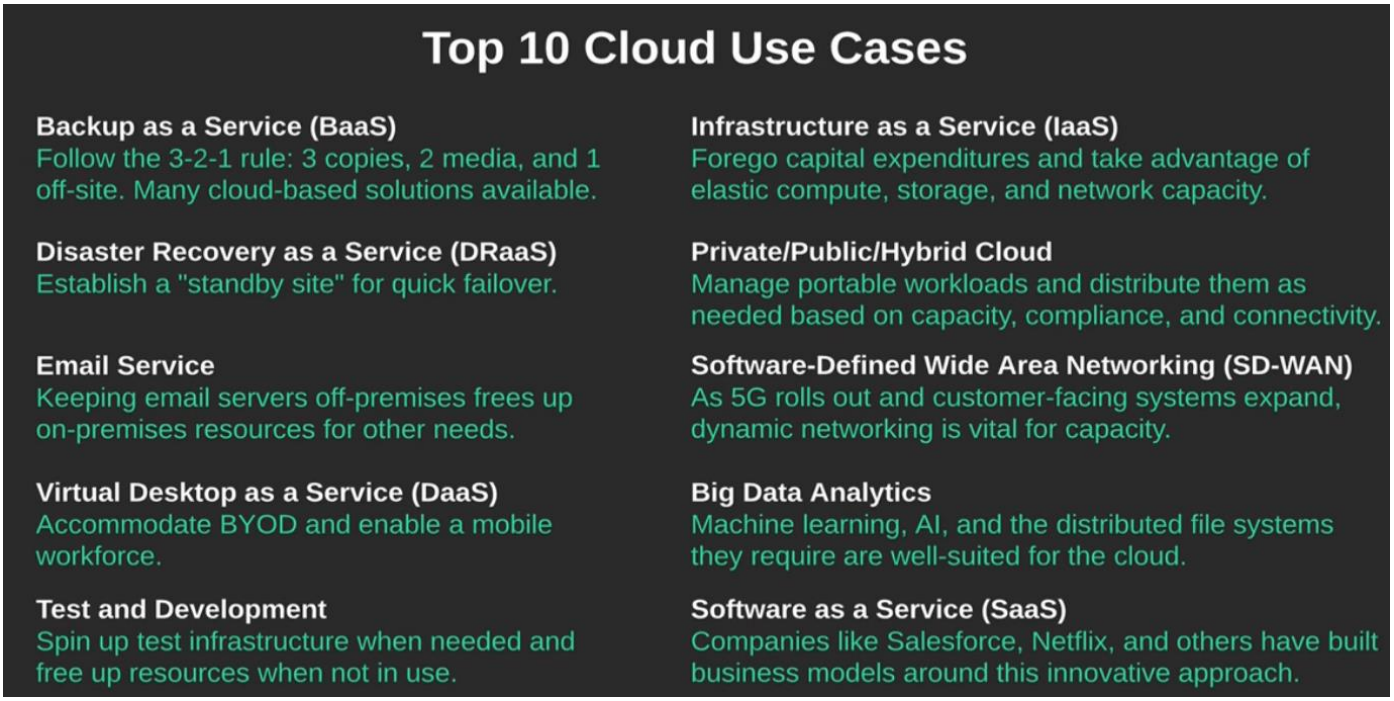
# :Cloud Migration Fundamentals:

Login: type FOC  email id in login email text box: pavankumarpabbisetty@quickenloans.com

Training: https://learn.acloud.guru/course/3f72b5d3-596c-4540-b43c-643004dba153/learn/26a66438-c669-4cc4-85dd-fa4746db8030/902f2e08-3fe6-4bb2-b190-05bc3fb3115d/watch

Interactive session: https://lucid.app/lucidchart/2f381762-3aa6-4620-890b-71c92e1007d6/view?page=~EoC788TA7_d#



# Cloud Computing Constraints

**Data Governance**
Many industries and locales have regulations regarding privacy and data residency that may impair or prevent cloud adoption.

**Regulatory Compliance**
Regulators may be unprepared for cloud implications.

**Security**
Perimeter security paradigms break down in highly distributed and off-premises environments.

**Third-Party Vendors and Licensing**
Vendors may use cloud adoption to request additional licensing or purchases.

**Suitability of Applications**
Monolithic applications and applications with device dependencies are difficult to migrate to cloud environments.

**Need for Advanced Tooling**
Hygiene, patching, version control, automated deployment, and cloud orchestration may be new requirements for operations teams.

**Outsourcing Agreements in Place**
Multi-year data center outsourcing agreements often lack provisions for cloud computing models.

**Financial Implications**
Before the assets of existing on-premises data centers are fully depreciated, the addition of pay-per-use cloud costs results in a double expense.

**Executive Awareness & Lack of Skills**
Cloud computing requires new approaches to applications and infrastructure architecture, development, and deployment. These skills remain scarce, and not all executive leadership has been able to adapt to these new paradigms.

Use Cases | Constraints

## Centralized

Began as a single data center.

Compute, storage, and network were often on one campus.

"Hands-on" meant *hands-on*. Systems could be touched and operated from the data center.

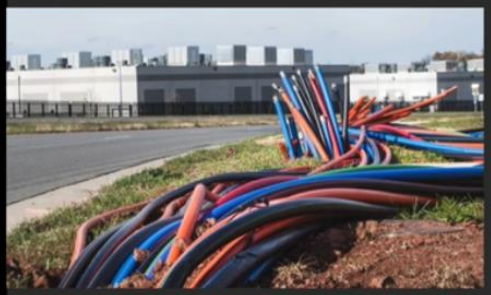
## Distributed

Less expensive systems based on micro-processors began to be utilized.

Network backbones became faster to connect systems and workstations.

Redundancy and co-location developed as a means of HA.

## Cloud



Massive data centers occupying whole buildings and complexes became the norm.

High-speed fiber-optic networks enabled faster connectivity.

Elasticity developed as a means to facilitate pay-for-what-you-use cost models.

Hardware | Software | Decoupling | Decoupling 2 | Decoupling 3 | Decoupling 4 | Decoupling 5

## Monolithic

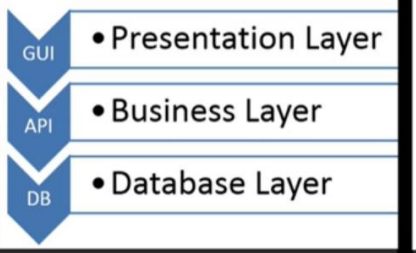
```
000100 IDENTIFICATION DIVISION.
000200 PROGRAM-ID. HELLOWORLD.
000300
000400 ENVIRONMENT DIVISION.
000500 CONFIGURATION SECTION.
000600 SOURCE-COMPUTER. RM-COBOL.
000700 OBJECT-COMPUTER. RM-COBOL.
000800
000900 DATA DIVISION.
001000 FILE SECTION.
001100
101200 PROCEDURE DIVISION.
101300
101400 MAIN-LOGIC SECTION.
101500     DISPLAY "Hello world!"
101600 STOP RUN.
```

Often a single large program contained all logic, storage, and user interface code.

One program to run on one machine.

Programs often included many system functions.

## Client/Server & N-Tier




To scale throughput and accommodate many more users, presentation, business logic, and database were run as separate programs on separate machines.

The internet "web farm" became the primary data center and application architecture.

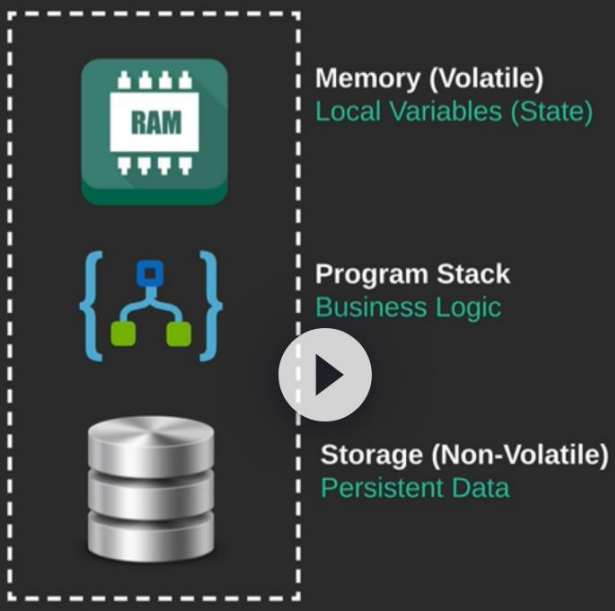
## Containers & Micro-Services

Microservices

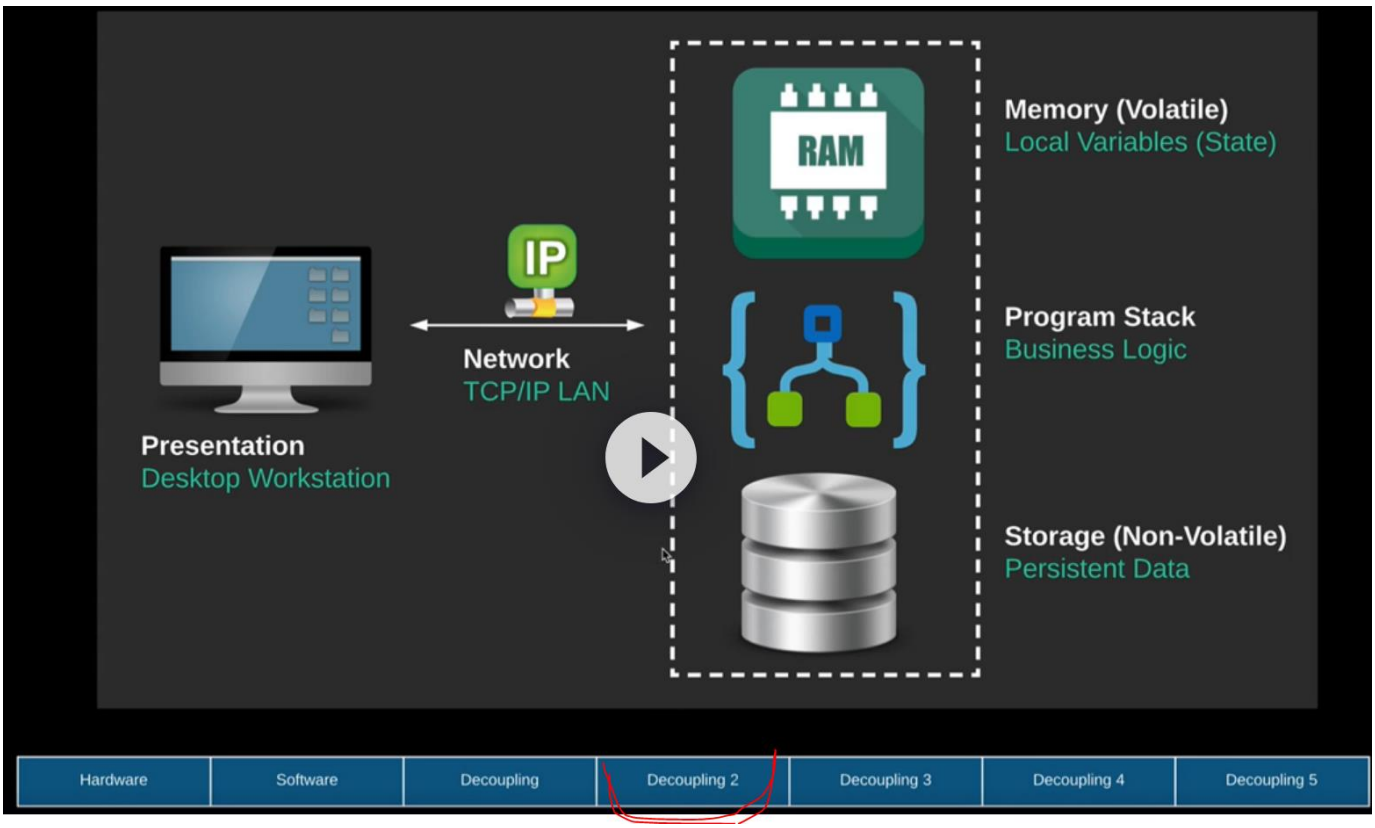
As globalization demanded even greater scale, workloads had to be replicated quickly, often in disparate global data centers.

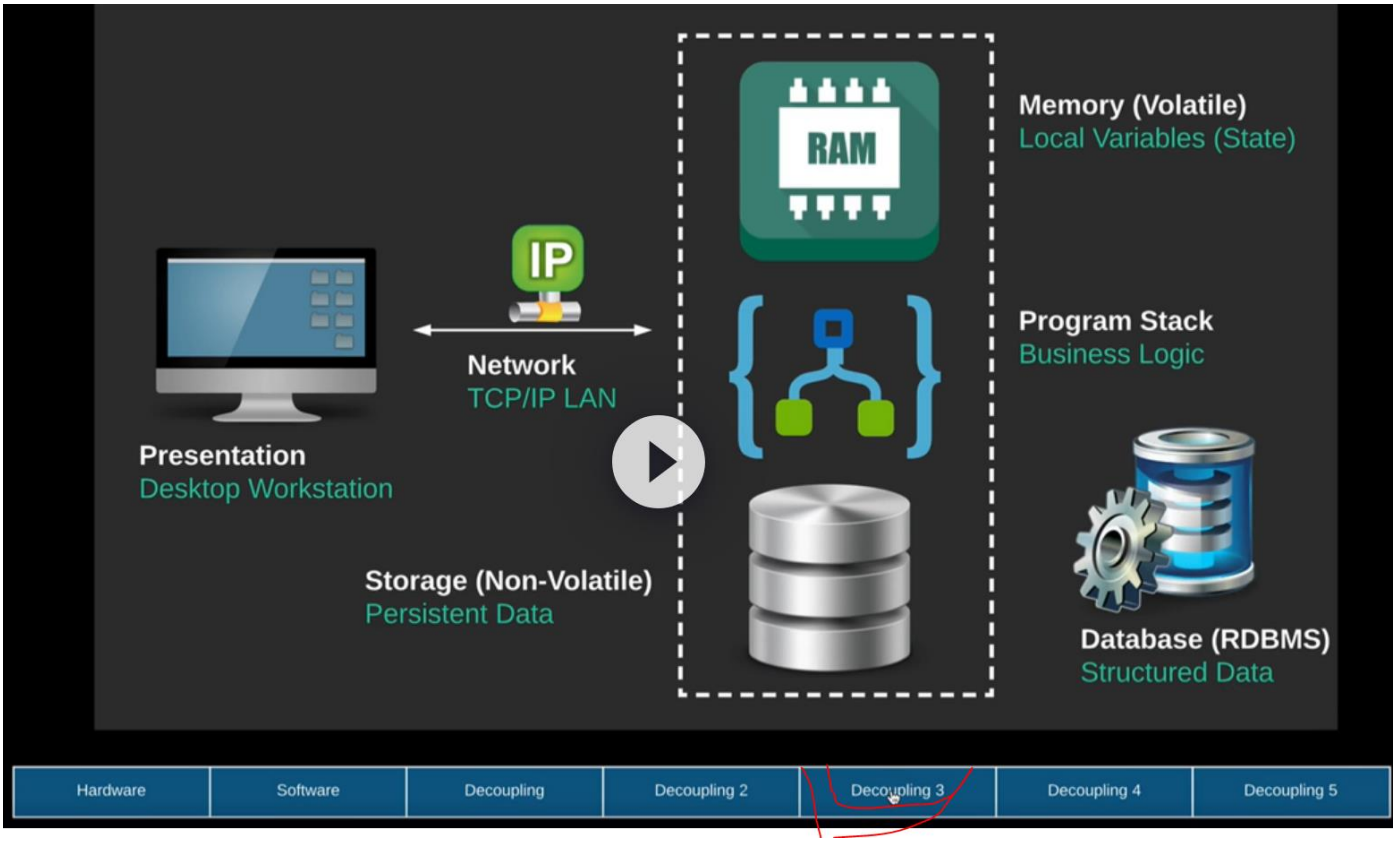
Self-healing architectures required smaller, easy-to-instantiate workloads that could utilize infrastructure elasticity.

