Maintaining Efficient Process Utilization on Your Computer in Windows

Head's up: You'll experience a delay as the labs initially load, particularly for Windows labs.

**Introduction**

In this lab, you'll use the new commands you learned to do some process maintenance on a Windows virtual machine. As an IT Support Specialist, it’s super important that you maintain efficient process utilization on your machines.

**What you’ll do**

* Collect process information using the Task Viewer.
* Terminate a specific process using Powershell.
* Terminate multiple processes using Powershell.

**You will have 60 minutes to complete this lab.**

# **Maintaining Efficient Process Utilization on Windows**

External IP address



content\_copy

username



content\_copy

password



content\_copy

**Introduction**

In this lab, you'll use the new commands you learned to do some process maintenance on a Windows virtual machine. As an IT Support Specialist, it's super important that you maintain efficient process utilization on your machines.

**Head's up**: You'll experience a delay as the labs initially load (particularly for Windows labs). So, please **wait a couple of minutes for the labs to load**. Please also make sure to access the labs **directly through Coursera** and not in the Qwiklabs catalog. If you access the labs through the Qwiklabs catalog, you will *not* receive a grade. (As you know, a passing grade is required to matriculate through the course.) The grade is calculated when the lab is complete, so be sure to hit "**End Lab**" when you're done!

You'll have 60 minutes to complete this lab.

**What you'll do**

* Collect process information using the Task Viewer.
* Terminate a specific process using Powershell.
* Terminate multiple processes using Powershell.

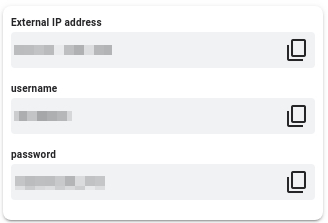
Start the lab

You'll need to start the lab before you can access the materials in the virtual machine OS. To do this, click the green “Start Lab” button at the top of the screen.

**Note:** For this lab you are going to access the **Windows VM** through your **local RDP Client**, and not use the **Google Console** (**Open GCP Console** button is not available for this lab).

Start Lab

After you click the “Start Lab” button, you will see all the connection details on the left-hand side of your screen. You should have a screen that looks like this:



**Note:** Working with Qwiklabs may be similar to the work you'd perform as an IT Support Specialist; you'll be interfacing with a cutting-edge technology that requires multiple steps to access, and perhaps healthy doses of patience and persistence(!). You'll also be using **RDP** to enter the labs -- a critical skill in IT Support that you’ll be able to practice through the labs.

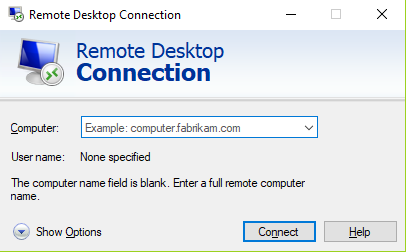
**Accessing the virtual machine**

Please find one of the four relevant options below based on your device's operating system.

Option 1: Windows Users: Connecting to your VM via RDP

In this section, you will use Remote Desktop Connection to connect to your windows instance using its external IP address.

1. Open Remote Desktop Connection by clicking the **Start** button. In the search box, type Remote Desktop Connection, and then, in the list of results, click Remote Desktop Connection.
2. Enter the external IP address of the instance you want to connect to in the **Computer** field. Find the external IP address for your instance from the Connection Details Panel on the left side. Click on **connect**.



1. Change the username to **student**. And use the password mentioned in the Connection Details Panel on the left side. Click **OK**.
2. Click **Yes** to accept the certificate.

