Use Logs to Help You Track Down an Issue 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 logs to help you troubleshoot and track down an issue. As an IT Support Specialist, it’s crucial that you know how to troubleshoot and “follow the cookie crumbs.” There are five different issues that you'll need to resolve, using the skills you’ve learned so far in this course.

**What you’ll do**

There are five different issues on the VM that you need to identify and fix. We’ll help with the first one of each, then you’re on your own!

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

# **Use Logs to Help You Track Down an Issue in Windows**

External IP address



content\_copy

username



content\_copy

password



content\_copy

## Introduction

In this lab, you'll use logs to help you troubleshoot and track down an issue. As an IT Support Specialist, it's crucial that you know how to troubleshoot and "follow the cookie crumbs." There are five different issues that you'll need to resolve, using the skills you've learned so far in this course.

**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.

**WARNING** - If it's your **second** attempt of this lab: go back to Coursera and retry this lab by hitting the **"Open Tool button"** in order to get the full score for this attempt.

**What you'll do**

Here are the concepts you need to be familiar with before taking this lab:

* Updating software that's out-of-date
* Finding and deleting files
* Modifying file permissions
* Finding and terminating specific processes

**The scenario**

Your computer is having some issues and you can't seem to figure out what's wrong. Argh! Dig through the logs to figure out how to fix these issues.

You'll use logs to identify issues on a Windows VM, which you'll then fix using the knowledge you've gained from the other labs that you've completed.

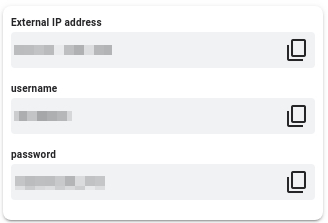
### Start the lab

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.

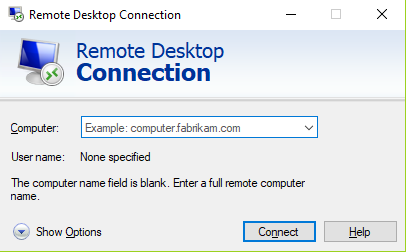
## Accessing the virtual machine

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.

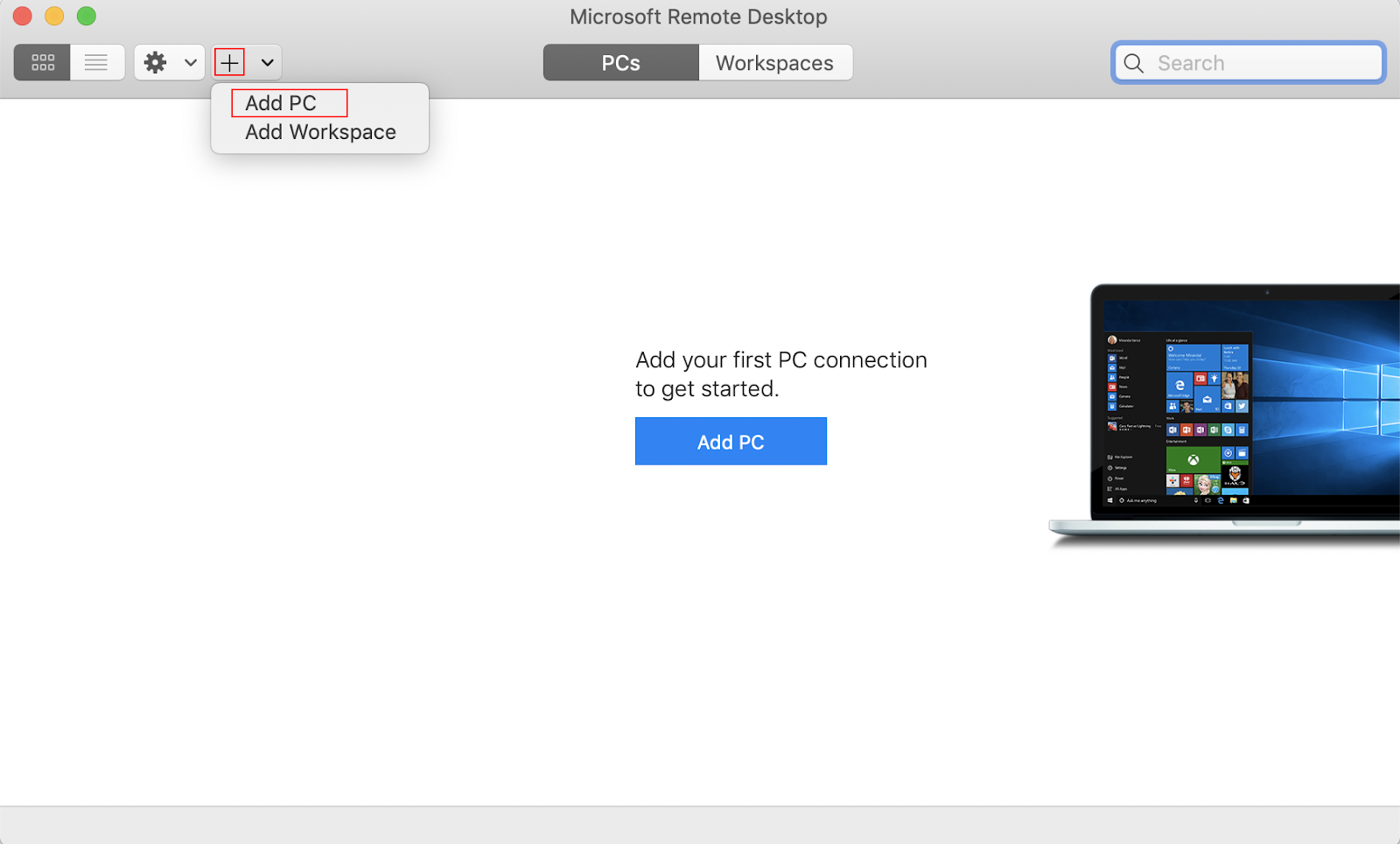
You should now see a visual interface that looks exactly like the Windows 10 OS!

