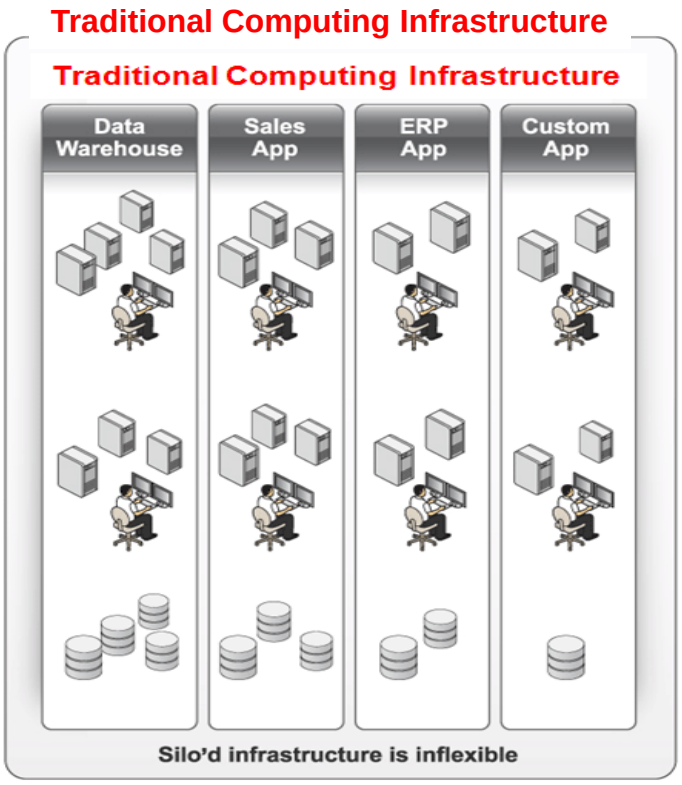
ORACLE®

Deploying a Geospatial Cloud

Traditional Public Sector Computing Environment



- Silos of dedicated hardware and software
- Single application per silo
- Expensive to size for peak load
- Difficult to scale
- Expensive to manage

NIST Definition of Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model promotes availability and is composed of:

5 Essential Characteristics
- On-demand self-service
- Resource pooling
- Rapid elasticity
- Measured service
- Broad network access

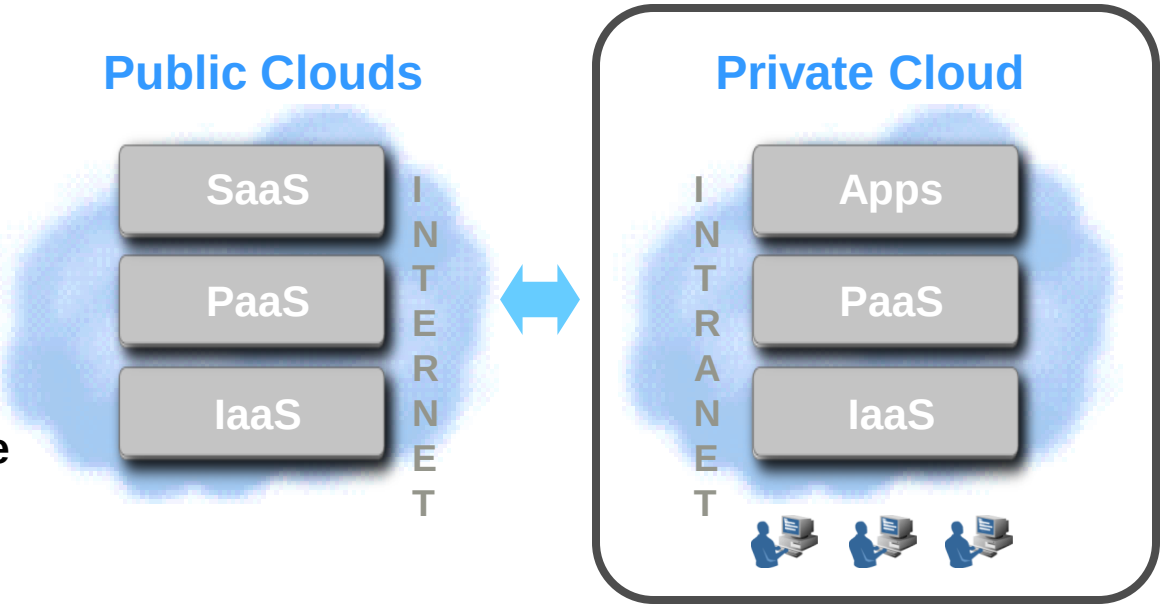
3 Service Models
- SaaS
- PaaS
- IaaS

4 Deployment Models
- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Source: NIST Definition of Cloud Computing v15

Public Clouds and Private Clouds

- Used by multiple tenants on a shared basis
- Hosted and managed by cloud service provider



