**Configure Secure RDP using a Windows Bastion Host: Challenge Lab**

experimentLabschedule1 houruniversal\_currency\_alt5 Creditsshow\_chartIntermediate

Rate Lab

**GSP303**



**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 course 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 recommended for students preparing for the [Google Cloud Certified Professional Cloud Architect](https://cloud.google.com/certification/cloud-architect) certification exam. Are you up for the challenge?

**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 accessed 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. For the purposes of this lab, all resources should be provisioned in the following region and zone:

* **Region**: us-central1
* **Zone**: us-central1-c

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.

**Task 1. Create the VPC network**

1. Create a new VPC network called securenetwork.

Click **Check my progress** to verify the objective.

Create the VPC network.

Check my progress

1. Create a new VPC subnet inside securenetwork in the us-central1 region.

Click **Check my progress** to verify the objective.

Create the VPC subnet.

Check my progress

1. 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.

Click **Check my progress** to verify the objective.

Create the firewall rule.

Check my progress

**Task 2. Deploy your Windows instances and configure user passwords**

1. Deploy a Windows 2016 server (Server with Desktop Experience) instance called vm-securehost with two network interfaces in the us-central1-c zone.
   * Configure the first network interface with an internal only connection to the newly created VPC subnet.
   * The second network interface with an internal only connection to the default VPC network. This is the secure server.

Click **Check my progress** to verify the objective.

Create the vm-securehost instance.

Check my progress

1. Deploy a second Windows 2016 server (Server with Desktop Experience) instance called vm-bastionhost with two network interfaces in the us-central1-c zone.
   * Configure the first network interface to connect to the newly created VPC subnet with an ephemeral public (external NAT) address.
   * The second network interface with an internal only connection to the default VPC network. This is the jump box or bastion host.

Click **Check my progress** to verify the objective.

Create the vm-bastionhost instance.

Check my progress

Configure user passwords

1. After your Windows instances have been created, create a user account and reset the Windows passwords in order to connect to each instance.

**NOTE:** Copy the User name and Password of both instances for later use.

1. 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-c zone:

gcloud compute reset-windows-password vm-bastionhost --user app\_admin --zone us-central1-c

Copied!

content\_copy

1. The following gcloud command creates a new user called app-admin and resets the password for a host called vm-securehost located in the us-central1-c zone:

gcloud compute reset-windows-password vm-securehost --user app\_admin --zone us-central1-c

Copied!

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.

**Task 3. Connect to the secure host and configure Internet Information Server**

1. To connect to the secure host, you have to RDP into the **bastion host** first. 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.
2. Once you are connected to the bastion host using RDP session then open a new RDP session inside the **bastion host** to connect to the internal private network address of the **secure host**.
3. 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.

Once you connect to the vm-securehost machine through RDP then configure Internet Information Server.

1. Once you log in to the vm-securehost machine, Open the Server Management window. And Configure the local server to Add **roles and features**.
2. Use the **Role-based or feature-based installation** to add the **Web Server (IIS)** role.

Click **Check my progress** to verify the objective.

Please configure IIS server in vm-securehost.

Configure the IIS web server software.

Check my progress

*Please configure IIS server in vm-securehost.*

**Troubleshooting**