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.

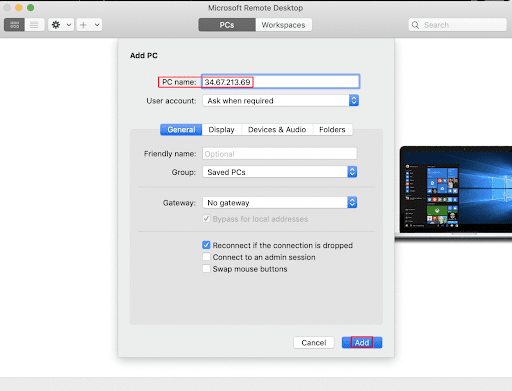
### Option 2: OS X users: Connecting to your VM via RDP

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.

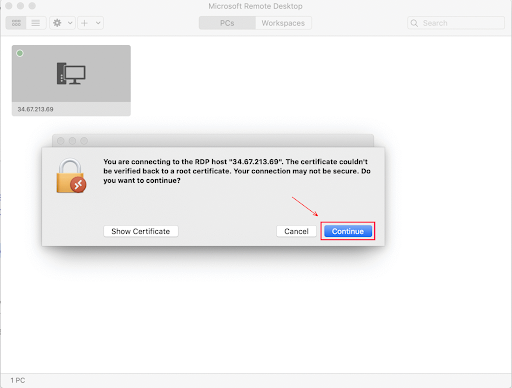
1. Open Microsoft Remote Desktop 10 application.
2. Click on **+** sign above, followed by **Add PC**.



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

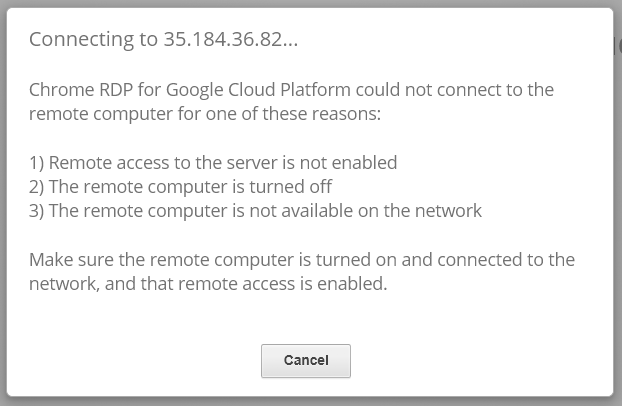
In this section, you will use Chrome RDP to connect to your windows instance using its external IP address.

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.