- Exclusively used by a single organization
- Controlled and managed by in-house IT

Trade-offs

Lower *upfront* costs	⟷	Lower *total* costs
Outsourced management	⟷	Greater control over security, compliance, QoS
OpEx	⟷	CapEx & OpEx

Enterprises will adopt a mix of public and private clouds

Why a Cloud Framework Make Sense

- Reduced Cost
  Cloud technology is paid incrementally, saving organizations money.
- Increased Storage
  Organizations can store more data than on siloed computer systems.
- Flexibility
  Cloud computing offers much more flexibility than past computing methods.
- More Mobility
  Employees can access information wherever they are, rather than having to remain at their desks.
- Highly Automated , Allows IT to Shift Focus
- No longer do IT personnel need to worry about keeping software up to date
  No longer having to worry about constant server updates and other computing issues, government organizations will be free to concentrate on innovation.

3 Cloud Computing Concepts

- Application as a Service
  - End user apps delivered as service
  - Example: Google Earth
- Platform as a Service
  - Application platform middleware for developers to develop and deploy custom apps
  - Example: Oracle Public Cloud
- Infrastructure as a Service
  - Hardware and technology for computing power, storage, operating systems available for customer apps
  - Example: Amazon EC2, Amazon S3, Oracle Public Cloud

Welcome to the

Oracle Public Cloud

An Enterprise Cloud for your Business

Notify Me of Updates

Application Services

Fusion CRM
Sell smarter with Fusion CRM in the cloud.

Fusion HCM
Bring power to your people with Fusion HCM.

Social Network
A secure collaboration tool for everyone you work with.

Platform Services

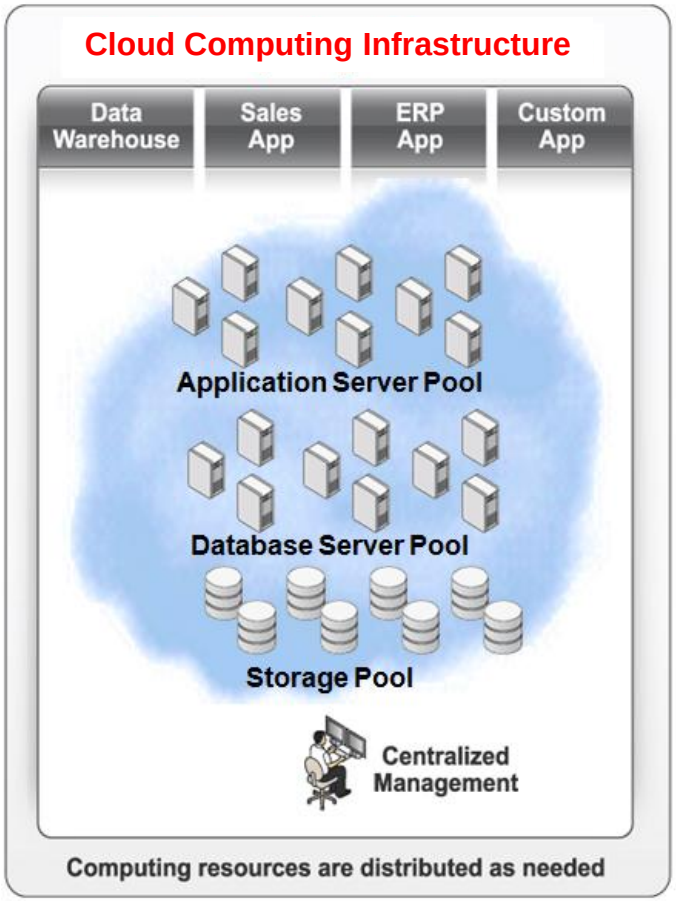
Java
All the productivity of Java, without the IT.

Database
The Oracle database you love, now in the cloud.

