CS370 Operating Systems
Colorado State University
Yashwant K Malaiya
Fall 2022 L20
Containers, Virtual Memory

Slides based on
- Text by Silberschatz, Galvin, Gagne
- Various sources
Implementation of VMMs

Type 1: (ex VMWare esx) Low overhead, choice for data centers
   – Run in kernel mode, Implement device drivers, provide traditional OS services

Type2: (ex Virtualbox) Individuals, small organizations
   – VMM is simply a process, managed by host OS

Q: Do we really always need multiple copies of the OS?
Type 1 Hypervisors

• Run on top of *bare metal*
• Guest OSs believe they are running on bare metal, are unaware of hypervisor
  – are not modified
  – Better performance
• Choice for data centers
  • Consolidation of multiple OSes and apps onto less HW
  • Move guests between systems to balance performance
  • Snapshots and cloning
• Hypervisor creates runs and manages guest OSes
  – Run in kernel mode
  – Implement device drivers
  – provide traditional OS services like CPU and memory management
• Examples: VMWare esx (dedicated), Windows with Hyper-V (includes OS)
Type 2 Hypervisors

- Run on top of host OS
- VMM is simply a process, managed by host OS
  - host doesn’t know they are a VMM running guests
- poorer overall performance because can’t take advantage of some HW features
- Host OS is just a regular one
  - Individuals could have Type 2 hypervisor (e.g. Virtualbox) on native host (perhaps windows), run one or more guests (perhaps Linux, MacOS)
Virtualization support

• Terminology:
  – Guest Operating System
    • The OS running on top of the hypervisor
  – Host Operating System
    • For a type 2 hypervisor: the OS that runs on the hardware executions

• Create environments in which VMs can be run

• When a guest OS is started in an environment, continues to run until it causes an exception and traps to the hypervisor
  – For e.g., by executing an I/O instruction

• Set of operations that trap is controlled by a hardware bit map set by hypervisor
  – trap-and-emulate approach becomes possible
Virtualization benefits

• Run multiple OSes on a single machine
  – Consolidation, app dev, ...

• Security: Host system protected from VMs; VMs protected from each other
  – Sharing though shared file system volume, network communication

• Freeze, suspend, running VM
  – Then can move or copy somewhere else and resume
    • Live migration
  – Snapshot of a given state, able to restore back to that state
  – Clone by creating copy and running both original and copy

• Hence – cloud computing
Building Block – Trap and Emulate

• VM needs two modes: both in real user mode
  – virtual user mode and virtual kernel mode
• When Guest OS attempts to execute a privileged instruction, what happens?
  – Causes a trap
  – VMM gains control, analyzes error, executes operation as attempted by guest
  – Returns control to guest in user mode
  – Known as trap-and-emulate
• Trap-and-emulate was the technique used for implementing floating point instructions in CPUs without floating point coprocessor
Full vs Para-virtualization

• Full virtualization: Guest OS is unaware of the hypervisor. It thinks it is running on bare metal.

• Para-virtualization: Guest OS is modified and optimized. It sees underlying hypervisor.
  – Introduced and developed by Xen
    • Modifications needed: Linux 1.36%, XP: 0.04% of code base
  – Does not need as much hardware support
  – allowed virtualization of older x86 CPUs without binary translation
  – Not used by Xen on newer processors
D2 Submission

• Research and Development Canvas groups will be created in a couple of days by us.
  – All members of a team must join an applicable type of Canvas Groups.

• Only one team member (leader) will submit. Submission will be in the team leaders’ section.
  – Grade will automatically apply to all members, if they are in the same section.
  – Please give section numbers of all members in a multi-section team.
CPU Scheduling

• One or more virtual CPUs (vCPUs) per guest
  – Can be adjusted throughout life of VM

• When enough CPUs for all guests
  – VMM can allocate dedicated CPUs, each guest much like native operating system managing its CPUs

• Usually not enough CPUs (CPU overcommitment)
  – VMM can use scheduling algorithms to allocate vCPUs
  – Some add fairness aspect

• Oversubscription of CPUs means guests may get CPU cycles they expect
  – Time-of-day clocks may be incorrect
  – Some VMMs provide application to run in each guest to fix time-of-day
Memory Mapping:

- On a bare metal machine: OS uses page table/TLB to map Virtual page number (VPN) to Physical page number (PPN) (physical memory is shared). Each process has its own page table/TLB.
  - VPN -> PPN

- VMM: Real physical memory (machine memory) is shared by the OSs. Need to map PPN of each VM to MPN (Shadow page table)
  - PPN -> MPN
Memory Management

