

docker

by Paul Newman

Submission date: 11-May-2026 02:30PM (UTC+0100)

Submission ID: 283078019

File name: 11910_Paul_Newman_docker_726729_1149192290.docx (805.98K)

Word count: 6720

Character count: 43253

Paul Newman 1805454



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Cloud Engineering Principles and Practice

ACCA7027

M. Dacey

Paul Newman 1805454

Paul Newman 1805454

Contents

Cloud Engineering Principles and Practice	1
Table of Figures	3
Cloud Computing	4
Advantages	5
Disadvantages.....	10
Scalability.....	12
Node.JS	13
Docker: Revolutionizing Containerization Technology.....	14
Containers.....	15
Web applications	17
Virtual machines.....	18
Virtual Infrastructure.....	19
Virtual Machine Components	20
Docker Assignment practical.....	21
Bibliography	24

Table of Figures

Figure 1 Cloud Computing at its most simple [5].....	5
Figure 2 Docker Containers [16].....	14
Figure 3 Containerized Applications [16].....	16
Figure 4 How Virtual Machines work within Docker [16].....	18
Figure 5 Web page hosted in web browser.....	22
Figure 6 Docker image build process	22
Figure 7 Docker commands (clear, simple)	22
Figure 8 Docker Desktop Containers tab.....	22
Figure 9 Docker image details view.....	23

Cloud Computing

Cloud computing is the delivery of services—such as servers, storage, databases, networking, software, and analytics—over the internet ('the cloud') to enable faster innovation, flexible resources, and cost-efficiency. The concept evolved from 1960s time-sharing systems, championed by pioneers like John McCarthy and J.C.R. Licklider. Cloud models let users access resources on-demand without owning physical infrastructure, enhancing scalability, mobility, and efficiency. Core service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—enable virtualized services, application development, and cloud-hosted software with minimal local setup. Cloud computing underpins digital transformation across industries due to its flexibility, reliability, and on-demand access [1] [2].

In the 1960s, when punched cards, batch processing, and mainframes dominated computing, J.C.R. Licklider emerged as a visionary leader. He shaped modern computing through his work at ARPA and BBN, a pioneering R&D corporation. At a time of centralized, hardware-limited systems, Licklider promoted interactive, networked computing—envisioning seamless communication and resource sharing. His groundbreaking ideas laid the foundation for the internet and ultimately, cloud computing [3] [4].

Cloud computing is a modern model that uses the internet and centralized servers to manage data and applications, eliminating the need for local storage and extensive hardware. It allows individuals and businesses to access software and files remotely, boosting convenience and flexibility. The system leverages virtualized resources—computing, storage, and networking—delivered via APIs and distributed across global data centres for availability and scalability.

Organizations can deploy applications using infrastructure hosted internally, externally, or in hybrid models. This centralized approach enhances performance, enables pay-as-you-go pricing, and reduces upfront costs—beneficial for both startups and enterprises. Services, accessed over IP networks, include IaaS, PaaS, and SaaS. Cloud computing supports AI, analytics, cybersecurity, and collaboration across industries like healthcare and finance. It improves disaster recovery, strengthens security, and boosts agility. As it evolves, it remains a vital enabler of scalable, reliable, and cost-effective digital transformation [5].

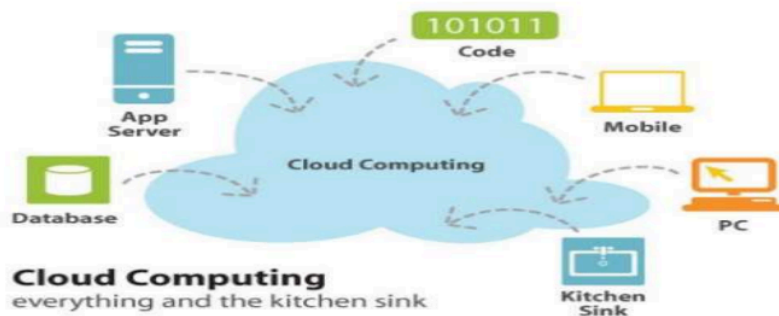


Figure 1 Cloud Computing at its most simple [5]

Advantages

- **Reduced Cost: Maximizing Budget Efficiency**

Cloud computing provides many advantages: lower operational costs through pay-as-you-go models, scalable and secure storage, and automation that reduces IT maintenance workloads. It enables flexibility by dynamically scaling resources, supports mobility via remote access, and enhances collaboration through real-time tools. By shifting IT focus from maintenance to innovation, cloud services promote agility and growth. Cloud platforms offer global availability, compliance support, disaster recovery, and elastic scalability. Deployment models—public, private, hybrid, and community—offer varying levels of control, cost, and security. Public clouds provide affordability and speed, private clouds offer enhanced control, and hybrid models combine both for adaptable solutions [6].

- **Enhanced Storage: Expanding Capacity Beyond Limits**

A key advantage of cloud computing is its vast, scalable data storage capacity—surpassing that of personal computers or on-premises servers. Traditional storage is limited, expensive, and vulnerable to hardware failures. In contrast, cloud storage offers near-unlimited scalability, with data distributed across multiple data centres to ensure availability, security, and disaster recovery. Providers manage infrastructure, updates, backups, and maintenance, removing the need for in-house IT. Cloud storage supports remote access for improved collaboration and device integration. Businesses can choose from object, block, or file storage based on specific needs. Overall, it enhances efficiency, reduces costs, and improves data protection—making it a modern, adaptable solution [7].

- **High Automation: Reducing Manual Effort and Enhancing Efficiency**

Cloud computing provides a high level of automation, reducing IT workloads by eliminating manual tasks such as software updates, security patching, and hardware maintenance. Service providers handle these automatically, keeping systems secure, up to date, and optimized without intervention. Cloud platforms also offer automated backups and disaster recovery, safeguarding data against failures and attacks.

Auto-scaling adjusts resources based on demand, eliminating manual provisioning during spikes or lulls. This automation improves efficiency, reliability, and cost-effectiveness. By freeing IT teams from routine tasks, cloud automation enables greater focus on innovation, making it a key driver of productivity and growth in modern enterprises [2].

- **Flexibility: Adapting to Changing Business Needs with Ease**

Cloud computing offers unmatched flexibility, enabling businesses to adapt quickly to changing demands—unlike traditional systems reliant on fixed hardware and long procurement cycles. Organizations can instantly scale resources to meet fluctuating workloads and seasonal spikes without major infrastructure costs. A key benefit is remote, multi-device access, supporting global collaboration, remote work, and hybrid models. Cloud platforms offer customizable deployment options—public, private, or hybrid—based on operational and security needs, and integrate smoothly with various tools. With on-demand computing, storage, and applications, the cloud helps businesses stay agile, efficient, and innovative. From startups to enterprises, it ensures IT resources align with evolving goals and turn technology into a strategic asset [3] [5].