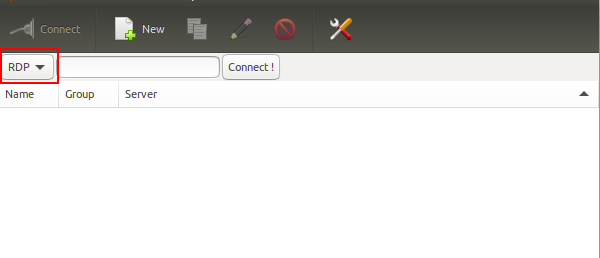


### Option 4: Linux users: Connecting to your VM via RDP

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:



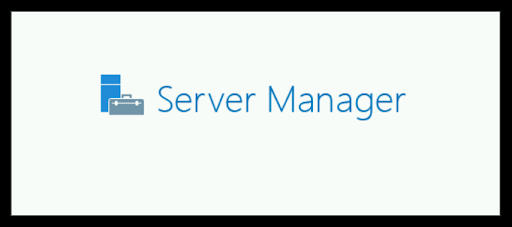
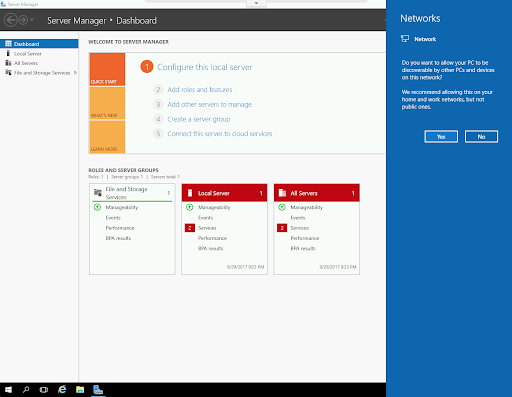
1. A window appears asking you accept the certificate, click **Ok** to continue.
2. Leave the domain field blank. Change the username to **student**. And use the password mentioned in the Connection Details Panel on the left side, for the **Password** field. Click **Ok** to continue.

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

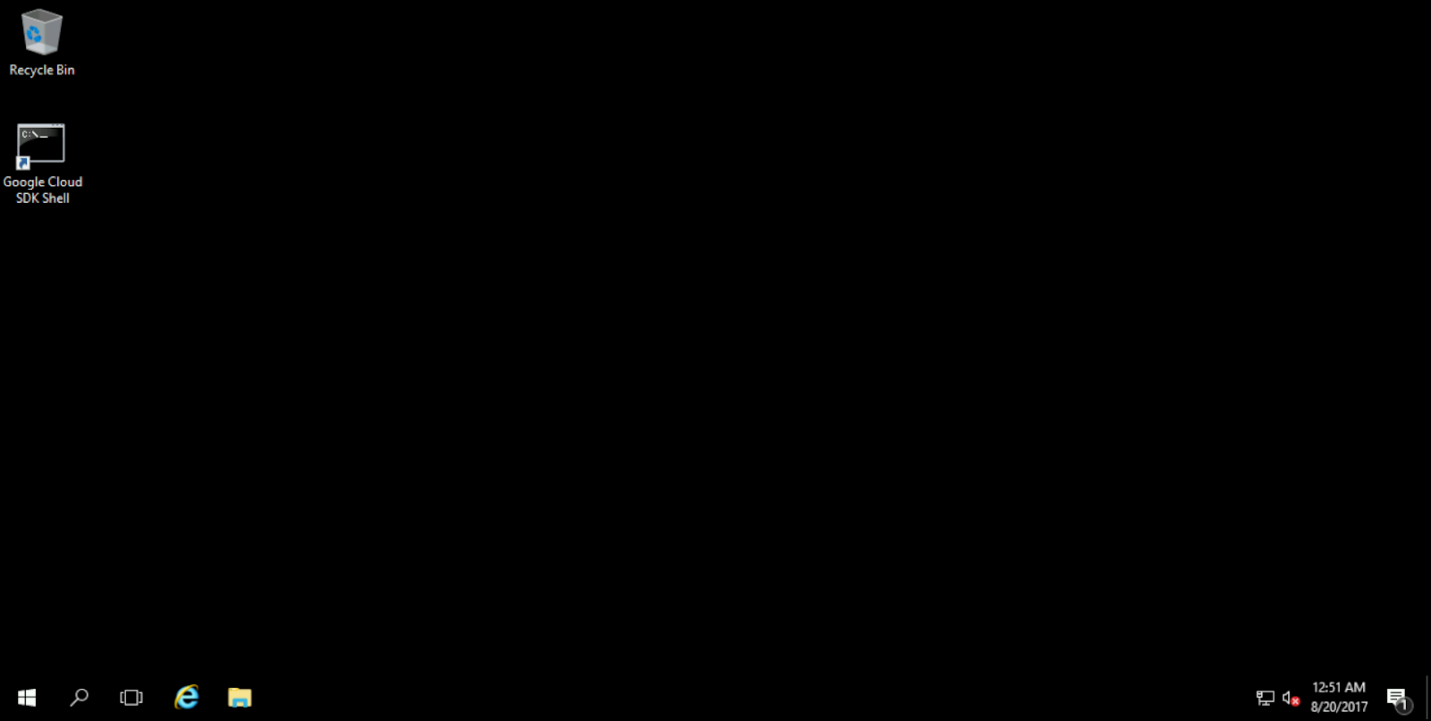
Now you have access to the Windows instance, you're ready to start using it! This version of Windows is intended to be used on a Server, and auto-starts a server-management program. We don't need this for this lab, so wait for it to finish starting and then close it. You may see the desktop appear for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

