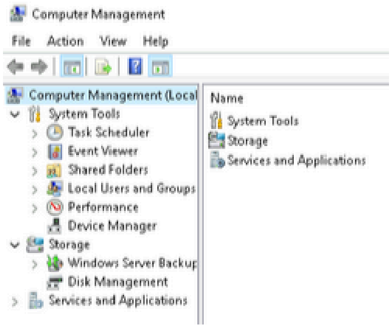
3 - Computer Management

Task 4 ○ Computer Management

We're continuing with Tools that are available through the **System Configuration** panel.

The **Computer Management** (`compmgmt`) utility has three primary sections: **System Tools**, **Storage**, and **Services and Applications**.

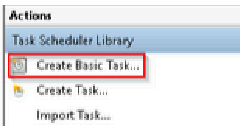


System Tools

Let's start with **Task Scheduler**. Per Microsoft, with Task Scheduler, we can create and manage common tasks that our computer will carry out automatically at the times we specify.

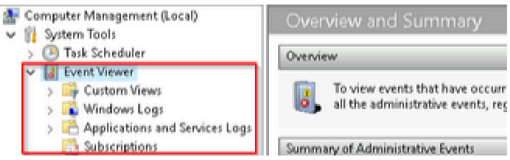
A task can run an application, a script, etc., and tasks can be configured to run at any point. A task can run at log in or at log off. Tasks can also be configured to run on a specific schedule, for example, every five mins.

To create a basic task, click on `Create Basic Task` under **Actions** (right pane).



Next is **Event Viewer**.

Event Viewer allows us to view events that have occurred on the computer. These records of events can be seen as an audit trail that can be used to understand the activity of the computer system. This information is often used to diagnose problems and investigate actions executed on the system.



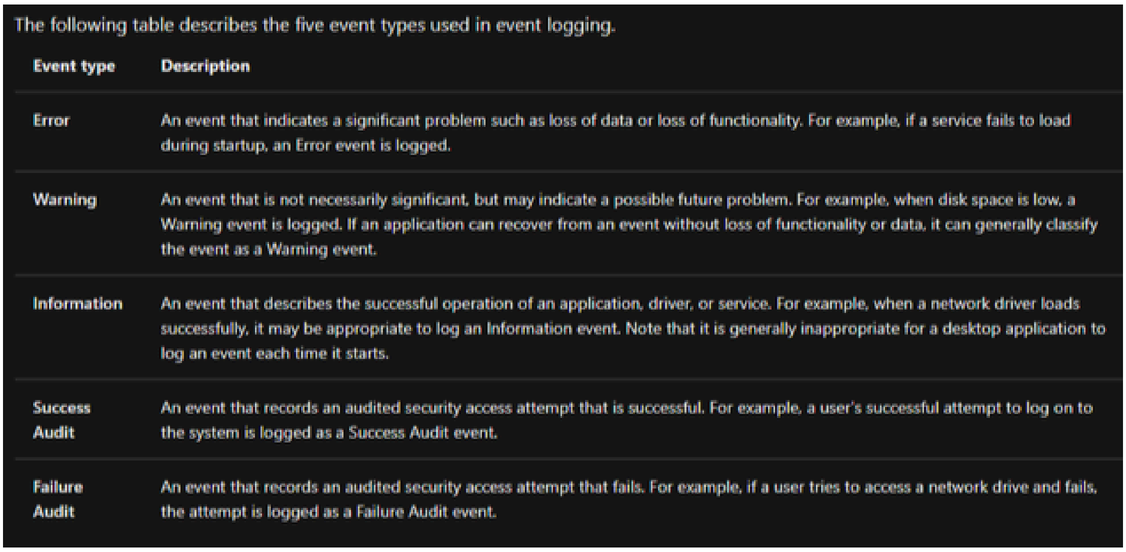
To view events that have occurr
all the administrative events, reg

Event Viewer has three panes.

1. The pane on the left provides a hierarchical tree listing of the event log providers. (as shown in the image above)
2. The pane in the middle will display a general overview and summary of the events specific to a selected provider.
3. The pane on the right is the actions pane.

There are five types of events that can be logged. Below is a table from docs.microsoft.com providing a brief description for each.