- **Greater Mobility: Empowering a Workforce Without Boundaries**

Cloud computing enhances mobility by allowing employees to access essential data, applications, and resources from anywhere using internet-connected devices like laptops, smartphones, and tablets—removing the limitations of traditional office setups. This supports remote work, flexible schedules, and global collaboration without compromising productivity.

Tools like Google Workspace, Microsoft 365, and cloud-based project platforms enable real-time communication and file sharing across distributed teams. Security measures such as multi-factor authentication (MFA), encryption, and VPNs protect remote access from cyber threats. Cloud services also sync files across devices, ensuring users always have the latest versions. Enhanced mobility boosts productivity, work-life balance, and talent access—offering a competitive edge in today's global market [8] [2].

- **Enabling IT to Focus on Innovation: Shifting Priorities from Maintenance to Progress**

Cloud computing enables IT departments—especially in government and large enterprises—to shift focus from routine maintenance to innovation and strategy. Traditionally, teams managed on-premises servers, updates, and hardware issues, limiting progress on new initiatives.

Cloud providers now handle infrastructure, security patches, and monitoring, allowing IT professionals to prioritize digital transformation and service improvement. For government agencies, this supports public service modernization, AI adoption, and enhanced cybersecurity—without outdated system constraints. Cloud computing also boosts agility, enabling rapid app deployment, data analysis, and emerging tech adoption. Its scalability allows quick adaptation to policy changes and security needs. By reducing infrastructure demands, the cloud helps organizations optimize resources and drive progress.

- **On-Demand Self-Service: Empowering Users with Instant Access to Cloud Resources**

Cloud computing provides on-demand self-service, allowing users to access and manage resources like storage, computing power, and applications without human interaction. Through a self-service portal or API, businesses can instantly provision, scale, and deploy services based on real-time needs. This eliminates manual resource allocation, increasing flexibility and cost-efficiency—users pay only for what they use.

For example, companies can scale up during peak times and scale down afterward, avoiding excess infrastructure costs. Cloud interfaces offer automated provisioning, monitoring, and management tools. IT teams can automate backups, schedule workloads, and manage security from a centralized

dashboard, reducing overhead. This autonomy removes bottlenecks, accelerates digital transformation, and enhances operational agility for both users and providers [6].

- **Widespread Network Access: Seamless Connectivity Anytime, Anywhere**

A core feature of cloud computing is widespread network access, enabling users to reach data and applications anytime, anywhere, on any internet-connected device. Unlike traditional infrastructure, the cloud ensures uninterrupted, cross-platform access—boosting business continuity, productivity, and collaboration. Providers deliver fast, reliable connectivity through high-speed networks, redundant data centres, and optimized systems. Strong security—encryption, identity management, and MFA—protects access. Cross-platform compatibility supports BYOD environments, allowing seamless use across devices. With universal access and strong security, cloud computing empowers today's mobile, collaborative workforce [3].

- **Geographical Independence: Access Cloud Services from Anywhere in the World**

Cloud computing offers geographical independence, enabling users and organizations to access services, applications, and data from anywhere via the internet. Unlike traditional systems tied to on-premises servers, cloud platforms provide global accessibility—ideal for remote teams, multinational companies, and cross-border collaboration. This eliminates the need for local infrastructure in every region, as providers deliver secure, scalable access across devices. Distributed data centres ensure high availability, redundancy, and disaster recovery, supporting continuity during outages. CDNs and edge computing enhance performance by delivering data from the nearest server, reducing latency. Geographical independence keeps businesses agile, mobile, and globally connected [9] [10].

- **Accessing Applications via SaaS: Seamless Cloud-Based Software Delivery**

Cloud computing enables application access via Software as a Service (SaaS), eliminating the need for local installations, maintenance, or updates. Hosted on remote servers and delivered online, SaaS offers efficiency, scalability, and cost savings across devices and locations. Platforms like Google Workspace, Microsoft 365, Salesforce, and Dropbox support collaboration and operations in various industries.

With a subscription or pay-as-you-go model, SaaS lowers upfront costs and removes licensing burdens. Providers handle updates, security, and performance, ensuring users always access the latest versions without IT support. SaaS apps integrate with other cloud services for workflow automation and productivity. Backed by global data centres, SaaS delivers fast, secure, and flexible software access for businesses and individuals [11].

- **Deploying Applications with PaaS: Simplifying Development and Deployment**

Cloud computing allows developers to deploy applications using Platform as a Service (PaaS), offering a complete development environment without managing hardware, operating systems, or middleware. Developers can focus on building and testing, while the platform handles infrastructure.

PaaS solutions like Google App Engine, Azure App Services, AWS Elastic Beanstalk, and Heroku offer pre-configured environments with tools, APIs, and multi-language support. A major advantage is automatic scalability—applications adjust to traffic demands without manual input. PaaS integrates with DevOps tools, CI/CD pipelines, and technologies like Kubernetes and Docker, streamlining deployment and lifecycle management. Centralized access supports agile workflows, making PaaS a scalable, efficient, and cost-effective platform for cloud-native innovation [6].

- **Renting Computing Resources with IaaS: Scalable and Cost-Effective IT Infrastructure**

Cloud computing allows businesses to rent IT infrastructure—such as processing power, storage, and networking—through Infrastructure as a Service (IaaS). Unlike expensive on-premises setups, IaaS offers a flexible, pay-as-you-go model that lowers costs and improves efficiency. Companies can dynamically scale resources like CPU, RAM, storage, and bandwidth.

Providers such as AWS, Azure, and Google Cloud offer virtual machines, databases, and networking with built-in security, backups, and disaster recovery. IaaS speeds up application deployment and ensures global access without physical server maintenance. It integrates with AI, ML, analytics, and IoT, giving businesses a technological edge. IaaS reduces overhead, streamlines operations, and supports innovation—making it essential for digital transformation and cloud-native growth.

- **Private Cloud: Dedicated and Secure Cloud Infrastructure for Organizations**

A private cloud is a dedicated environment owned or managed by a single organization, offering enhanced security, control, and customization over public cloud options. Hosted on-premises or by a third party, it's not shared with others—making it ideal for sectors like healthcare, finance, and government with strict compliance needs (e.g., HIPAA, GDPR, PCI DSS).

Organizations retain full control over data privacy, encryption, and network security. Private clouds deliver better performance through tailored configurations and dedicated resources. Though costlier upfront, they offer long-term benefits in security, stability, and utilization. Private clouds also integrate with hybrid models, balancing control with public cloud scalability—ideal for businesses requiring compliance, performance, and data sovereignty [2].

- **Community Cloud: A Shared Infrastructure for Organizations with Common Interests**

A community cloud is a shared environment for organizations with common interests, regulatory requirements, or operational goals. Unlike public (open to all) or private (single-tenant) clouds, it provides tailored infrastructure that balances security, collaboration, and cost-efficiency. It's ideal for sectors like healthcare, finance, education, and government, where compliance and data governance are essential.