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

**Finishing the login process**

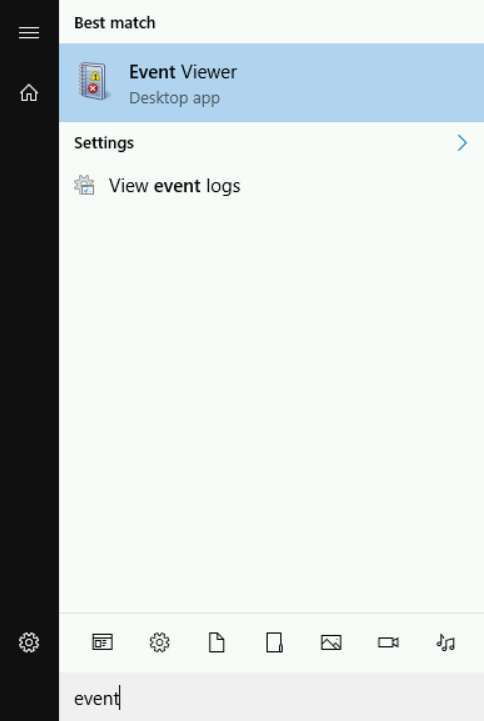
Now you‘ll see a Windows desktop background that looks like this:



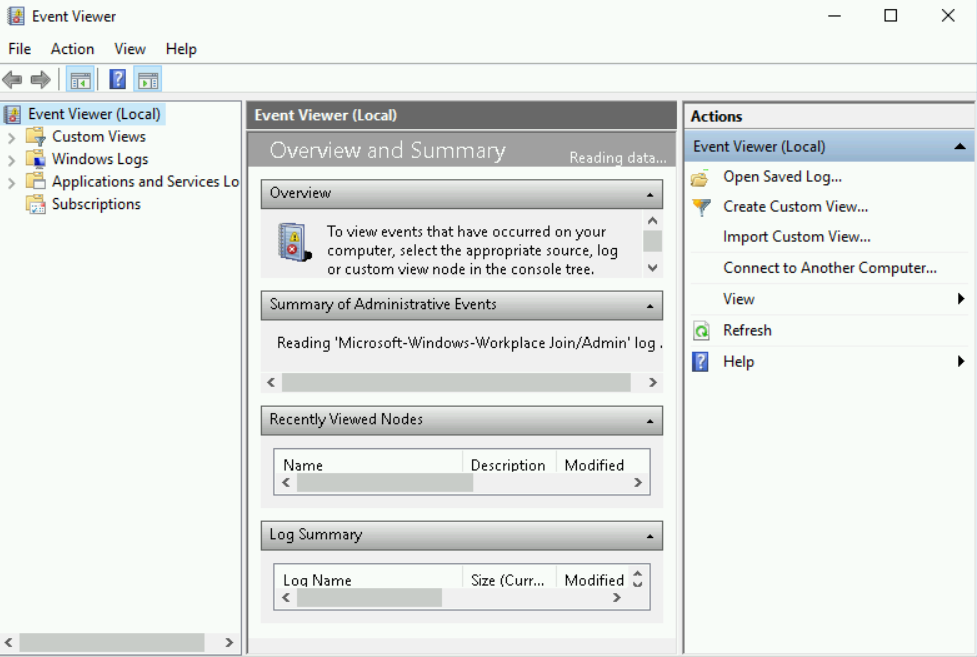
**Note**: Please make sure that you have connected your RDP session with the username ‘student’ otherwise you will not earn the score for your lab objectives.