• VMM: Real physical memory (*machine memory*) is shared by the OSs. Need to map PPN of each VM to MPN (Shadow page table)

  **PPN -> MPN**

• Where is this done?
  – Has to be done by hypervisor *type 1*. Guest OS knows nothing about MPN.
  – Page Table/TLB updates are trapped to VMM. It needs to do VPN->PPN -> MPN.
  – It can do VPN->MPN directly (VMware ESX)
Virtual Machine (VM) as a software construct

• Each VM is configured with some number of processors, some amount of RAM, storage resources, and connectivity through the network ports.
• Once the VM is created it can be activated on like a physical server, loaded with an operating system and software solutions, and used just like a physical server.
• Unlike a physical server, VM only sees the resources it has been configured with, not all of the resources of the physical host itself.
• The hypervisor facilitates the translation and I/O between the virtual machine and the physical server.
Virtual Machine (VM) as a set of files

• Configuration file describes the attributes of the virtual machine containing
  – server definition,
  – how many virtual processors (vCPUs)
  – how much RAM is allocated,
  – which I/O devices the VM has access to,
  – how many network interface cards (NICs) are in the virtual server
  – the storage that the VM can access

• When a virtual machine is instantiated, additional files are created for logging, for memory paging etc.

• Copying a VM produces not only a backup of the data but also a copy of the entire server, including the operating system, applications, and the hardware configuration itself
Live Migration

Running guest can be moved between systems, without interrupting user access to the guest or its apps
  – for resource management,
  – maintenance downtime windows, etc

• Migration from source VMM to target VMM
  – Needs to migrate all pages gradually, without interrupting execution (details in next slide)
  – Eventually source VMM freezes guest, sends vCPU’s final state, sends other state details, and tells target to start running the guest
  – Once target acknowledges that guest running, source terminates guest
Live Migration

- Migration from source VMM to target VMM
  - Source establishes a connection with the target
  - Target creates a new guest
  - Source sends all read-only memory pages to target
  - Source starts sending all read-write pages
  - Source VMM freezes guest, sends final stuff,
  - Once target acknowledge that guest running, source terminates guest.
VIRTUAL APPLIANCES: “shrink-wrapped” virtual machines

• Developer can construct a virtual machine with
  – required OS, compiler, libraries, and application code
  – Freeze them as a unit ... ready to run
• Customers get a complete working package
• Virtual appliances: “shrink-wrapped” virtual machines
• Amazon’s EC2 cloud offers many pre-packaged virtual appliances examples of *Software as a service*

• *Question:* do we really have to include a whole kernel in a shrink wrapped VM?
CS370 Operating Systems
Colorado State University
Yashwant K Malaiya
Spring 2022

Containers

Slides based on
• Various sources
Linux Containers and Docker

- Linux containers (LXC 2008) are “lightweight” VMs
- Comparison between LXC/docker (2013) and VM

Containers provide “OS-level Virtualization” vs “hardware level”.
- Containers can be deployed in seconds.
- Very little overhead during execution, even better than Type 1 VMM.
### VMs vs Containers

<table>
<thead>
<tr>
<th>VMs</th>
<th>Containers (&quot;virtual environment&quot;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heavyweight</td>
<td>Lightweight tens of MB</td>
</tr>
<tr>
<td>Limited performance</td>
<td>Native performance</td>
</tr>
<tr>
<td>Each VM runs in its own OS</td>
<td>All containers share the host OS</td>
</tr>
<tr>
<td><strong>Hardware-level virtualization</strong></td>
<td><strong>OS virtualization</strong></td>
</tr>
<tr>
<td>Startup time in minutes</td>
<td>Startup time in milliseconds</td>
</tr>
<tr>
<td>Allocates required memory</td>
<td>Requires less memory space</td>
</tr>
<tr>
<td>Fully isolated and hence more secure</td>
<td>Process-level isolation, possibly less secure</td>
</tr>
</tbody>
</table>
Linux kernel provides

• “control groups” (cgroups) functionality for a set of processes
  – allows allocation and prioritization of resources (CPU, memory, block I/O, network, etc.) without the need for starting any VM

• “namespace isolation” functionality
  – allows complete isolation of an applications' view of the operating environment including Process trees, networking, user IDs and mounted file systems.

• Managed by
  – Docker (or competitors): build, share, run containerized apps.
  – Kubernetes (or competitors): orchestration platform for managing, automating, and scaling containerized applications
What is a container?