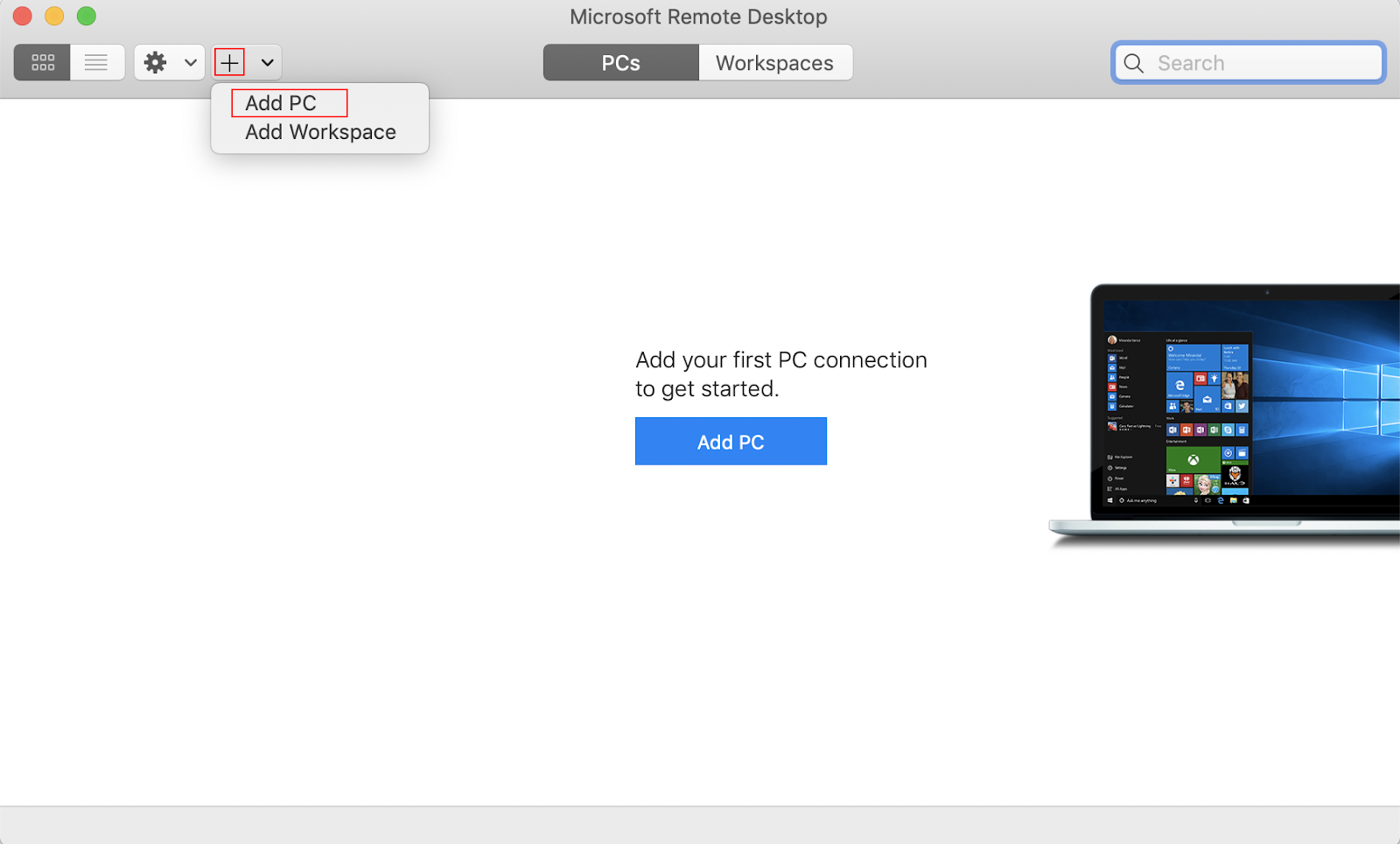
You should now see a visual interface that looks exactly like the Windows 10 OS!

If you see any error message, close the window and wait a minute or so. Sometimes the VM-creation process takes a few minutes, and you won't be able to access the VM until it's finished. This also applies to any errors that say your credentials (username and password) are incorrect.

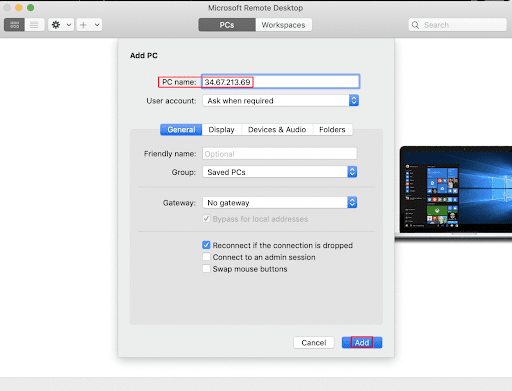
Option 2: OS X users: Connecting to your VM via RDP

In this section, you will use Microsoft Remote Desktop 10 to connect to your windows instance using its external IP address. OSX users can [download Microsoft Remote Desktop from the Mac App Store](https://apps.apple.com/us/app/microsoft-remote-desktop-10/id1295203466?mt=12). If you are using Microsoft Remote Desktop 8, note that the interface will vary slightly than what’s listed below.