## Viewing logs on Windows

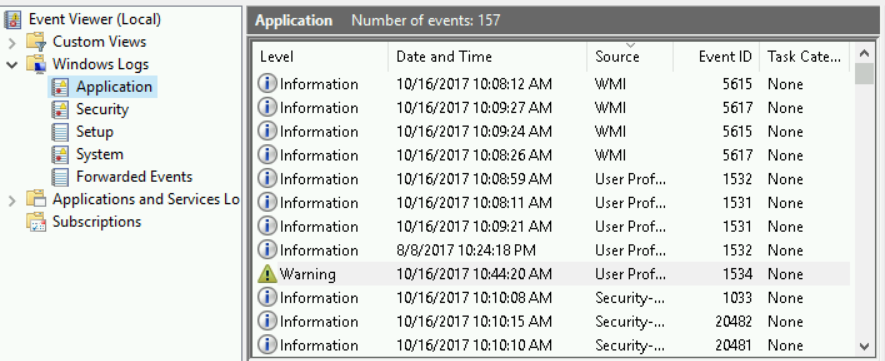
To view logs on Windows, you should use the Event Viewer application. To open Event Viewer, open the Start menu and search for "event viewer". The application icon should look like the image below. Click it to open the application.



Once open, it should look like this:



Feel free to resize the window at any time, to make the text easier to read. Next, click on the "Windows Logs" folder in the far-left column. Then, select "Application" to view the application logs, where the logs for this lab are located:

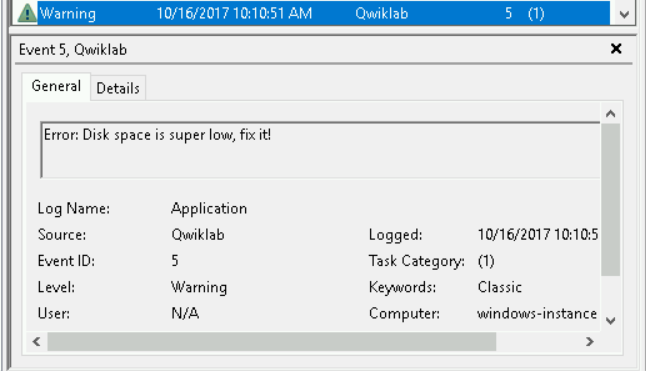


Scroll through the logs to find the five logs that you need to fix for this lab. They should have a time that's close to when you started the lab, and the "Source" field should be "Qwiklab". To view details of a log entry, click on it in Event Viewer, and a message window will open at the bottom of the Event Viewer window.

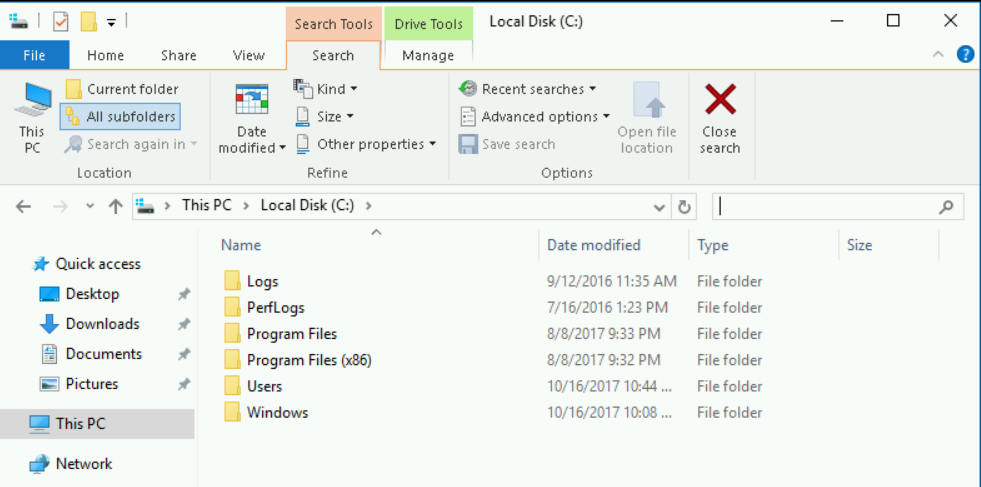
We'll walk through one of the logs, then the other four will be up to you. You're on your own...but you've got this!