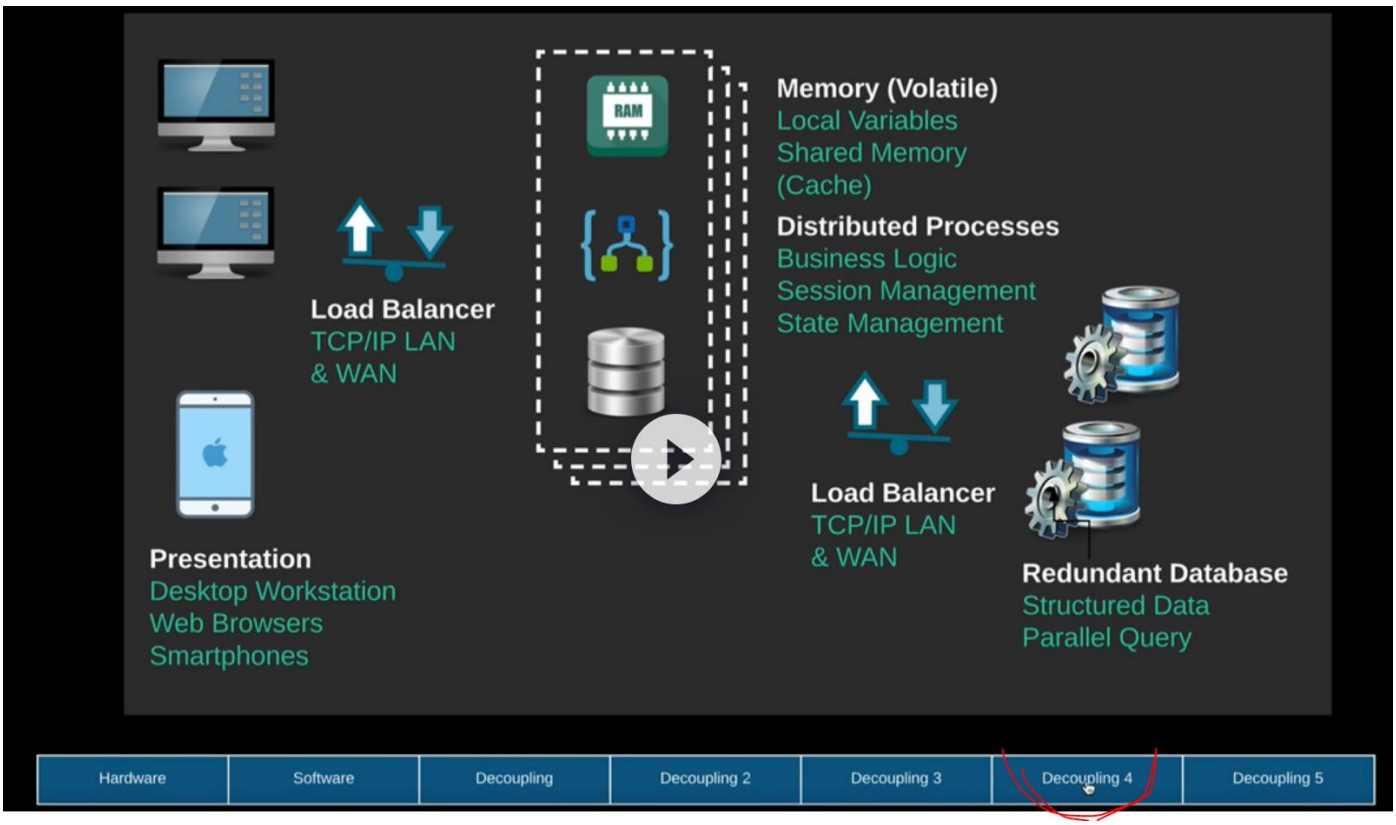
| Hardware | Software | Decoupling | Decoupling 2 | Decoupling 3 | Decoupling 4 | Decoupling 5 |
|---|---|---|---|---|---|---|

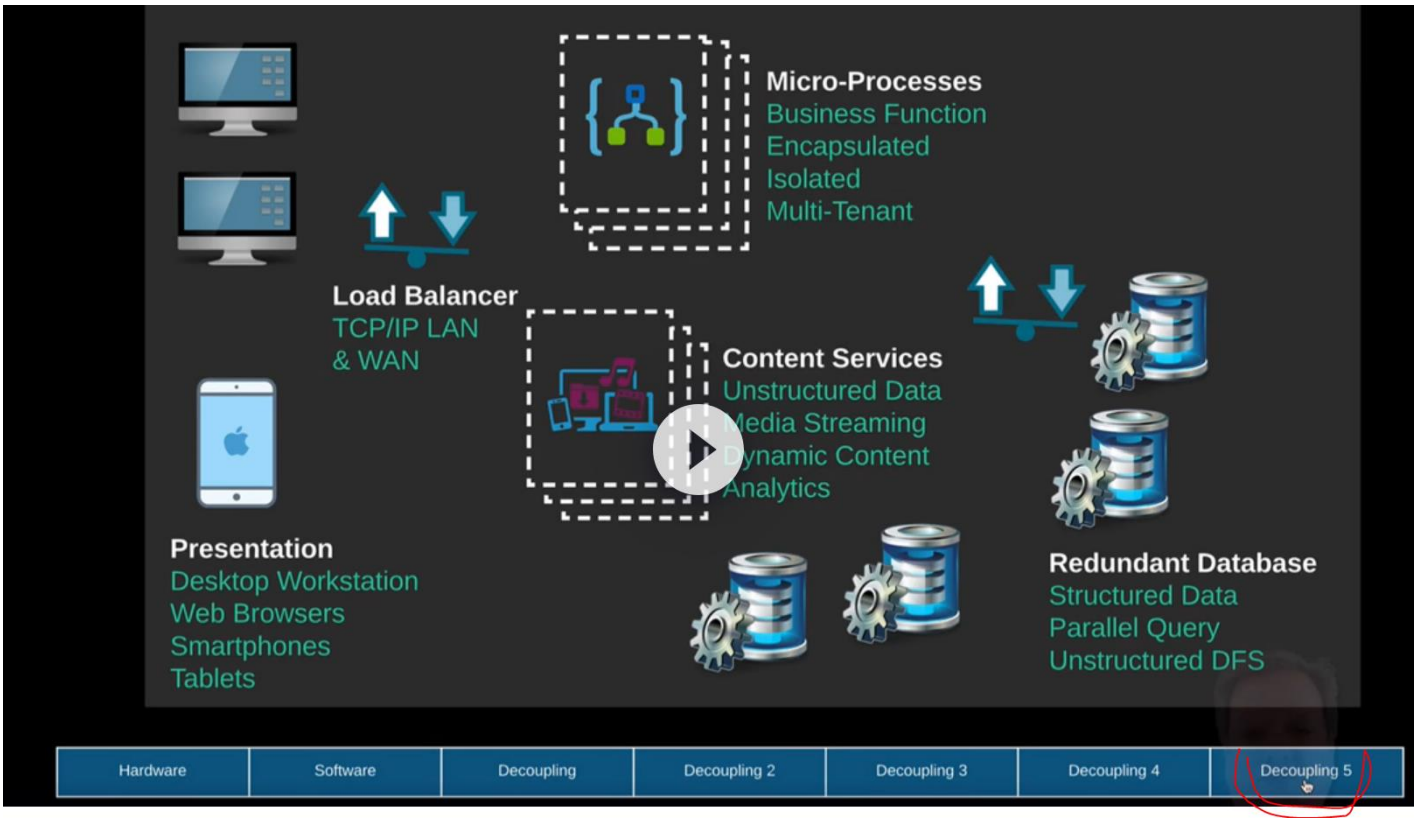


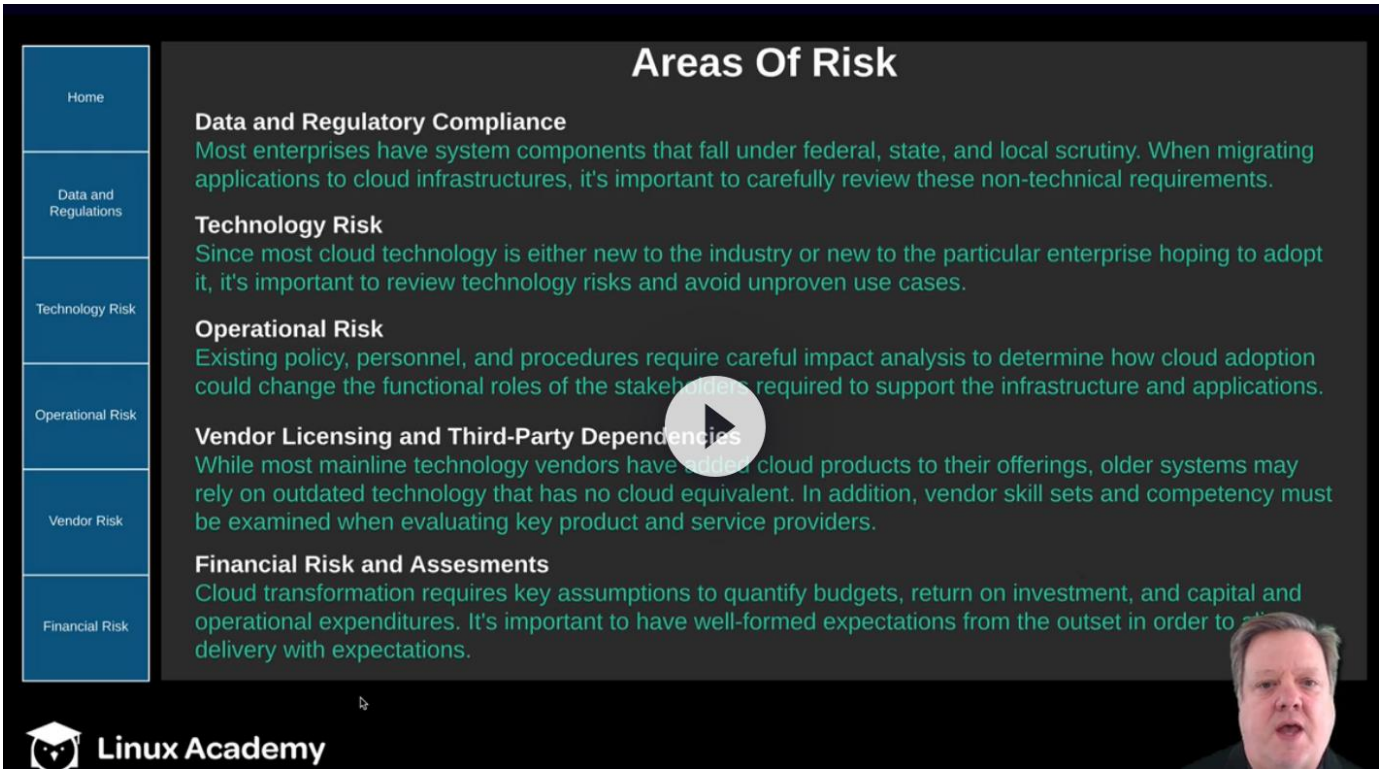

| Hardware | Software | Decoupling | Decoupling 2 | Decoupling 3 | Decoupling 4 | Decoupling 5 |
|---|---|---|---|---|---|---|


RAM
Memory (Volatile)
Local Variables (State)
IP
Network
TCP/IP LAN
Program Stack
Business Logic
Presentation
Desktop Workstation
Storage (Non-Volatile)
Persistent Data
Hardware
Software
Decoupling
Decoupling 2
Decoupling 3
Decoupling 4
Decoupling 5

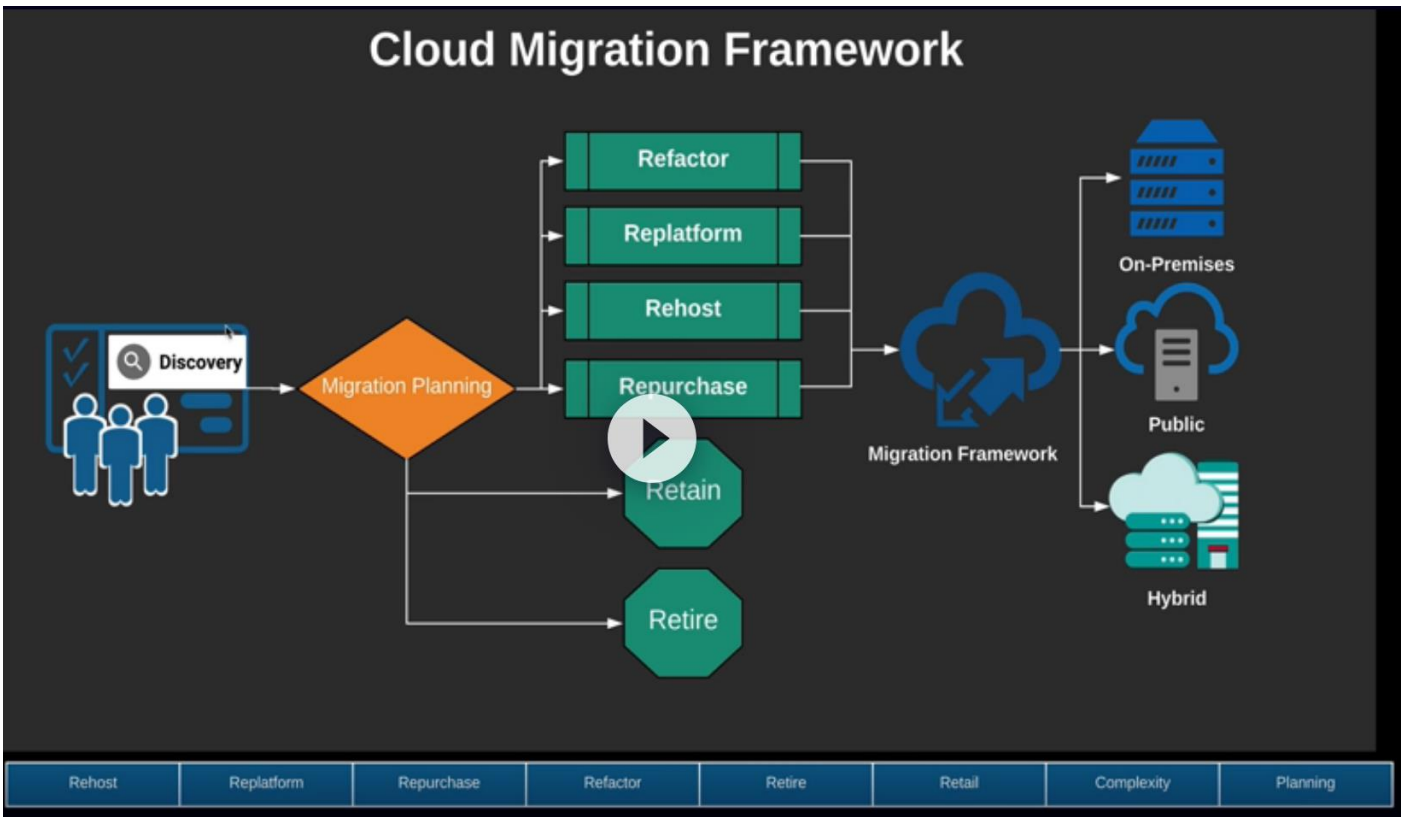

RAM
Memory (Volatile)
Local Variables (State)
IP
Network
TCP/IP LAN
Program Stack
Business Logic
Presentation
Desktop Workstation
Storage (Non-Volatile)
Persistent Data
Database (RDBMS)
Structured Data
Hardware
Software
Decoupling
Decoupling 2
Decoupling 3
Decoupling 4
Decoupling 5

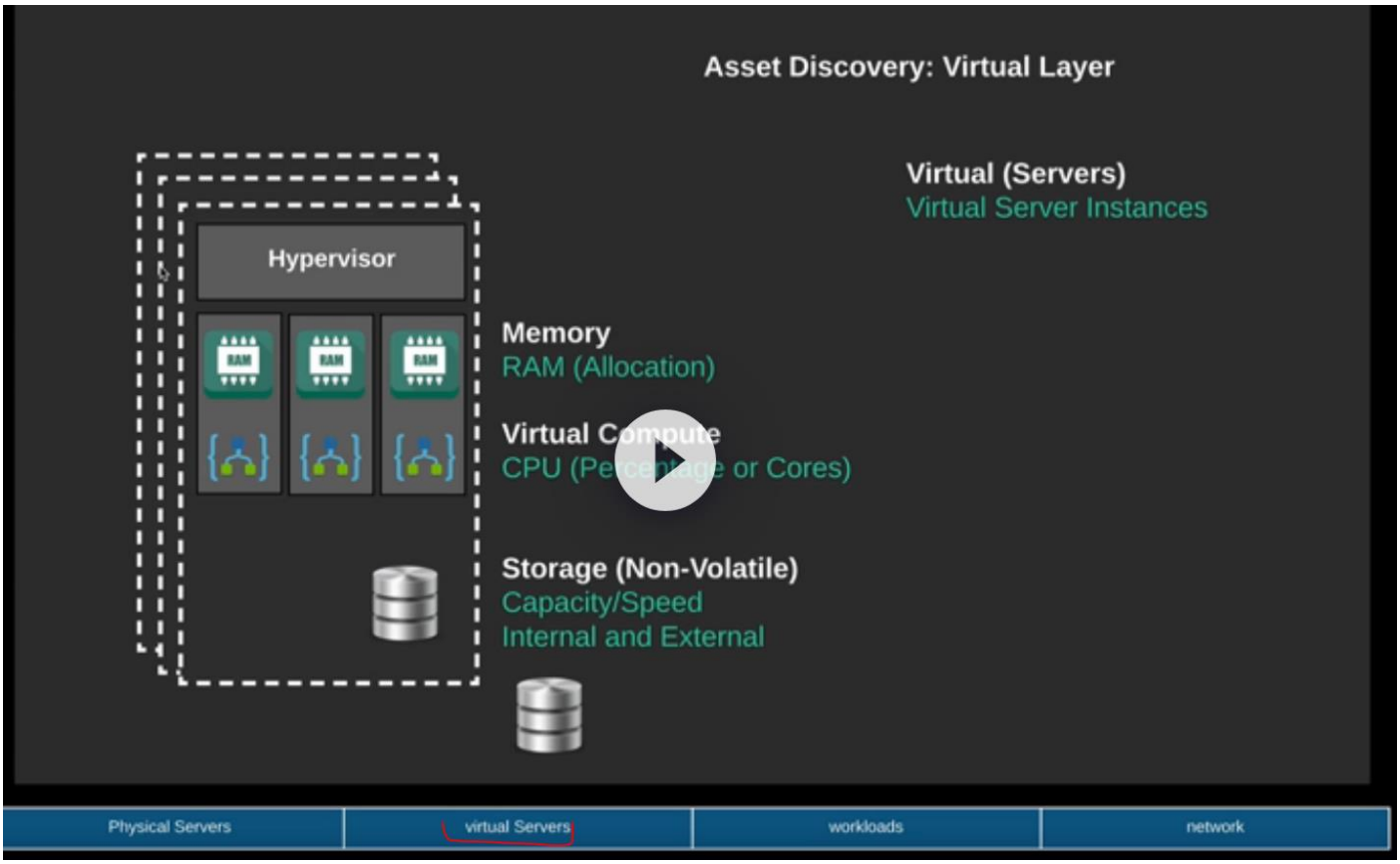

Memory (Volatile)
Local Variables
Shared Memory
(Cache)
Distributed Processes
Business Logic
Session Management
State Management
Load Balancer
TCP/IP LAN
& WAN
Load Balancer
TCP/IP LAN
& WAN
Presentation
Desktop Workstation
Web Browsers
Smartphones
Redundant Database
Structured Data
Parallel Query
Hardware
Software
Decoupling
Decoupling 2
Decoupling 3
Decoupling 4
Decoupling 5


Micro-Processes
Business Function
Encapsulated
Isolated
Multi-Tenant
Load Balancer
TCP/IP LAN
& WAN
Content Services
Unstructured Data
Media Streaming
Dynamic Content
Analytics
Presentation
Desktop Workstation
Web Browsers
Smartphones
Tablets
Redundant Database
Structured Data
Parallel Query
Unstructured DFS
Hardware
Software
Decoupling
Decoupling 2
Decoupling 3
Decoupling 4
Decoupling 5

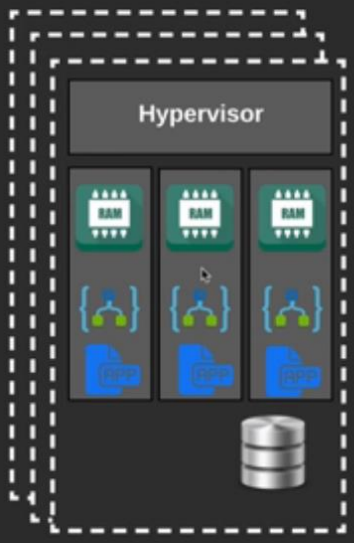

Areas Of Risk
Home
Data and Regulations
Technology Risk
Operational Risk
Vendor Risk
Financial Risk
Data and Regulatory Compliance
Most enterprises have system components that fall under federal, state, and local scrutiny. When migrating applications to cloud infrastructures, it's important to carefully review these non-technical requirements.
Technology Risk
Since most cloud technology is either new to the industry or new to the particular enterprise hoping to adopt it, it's important to review technology risks and avoid unproven use cases.
Operational Risk
Existing policy, personnel, and procedures require careful impact analysis to determine how cloud adoption could change the functional roles of the stakeholders required to support the infrastructure and applications.
Vendor Licensing and Third-Party Dependencies
While most mainline technology vendors have added cloud products to their offerings, older systems may rely on outdated technology that has no cloud equivalent. In addition, vendor skill sets and competency must be examined when evaluating key product and service providers.
Financial Risk and Assesments
Cloud transformation requires key assumptions to quantify budgets, return on investment, and capital and operational expenditures. It's important to have well-formed expectations from the outset in order to
delivery with expectations.
Linux Academy


Home
Data and Regulations
Technology Risk
Operational Risk
Vendor Risk
Financial Risk
Risk Areas
Data and Regulatory Compliance
Potential Mitigation
Data Governance
Many industries and locales have regulations regarding privacy and data residency that may impair or prevent cloud adoption.
Public Cloud Provider Offerings
AWS, Azure, Google and other cloud providers have established locale-specific data centers to accommodate even stringent regulatory burdens.
Regulatory Compliance
Regulators may be unprepared for cloud implications.
Take a Collaborative Approach
Most regulators are anxious to improve their ability to govern cloud technologies. Many will invest in a collaborative effort to refine practice and policy.
Data Security
Perimeter security paradigms break down in highly distributed and off-premises environments.
Consider On-Premises and New Paradigms
Perimeter and facility boundaries serve on-premises data but fall short in public cloud models. Consider new paradigms and tooling.
Transparency and Monitoring
Cloud providers must accommodate monitoring and analytics to ensure ongoing stability.
Many Advanced Technologies Are Available
Ops centers have radically changed with globalization. Many vendors provide automated tools for this purpose.
Controls and Operational Disciplines
Automated provisioning, deployment, and orchestration are key considerations in cloud environments.
DevOps Pipelines Become a Necessity
Continous deployment and delivery and competent
configuration management are key to succes
Linux Academy


Cloud Migration Framework
Discovery
Migration Planning
Refactor
Replatform
Rehost
Repurchase
Retain
Retire
Migration Framework
On-Premises
Public
Hybrid
Rehost
Replatform
Repurchase
Refactor
Retire
Retail
Complexity
Planning


Asset Discovery: Virtual Layer
Hypervisor
RAM
RAM
RAM
Virtual (Servers)
Virtual Server Instances
Memory
RAM (Allocation)
Virtual Compute
CPU (Percentage or Cores)
Storage (Non-Volatile)
Capacity/Speed
Internal and External
Physical Servers
virtual Servers
workloads
network

## Asset Discovery: Application Layer




**Memory**
RAM (Allocation)

**Virtual Compute**
CPU (Percentage or Cores)

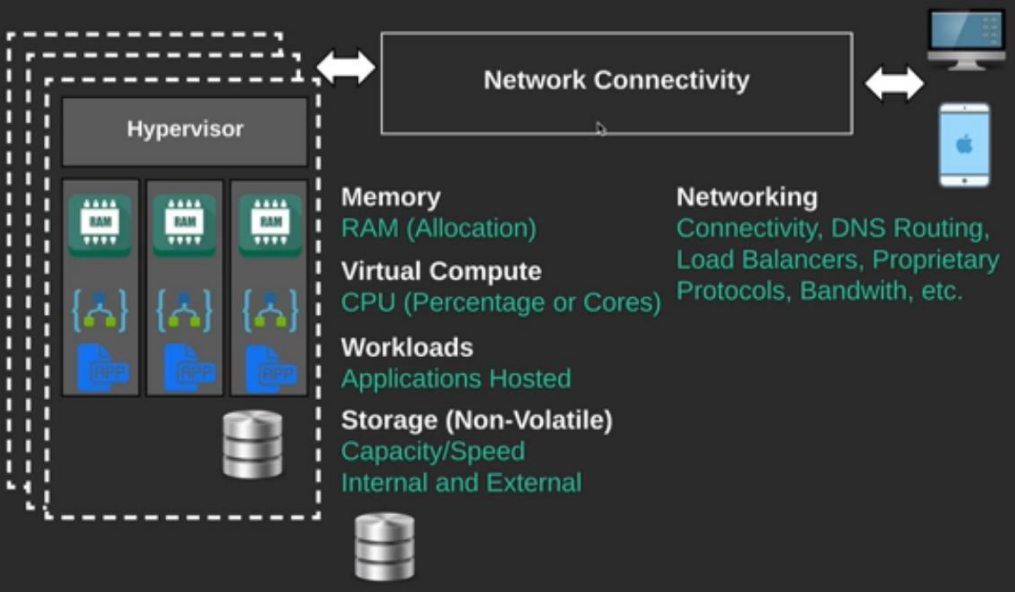
**Workloads**
Applications Hosted

**Storage (Non-Volitile)**
Capacity/Speed
Internal and External

**Application Workloads**
Profile of application workloads: Language, Versions, Dependencies, Proprietary Interfaces, etc.

| Physical Servers | virtual Servers | workloads | network |
|---|---|---|---|

## Asset Discovery: Network Layer




**Memory**
RAM (Allocation)

**Virtual Compute**
CPU (Percentage or Cores)

**Workloads**
Applications Hosted

**Storage (Non-Volatile)**
Capacity/Speed
Internal and External

**Networking**
Connectivity, DNS Routing, Load Balancers, Proprietary Protocols, Bandwith, etc.

| Physical Servers | Virtual Servers | Workloads | Network |
|---|---|---|---|

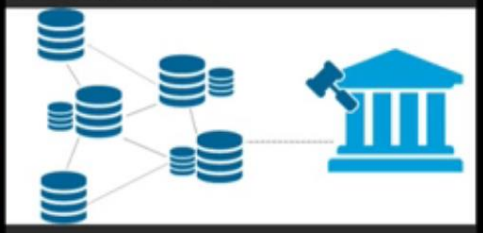
## Licensing


When planning a cloud migration, it's important to identify all of the third-party software licensing required and to review those licenses to determine whether cloud usage requires amendments or additional licensing. Most, but not all, vendors have created licensing models that accommodate cloud usage.

## Data Sovereignty

Data sovereignty is the idea that data is subject to the laws and governance structures of the nation in which it is collected. The concept of data sovereignty is closely linked with data security and cloud computing. In many locales and industries, regulations require specific processes and safeguards.

## Governance



Certain industries and use cases impose specific compliance requirements that may be impacted by the migration of an application workload to a public, private, or hybrid cloud infrastructure. The migration plan should identify and accommodate these regulations to ensure ongoing conformity to legal constraints.

# Software Licensing and Cloud Migrations

**Cloud Provider Agreements**
Service-oriented architectures (SOA) require that an agreement be signed with the cloud provider. These contracts often contain various options for the service-level agreement (SLA). Different applications may tolerate lower levels of uptime assurance and mean time to recovery. Stringent applications may require high availability or other considerations. In all cases, the cloud provider agreement contains terms and conditions that affect any application or tooling agreements that may ultimately be used on the cloud infrastructure.

**Hardware Ownership Provisions**
Some software vendors have usage rights that are specific to virtualization or cloud computing. Previously owned licenses that are in use on owned hardware are particularly likely to have provisions that prohibit installing that software on hardware that isn't owned by the licensee—making it illegal to install that software in an IaaS environment. Others might allow virtualized installations, but only with very heavy usage fees. Make sure you read the fine print in your software agreements to check for these provisions.

**Licensing Per CPU or CPU Core**
Software vendors often sell their product per CPU core, but once you install in a virtual environment, CPUs become much more flexible. Virtual CPUs can move from machine to machine along with the VM, or they can fluctuate in processing power. Elastic architectures often require a license for the maximum potential allowed.

**Subscription and Pay-Per-User vs. Perpetual**
Perpetual licenses or subscriber access licenses (SAL) are usually based on the number of users. A subscription model can be either per user or based on metered usage, with per-hour, per-week, per-month, or per-year licenses available. Perpetual licenses are not ideal for the cloud unless they were paid for before the migration. Since VMs are powered on and off, some organizations may not use the full amount allowed by their license, reducing the cost advantages of the cloud. In addition, perpetual licenses sometimes mandate hybrid cloud use, where all existing software stays in the legacy data center and new software may be used in the public cloud.

# Data Sovereignty and Cloud Migrations

**Data Sovereignty and Privacy Law**
As governments navigate the new realities brought on by social networks, globalization, and increased cyberterrorism, many locales have begun to institute regulations that affect organizations using cloud systems and storage. This fast-changing reality has affected many enterprises as they plan migrations. Fortunately, most mainstream cloud providers can quickly tell prospective customers the current and future offerings they provide to meet these new and evolving regulatory requirements.

**Canada**
Canada has enacted various data sovereignty measures, primarily pertaining to the storage of Canadian data on Canadian servers. Canada's IT Strategic Plan 2016-2020 enacted new data localization measures in order to uphold citizens' privacy. Storing Canadian data on Canadian servers (instead of American ones) prevents Canadian data from being subject to the US Patriot Act.

**European Union**
In 2016, the EU Parliament approved their own data sovereignty measures in the form of the General Data Protection Regulation (GDPR). This regulatory package governs data protection policy for all European Union members. It includes an addendum that establishes extraterritorial jurisdiction by extending its rules to any data controller or processor whose subjects are EU citizens, regardless of where the holding or processing is conducted. This forces companies based outside of the EU to reevaluate their site-wide policies and potentially align them with the laws of another country (or countries). The GDPR replaced the 1995 European Data Protection Directive that established the free movement of personal data between member state borders.

**Brexit**
The separation of the United Kingdom from the EU has brought new challenges to regulated industries like banking. The Brexit plan recently approved by the EU and British Parliament will have a major impact on the regulation of banking data in the United Kingdom.

# Governance and Cloud Migrations

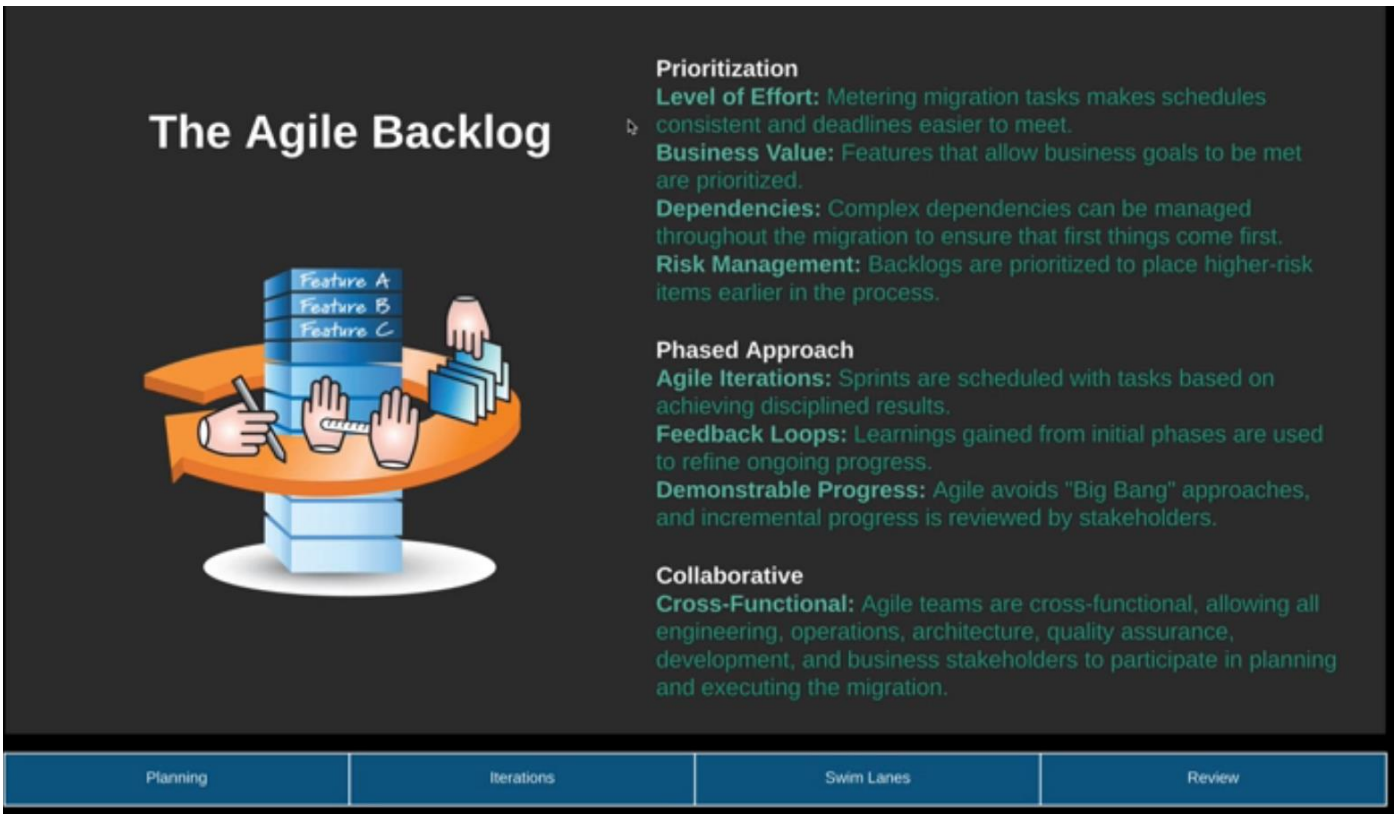
**Governance and Cloud Computing**
Regulated industries have sophisticated processes in place to ensure ongoing compliance with legal regulations. In the past, cloud computing brought new challenges because existing regulations did not properly articulate or accommodate the service-oriented model of cloud computing.

Fortunately, now that over 20% of the workloads used in large enterprises have been migrated to the cloud, pioneering organizations have worked closely with regulators to close the gap in most standards and regulatory bodies.

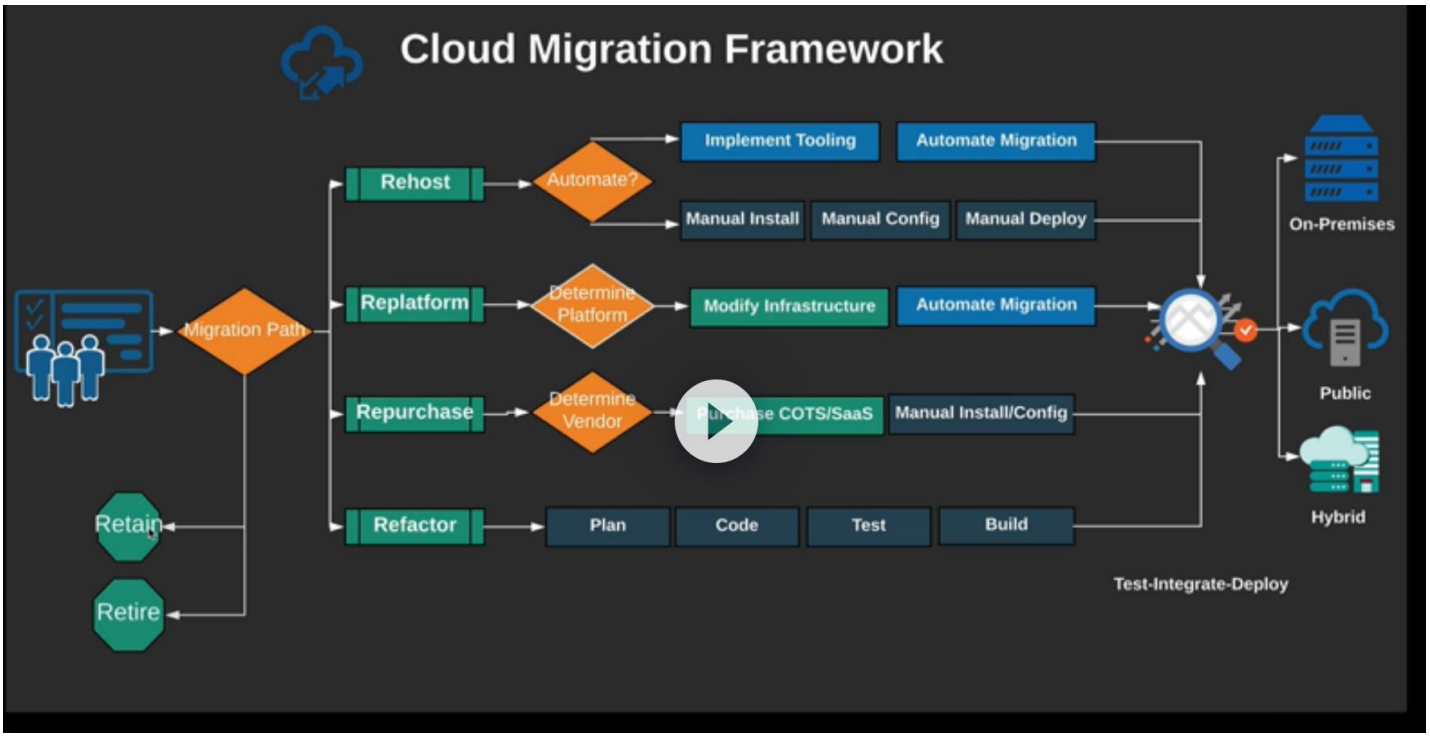
**Banking and the Payment Card Industry (PCI)**
Card issuers like Visa, MasterCard, Discover, and American Express perform regular audits of card providers to ensure ongoing compliance. Additionally, each locale's central bank regulates international currency exchanges and the clearing of financial transactions. Cloud computing models must accommodate the auditing requirements of these governing entities. The Securities industry, along with many others, also carries a number of regulatory standards.

**Security and Cloud Surrogates**
Perimeter and campus security practices have adapted to the colocation of dark and remote data centers. Now that public cloud providers are in control of the computing facilities they use, they often have to include in their agreements the compliance and ongoing disciplines required by third-party regulators and global enterprises. Many public cloud users have regular reviews with their cloud providers to ensure ongoing compliance. Conventional digital security methods generally apply to cloud models like they do at virtual data centers. For this reason, most digital security techniques are merely replicated in cloud service models. Private network links to cloud data centers and the Virtual Private Cloud (VPC) are one example.

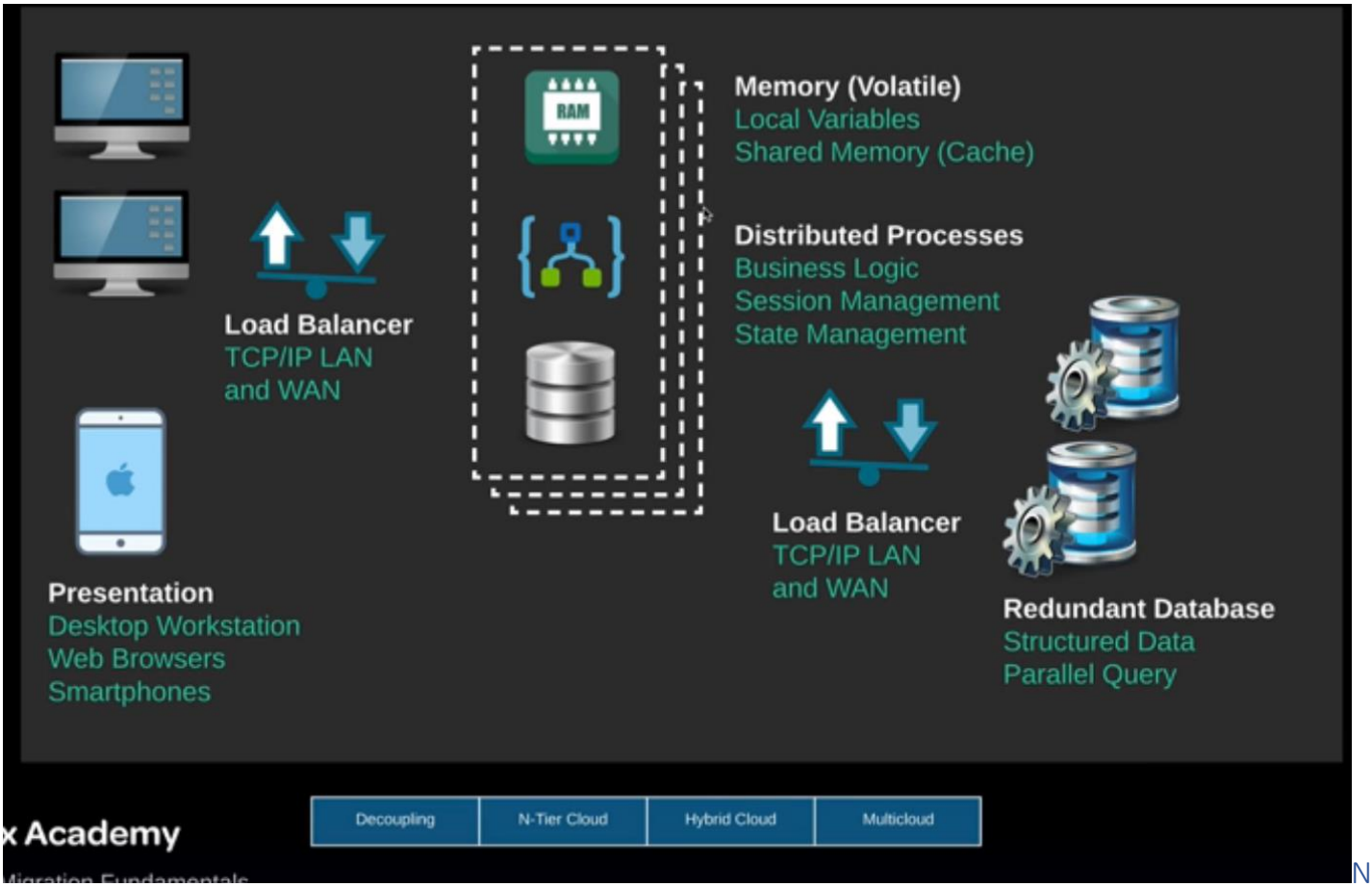
**RegTech**
An entire industry of third-party service providers has sprung up around the service-oriented model. "RegTech" is an industry that provides enterprise users digital tooling and other processes to ensure ongoing compliance with changing regulations.