For information about Oracle's other offerings for cloud computing, go to oracle.com/cloud

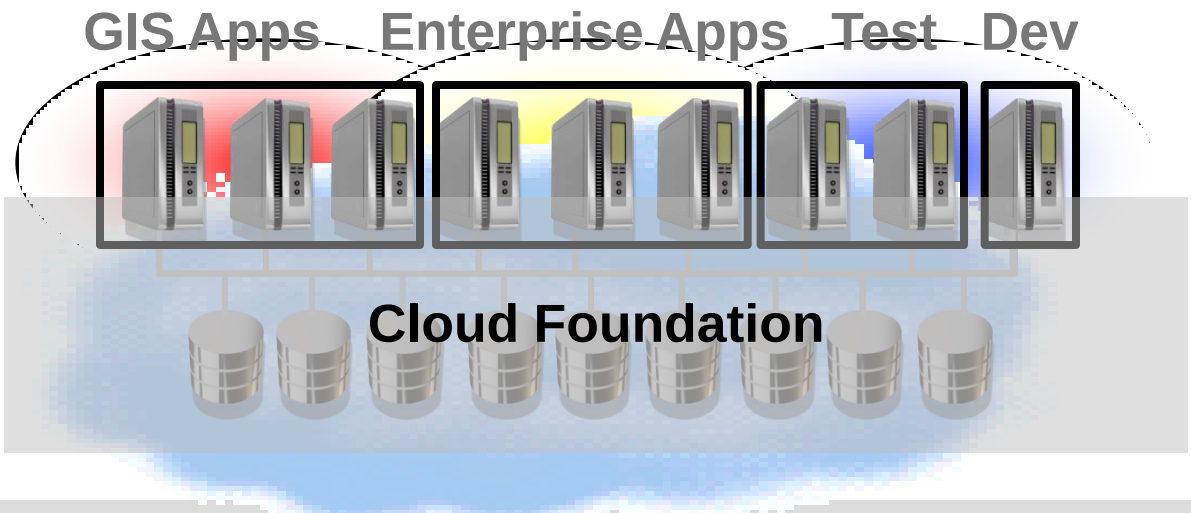
Characteristics of Cloud Frameworks

- Multi-tenanancy
- Rapid provisioning
  - Add Resources in Real TIme
- Elasticity
  - Terabytes, Petabytes
- Automated QoS
- Pay-for-use pricing



Can be deployed in a physical or virtual environment

Cloud Platform Framework for GIS



- Application Server: SOA, Identity Management, OGC Web Services, Geocoding, Routing, Java and XML Frameworks, Process Execution, Portals; Java, XML, C, and .Net APIs
- Spatial Database:ISO/OGC-compliant. Native Raster, 3D/LiDAR, Planar and Network Topology. Coordinate Transformation, Spatial indexes, functions, and operators.
- Massively parallel, highly available and scalable processors and storage