For example, hospitals and insurers can share a HIPAA-compliant cloud to securely exchange data, while government agencies can standardize IT services across departments. Community clouds enhance security and compliance through aligned policies and allow customized resource allocation. With shared costs and improved scalability, they offer a collaborative, secure, and efficient cloud solution.

- **Public Cloud: Mega-Scale Infrastructure for Universal Access**

A public cloud is a large-scale, shared infrastructure offered on a pay-as-you-go basis by providers like AWS, Azure, Google Cloud, and IBM Cloud. These platforms deliver computing, storage, networking, and applications over the internet to individuals and businesses. Scalability is a key advantage—resources can be rapidly provisioned across global data centres for instant deployment without investing in physical infrastructure. Public clouds are cost-effective, letting organizations pay only for what they use—ideal for startups, small businesses, and enterprises needing fast growth. Security features now include encryption, MFA, AI-driven threat detection, and compliance tools. However, multi-tenancy can raise concerns for sensitive data, making hybrid or private models preferable in such cases. Public cloud services span IaaS, PaaS, and SaaS—offering flexible, scalable solutions for a wide range of needs:

- A.) Infrastructure as a Service (IaaS) – Provides virtualized computing resources, such as servers, storage, and networking.
- B.) Platform as a Service (PaaS) – Offers a development platform with tools and frameworks for building applications.
- C.) Software as a Service (SaaS) – Delivers fully functional software applications over the internet, such as Google Workspace and Microsoft 365.

By leveraging public cloud infrastructure, businesses can innovate faster, reduce costs, and improve operational efficiency while taking advantage of a highly scalable, globally distributed computing environment. This model enables organizations to focus on growth, digital transformation, and customer engagement without worrying about hardware limitations [8].

- **Hybrid Cloud: Combining Multiple Clouds for Flexibility and Efficiency**

A hybrid cloud combines two or more cloud models—public, private, or community—into a unified, flexible infrastructure. This approach lets businesses balance public cloud scalability with private cloud control and security, adapting to diverse workload needs. For example, a financial firm might use a private cloud for sensitive data (e.g., GDPR, PCI DSS compliance) and a public cloud for analytics or customer-facing applications.

Hybrid clouds improve disaster recovery and continuity by enabling workload migration during outages. They also support multi-cloud strategies using multiple providers (e.g., AWS, Azure, GCP), reducing vendor lock-in. Hybrid architectures can integrate edge computing—processing data near devices like IoT sensors—while storing data centrally. Overall, hybrid clouds deliver the agility, resilience, and scalability modern businesses require [3].

Disadvantages

- **Security Risks: Data Leakage and Unauthorized Access in Virtualized Environments**

A major disadvantage of cloud computing—especially in multi-tenant environments—is the risk of data leakage and unauthorized access between virtual machines (VMs) on shared physical servers. Despite encryption and access controls, vulnerabilities persist due to misconfigurations, insecure APIs, or hypervisor flaws. Side-channel attacks can exploit virtualization weaknesses to access another user's data. Cross-tenant breaches are a concern in public and hybrid clouds, where a compromised hypervisor or orchestrator can expose co-hosted data. These risks are especially critical in finance, healthcare, and government, where breaches can cause regulatory and reputational damage. Insider threats from provider staff with elevated access also raise concerns if controls are lacking [7] [8].

- **Risk of Improper Data Handling by Cloud Providers**

A key disadvantage of cloud computing is the risk of providers mishandling sensitive data. When organizations store financial records, customer information, or IP in the cloud, they depend on the provider for security and compliance. Misconfigured access controls and weak protections can lead to data breaches, unauthorized access, or loss. Common issues include exposed storage—like open buckets or unsecured databases—and poor encryption, especially if providers retain the keys. Compliance is another challenge, with industries bound by GDPR, HIPAA, or PCI DSS potentially facing penalties if providers fall short. Weak security or non-compliance can cause financial loss, reputational damage, and legal consequences for clients.

- **Risk of Unauthorized Data Disclosure to Government or Law Enforcement**

A major disadvantage of cloud computing is the risk that providers may release sensitive client data to government or law enforcement agencies without the customer's knowledge. Providers are often legally required to comply with subpoenas or national security laws, raising serious privacy concerns.

The U.S. CLOUD Act, for instance, permits access to data from U.S.-based providers even if stored abroad. Similar laws exist in other countries, potentially overriding privacy protections. A lack of transparency compounds the issue, as providers may be barred from notifying clients. This is especially concerning for sectors like finance, healthcare, and legal services, where confidentiality is crucial. Governments may also cite vague security claims, increasing the risk of data misuse and overreach [10].

- **Challenges in Meeting Compliance and Legal Standards in Cloud Computing**

A key disadvantage of cloud computing is the challenge of meeting compliance and legal standards, especially in regulated industries like finance, healthcare, government, and e-commerce. Ensuring compliance is complex due to data sovereignty, shared responsibility models, and differing international laws. Data residency—where data is stored and governed—is critical, as some countries require sensitive data to remain within national borders. Storing it elsewhere can result in legal risks, fines, or lawsuits.

Cloud providers may host data in jurisdictions that conflict with an organization's legal obligations. Under the shared responsibility model, providers secure infrastructure, but customers must manage access, configure settings, and ensure compliance. Auditability is another hurdle—many regulations require logs and reports, but some providers restrict visibility, complicating compliance verification.

- **System Failures and Downtime: The Risk of Cloud Service Unavailability**

A major disadvantage of cloud computing is the risk of system failures and service outages, which can render services unavailable for extended periods. Unlike on-premises setups, cloud computing relies on third-party providers to manage infrastructure. Technical failures, cyberattacks, or data centre outages can disrupt access to applications, data, and operations. Prolonged downtime may lead to financial loss, reduced productivity, and customer dissatisfaction. Even major providers like AWS, Azure, and Google Cloud have experienced high-profile outages affecting industries such as e-commerce, finance, and healthcare. These incidents highlight the risks of relying solely on external providers for business continuity [5].

- **Security Breaches in Cloud-Based Applications: The Risk of Data Theft and Exposure**

One of the major disadvantages of cloud computing is the risk of cyberattacks targeting cloud-based applications, where hackers breach client apps, steal sensitive data, and distribute it illegally. As businesses increasingly rely on cloud services to store and process confidential information, cybercriminals are constantly developing new attack methods to exploit vulnerabilities in cloud security.

How Hackers Exploit Cloud-Based Applications

- *Phishing attacks – Hacker’s trick users into revealing login credentials, granting unauthorized access to cloud applications.*
- *Weak authentication mechanisms – If cloud apps lack multi-factor authentication (MFA), hackers can easily gain access using compromised passwords.*
- *API vulnerabilities – Poorly secured application programming interfaces (APIs) can allow attackers to manipulate cloud services and extract data.*
- *Malware injection – Attackers embed malicious code in cloud applications to compromise data integrity and gain persistent access.*
- *Misconfigured security settings – Many breaches occur due to human error, such as leaving cloud storage (e.g., AWS S3 buckets) open to public access.*

- **Effectiveness of Cloud Provider Security Measures: A Critical Concern**

One of the key disadvantages of cloud computing is that organizations must rely on the cloud provider’s security measures to protect their data and applications. While top-tier cloud providers invest heavily in cybersecurity, encryption, and compliance certifications, the effectiveness of these security measures varies across providers, and customers often have limited visibility and control over how their data is safeguarded [4].

