Department of Homeland Security - “Cloud First”

By: Sarang Patel, Eddierick Preza, Sean Ulep

The Problem at Hand

Department of Homeland Security is attempting to have 12 cloud service offerings. The private cloud is expected to greatly increase delivery time of many services. Processes that take up to normally six months will be completed in a single day!

Our primary goal is to create this cloud service and submit a proposal on what should be prioritized as well as explain (to the best of our ability) optimization.

The cloud in terms of the government

- “Cloud” is a broad term in Fed Govt. and refers to any technology utilized from an outside vendor
- Cloud models
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- To use the term “cloud”, according to NIST has to have:
  - Broad network access
  - Measured service
  - Resource pooling
  - On-demand service
  - Rapid elasticity

Cloud overview

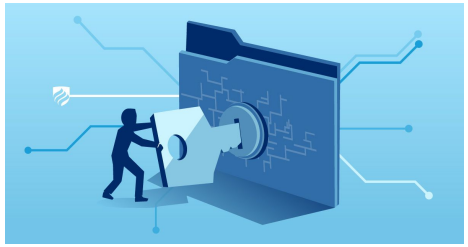
- Cloud types
  - Public
    - Pros: Scalability, low overhead cost, no capital cost
    - Cons: Decreased security, not easily customizable
  - Private
    - Pros: Increased security, completely customizable
    - Cons: High capital costs, high overhead costs
- “Cloud First” Policy
  - Effort to become more operationally efficient by embracing shared services
  - Governmental agencies must prioritize web-based services and applications

Department of Homeland Security

- Department of Homeland Security (DHS)
  - Specialization in cyber security
  - Terrorist Attacks
  - Defend America’s borders

- Implement “Cloud First” policy to reduce their server provisioning time
  - By use of on-demand testing and app management
  - Data will be shared on a private cloud

Security



- “Cloud First” policy speeds things up, but at the same time it puts the organization more at risk
  - Cloud First
  - Data leakage
  - Data must be encrypted and also monitored by government or other agency
- Take a risk-based approach
  - Prioritize data protection at all layers. (Network,physical-infrastructure,etc)
- Private Cloud is more secure than a Public Cloud
  - Ensures that only certified users have access to data

Data Protection

- Modern Identity, Credential, and Access Management (ICAM)
- Log data continuously provided
- Immediately informed when cybersecurity incident/event occurs
- Utilization of Federal Risk and AUthorization Management Program
  - FedRAMP
  - Provides security approach
  - Allows providers to demonstrate meeting Federal security requirements
  - Authorized cloud providers for use by the government

Benefits of testing in the cloud

- Customization
  - Several scenarios and variables can be simulated such as different hardware
  - Multiple instances of the same software can be run concurrently
- Scalability
  - Easy to scale up/down depending on required resources
  - Fluctuates based on testing demand
- Availability
  - Internal resources are shared to entire organization
  - Collaboration is intensified
  - Access can be strictly controlled as well as permissions
- Recovery
  - Data backups are easy and can run automatically via scripts
  - Easy to roll back a change if need be
    - If testing breaks the code, it can still be recovered

Speeding Up Provisioning Time!

- Create scripts to automate the following:
  - IP configuration
  - DNS configurations
  - Backup configuration
  - Rapid Deployment
  - Automation
- Template that contains a pre-configured OS and applications must be made so it can be built upon with more features
- Linking an automatic payment system with a billing portal in order to add more servers with the correct applications and basic resource configuration made

Must HAVES for Cloud Optimization

- Cost
  - Considered the most important of the four
  - Monitoring tools helps prevent too much of a price problem (so long as they are effective)
  - The issue: third party tools/methods are needed
- Performance
  - Dependent on architecture design, aka working on network latency and bottlenecks
  - Regularly test the performance in order to ensure quality
- Reliability
  - Prevents a company from deploying multiple instances across multiple regions in order to solve a single workload
- Sustainability
  - Pre-event awareness
  - Post-event awareness

Proposal

- Procurement
- Contractual agreement for operating methods
- Service Level Agreements (SLA)
- Security Requirements

Sources

- https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cloud-first-policy--121910.html
- https://www.herdingcoders.com/blog/how-cloud-can-speed-up-product-development-time/
- https://www.simplilearn.com/cloud-first-strategy-article#:~:text=Cloud%2Dfirst%20strategy%20is%20an,services%20over%20legacy%20IT%20systems
- https://spot.io/resources/cloud-cost/cloud-optimization-the-4-things-you-must-optimize/
- https://www.techtarget.com/searchstorage/definition/cloud-testing
- https://www.dhs.gov/sites/default/files/publications/cybersecurity_in_a_cloud_future_ziring.pdf
- https://www.informationweek.com/cloud/homeland-security-plans-12-cloud-services
- https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf