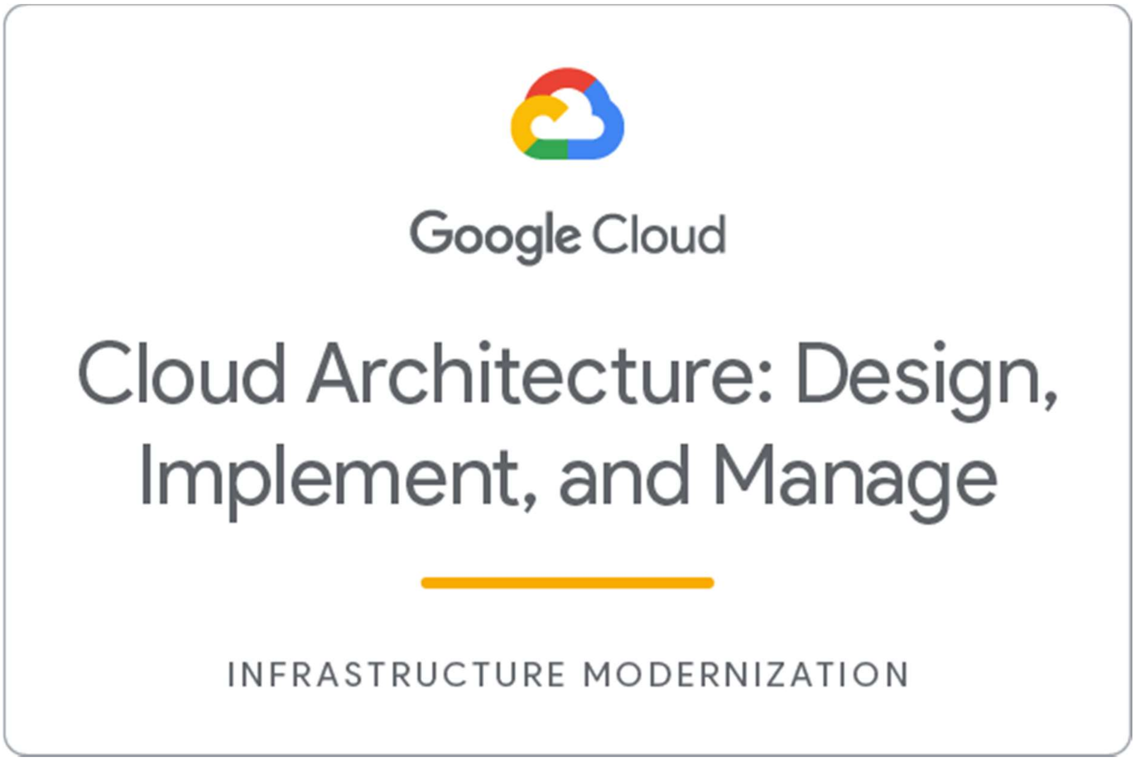
When connected to a Windows server you can launch the Microsoft RDP client using the command `mstsc.exe`, or you can search for `Remote Desktop Manager` from the Start menu. This will allow you to connect from the bastion host to other compute instances on the same VPC even if those instances do not have a direct internet connection themselves.

Troubleshooting

- **Unable to connect to the Bastion host:** Make sure you are attempting to connect to the external address of the bastion host. If the address is correct you may not be able to connect to the bastion host if the firewall rule is not correctly configured to allow TCP port 3389 (RDP) traffic from the internet, or your own system's public IP-address, to the network interface on the bastion host that has an external address. Finally, you might have issues connecting via RDP if your own network does not allow access to internet addresses via RDP. If everything else is definitely OK you will need to talk to the owner of the network you are connected to the internet with to open up port 3389 or connect using a different network.

- **Unable to connect to the Secure Host from the Bastion host:** If you can successfully connect to the bastion host but are unable to make the internal RDP connection using Microsoft Remote Desktop Connection application, check that both instances are connected to the same VPC network.

Congratulations!


Google Cloud
Cloud Architecture: Design, Implement, and Manage
INFRASTRUCTURE MODERNIZATION

Finish Your Quest

This self-paced lab is part of the Qwiklabs Cloud Architecture: Design, Implement, and Manage Quest. A Quest is a series of related labs that form a learning path. Completing this Quest earns you the badge above, to recognize your achievement. You can make your badge (or badges) public and link to them in your online resume or social media account. Enroll in this Quest and get immediate completion credit if you've taken this lab. See other available Qwiklabs Quests.

Take Your Next Lab

Continue your Quest with Build and Deploy a Docker Image to a Kubernetes Cluster, or check out these suggestions:

- Scale Out and Update a Containerized Application on a Kubernetes Cluster
- Deploy a Compute Instance with a Remote Startup Script

Next Steps / Learn More

Have you checked out the Data Science on the Google Cloud Platform Quest? Students are given the opportunity to practice all aspects of ingestion, preparation, processing, querying, exploring and visualizing data sets using Google Cloud tools and services. The exercises in the quest are taken from book **Data Science on the Google Cloud Platform** by Valliappa Lakshmanan, published by O'Reilly Media, Inc.

Google Cloud Training & Certification

...helps you make the most of Google Cloud technologies. Our classes include technical skills and best practices to help you get up to speed quickly and continue your learning journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. Certifications help you validate and prove your skill and expertise in Google Cloud technologies.

Manual Last Updated February 11, 2021

SOLUTION:

https://www.youtube.com/watch?v=jfIxkg4RiS8