- **Cloud Compatibility and Vendor Lock-In: The Challenge of Migrating Between Providers**

A key disadvantage of cloud computing is the challenge of migrating applications and data between providers, often leading to vendor lock-in. Organizations rely on proprietary infrastructure, APIs, and services, making transitions complex and costly. This raises concerns about data availability, privacy, and provider trust. While cloud computing offers scalability and convenience, users must guard against potential misuse of sensitive data. Encryption protects data from unauthorized access, but it complicates tasks like searching, indexing, and analysis, possibly affecting performance. This book addresses these challenges and provides strategies to strengthen cloud security, ensure compliance, and maintain data control—helping organizations optimize cloud use while managing risks [3].

Scalability

In today's fast-changing business environment, adaptability is crucial. A key advantage of cloud computing is its ability to dynamically scale resources, allowing businesses to respond to fluctuating workloads without disruption. Whether facing a demand surge or a slowdown, cloud solutions automatically adjust computing power to match real-time needs. This elasticity ensures performance, cost efficiency, and eliminates the need for over-investing in temporary infrastructure. By leveraging cloud scalability, organizations maintain continuity, optimize operations, and stay flexible. Cloud computing's real-time responsiveness makes it vital for businesses aiming to remain agile, resilient, and competitive in an evolving market [3] [2].

- *Data centre streamlining:*
Any business, no matter how big or little, will have invested heavily in its data center. This entails hiring the personnel in charge of keeping the data center running, providing the locations where the hardware is stored, and buying and maintaining the equipment and software.
- *Enhancing corporate processes:* An infrastructure for achieving this is provided by the cloud. Suppliers and partners can share apps and data in the cloud, freeing up all parties to focus on the business process rather than the supporting infrastructure.
- *lowering initial costs:*
For startups, companies in developing markets, and even advanced technology divisions within larger corporations, cloud computing dramatically reduces startup costs. The recently established organization starts with pre-made infrastructure [3].

Not Cloud Computing

Cloud computing and utility computing are distinct. Unlike utility computing, which typically uses a metered service model, cloud computing can operate on dispersed, virtualized platforms without relying on centralized resources or fixed pricing.

While often seen as an alternative to grid computing, cloud computing differs. Grid computing also uses distributed virtual machines but typically focuses on a single, highly complex task—unlike the broader flexibility offered by cloud environments [3] [7].

Some view cloud computing as a form of client/server computing, with the cloud acting as the server. However, unlike traditional client-server models—where the server is a specific machine at a fixed location—cloud computing uses virtualized platforms that may be distributed across many machines, often hidden from the user. Users understand they need to access, process, and store resources to generate results, but the underlying infrastructure remains abstracted and location-independent in a cloud environment [3].

Software as a Service, or SaaS, is software that companies can purchase, administer, and use to operate on their own or third-party hardware. Cloud computing is not SaaS.

Virtualization is not clouding computing either, despite the fact that it can be used to accomplish cloud computing. Operating system virtualization can be used in a data centre or on the personal computers of an enterprise, not using the cloud. Virtualization can, however, be used with cloud computing resources [3] [5].

Service-oriented architecture (SOA) and cloud computing are distinct concepts, despite both facilitating data exchange and interaction between applications used in business processes. While SOA focuses on structuring software applications to communicate and share services efficiently, cloud computing revolves around delivering computing resources over the internet. Ultimately, although the principles discussed may not be directly linked to cloud computing, their relevance depends on how they are implemented. In certain scenarios, SOA and cloud computing can complement each other, enhancing scalability, integration, and operational efficiency within an organization's IT infrastructure [3] [4].

Node.JS

Node.js is an open-source, cross-platform runtime environment for building server-side web applications using JavaScript. It supports multiple operating systems and is optimized for scalability and throughput, making it ideal for real-time applications. With its event-driven, non-blocking I/O architecture, Node.js enables asynchronous task execution, improving performance. Unlike traditional stateless web frameworks that required extra effort for session management, Node.js supports two-way, real-time communication between client and server, streamlining data exchange and enhancing user experience in dynamic applications [12] [13].

Traditionally, applications were built on stateless request-response frameworks, requiring developers to manually manage session continuity and maintain data consistency. This added complexity to web development. Node.js changed that by enabling real-time, bidirectional communication. Both client and server can now actively exchange data while preserving application state, creating a more interactive and seamless user experience [12].

Node.js is used by many large companies. A brief list of a few of them is as follows:

- **PayPal:** Several platforms within PayPal have started transitioning to Node.js for their development.
- **LinkedIn:** The mobile servers that support LinkedIn's iPhone, Android, and mobile web applications operate using Node.js.
- **Mozilla:** Mozilla has implemented Node.js to support its browser APIs, with the platform reaching 500 million installations.
- **eBay:** eBay utilizes Node.js to power and manage its HTTP API service, ensuring efficient handling of high-traffic requests and seamless performance [12].

Node.js is a versatile platform ideal for building real-time web services, APIs, and lightweight microservices. However, it's less suited for CPU-intensive tasks due to its single-threaded, event-driven architecture, which can block the event loop and reduce responsiveness. When handling resource-heavy computations, the event loop may become unresponsive, delaying additional requests. To avoid this, such tasks should be offloaded to separate services or worker threads. Node.js excels in I/O-bound scenarios like data streaming and real-time communication, where heavy computation is minimal or managed externally [12].

Docker: Revolutionizing Containerization Technology

Docker Inc. was founded in 2010 by Solomon Hykes as dotCloud Inc., aiming to simplify Linux container usage. The team developed tools leveraging Linux kernel features like cgroups and namespaces to improve containerization. Originally a PaaS provider, dotCloud later pivoted to focus solely on containers. Its tooling was open-sourced, forming the foundation of Docker. Eventually, Docker Inc. sold dotCloud to Cloud Control, which later went bankrupt—cementing Docker's commitment to container technology [14].

Docker is a containerization platform that enables OS-level virtualization, unlike traditional hypervisors that emulate entire operating systems. Docker runs multiple isolated applications on a single physical or virtual machine using Linux kernel features like cgroups, namespaces, and OverlayFS. OverlayFS merges directories into a unified view, allowing multiple independent applications to run efficiently within one system. This approach enhances portability, scalability, and resource efficiency, making Docker ideal for modern app deployment and cloud computing [15].