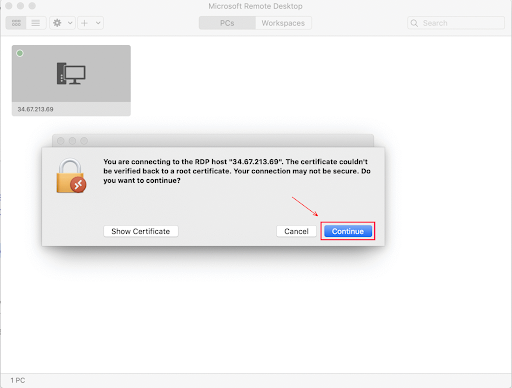
1. Open Microsoft Remote Desktop 10 application.
2. Click on **+** sign above, followed by **Add PC**.



1. Enter the external IP address of the instance you want to connect to in the **PC name** field. Find the external IP address for your instance from the Connection Details Panel on the left side. Click on the **Add** button.



1. You should now be able to see your desktop represented by the external IP address of your VM instance under **PCs**. Double click on your VM’s external IP address.
2. The application will now prompt you for username and password. Change the username to **student**. And use the password mentioned in the Connection Details Panel on the left side. Once you have entered the details click **Continue**.
3. For any prompt regarding ‘Certificate verification’, click **continue**.



You should now see a visual interface that looks exactly like the Windows 10 OS!

If you see any error message, close the window and wait a minute or so. Sometimes the VM-creation process takes a few minutes, and you won't be able to access the VM until it's finished. This also applies to any errors that say your credentials (username and password) are incorrect.

Option 3: Chrome OS users: Connecting to your VM via RDP

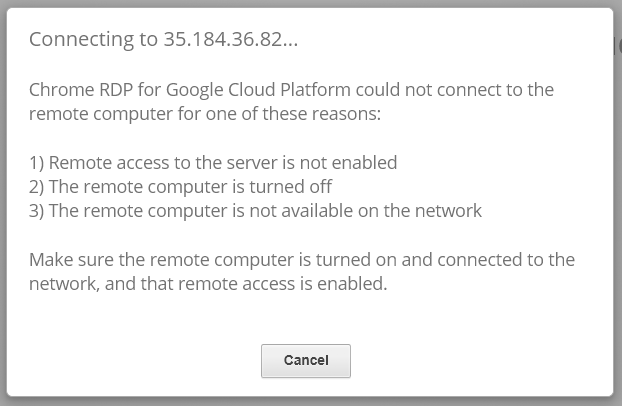
In this section, you will use Chrome RDP to connect to your windows instance using its external IP address.

Chrome OS users can [download Chrome RDP from Chrome Web Store](https://chrome.google.com/webstore/detail/chrome-rdp/cbkkbcmdlboombapidmoeolnmdacpkch). Once you navigate to the download page, click on the **Add to Chrome** button. Click on **Add app** in case of any pop-ups. Then, click on **Launch app** to start the application.

1. Open the Chrome RDP application.
2. Enter the external IP address of the instance you want to connect to in the **Enter the computer name or address to connect to** field. Find the external IP address for your instance from the Connection Details Panel on the left side. Click on **connect**.
3. Leave the domain field blank. Change the username to **student**. And use the password mentioned in the Connection Details Panel on the left side. Click **OK**.
4. Click **Continue** for any window related to certificate verification.

You should now see a visual interface that looks exactly like the Windows 10 OS!

If you see any error message (an example of one is shown below), close RDP and wait a minute or so. Sometimes the VM-creation process takes a few minutes, and you won't be able to access the VM until it's finished. This also applies to any errors that say your credentials (username and password) are incorrect.

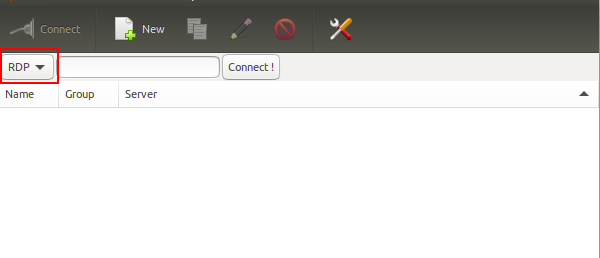


Option 4: Linux users: Connecting to your VM via RDP

In this section, you will use **Remmina** to connect to your windows instance using its external IP address. Open Remmina in your Linux machine. Linux users can [install Remmina](https://remmina.org/how-to-install-remmina/) if it is not pre-installed.

1. Open Remmina.
2. Enter the external IP address of the instance you want to connect to. Find the external IP address for your instance from the Connection Details Panel on the left side. Click on **Connect**.