- Standardized packaging for software and dependencies
- Isolate apps from each other
- Share the same OS kernel
- Works for all major Linux distributions
- Docker Desktop for Windows uses Windows-native Hyper-V virtualization (Win10)
- Containers native to Windows Server 2016
- Docker: a popular container management service technology.

Alternatives: Podman etc
Some Docker vocabulary

- **Docker Image**
  - The basis of a Docker container. Represents a full application

- **Docker Container**
  - The standard unit in which the application service resides and executes

- **Docker Engine**
  - Creates, ships and runs Docker containers deployable on a physical or virtual, host locally, in a datacenter or cloud service provider

- **Registry Service (Docker Hub(Public) or Docker Trusted Registry(Private))**
  - Cloud or server based storage and distribution service for images (can be **pulled** or **pushed**)

- **Dockerfile** is a text document that contains all the commands a user could call on the command line to assemble an image using **docker build** command.

Correspondence: executable:image  container:process
Containers have their own jargon. Here are some analogous terms. Note that some analogies can be questionable.

<table>
<thead>
<tr>
<th>Docker</th>
<th>Non-containerized code</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is executed</td>
<td>Docker Image</td>
</tr>
<tr>
<td>Isolation unit</td>
<td>Docker Container</td>
</tr>
<tr>
<td>to create what is executed</td>
<td>Dockerfile</td>
</tr>
<tr>
<td></td>
<td>Docker engine</td>
</tr>
<tr>
<td></td>
<td>Registry Service</td>
</tr>
</tbody>
</table>

- Only a high-level look here. For details see documentation and videos.
- Help Session this Wed 5:30 PM.
- Several interrelated technologies. Significant experience needed to gain expertise.
Some Docker vocabulary

- **Dockerfile** is a text document that contains all the commands a user could call on the command line to assemble an image using `docker build` command.
- Ex:

```
# syntax=docker/dockerfile:1
FROM ubuntu:18.04
COPY . /app
RUN make /app
CMD python /app/app.py
```

Each instruction creates one layer:
- FROM creates a layer from the ubuntu:18.04 Docker image.
- COPY adds files from your Docker client’s current directory.
- RUN builds your application with make.
- CMD specifies what command to run within the container.
Docker Volumes

- Volumes mount a directory on the host into the container at a specific location

- Can be used to share (and persist) data between containers
  - Directory persists after the container is deleted
    - Unless you explicitly delete it

- Can be created in a Dockerfile or via CLI
Docker Compose: Multi Container Applications

- Build and run one container at a time
- Manually connect containers together
- Must be careful with dependencies and start up order

- Define multi container app in compose.yml file
- Single command to deploy entire app
- Handles container dependencies
- Works with Docker Swarm, Networking, Volumes, Universal Control Plane
version: '2' # specify docker-compose version

# Define the services/containers to be run
services:
  angular: # name of the first service
    build: client # specify the directory of the Dockerfile
    ports:
      - "4200:4200" # specify port forwarding
  express: # name of the second service
    build: api # specify the directory of the Dockerfile
    ports:
      - "3977:3977" # specify ports forwarding
  database: # name of the third service
    image: mongo # specify image to build container from
    ports:
      - "27017:27017" # specify port forwarding

compose.yml
images
ports
volumes
links
• **Docker** technology used for containers and can deploy single, containerized applications.
• **Docker Compose** for configuring and starting multiple Docker containers on the same host.
• **Docker swarm** is a container orchestration tool that allows you to run and connect containers on multiple hosts.
• **Kubernetes** is a container orchestration tool that is similar to Docker swarm, but has ease of automation and ability to handle higher demand.
Some Docker Commands

- `docker --version` get the currently installed version of docker
- `docker build <path to docker file>` build an image from a specified docker file
- `docker login` login to the docker hub repository
- `docker pull <image name>` pull images from the docker repository hub.docker.com
- `docker push <username/image name>`
- `docker run -it -d <image name>` create a container from an image
- `docker stop <container id>` stops a running container
- `docker kill <container id>` kills the container by stopping its execution immediately
- `docker rm <container id>` delete a stopped container
- `docker exec -it <container id> bash` to access the running container
- `docker commit <conatainer id> <username/imagemename>` creates a new image of an edited container
- `docker images` lists all the locally stored docker images
Unique features

• Containers run in the user space
• Each container has its own: process space, network interface, booting mechanism with configuration
• Share kernel with the host
• Can be packaged as Docker images to provide microservices.
Monolithic architecture vs microservices
Microservices Accessing the Shared Database

Each container is full self-sufficient except that it uses a subset of the shared DB. A single DB subset can be accessed only by a dedicated container.
Microservices Characteristics

- Many smaller (fine grained), clearly scoped services
  - Single Responsibility Principle
  - Independently Managed
- Clear ownership for each service
  - Typically need/adopt the “DevOps” model
- 100s of MicroServices
  - Need a Service Metadata Registry (Discovery Service)
- May be replicated as needed
- A microservice can be updated without interruption
Microservices. Scalability

A monolithic application puts all its functionality into a single process...