Moving Toward Simplified Pricing Models

Simple monthly based subscription

Multiple tiers with growth option

Elastic consumption model grow and shrink as needed

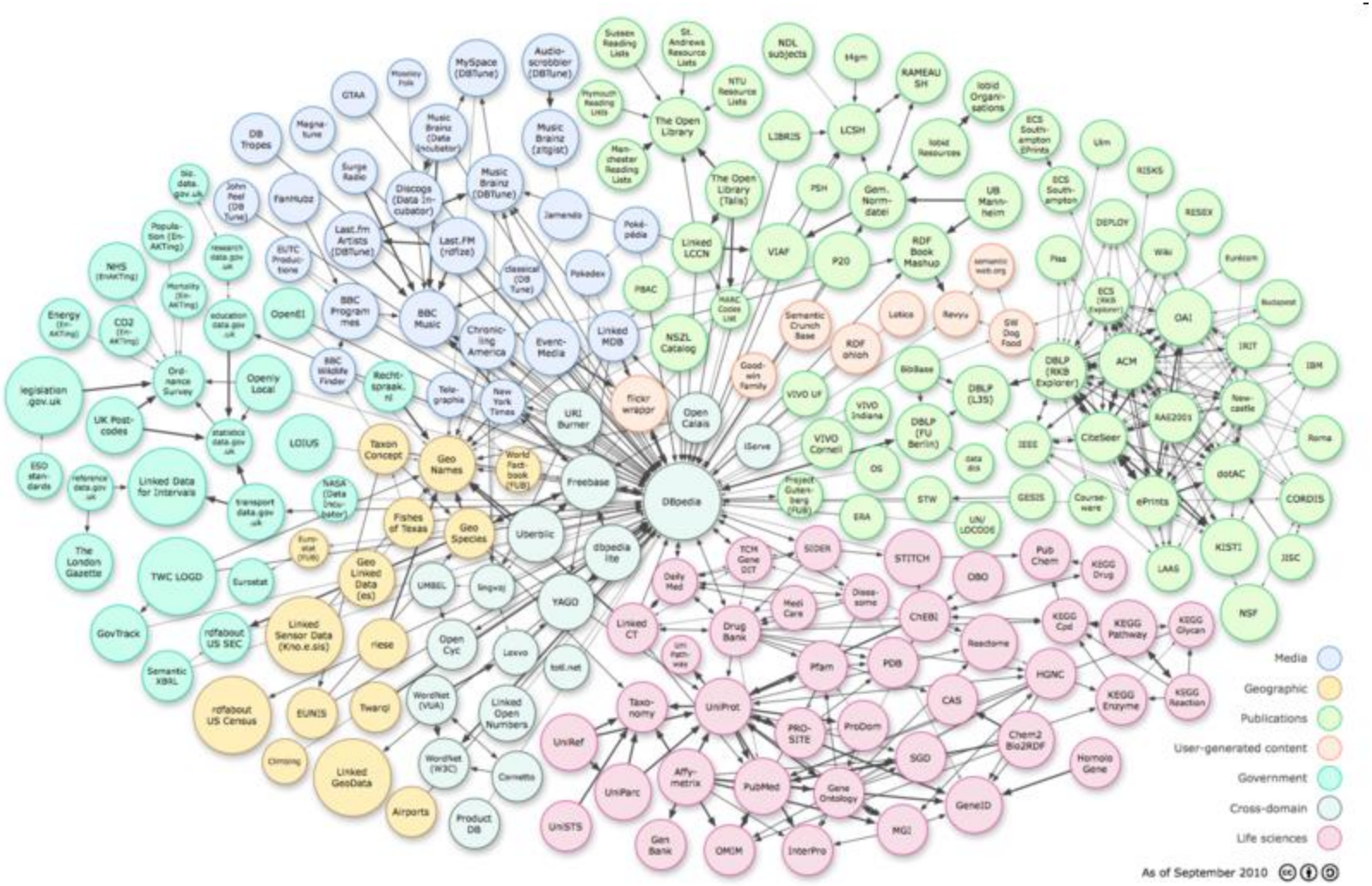
Some Cloud Security Concerns:

- Data Storage
- Data Transfer
- Data Privacy
- Identify Management
- Vulnerability Management
- Application Security
- Personnel and Physical Security
- Liability and Recourse

A Cloud is More than Just Technology…

- Shared Infrastructure
- Common Geospatial Data, Services, and Applications
- Governance Structure – Policy and Operations
- Geospatial Information Portfolio Management (Data agreements, licensing)