Make sure the connection protocol is set to **RDP**, as shown in the image below:



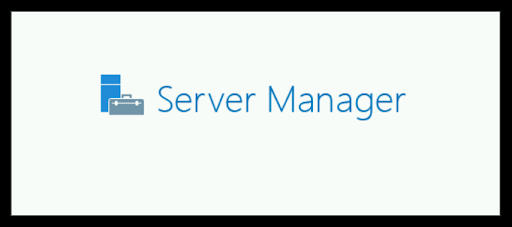
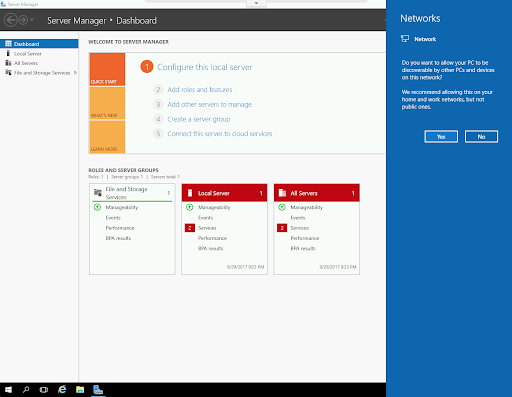
1. A window appears asking you accept the certificate, click **Ok** to continue.
2. Leave the domain field blank. Change the username to **student**. And use the password mentioned in the Connection Details Panel on the left side, for the **Password** field. Click **Ok** to continue.

You should now see a visual interface that looks exactly like the Windows 10 OS!

If you see any error message, close the window and wait a minute or so. Sometimes the VM-creation process takes a few minutes, and you won't be able to access the VM until it's finished. This also applies to any errors that say your credentials (username and password) are incorrect.

Using the Windows instance

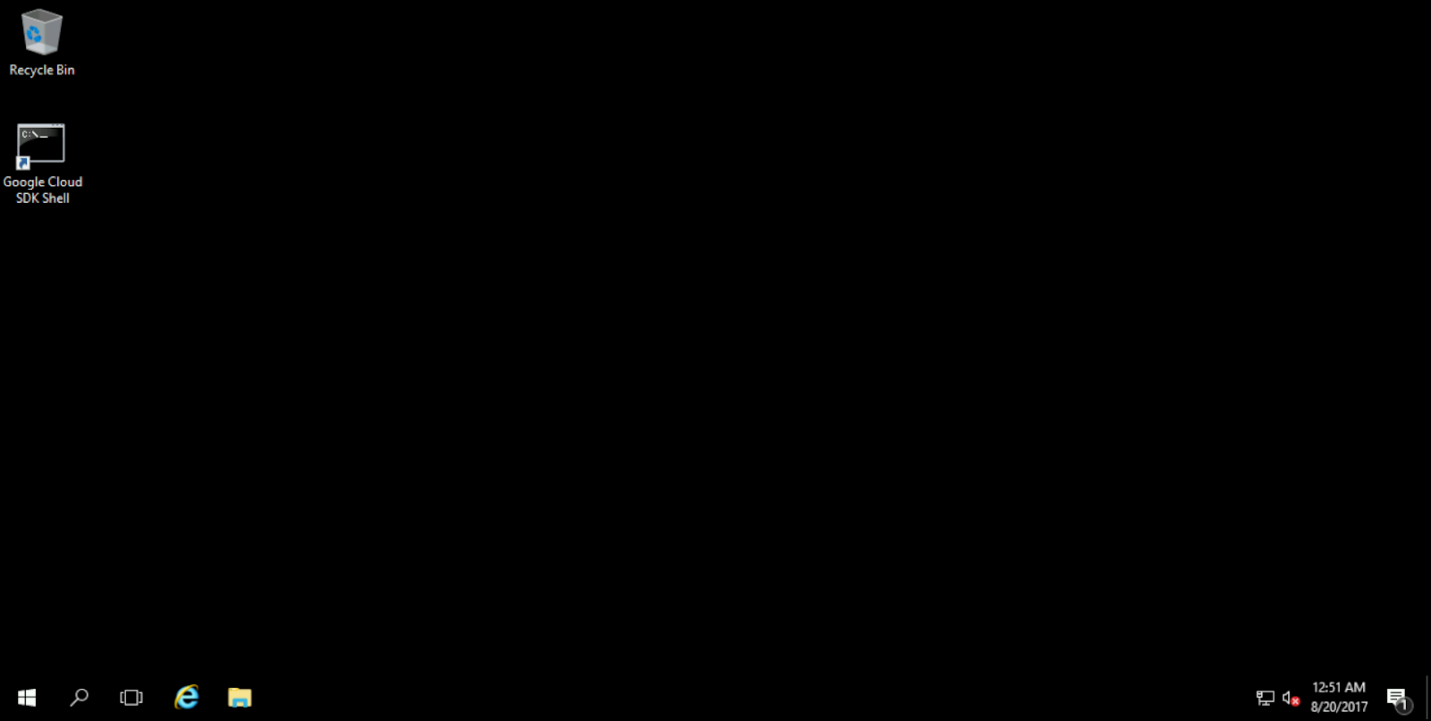
Now you have access to the Windows instance, you're ready to start using it! This version of Windows is intended to be used on a Server, and auto-starts a server-management program. We don't need this for this lab, so wait for it to finish starting and then close it. You may see the desktop appear for a few seconds before the program launches.

Once that's closed, the Windows OS is ready for you to use.

**Finishing the login process**

Now you‘ll see a Windows desktop background that looks like this:



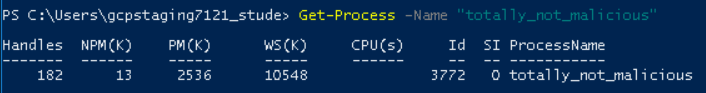
**Terminating a specific process**

On Windows, you can view running processes in the Task Viewer, or use Powershell (this is what you'll be using for this lab). For these operations, you'll need to be running a Powershell terminal in ***Administrative*** mode. So, search the Start Menu for Powershell, right-click it, and select **"Run as Administrator"**.

From Powershell, you can use Get-Process to search for a process by name. The "totally\_not\_malicious" process is running on this machine, too. Search for it, using this command:

Get-Process -Name "totally\_not\_malicious"

Each row represents a process, and one of the columns shows the process ID:



To end a process, you can use taskkill and specify the Process ID, or PID, of the process:

**Note:** Make sure you **replace/substitute** the "[PROCESS ID]" with id of the process you got from the previous command.

taskkill /F /PID [PROCESS ID]

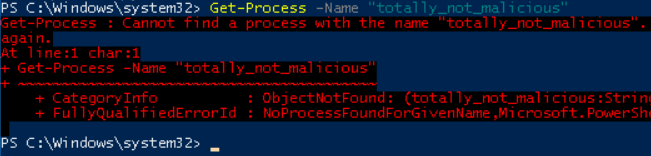
You should see this message after running taskkill with the PID for your process, which will likely be different than the ID specified here:



To verify that the process is no longer running, you can search for it again:

Get-Process -Name "totally\_not\_malicious"

This should throw an error because no process by that name exists anymore, indicating that you've successfully ended it:



Click Check my progress to verify the objective.

Malicious Process

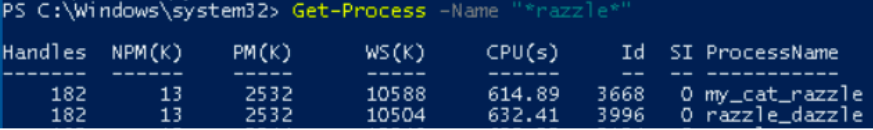
Check my progress

**Terminating multiple processes**

There are processes containing the word "razzle" also running on this VM. Get-Process doesn't handle processes with partially-matching names, like grep does, and running Get-Process -Name "razzle" would result in no matches. However, you can use "wildcards" (asterisks) to look for processes that contain "razzle" in their name:

Get-Process -Name "\*razzle\*"

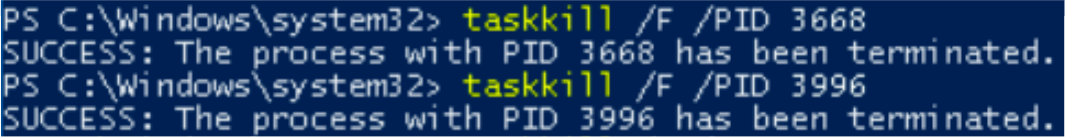
This will show two processes that contain "razzle" in their name:



You can use taskkill, like before, once for each of the "razzle" processes:

**Note:** Make sure you **replace/substitute** the "[PROCESS ID]" with id of the process you got from the previous command.

taskkill /F /PID [PROCESS ID]



You can use Get-Process again to verify that the processes have been ended:

Get-Process -Name "\*razzle\*"

You shouldn't see any processes in the output. When you ran this before to verify that the malicious process had been terminated, it printed an error message because the specifically-named process was not present. When you use a wildcard (\*) in the search, you aren't looking for an exact match. So, rather than an error message, the command outputs nothing at all (because there are no matches):



Click Check my progress to verify the objective.

Razzle

Check my progress

**Conclusion**

Congrats! You've successfully used the Powershell commands Get-Process to find Windows processes, and taskkill to end them. As an IT Support Specialist, it's important for you to monitor system processes and maintain them using the Task Viewer and Powershell.

**End your lab**