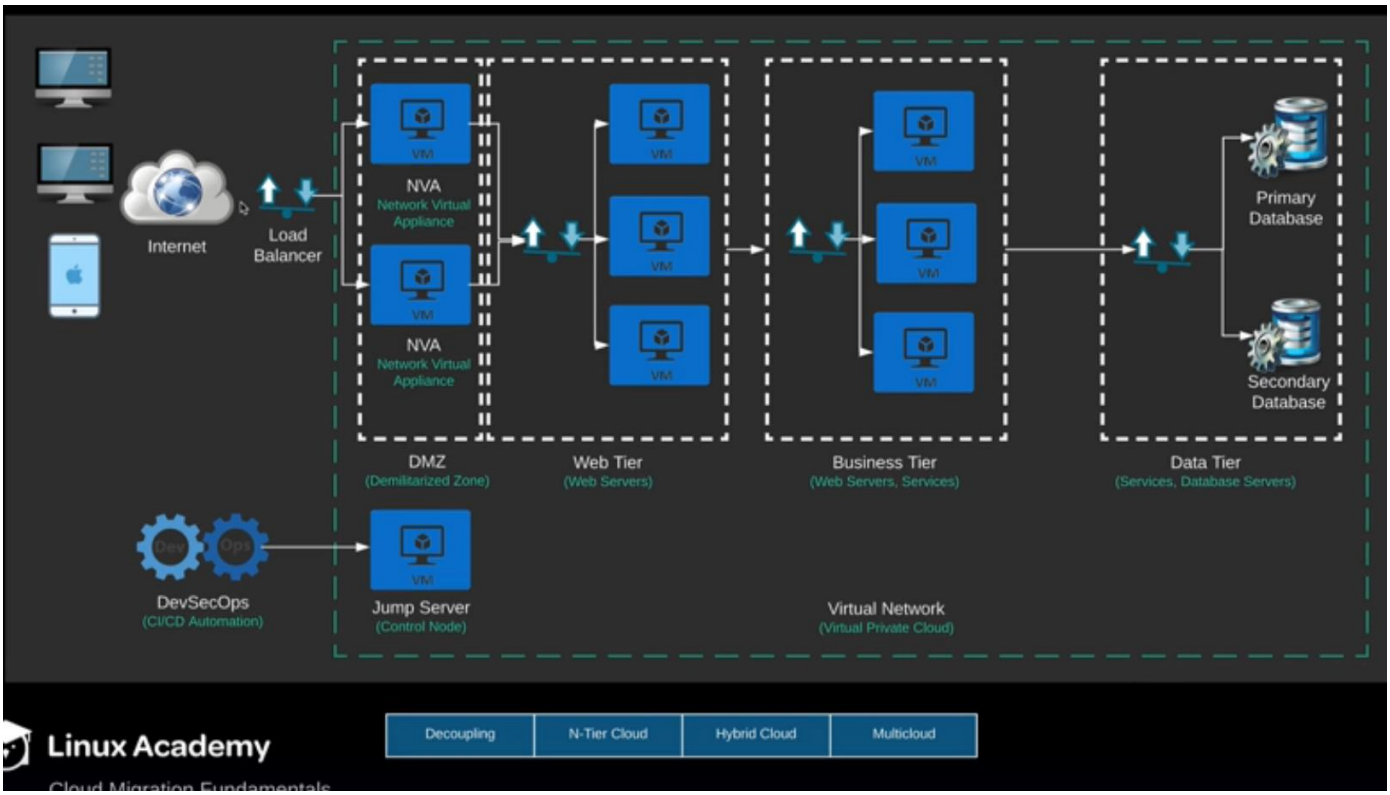

## Cloud Migration Framework:



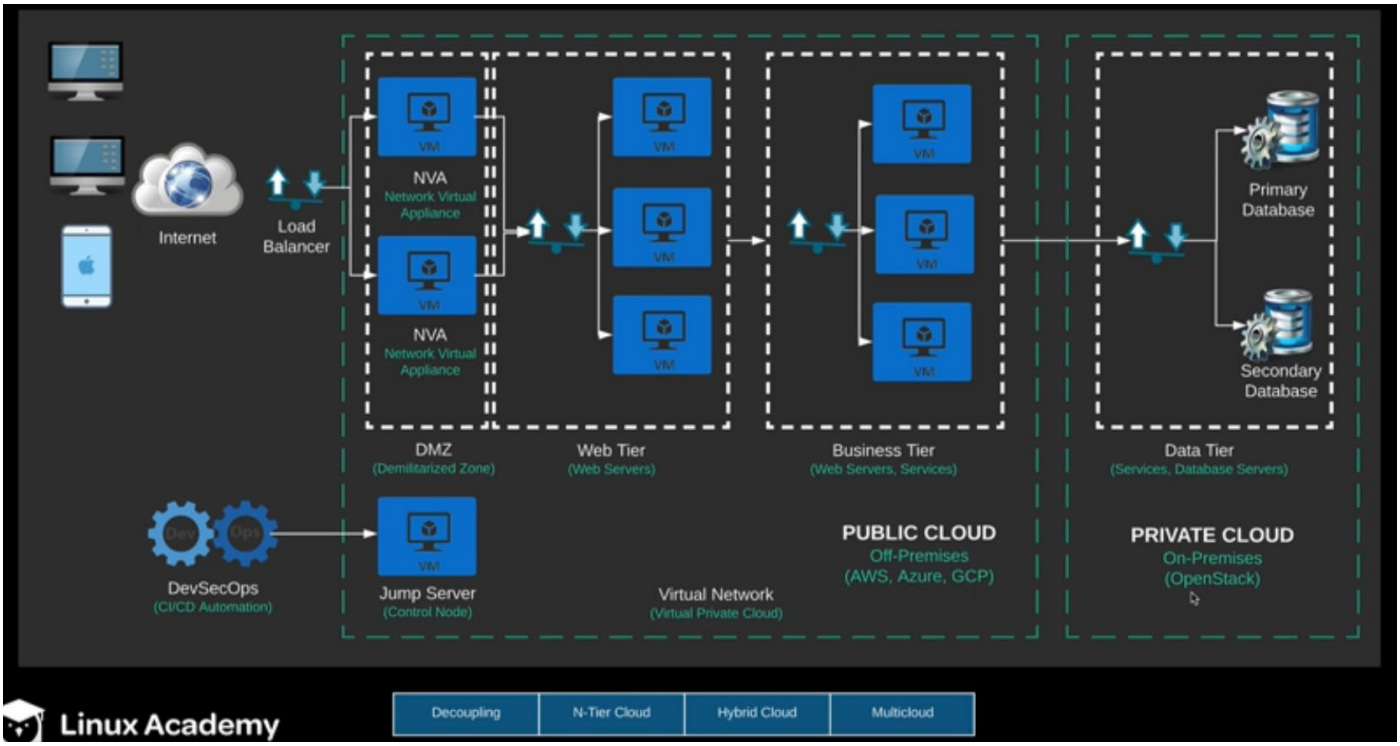
N-Tier architecture:



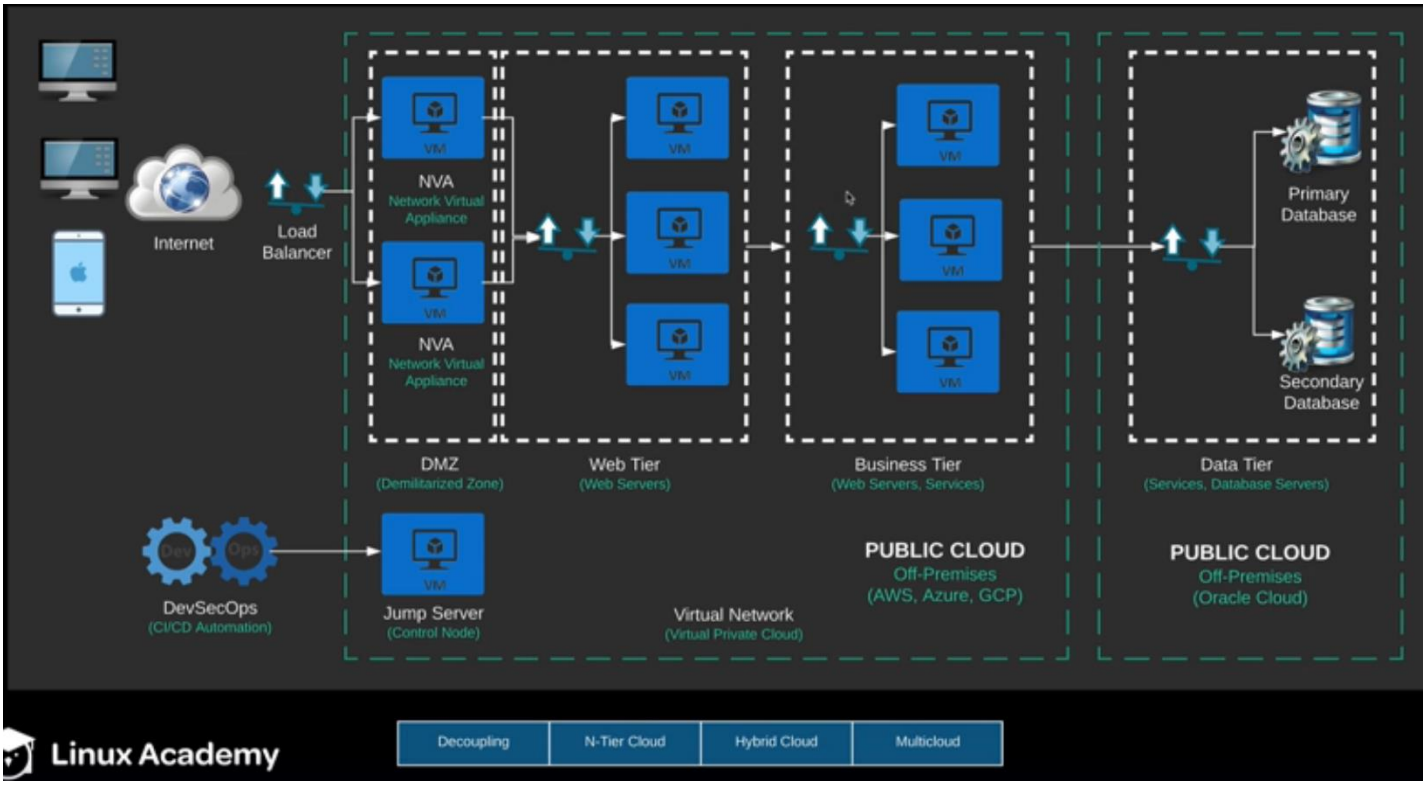

N-tier cloud architecture:



## Hybrid cloud architecture:




## Multi cloud architecture



# Data transport to Cloud:

**Data Transport**

**How Long Will It Take?**

*Number of days = (Total bytes)/(Megabits per second * 125 * 1000 * Network Utilization * 60 seconds * 60 minutes * 24 hours)*

**Challenges of Network-Based Transfer**
Transporting data over the network requires careful planning. To move 1 terabyte of data using a T1 connection would require 82 days!

**Unmanaged Data Migration**
Tools such as rsync, command line access to cloud storage such as S3, and utilities such as Amazon's Glacier command line interface are ways enterprises migrate data without third-party management.


**Managed Migration Services**
Migration services are also available from most cloud providers that include physical data transport, dedicated and redundant network links, and many other innovative approaches.

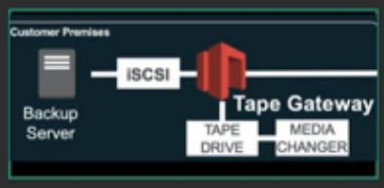
Linux Academy

| Transport | Examples | Replication Methods | Replication Value |
|---|---|---|---|

**Data Transport: Examples**

**Direct Connect**
Direct Connect interfaces are dedicated to wide area network links between on-premises data centers and the public cloud provider data centers. These connections bypass the internet and provide a private data link for replication or migration.

**Physical Data Transport**
Data transport services involve the duplication of data to offline devices such as SSDs (solid state drives) or data batteries that are physically transported to cloud data centers and then directly mounted to the cloud systems. AWS Snowball and AWS Snowmobile are examples of this approach.




**Cloud Storage Gateways**
Storage gateways are devices provided by public cloud providers that compress data, provide a storage area network (SAN) connection to cloud storage, and seamlessly integrate with virtual tape libraries and other backup methods.

Linux Academy

| Transport | Examples | Replication Methods | Replication Value |
|---|---|---|---|

## Data Replication Methods


**Basic Read-Only Replication**
A "master" database or data image is replicated to a "slave" site, and the slave image is only available to applications for read-only use.

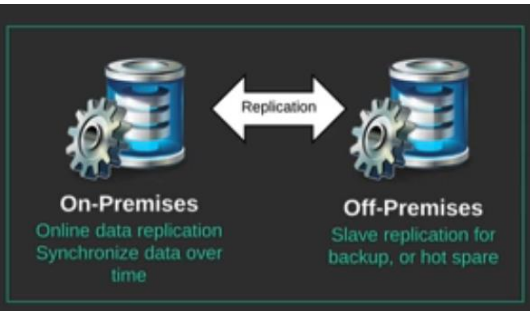
**Snapshot Replication**
A read-only snapshot of the live database is created, and then that snapshot may be used for subsequent duplication or ongoing read-only access.

**Transactional Replication**
Transactional replication is done as individual records are inserted or updated in the primary database. These transactions then commit the same data to a remote or cloud-based database that remains in sync with the master given network latency and time to complete the update.

**Data Synchronization**
This is a batch-style process and is time- and compute-intensive. This process compares a primary and secondary database and ensures all records match upon completion.



## Data Replication: Use Cases and Business Value



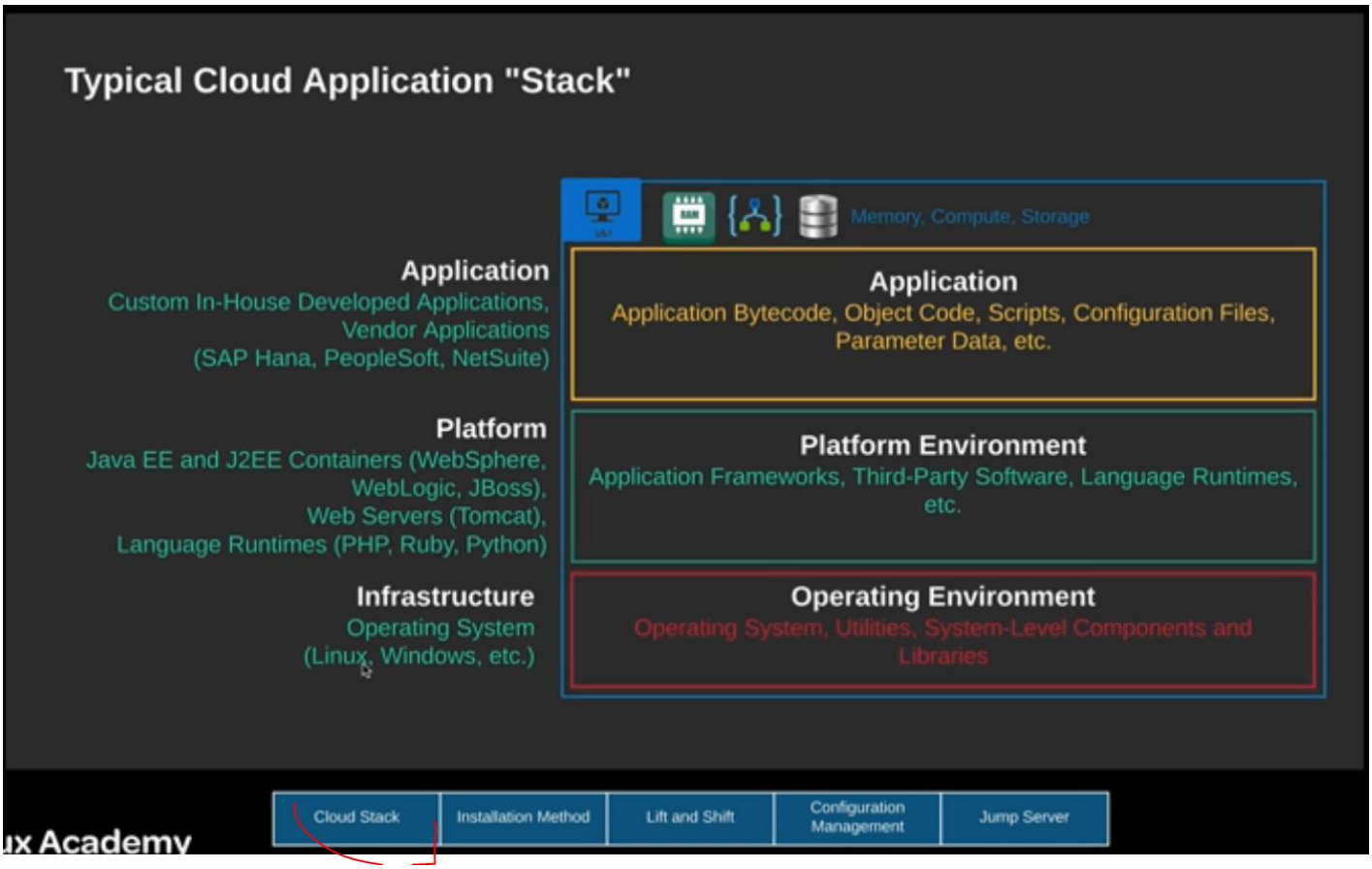

**Supplemental Transaction Systems**
Detecting and reacting to business events in real time. Oftentimes, supplemental transactions may be performed in the background.