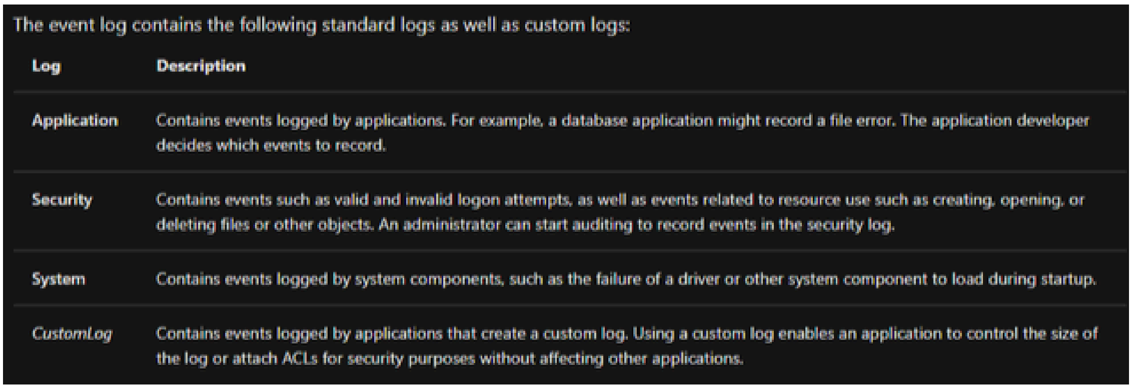
There are five types of events that can be logged. Below is a table from docs.microsoft.com providing a brief description for each.



The following table describes the five event types used in event logging.

Event type	Description
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event.
Information	An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.
Failure Audit	An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

The standard logs are visible under **Windows Logs**. Below is a table from docs.microsoft.com providing a brief description for each.

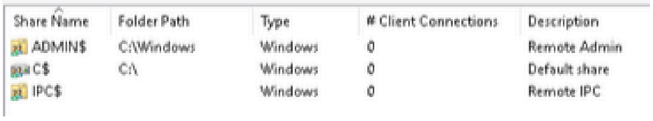


The event log contains the following standard logs as well as custom logs:

Log	Description
Application	Contains events logged by applications. For example, a database application might record a file error. The application developer decides which events to record.
Security	Contains events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can start auditing to record events in the security log.
System	Contains events logged by system components, such as the failure of a driver or other system component to load during startup.
CustomLog	Contains events logged by applications that create a custom log. Using a custom log enables an application to control the size of the log or attach ACLs for security purposes without affecting other applications.

For more information about Event Viewer and Event Logs, please refer to the Windows Event Log room.

Shared Folders is where you will see a complete list of shares and folders shared that others can connect to.



Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC

In the above image, under Shares, are the default share of Windows, C$, and default remote administration shares created by Windows, such as ADMIN$.

As with any object in Windows, you can right-click on a folder to view its properties, such as Permissions (who can access the shared resource).

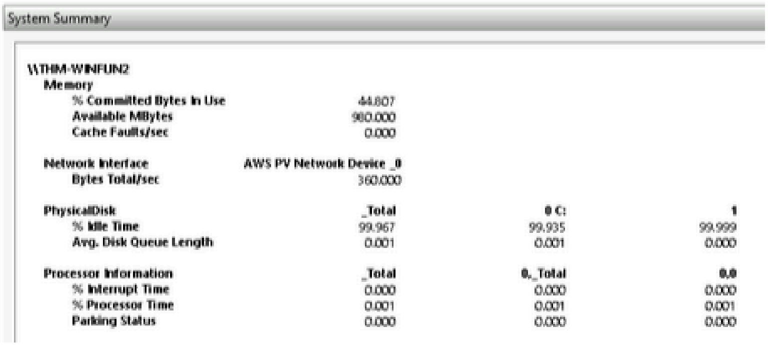
Under **Sessions**, you will see a list of users who are currently connected to the shares. In this VM, you won't see anybody connected to the shares.

All the folders and/or files that the connected users access will list under **Open Files**.

The **Local Users and Groups** section you should be familiar with from Windows Fundamentals 1 because it's `lusrmgr.msc`.

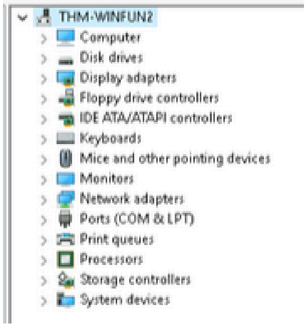
In **Performance**, you'll see a utility called **Performance Monitor** (`perfmon`).

Perfmon is used to view performance data either in real-time or from a log file. This utility is useful for troubleshooting performance issues on a computer system, whether local or remote.



```
System Summary

\\THM-WINFUN2
    Memory
        % Committed Bytes In Use                44.807
        Available MBytes                       980.000
        Cache Faults/sec                         0.000

    Network Interface            AWS PV Network Device _0
        Bytes Total/sec                        360.000

    PhysicalDisk                            _Total             0 C:                1
        % Idle Time                         99.967           99.935           99.999
        Avg. Disk Queue Length               0.001            0.001            0.000

    Processor Information                   _Total          0,_Total             0,0
        % Interrupt Time                     0.000            0.000            0.000
        % Processor Time                     0.001            0.001            0.001
        Parking Status                       0.000            0.000            0.000
```

Device Manager allows us to view and configure the hardware, such as disabling any hardware attached to the computer.