**Low disk space!**

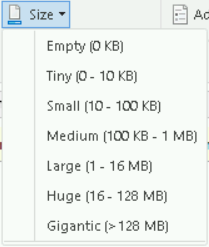
Find and click on the log with "Qwiklab" as the source and Event ID 5:



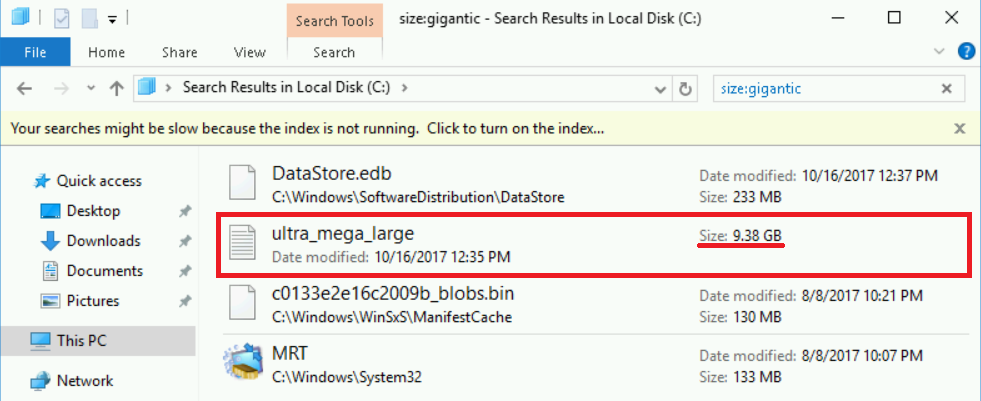
This log is warning you about a large file that's taking up disk space, but it doesn't specify the file name. On Windows, you can find large files using the File Explorer. Open it and navigate to your C:\ directory, then click the search bar at the top right. A "Search Options" tab should appear. Click on it to view the different ways you can configure your search:



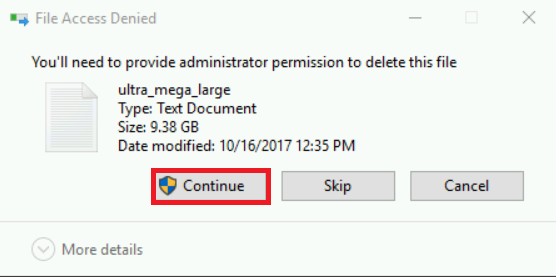
You're only interested in file size at the moment, so click the "Size" dropdown and choose "Gigantic" to start a search for files over 128 MB.



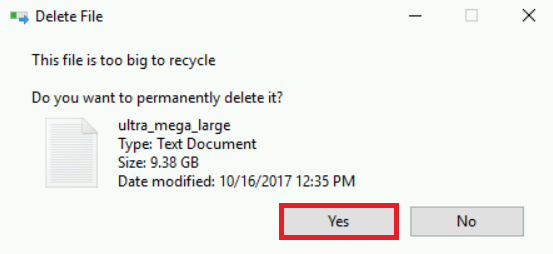
The search can take some time, and multiple files may appear in your search, but we're only interested in the largest (which is almost 10 gigabytes):



Now that you know which file is causing the low-memory error, you can delete it by right-clicking the file in the search results, and selecting "delete". You'll need to provide admin privileges to delete it. When this popup appears, click "continue":



Files over a certain size don't fit in the Windows "Recycle Bin", and can only be permanently deleted. After clicking "Continue", you'll see this message, indicating that the file is too large to recycle. Press "Yes" to delete permanently.



The file will delete, fixing the log issue! Note that the log will still remain in Event Viewer, because logs aren't deleted when the issues that caused them are removed.

**The remaining log entries**

The rest of the logs involve issues that you have already successfully fixed in earlier labs in this course. Refer back to those lessons and labs to refresh yourself on the required steps, if you’re stuck:

* Updating software that's out-of-date (Week 3 Labs)
* Finding and deleting files (Week 1 Labs)
* Modifying file permissions (Week 2 Labs)
* Finding and terminating specific processes (Week 5 Labs)

If you’d like to check your steps along the way, refer to your score in the top right of the lab. Click the score and run each step to check individually as you go. Good luck!

## Conclusion

Congrats! You've successfully used logs to track down and fix issues on a Windows machine. This is a crucial skill that you'll need to develop as an IT Support Specialist.

## End your lab