... and scales by replicating the monolith on multiple servers

A microservices architecture puts each element of functionality into a separate service...

... and scales by distributing these services across servers, replicating as needed.
Back from VMs & Containers

• We need to do a context switch back here.
Virtual Memory

Slides based on
- Text by Silberschatz, Galvin, Gagne
- Various sources
Page Replacement Algorithms

• **Page-replacement algorithm**
  – Which frames to replace
  – Want lowest page-fault rate

• **Evaluate algorithm** by running it on a particular string of memory references (reference string) and computing the number of page faults on that string
  – String is just page numbers, not full addresses
  – Repeated access to the same page does not cause a page fault
  – Results depend on number of frames available

• In all our examples, we use 3 frames, and the **reference string** of referenced page numbers is

\[ 7,0,1,2,0,3,0,4,2,3,0,3,2,1,2,0,1,7,0,1 \]
Graph of Page Faults Versus The Number of Frames

What we would generally expect
Page Replacement Algorithms

Algorithms

• FIFO
• “Optimal”
• The Least Recently Used (LRU)
  – Exact Implementations
    • Time of use field, Stack
  – Approximate implementations
    • Reference bit
    • Reference bit with shift register
    • Second chance: clock
    • Enhanced second chance: dirty or not?

• Other
FIFO page replacement algorithm: Out with the old; in with the new

• When a page must be replaced
  – Replace the oldest one

• OS maintains list of all pages currently in memory
  – Page at head of the list: Oldest one
  – Page at the tail: Recent arrival

• During a page fault
  – Page at the head is removed
  – New page added to the tail
First-In-First-Out (FIFO) Algorithm

• Reference string:
  7,0,1,2,0,3,0,4,2,3,0,3,2,1,2,0,1,7,0,1

• 3 frames (3 pages can be in memory at a time per process)

• 15 page faults (out of 20 accesses)

• Sometimes a page is needed soon after replacement 7,0,1,2,0,3 (0 out),0, ..
Belady’s Anomaly

• Consider Page reference string 1,2,3,4,1,2,5,1,2,3,4,5
  – 3 frames, 9 faults, 4 frames 10 faults! Try yourself.
  – Sometimes adding more frames can cause more page faults!

  • Belady’s Anomaly

Budapest, 1928

Lazlo Belady was here at CSU. Guest in my CS530!
**“Optimal” Algorithm**

- Replace page that will not be used for longest period of time

- 4\textsuperscript{th} access: replace 7 because we will not use if got the longest time...
- 9 page replacements is optimal for the example

- But how do we know the future pages needed?
  - Can’t read the future in reality.

- Used for *measuring* how well an algorithm performs.
Least Recently Used (LRU) Algorithm

- Use past knowledge rather than future
- Replace page that has not been used in the most amount of time (4th access – page 7 is least recently used ...)
- Associate time of last use with each page

Reference string:

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Page frames:

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>7</td>
<td>7</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>7</td>
</tr>
</tbody>
</table>

12 faults – better than FIFO (15) but worse than OPT (9)
Generally good algorithm and frequently used
But how to implement it by tracking the page usage?

LRU and OPT are cases of stack algorithms that don’t have Belady’s Anomaly
Least Recently Used (LRU) Algorithm

LRU page number is marked (*). Unmarked if that page is accessed.

LRU applied to cache memory.
Least Recently Used (LRU) Algorithm

* Use past knowledge rather than future

• 12 faults – better than FIFO (15) but worse than OPT (9)

• Tracking the page usage. One approach: mark least recently used page each time.

| 7 | 0 | 1 | 2 | 0 | 3 | 0 | 4 | 2 | 3 | 0 | 3 | 2 | 1 | 2 | 0 | 1 | 7 | 0 | 1 |
| 7 | 7* | 7* | 2 | 2 | 2* | 2* | 4 | 4 | 4* | 0 | 0 | 0* | 1 |
| 0 | 0 | 0* | 0 | 0 | 0 | 0* | 3 | 3 | 3 | 3 | 3 |
| 1 | 1 | 1* | 3 | 3 | 3* | 2 | 2 | 2 | 2* | 2 | 2 |

• Other approach: use stack for tracking (soon)