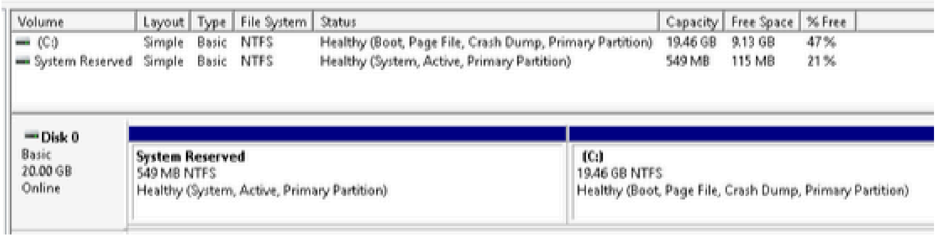


- THM-WINFUN2
  - Computer
  - Disk drives
  - Display adapters
  - Floppy drive controllers
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Ports (COM & LPT)
  - Print queues
  - Processors
  - Storage controllers
  - System devices

Storage

Under Storage is **Windows Server Backup** and **Disk Management**. We'll only look at Disk Management in this room.

Note: Since the virtual machine is a Windows Server operating system, there are utilities available that you will typically not see in Windows 10.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	19.46 GB	9.13 GB	47 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	549 MB	115 MB	21 %

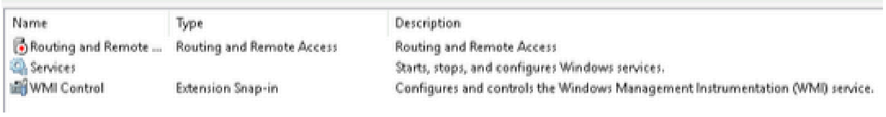
Disk 0 Basic 20.00 GB Online	**System Reserved** 549 MB NTFS Healthy (System, Active, Primary Partition)	**(C:)** 19.46 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. Some tasks are:

- Set up a new drive
- Extend a partition

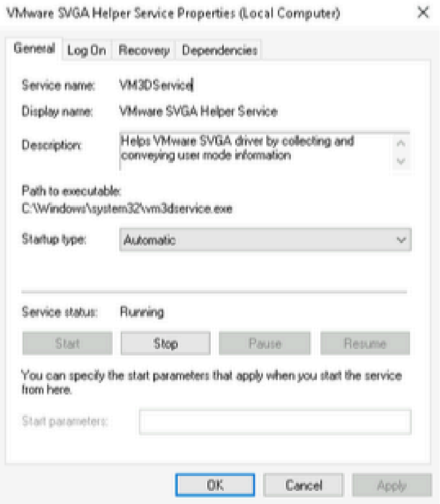
- Extend a partition
- Shrink a partition
- Assign or change a drive letter (ex. E:)

Services and Applications



Name	Type	Description
Routing and Remote ...	Routing and Remote Access	Routing and Remote Access
Services		Starts, stops, and configures Windows services.
WMI Control	Extension Snap-in	Configures and controls the Windows Management Instrumentation (WMI) service.

Recall from the previous task; a service is a special type of application that runs in the background. Here you can do more than enable and disable a service, such as view the Properties for the service.



VMware SVGA Helper Service Properties (Local Computer)

Service name: VM3DService

Display name: VMware SVGA Helper Service

Description: Helps VMware SVGA driver by collecting and conveying user mode information

Path to executable:
C:\Windows\system32\vm3dservice.exe

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

WMI Control configures and controls the **Windows Management Instrumentation** (WMI) service.

Per Wikipedia, "*WMI allows scripting languages (such as VBScript or Windows PowerShell) to manage Microsoft Windows personal computers and servers, both locally and remotely. Microsoft also provides a command-line interface to WMI called Windows Management Instrumentation Command-line (WMIC).*"

Note: The WMIC tool is deprecated in Windows 10, version 21H1. Windows PowerShell supersedes this tool for WMI.

Answer the questions below

What is the command to open Computer Management? (The answer is the name of the .msc file, not the full path)

compmgmt.msc

✓ Correct Answer

At what time every day is the GoogleUpdateTaskMachineUA task configured to run?

6:15 AM

✓ Correct Answer

What is the name of the hidden folder that is shared?

sh4r3dF0Ld3r

✓ Correct Answer