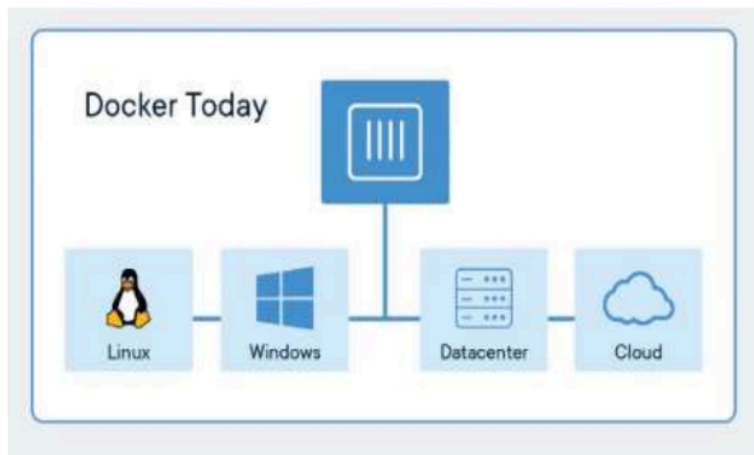


Figure 2 Docker Containers [16]

Containers

While containerization has surged in popularity recently, the concept dates back to the 1970s. It allows multiple applications to run in isolated environments on the same physical or virtual machine, improving resource efficiency, scalability, and security through strict workload separation. The technology has since evolved into modern orchestration systems like Kubernetes, which enhance automation, deployment flexibility, and cloud-native development across industries [17].

1979: In 1979, UNIX Version 7 introduced the chroot system call, which modified the visible root directory for a process and its children. This restricted access to files outside the defined directory tree, isolating processes within a chroot environment. Known as a chroot jail, this early form of process isolation laid the foundation for today's containerization and sandboxing technology [15].

2000: FreeBSD improved on the chroot concept with jails, which allow a system to be partitioned into multiple isolated environments. Each jail functions as a virtual instance with its own file system, processes, and user accounts, offering stronger isolation than chroot by restricting access to network interfaces and assigned IPs.

This deep isolation enables users to test and run internet-connected software safely, ensuring any changes or vulnerabilities stay contained. FreeBSD jails became a valuable tool for secure development and deployment, significantly influencing the evolution of containerization and system-level virtualization in modern computing [15].

2006: OpenVZ gained popularity among low-end VPS providers by enabling multiple isolated OS instances on a single physical server. It creates lightweight containers that share a patched Linux kernel while maintaining virtualized resources like files, user accounts, processes, and network devices.

Each container operates independently with isolated workloads, ensuring separation despite shared infrastructure. By leveraging a shared kernel, OpenVZ delivers strong performance, efficiency, and scalability—making it a cost-effective solution for VPS hosting and container-based virtualization [15].

2006: Introduced in 2006 by Google engineers, control groups (cgroups)—originally called process containers—were developed to manage and isolate system resources for groups of processes. This Linux kernel feature lets administrators control CPU, memory, disk I/O, and network usage, preventing processes from affecting each other's performance.

Cgroups have since evolved through several redesigns, adding advanced functionality and broader support. Today, they are a core component of containerization and resource management, underpinning technologies like Docker, Kubernetes, and other cloud-native platforms [15].

2008: LXC (Linux Containers) combines control groups (cgroups) and isolated namespaces to enable OS-level virtualization, allowing applications to run in self-contained environments with dedicated resources. This ensures strong isolation while sharing the Linux kernel for optimal performance. Docker initially used LXC as its container runtime but later developed its own to improve flexibility, scalability, and security in modern deployments [15].

Difference Between Containers and Virtual Machines

Containers are often mistaken for virtual machines (VMs) due to their isolation capabilities, but they differ fundamentally. Unlike VMs, which run full operating systems, containers share the host machine's kernel. This makes containers far more lightweight, efficient, and faster to deploy. They use fewer resources, start almost instantly, and offer excellent scalability—ideal for modern cloud-native applications and microservices architectures [18].

All containers run on the same host system, with Docker isolating a single process or group of processes based on the container image. Unlike virtual machines, which each require a separate OS instance, containers use kernel-level isolation, allowing multiple applications to share the host OS efficiently.

Without a full OS, containers consume fewer resources, start nearly instantly, and introduce minimal overhead. When launched, the designated processes run directly on the host system, eliminating the need for hardware-level virtualization or emulation [19].

This approach boosts performance, scalability, and portability, making containers ideal for microservices, cloud-native applications, and DevOps workflows. Organizations can deploy, update, and manage applications rapidly without the overhead of full virtualized environments. Containerized apps scale easily, use resources efficiently, and move seamlessly across development, testing, and production—supporting faster, more consistent software delivery [15].

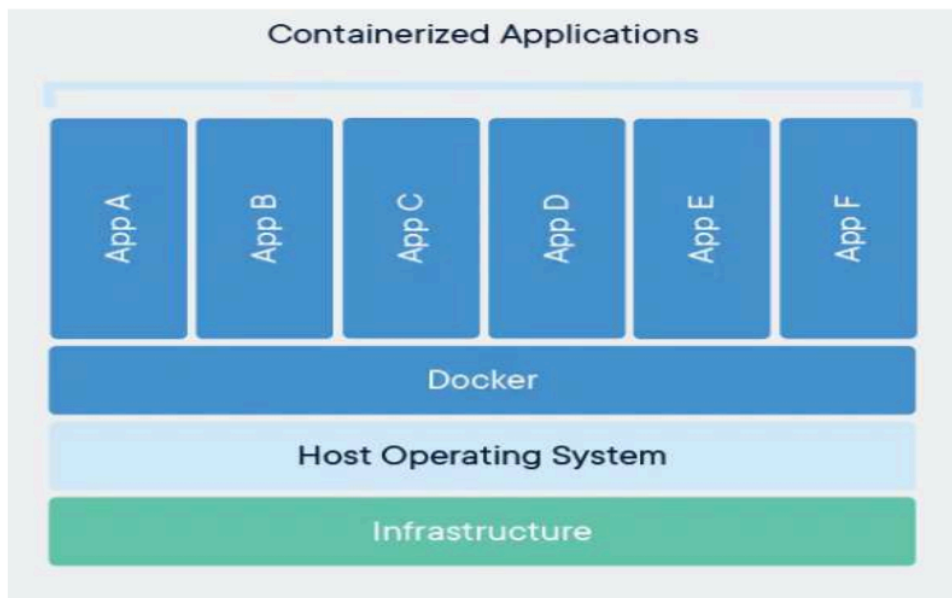


Figure 3 Containerized Applications [16]

Web applications

Virtualisation: The Foundation of Cloud Computing Efficiency

Server virtualization was initially adopted to reduce costs by maximizing hardware use. Over time, it evolved into a foundational technology that offers more than financial benefits. Today, virtualization enhances scalability, flexibility, and operational agility, and plays a critical role in enabling modern cloud computing [20].