Linking with other Services and Clouds



Leveraging Semantic Web

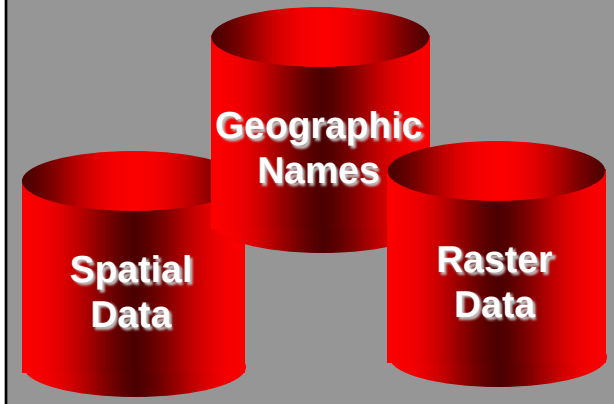
Application Ontologies

Environmental Monitoring

Famine Relief

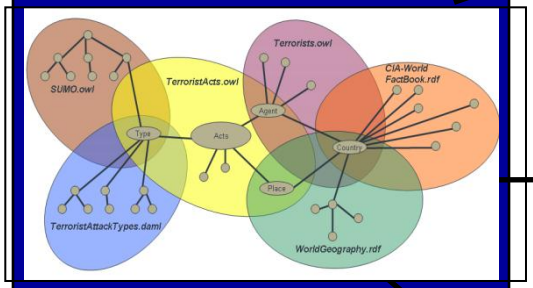
Disaster Response

National Mapping Private Cloud



- Simple Features
- GeoRaster
- Topology
- Networks
- Gazeteers
- …

RDF & OWL Metadata

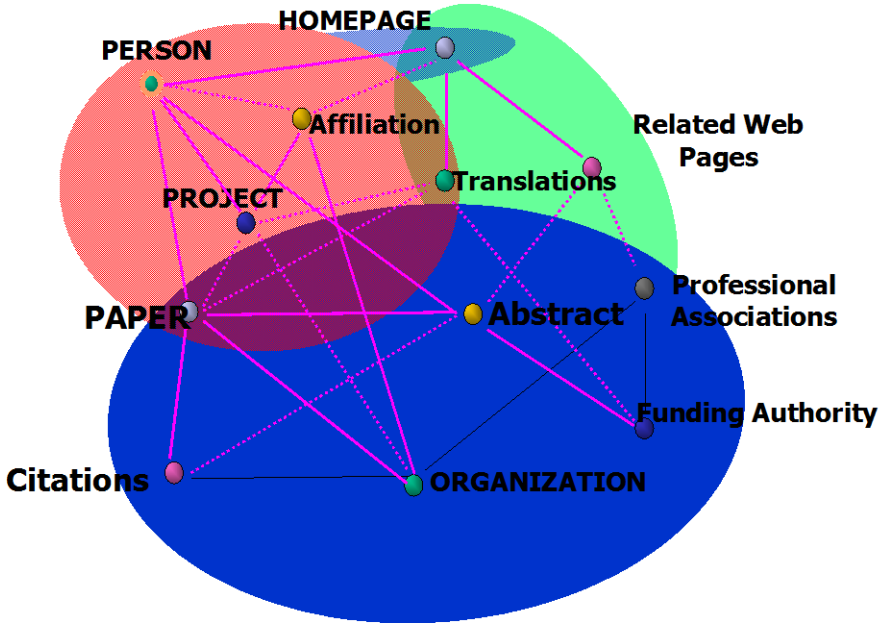


- Data Integration
- National Map schemas
- Geographic names
- Temporal
- Naïve Geography
- …

It's Not Just about "Linking"

- Integrate domains of knowledge through common vocabularies (ie SKOS)
- Manage relationships between collections of images and associated metadata
- RDF as flexible and extensible data model supports powerful search and end-user discovery of related content
- Rich platform for data integration, data repurposing, and better quality control and classification

Semantic Aggregation & Navigation of Data



Best Practices for Cloud Deployment

Best Practices 1*

- Licensing:
  - Ensure you use use cases are covered
  - Consider service spikes, high availability, etc.
- Data Transfer Costs:
  - Understand internal and external traffic costs of your overall service
  - When possible, make sure data transfer costs are internal to the cloud provider
- Latency:
  - Understand latency requirements of your app
  - Clouds are not ideal for low-latency operations

* Source: Jim Liddle, WebSphere Journal, Sept. 29, 2009

Best Practices 2

- State
  - Check if your cloud provider persists data
  - Ex: Amazon EC2 persistent storage, Oracle do
  - How will back-ups be initiated in system crash?
- Data Regulations
  - Data in the cloud may be breaching national data laws depending where your data is stored
  - Some providers allow you to specify where in the world to store data

Best Practices 3

- Compliance
  - National regulations may prevent some apps from being hosted on cloud (eg. Patriot Act)
  - National Compliance may even extend to the software/hardware components used by cloud provider and its partners
- Quality of Service
  - QoS encompasses scaling, reliability, service fluidity, monitoring, management and system performance
  - Ensure that monitoring tools are in place to track compliance with service level agreements

Best Practices 4

- Security
  - Understand security policy and technologies
  - Topics include: encryption, authentication, authorization, intrusion detection, etc.
- System Hardening
  - Ensure system is secure, robust, and achieves the necessary functional requirements
- Dependencies
  - Check dependencies of your service provider
  - If cloud provider A is dependent on service B, what happens if service B is disrupted?

http://otn.oracle.com