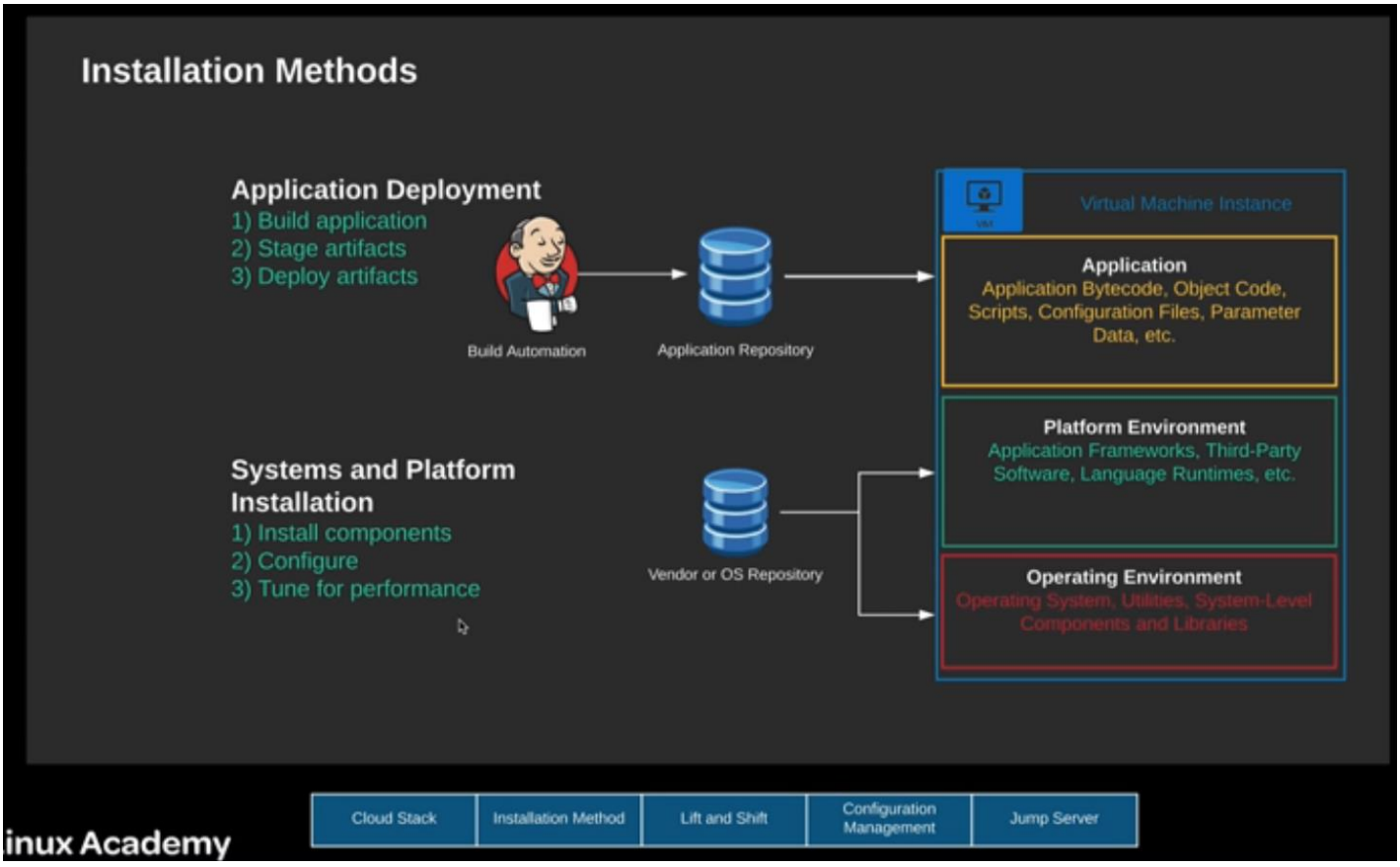
**Mobile Apps or Big Data Analytics Projects**
Up-to-the-minute data available to cloud-based applications, providing an increased scale of front-end users.

**Data Synchronization**
Master data management (MDM), data warehouses, analytical data marts, and mainframe environments may leverage synchronization for backup, alternative sourcing, or co-location for improved data proximity.

**Continuous Availability**
High availability, disaster recovery, and cross-site workload balancing all benefit from continuous replication. Fail-over recovery is made possible by having a hot spare always available.

# Typical cloud application ‘stack’

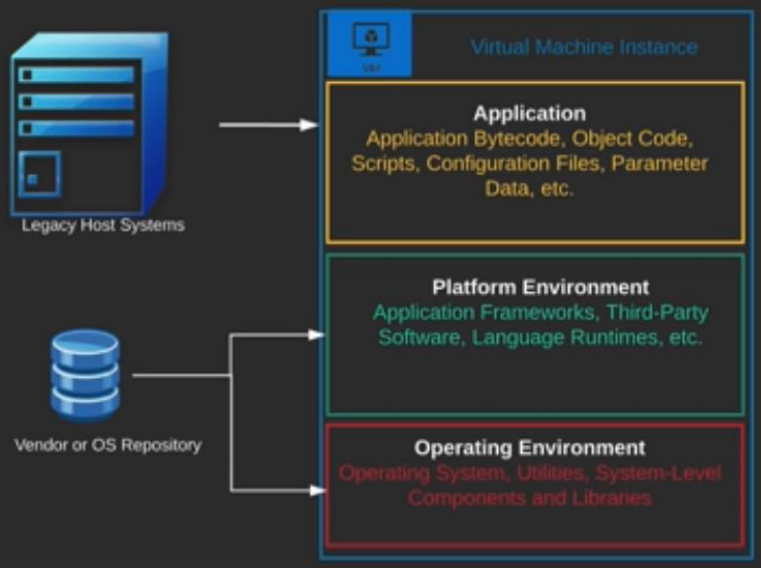


## "Lift and Shift"

**Simple Migration**
In some cases, when applications are older and thought to be stable, they can simply be copied from the legacy systems to the new virtual machines.

**Infrastructure and Platform**
The infrastructure and platform are typically deployed from vendor repositories to ensure ongoing support. The new environment is created to be as consistent as possible with the older legacy platforms.

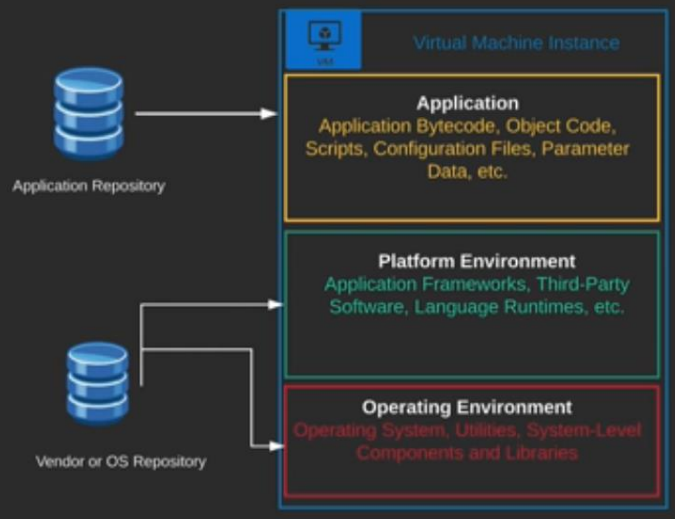


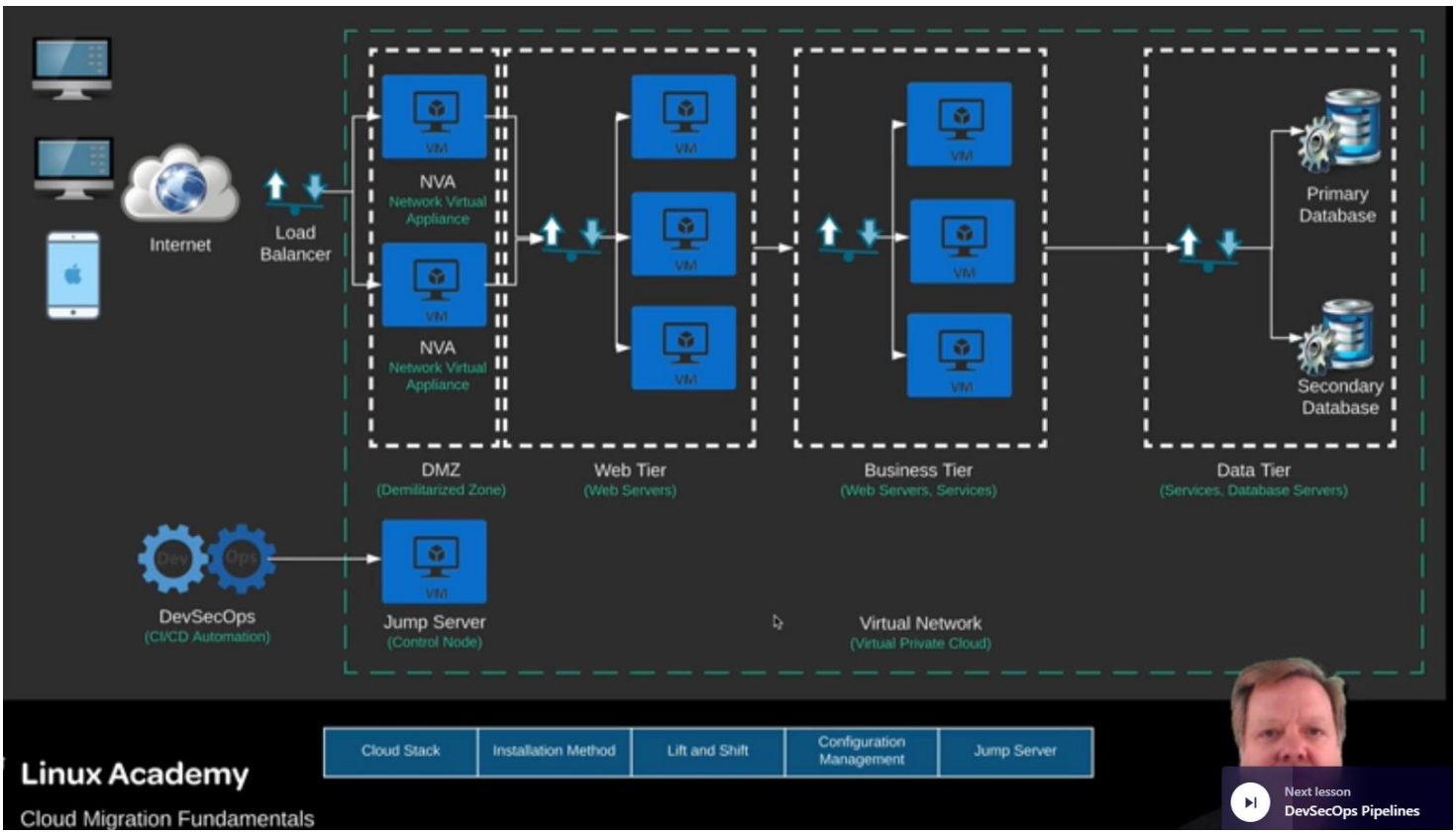



## Configuration Management

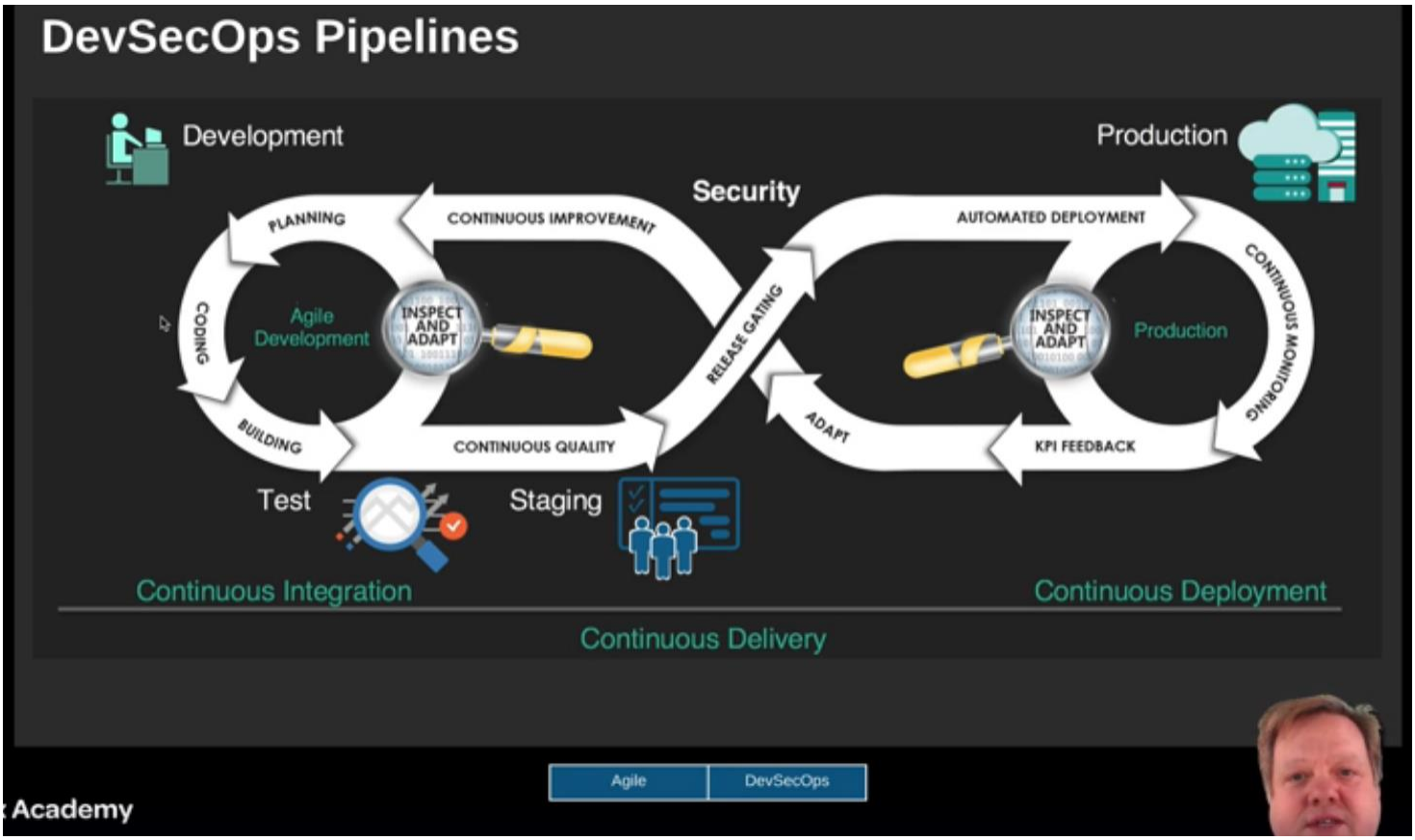
ANSIBLE

**Automated Deployment**
Tooling such as Ansible is used to run "playbooks" that contain "plays." Plays can instantiate virtual machines, install and configure infrastructure and platforms, and ultimately install and configure applications. Most importantly, they can run this in a uniform way across an entire "inventory" of systems.