Virtualization allows businesses to optimize computing resources dynamically, running workloads efficiently without constant hardware expansion. By abstracting physical infrastructure, multiple VMs or containers can run independently on the same system—minimizing downtime, enhancing disaster recovery, and improving security.

As the foundation of cloud computing, virtualization enables providers to deliver on-demand computing, storage, and networking services globally. For organizations, it offers greater resource control, improved workload balancing, seamless scalability, faster deployment, better performance, and reduced costs [21].

Below are some of the key advantages of virtualization in cloud computing, underscoring its essential role in modern IT infrastructure and driving digital transformation:

- Usage-based billing (utility pricing), allowing organizations to pay only for the computing resources they consume, rather than investing in fixed hardware capacity.
- Accelerated provisioning of virtual servers, reducing setup time and enabling swift environment replication for development, testing, or production.
- Facilitates economies of scale by consolidating workloads on shared infrastructure, optimizing resource utilization, and reducing per-unit computing costs.
- Abstracts physical server locations from end users, enabling resource access through logical environments without dependency on underlying infrastructure geography.
- Guided by Service-Level Agreements (SLAs) to define performance benchmarks, availability guarantees, and resource allocation standards within virtualized environments.
- Enables integration of alternative resource sources—such as hybrid clouds, edge computing, or third-party providers—for enhanced redundancy and flexibility.
- Enables seamless application portability across servers and data centres, supporting workload migration, load balancing, and high availability in distributed environments [3].

Virtualization offers customers flexibility and choice, while providers benefit from its efficiency, scalability, and cost savings. Many organizations start with hybrid cloud models, later moving to full virtualization as they align cloud capabilities with business needs. Adoption grows with experience, driven by virtualization's ability to scale resources dynamically. Organizations can reduce servers during low demand and rapidly provision them during peak times, supporting both expected and sudden usage spikes. Advances in autonomous computing and integrated change management add further value, accelerating development and reducing time-to-market. Virtualization also powers utility computing, allowing virtual machines to run on provider infrastructure as if on local hardware—ideal for efficiently handling fluctuating workloads [3].

Virtual machines

A virtual machine (VM) is a software-based emulation of a physical computer, running its own operating system and applications. It uses the physical resources of a host system and includes specification and configuration files that define its operation. Each VM contains virtualized components—CPUs, memory, storage, and network interfaces—that replicate physical hardware functionality while enhancing manageability, portability, and security [22].

Before you start creating and managing virtual machines, it's beneficial to have a foundational understanding of key concepts such as the virtual machine lifecycle, core components, and the use of VMware Tools.

This knowledge will help ensure efficient deployment, configuration, and maintenance of virtual environments.

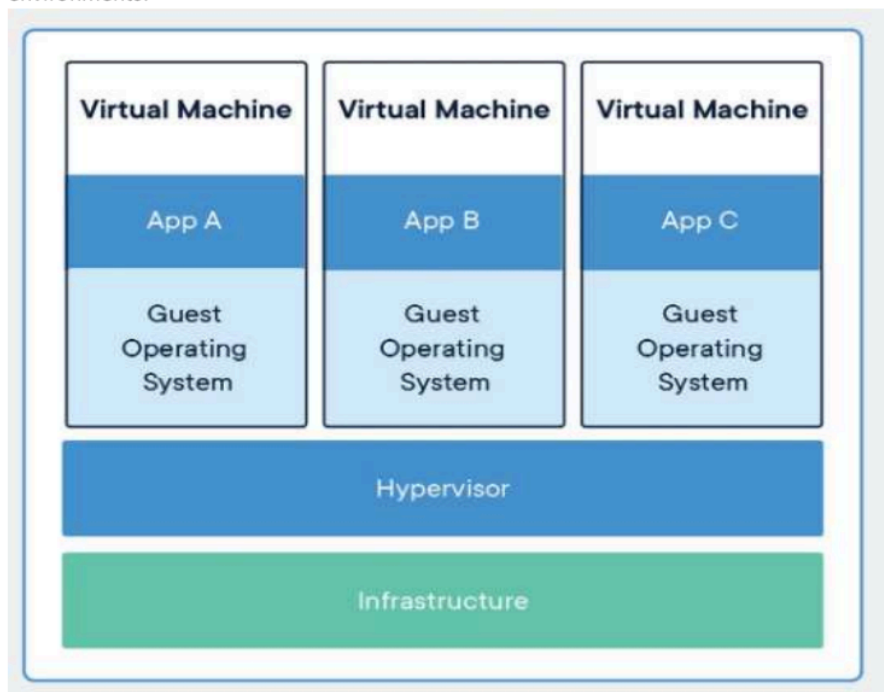


Figure 4 How Virtual Machines work within Docker [16]

A virtual machine consists of several key files stored on a storage device, each serving a specific function. These include the configuration file, which defines hardware settings; the virtual disk file, containing the operating system and data; the NVRAM file for BIOS/UEFI settings; and log files for tracking activity and troubleshooting [23].

Virtual Infrastructure

Virtual machine infrastructure typically includes two core software layers: virtualization and management. In VMware vSphere, the ESXi hypervisor delivers the virtualization layer by abstracting host hardware into standardized resources—CPU, memory, storage, and networking—shared efficiently across multiple virtual machines [23].

The management layer is provided by vCenter Server, which centrally manages ESXi hosts and the virtual machines running on them. It enables administrators to deploy, monitor, and manage virtual environments at scale, offering features like high availability, resource allocation, and automated workload balancing.

vCenter Server centralizes and pools resources across multiple hosts, allowing automation of routine tasks, VM provisioning and cloning, dynamic resource allocation, performance monitoring, and template creation. This centralized control greatly enhances scalability, efficiency, and management across virtualized environments [24].

There are several flexible options for deploying virtual machines. You can create a new VM from scratch by manually installing the guest OS and VMware Tools or clone an existing VM and convert it into a template for rapid, standardized deployment. VMs can also be deployed using OVF or OVA templates, which simplify distribution of pre-configured environments across platforms [23].

Virtual Machine Components

Virtual machines typically consist of a guest operating system, VMware Tools, virtualized resources (such as CPU, memory, storage, and networking), and virtual hardware components. These elements function and are managed similarly to those in a physical computer, allowing administrators to configure, monitor, and maintain VMs using familiar tools and processes.

- **Operating System**

Installing a guest operating system on a virtual machine is similar to doing so on a physical computer. You'll need an installation source—typically a CD/DVD-ROM or ISO image—containing the OS files. The virtual machine boots from this media to begin installation, just like a physical machine [23].

- **VMware Tools**

VMware Tools is a utility suite that enhances guest OS performance and improves virtual machine management. It includes drivers and components for better graphics, seamless mouse control, time sync, and optimized network and disk operations. With VMware Tools, administrators gain greater control and access to features like shared folders, clipboard sharing, and automatic guest OS shutdown, improving overall VM usability and integration [23].

- **Compatibility Setting**

In the vSphere Client, compatibility settings align each virtual machine with a specific ESXi host version, cluster, or data centre. This defines the VM's virtual hardware version, which determines available features and the range of compatible ESXi hosts. Ensuring compatibility maintains stability, supports features, and prevents issues during VM migration or power-on across environments [23] [25].

- **Hardware Devices**

Each virtual hardware component in a VM replicates its physical counterpart, with dedicated virtual resources like CPU, memory, and disk. CPU virtualization maximizes performance by executing instructions directly on the physical processor when possible, reducing overhead. The virtualization layer intervenes only when necessary, enabling most operations to run natively. This ensures virtual machines perform similarly to physical systems while maintaining isolation and efficient resource sharing [23].

Modern operating systems support virtual memory, letting applications use more memory than physically available. Likewise, the ESXi hypervisor supports memory overcommitment, allowing total VM memory allocations to exceed the host's physical RAM. This is accomplished using techniques like ballooning, compression, and swapping—enabling higher VM density and more efficient resource utilization, while maintaining acceptable performance[23]

Docker Assignment practical

These steps demonstrate Docker portability, volume use, image publishing, and networking by Paul S. Newman.

```
docker network create paul-net
docker run -d --name web1 --network paul-net nginx:alpine
docker run -it --rm --network paul-net busybox ping web1
```

Task Four: Docker Networking

```
docker volume create paul-vol
docker run -d -p 8081:80 --name vol-web -v paul-vol:/usr/share/nginx/html nginx:alpine
docker cp index.html vol-web:/usr/share/nginx/html/index.html
```

Task Three: Docker Volume Example

```
docker login
docker tag paul-html-app paulnewman123/paul-html-app
docker push paulnewman123/paul-html-app
```

Task Two: Publishing the Image

Visit <http://localhost:8080> to view the result.

```
docker build -t paul-html-app .
docker run -d -p 8080:80 --name webserver paul-html-app
```

Build & Run:

```
<!DOCTYPE html>
<html>
<head><title>Docker Web</title></head>
<body>
<h1>Hello from Docker!</h1>
<p>This was built by Paul S. Newman for the Cloud Engineering assignment.</p>
</body>
</html>
```

index.html:

```
FROM nginx:alpine
COPY index.html /usr/share/nginx/html/index.html
EXPOSE 80
```

Docker file:

This example shows how Paul S. Newman used Docker to serve a static HTML page using Nginx. The goal is to run this app anywhere without configuration hassles.

Task One: Portability

Task one:

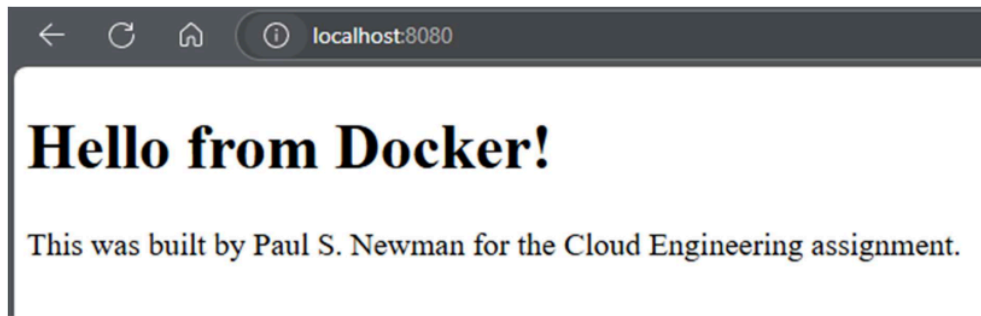


Figure 5 Web page hosted in web browser

```
PS C:\Users\paul_\OneDrive\Desktop\Cloud Engineering Principles and Practice\Docker> docker build -t paul-htal-app .
[*] Building 6.3s (8/8) FINISHED
=> [internal] load build definition from Dockerfile
=> transferring dockerfile: 11kB
=> [internal] load metadata for docker.io/library/nginx:alpine
[auth] library/nginx:pull token for registry-1.docker.io
=> [internal] load .dockerignore
=> transferring context: 2B
=> [internal] load build context
=> transferring context: 230B
[1/2] FROM docker.io/library/nginx:alpine@sha256:65645c7bb6a0661892a8b03b89d0743208a18dd2f3f17a54efub76fb8e2f2a10
=> resolve docker.io/library/nginx:alpine@sha256:65645c7bb6a0661892a8b03b89d0743208a18dd2f3f17a54efub76fb8e2f2a10
=> sha256:34c64644b756511a2e217f0508e11d1a572085d6cd6dc9a555a082ad49a3102 1.40kB / 1.40kB
=> sha256:39c2ddfd6010082a4a646e7c444e95aca9b3faebc00f17f7ccc2954004f2a7d 15.52MB / 15.52MB
=> sha256:197eb75867ef4fcedd4724f17b0972ab0489436860a594a9445f8eaff8155053 1.21kB / 1.21kB
=> sha256:81bd8ed7ec6789b0cb7f1b47ee731c522f6dba83201ec73cd6bca1350f582948 402B / 402B
=> sha256:d7e5f07248863957ebb0b5a44a5729963c3462666baa2947d00628cb5f2d5773 955B / 955B
=> sha256:b464cfd2a6319875aeb27359ec549790ce14d8214fcb16ef915e4530e5ed235 629B / 629B
=> sha256:61ca4f733c892af09e85a32fde8361b6d713b8b53292dc15fb093229f648670 1.79MB / 1.79MB
=> sha256:f18232174bc91741fd3da96d85011092101a032a93a388b79e99e69c2d5c870 3.64MB / 3.64MB
=> extracting sha256:f18232174bc91741fd3da96d85011092101a032a93a388b79e99e69c2d5c870
=> extracting sha256:61ca4f733c892af09e85a32fde8361b6d713b8b53292dc15fb093229f648670
=> extracting sha256:b464cfd2a6319875aeb27359ec549790ce14d8214fcb16ef915e4530e5ed235
=> extracting sha256:d7e5f07248863957ebb0b5a44a5729963c3462666baa2947d00628cb5f2d5773
=> extracting sha256:81bd8ed7ec6789b0cb7f1b47ee731c522f6dba83201ec73cd6bca1350f582948
=> extracting sha256:197eb75867ef4fcedd4724f17b0972ab0489436860a594a9445f8eaff8155053
=> extracting sha256:b464cfd2a6319875aeb27359ec549790ce14d8214fcb16ef915e4530e5ed235
=> extracting sha256:39c2ddfd6010082a4a646e7c444e95aca9b3faebc00f17f7ccc2954004f2a7d
[2/2] COPY index.html /usr/share/nginx/html/index.html
=> exporting to image
=> exporting layers
=> exporting manifest sha256:d842c3e389656216de0653aec45ec0a7a7ddfd04597bebf32b2041f5e04c9d37a
=> exporting config sha256:b670e7d7e8545cb91fbc689bb25cd609a32013e9bf945402763c161f1f09ec9c
=> exporting attestation manifest sha256:08a626ae3a12beb6715dc1019e541ff5897d9aa4c822369a81e53734731cf3ad
=> exporting manifest list sha256:feaa27de9e6a5782f61b8a1bb9c1ef5157a38df2b35d79deb5856afb4dc83af6
=> naming to docker.io/library/paul-htal-app:latest
=> unpacking to docker.io/library/paul-htal-app:latest

View build details: docker-desktop://dashboard/build/desktop-linux/desktop-linux/kegts80k7zf2ov3keqkvou2b
PS C:\Users\paul_\OneDrive\Desktop\Cloud Engineering Principles and Practice\Docker> docker run -d -p 8080:80 --name webserver paul-htal-app
```