Internet
Load Balancer
NVA
Network Virtual Appliance
NVA
Network Virtual Appliance
VM
Primary Database
Secondary Database
DMZ
(Demilitarized Zone)
Web Tier
(Web Servers)
Business Tier
(Web Servers, Services)
Data Tier
(Services, Database Servers)
DevSecOps
(CI/CD Automation)
Jump Server
(Control Node)
Virtual Network
(Virtual Private Cloud)
Cloud Stack
Installation Method
Lift and Shift
Configuration Management
Jump Server
Linux Academy
Cloud Migration Fundamentals
Next lesson
DevSecOps Pipelines

## DevSecOps:


DevSecOps Pipelines
Development
Production
Security
PLANNING
CODING
BUILDING
TESTING
CONTINUOUS IMPROVEMENT
Agile Development
INSPECT AND ADAPT
RELEASE GATING
CONTINUOUS QUALITY
AUTOMATED DEPLOYMENT
INSPECT AND ADAPT
Production
CONTINUOUS MONITORING
ADAPT
KPI FEEDBACK
Test
Staging
Continuous Integration
Continuous Deployment
Continuous Delivery
Agile
DevSecOps
Academy

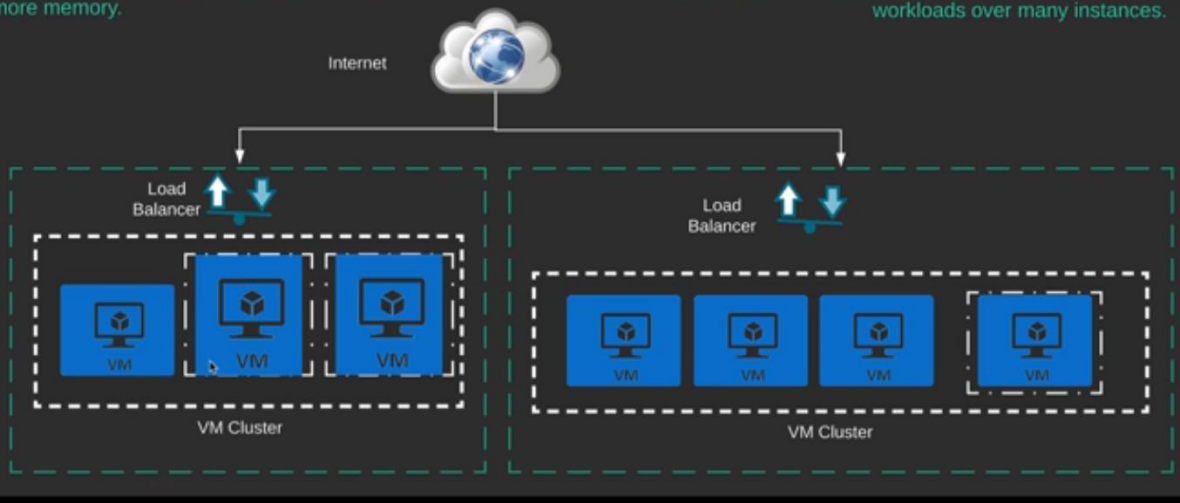
## Scaling Up or Scaling Out

**Scaling Up**

Scaling up is appropriate for applications that require more compute power and thus may be served by larger vCPUs and more memory.

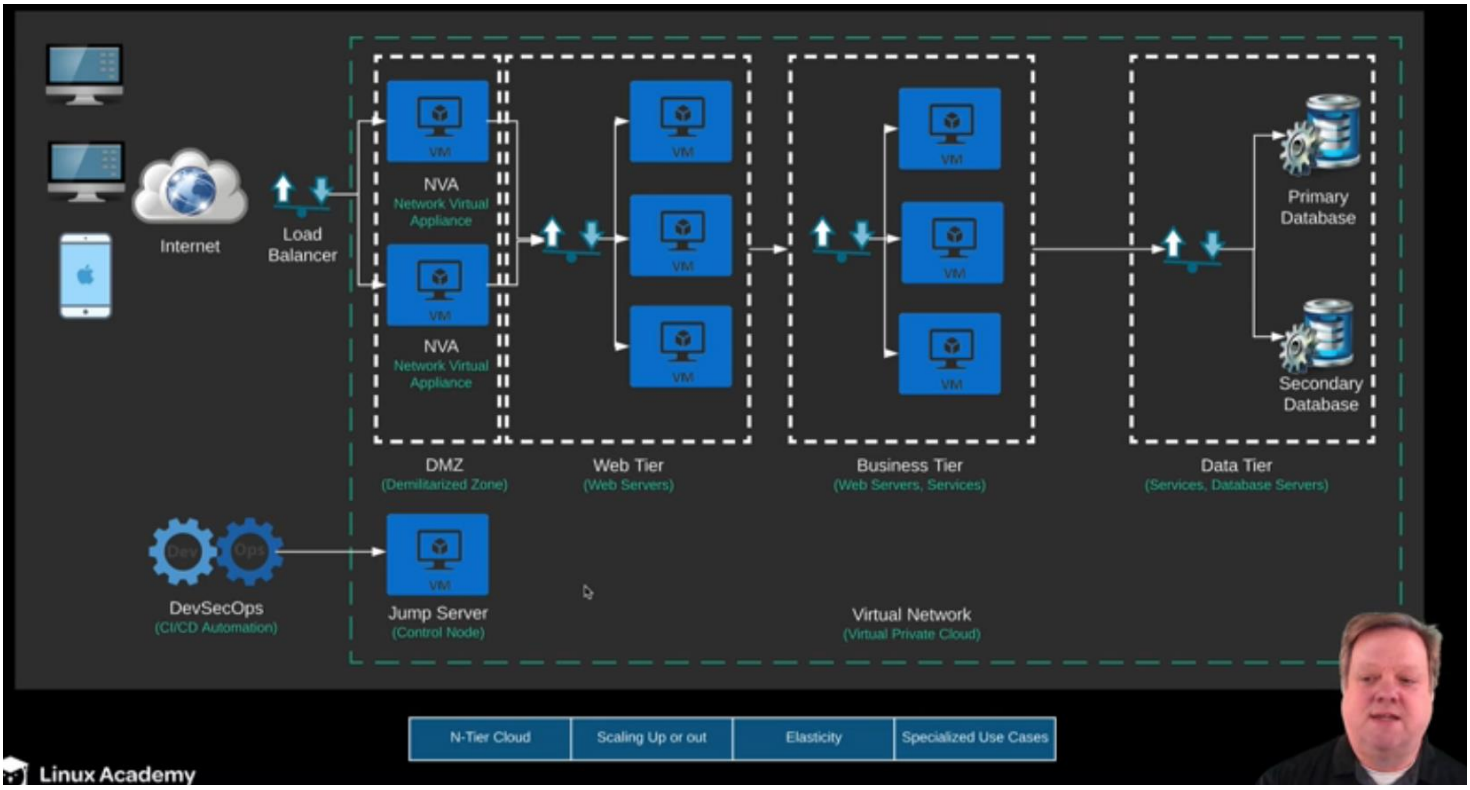
**Scaling Out**

Scaling out is appropriate when applications are highly modularized and can increase throughput by distributing workloads over many instances.




N-Tier Cloud | Scaling Up or out | Elasticity | Specialized Use Cases

Linux Academy




N-Tier Cloud | Scaling Up or out | Elasticity | Specialized Use Cases

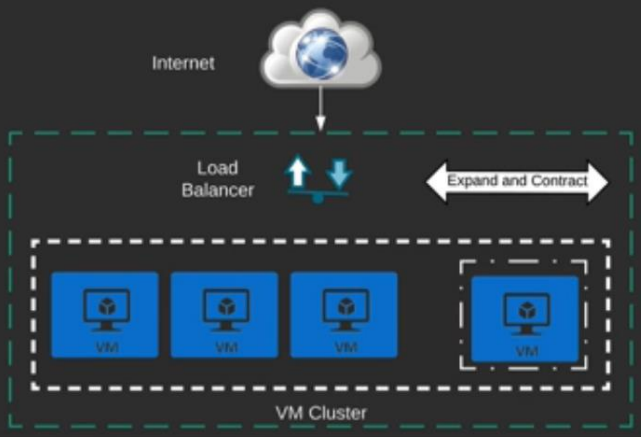
Linux Academy

# Elasticity

### Dynamic Expansion and Contraction
Since cloud providers utilize a pay-as-you-use model, it is important to expand cluster capacity dynamically when needed, but also allow it to contract when the added power and storage is not required. This is the elastic nature of cloud infrastructure and is key to realizing the cost advantages of cloud computing.

### Server Sprawl
Many on-premises data centers have had to size web farms and server clusters for the maximum workload at peak times. This is because it takes time to buy, install, and configure new servers. It also required deploying applications. Even when automated, this is time-consuming and costly, leading to waste. Cloud providers have servers already installed waiting to be utilized, which allows clients to vacate instances on demand whenever advantageous.

### Containers and Kubernetes
The use of technologies, such as containerization, and container orchestration, such as Kubernetes, makes the process of scaling workloads and taking advantage of elasticity quite feasible from a process perspective.




N-Tier Cloud | Scaling Up or out | Elasticity | Specialized Use Cases

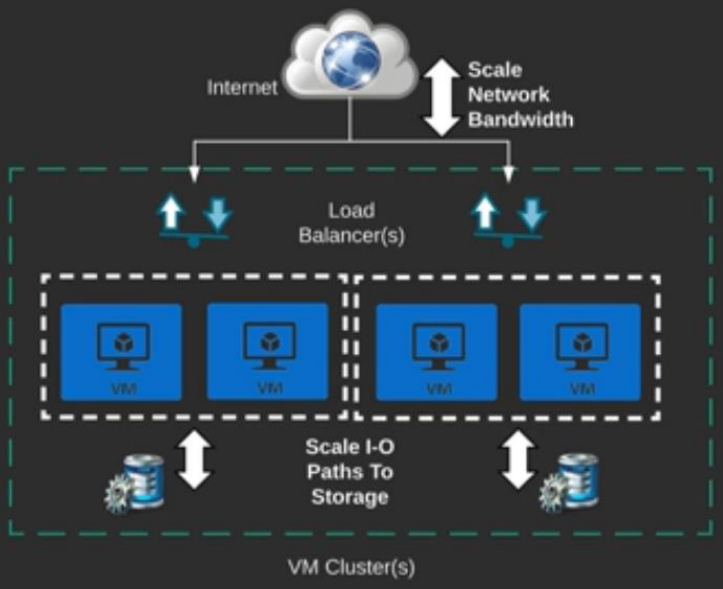
Linux Academy

# Specialized Use Cases
While micro-services architectures are advantageous for most business applications, there are special use cases that require other forms of scaling.

### Network-Dependent Applications
When bandwidth is the primary driver of transactional or computational throughput, it is appropriate to scale the network connections and load balancers. Excess compute or storage in these cases is costly. In some cases, additional clusters with redundant or segmented load balancing may be in order.

### Data-Dependent Applications
The input/output transfer rate to storage can also be a bottleneck, limiting transactional or network resources. So entire architectures have to be scaled to ensure that resources remain balanced or tuned for maximum efficiency.

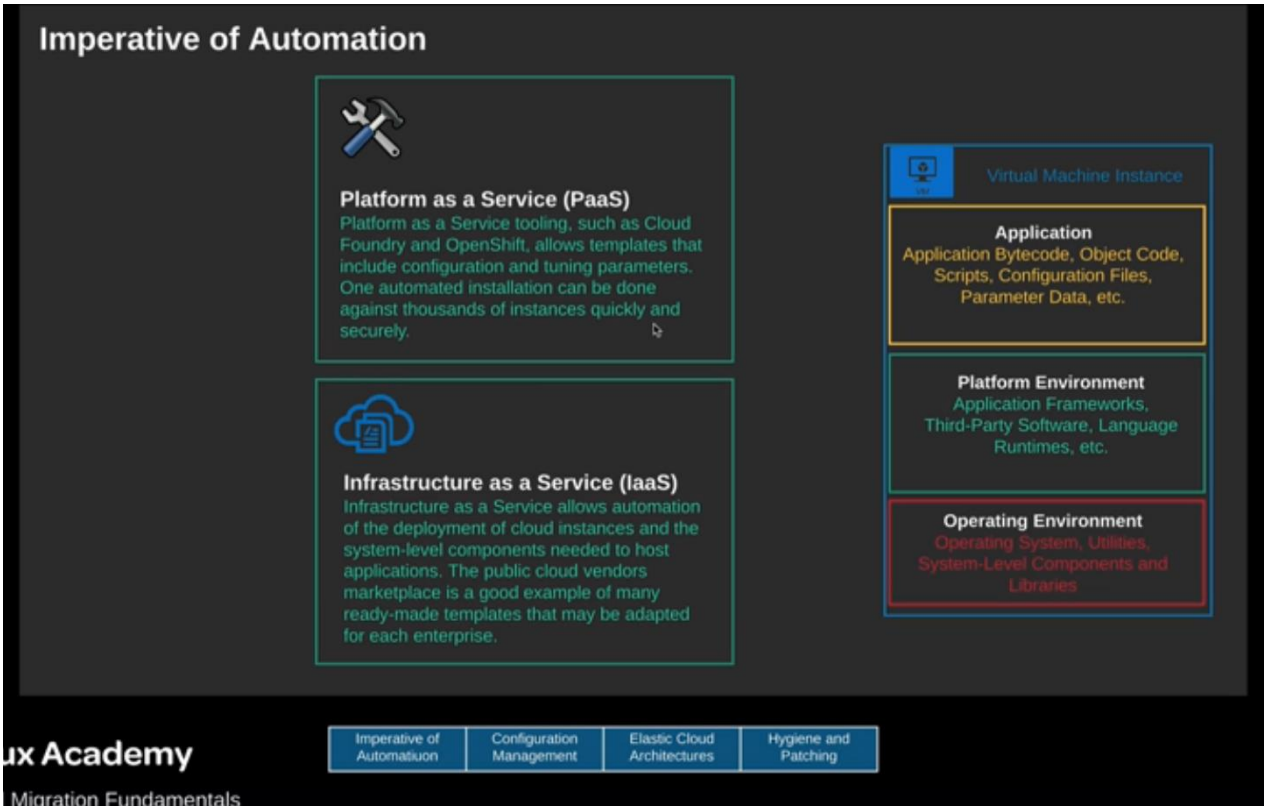
### Compute-Intensive Applications
Compute-intensive applications, such as machine learning or analytics processes, may require many vCPU cores or even GPU processors to scale adequately.

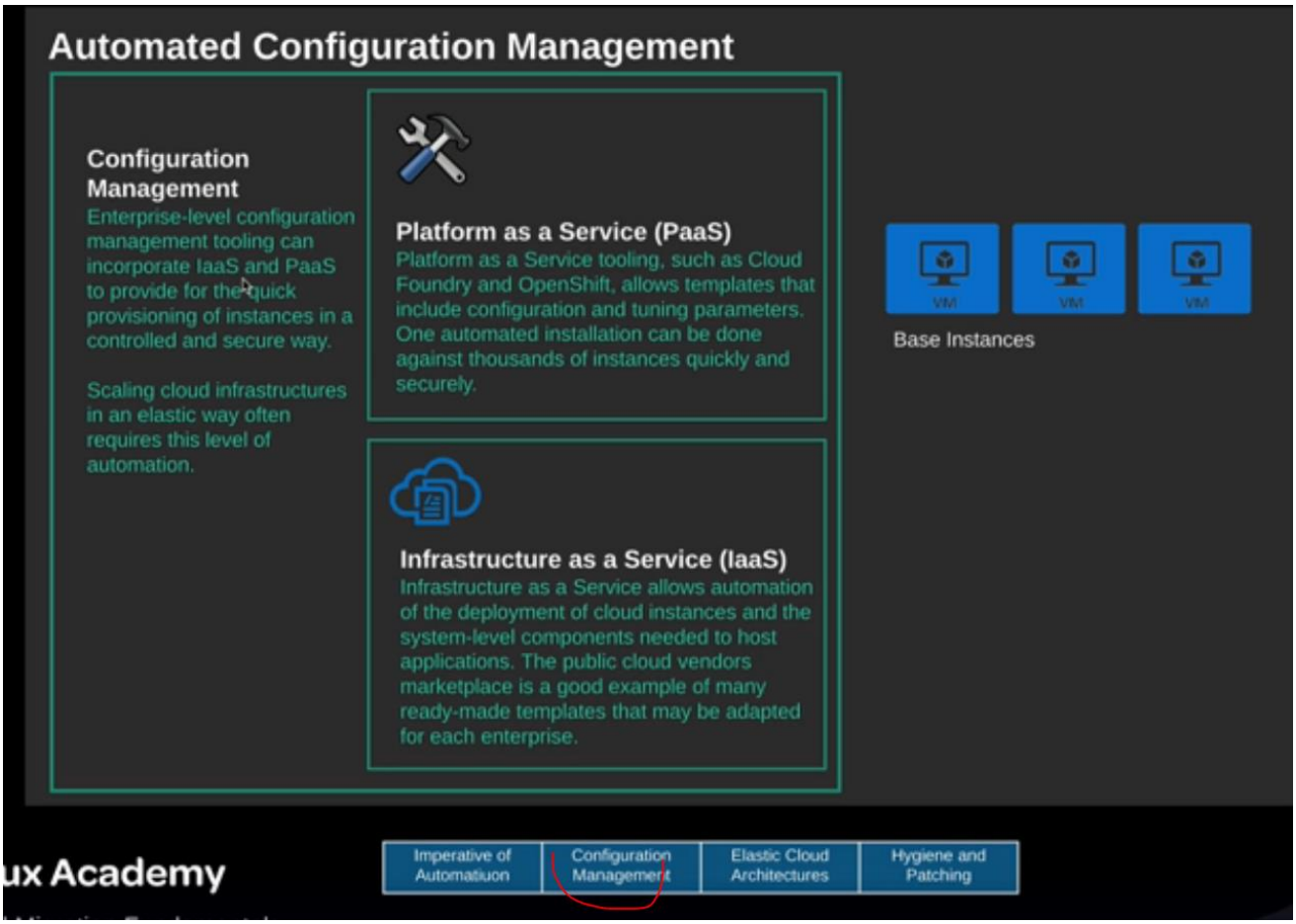



N-Tier Cloud | Scaling Up or out | Elasticity | Specialized Use Cases

cademy

Automation:


Imperative of Automation
Platform as a Service (PaaS)
Platform as a Service tooling, such as Cloud Foundry and OpenShift, allows templates that include configuration and tuning parameters. One automated installation can be done against thousands of instances quickly and securely.
Infrastructure as a Service (IaaS)
Infrastructure as a Service allows automation of the deployment of cloud instances and the system-level components needed to host applications. The public cloud vendors marketplace is a good example of many ready-made templates that may be adapted for each enterprise.
Virtual Machine Instance
Application
Application Bytecode, Object Code, Scripts, Configuration Files, Parameter Data, etc.
Platform Environment
Application Frameworks, Third-Party Software, Language Runtimes, etc.
Operating Environment
Operating System, Utilities, System-Level Components and Libraries
ux Academy
Migration Fundamentals
Imperative of Automatiuon
Configuration Management
Elastic Cloud Architectures
Hygiene and Patching


Automated Configuration Management
Configuration Management
Enterprise-level configuration management tooling can incorporate IaaS and PaaS to provide for the quick provisioning of instances in a controlled and secure way.
Scaling cloud infrastructures in an elastic way often requires this level of automation.
Platform as a Service (PaaS)
Platform as a Service tooling, such as Cloud Foundry and OpenShift, allows templates that include configuration and tuning parameters. One automated installation can be done against thousands of instances quickly and securely.
Infrastructure as a Service (IaaS)
Infrastructure as a Service allows automation of the deployment of cloud instances and the system-level components needed to host applications. The public cloud vendors marketplace is a good example of many ready-made templates that may be adapted for each enterprise.
VM
VM
VM
Base Instances
ux Academy
Imperative of Automatiuon
Configuration Management
Elastic Cloud Architectures
Hygiene and Patching

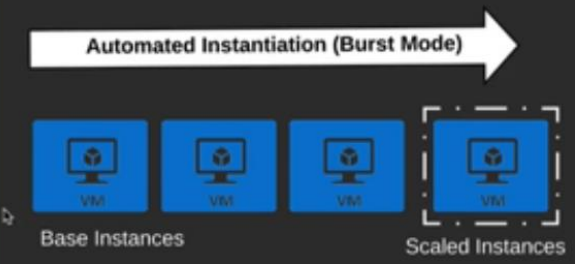
# Elastic Architectures

**Configuration Management**
Enterprise-level configuration management tooling can incorporate IaaS and PaaS to provide for the quick provisioning of instances in a controlled and secure way.

Scaling cloud infrastructures in an elastic way often requires this level of automation.

**Platform as a Service (PaaS)**
Platform as a Service tooling, such as Cloud Foundry and OpenShift, allows templates that include configuration and tuning parameters. One automated installation can be done against thousands of instances quickly and securely.

**Infrastructure as a Service (IaaS)**
Infrastructure as a Service allows automation of the deployment of cloud instances and the system-level components needed to host applications. The public cloud vendors marketplace is a good example of many ready-made templates that may be adapted for each enterprise.




**Using Cloud Elasticity to Burst Throughput**

Cloud systems are useful when organizations need to scale compute, storage, and throughput for peak volumes. Retailers, card providers, and other transactional businesses involved in Black Friday often burst into clouds for added capacity.



# Containerization vs. Virtualization

**Virtual Machines**

Virtual machines run a host OS, and a hypervisor facilitates the installation and running of guest virtual servers. Each guest server has its own operating system instance and libraries. Applications on each virtual server rely on the guest OS system instance and library versions.

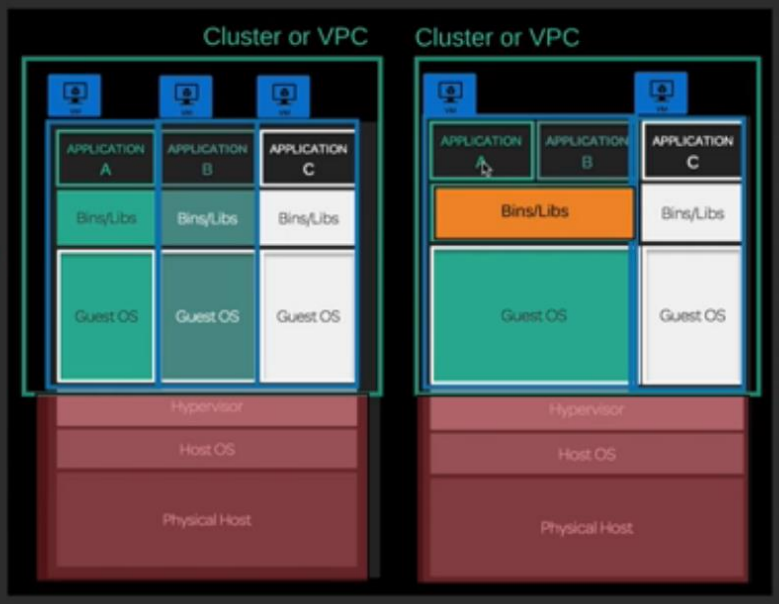

**Containers**

Containers rely on isolation techniques like control groups and namespaces to separate applications. They do not have a hypervisor and can share libraries if needed. Containers share the physical host's kernel, so they do not require an operating system. Container systems have processes in place to prevent a container from making potentially dangerous changes to the kernel.

# Cloud Containerization

## Virtual Machines

The public cloud provider provides the physical hardware and the host operating system and hypervisor. Each instance is its own virtual machine and shares the allocated physical resources.




## Containers

Containers in the cloud still rely on the virtual machine instance provided by the cloud provider, but containers allow more application workloads to be aggregated onto a single instance. This can be a huge money saver if multiple containerized applications can be run together on the same instance without scaling up to a larger cloud instance. Eliminating one of the guest operating systems makes the system cheaper and more efficient.

Containerization | Cloud Containerization | Container Orchestration

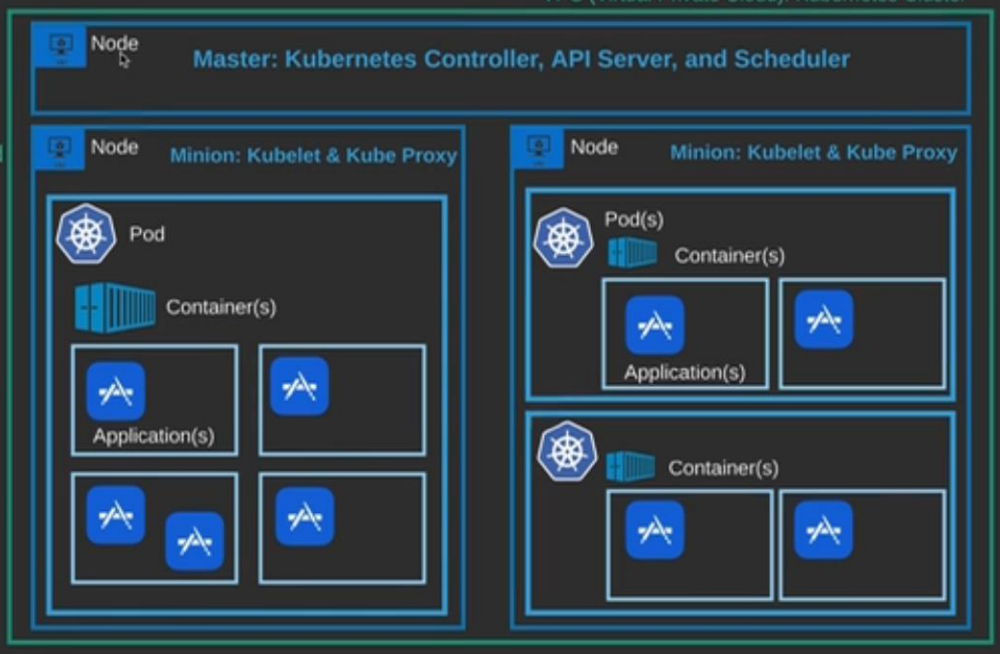
# Container Orchestration

## Kubernetes

Kubernetes has become the de facto standard for cloud orchestration. Invented and open-sourced by Google, Kubernetes allows enterprises to maintain massive cloud infrastructures and the applications that run on them.

## Kubernetes Benefits

There are many benefits to using Kubernetes, including enhanced security, self-healing environments, the ability to scale and optimize environments automatically, and the ability to deploy rolling updates.




Containerization | Cloud Containerization | Container Orchestration

Academy

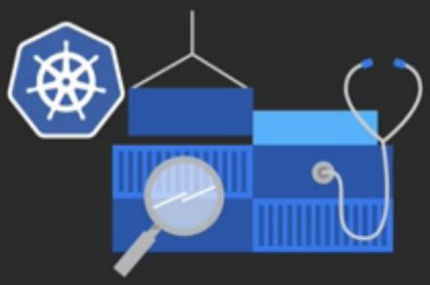
# Monitoring and Auditing Resources:


# Self-Healing Infrastructure

**High Availability**
High availability systems are the norm where no single instance causes the overall system to be down.

**Parallelism and Redundancy**
Massively parallel systems and redundancy increase throughput and allow individual instances to fail without compromising the overall system.

**Business Continuity**
Automated rollback and recovery allows thousand of instances of an application to be vacated, upgraded, and reinstantiated in a rolling update manner, avoiding any downtime.



**Automatic Workload (Re)Instantiation**
Container orchestration systems such as Kubernetes monitor application workloads and control the cluster. The controller and scheduler is able to vacate and reinstantiate workload instances upon failure or on demand. The scheduler is also able to scale instances based on throughput requirements and ensure capacity demands are met in an elastic infrastructure.

Log Management | Security Analytics | Self-Healing Infrastructures

Twelve Factors Apps: https://12factor.net/

# The Twelve-Factor App

## Introduction

In the modern era, software is commonly delivered as a service: called *web apps*, or *software-as-a-service*. The twelve-factor app is a methodology for building software-as-a-service apps that:

- Use **declarative** formats for setup automation, to minimize time and cost for new developers joining the project;
- Have a **clean contract** with the underlying operating system, offering **maximum portability** between execution environments;
- Are suitable for **deployment** on modern **cloud platforms**, obviating the need for servers and systems administration;
- **Minimize divergence** between development and production, enabling **continuous deployment** for maximum agility;
- And can **scale up** without significant changes to tooling, architecture, or development practices.

The twelve-factor methodology can be applied to apps written in any programming language, and which use any combination of backing services (database, queue, memory cache, etc).

## Background

The contributors to this document have been directly involved in the development and deployment of hundreds of apps, and indirectly witnessed the development, operation, and scaling of hundreds of thousands of apps via our work on the Heroku platform.

This document synthesizes all of our experience and observations on a wide variety of software-as-a-service apps in the wild. It is a triangulation on ideal practices for app development, paying particular attention to the dynamics of the organic growth of an app over time, the dynamics of collaboration between developers working on the app's codebase, and avoiding the cost of software erosion.

Our motivation is to raise awareness of some systemic problems we've seen in modern application development, to provide a shared vocabulary for discussing those problems, and to offer a set of broad conceptual solutions to those problems with accompanying terminology. The format is inspired by Martin Fowler's books *Patterns of Enterprise Application Architecture* and *Refactoring*.