Figure 6 Docker image build process

```
ac3f36ba693dc3d52ac51f9197caclacd12c9aa8a44e87eaf9bb348e2f2ee188
PS C:\Users\paul_\OneDrive\Desktop\Cloud Engineering Principles and Practice\Docker> docker ps
CONTAINER ID   IMAGE      COMMAND                  CREATED        STATUS      PORTS                    NAMES
ac3f36ba693dc paul-htal-app "/docker-entrypoint..." 13 seconds ago Up 11 seconds    0.0.0.0:8080->80/tcp    webserver
PS C:\Users\paul_\OneDrive\Desktop\Cloud Engineering Principles and Practice\Docker> |
```

Figure 7 Docker commands (clear, simple)

Container CPU usage 0.00% / 800% (8 CPUs available) Container memory usage 7.94MB / 3.43GB [Show charts](#)

Search Only show running containers

	Name	Container ID	Image	Port(s)	CPU (%)	Last started	Actions
☐	brave_gauss	407d657f45ef	docker:dockerfile:latest		0%	2 months ago	▶ ⋮ 🗑
☐	hello	e578eccc7c06	nginx		0%	3 months ago	▶ ⋮ 🗑
☐	hopeful_borg	3bd0d1c511a7	hello-world:latest		0%	3 months ago	▶ ⋮ 🗑
☐	hungry_hopper	980f9ac0128	hello-world		0%	3 months ago	▶ ⋮ 🗑
☒	webserver	ac3f36ba693dc	paul-htal-app	8080:80 (f)	0%	4 minutes ago	▶ ⋮ 🗑

Figure 8 Docker Desktop Containers tab

[Images](#) / paul-html-app:latest

<

paul-html-app:latest

IN USE

feaa274e9e6a

Layers (21) - 2 selected

Figure 9 Docker image details view

Bibliography

- [1] S. Jajodia, *Secure Cloud Computing*, Springer, 2014.
- [2] J. Broberg, *Cloud Computing Principles & Paradigms*, New Jersey: John Wiley & Sons, Inc., 2011.
- [3] R. L. Krutz, "Cloud Security," in *A Comprehensive Guide to Secure Cloud Computing*, Wiley Publishing Inc.
- [4] F. Shimba, "Cloud Computing," in *Strategies for Cloud Computing Adoption*, Dublin, Technological University Dublin, 2016, p. Dissertation.
- [5] G. Paliwal, "Cloud Computing," in *What is Cloud Computing*, 2010.
- [6] A. Sen, "What Is Cloud / Cloud Computing?," Avendus Capital Inc., 2017.
- [7] M. Luo, "Cloud Computing," in *CLOUD 2018, SCF 2018*, in Seattle, WA, USA,, Services Conference Federation,, 2018.
- [8] L. Chao, "Cloud Computing Networking," Taylor & Francis Group, LLC, 2015.
- [9] S. G., "Enterprise Cloud Computing," 2010.
- [10] C. Millard, "Cloud Computing Law," 2021.
- [11] K. Jayaswal, "Cloud Computing," in *Black Book*, Dreamleach, 2014.
- [12] K. Rungta, "Learn NodeJS in 1 Day," in *Learn NodeJS*, Krishna Rungta, 2016.
- [13] A. Mardan, "Practical Node.js," in *Building Real-World Scalable Web Apps*, Apress, 2018 .
- [14] N. Poulton, "Docker," in *Deep Dive*, 2025.
- [15] S. Bhat, "Practical Docker with Python," in *Build, Release and Distribute your Python App with Docker*, Apress, 2018.
- [16] "docker.com," 2022 Docker Inc., 2022. [Online]. Available: <https://www.docker.com/>. [Accessed 9 12 2022].
- [17] J. Turnbull, "Docker Book "What is a Docker image?"," Packet, 2016 .
- [18] S. Bhat, "Practical Docker with Python:," in *Build, Release and Distribute Your Python App with Docker*, Apress, 2018.
- [19] I. M. & A. H. Sayers, "Docker in Practice," Manning, 2019 .
- [20] P. R. & J. S. C. & V. Singh, "Learning Docker:," in *Optimize the power of Docker to run your applications quickly and easily*, 2015 .
- [21] S. P. K. & K. Matthias, "Docker: Up & Running:," in *Shipping Reliable Containers in Production*, Oriley, 2018 .

- [22] N. Marshall, "Mastering VMware vSphere 6.7," Sybex, 2019.
- [23] "vSphere Virtual Machine Administration," vmware, 16 OCT 2018.
- [24] M. Gavanda, "Mastering VMware vSphere 6.7:," in *Effectively deploy, manage, and monitor your virtual datacenter with VMware vSphere 6.7, 2nd Edition*, Packet, 2019.
- [25] M. Brown, "VMware vSphere 6.7 Data Center Design Cookbook:," in *Over 100 practical recipes to help you design a powerful virtual infrastructure based on vSphere 6.7, 3rd Edition*, Packt Publishing, 2019.
- [26] M. M. Waldrop, *The Dream Machine: J.C.R. Licklider and the Revolution That Made Computing Personal*, 2002.

FINAL GRADE

28/100

GENERAL COMMENTS

Your submission has a significant structural problem that substantially affects the mark: the majority of the report covers content that is not required by the brief. Extended sections on cloud computing history, advantages and disadvantages, deployment models (public, private, hybrid, community), IaaS/PaaS/SaaS, Node.js, and a detailed treatment of VMware vSphere including ESXi, vCenter, OVF/OVA templates and VMware Tools components are all absent from the assignment requirements. These sections, while not without content, do not attract marks because they do not address what was asked.

The Docker practical section is present but thin and structured in reverse order, which makes it difficult to follow. The Dockerfile is correct and brief commands for build, run, DockerHub push, volume creation and networking are shown. However there is no explanation of what the instructions do or why choices were made, no evidence of the practical outputs beyond referenced figures, and no video link. The three sections explicitly required by the brief, are entirely absent. These sections carry 45 of the 100 available marks and getting nothing for them has a severe impact on the overall mark. The reference list consists largely of general cloud computing books from 2011 to 2019 with limited relevance to the specific topics required.

- TB

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25