Implementing and Updating Cloud Computing Best Practices

Nathaniel Richmond

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Implementing and Updating Cloud Computing Best Practices

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM19-0900

Agenda

Introduction

Recap of previous work

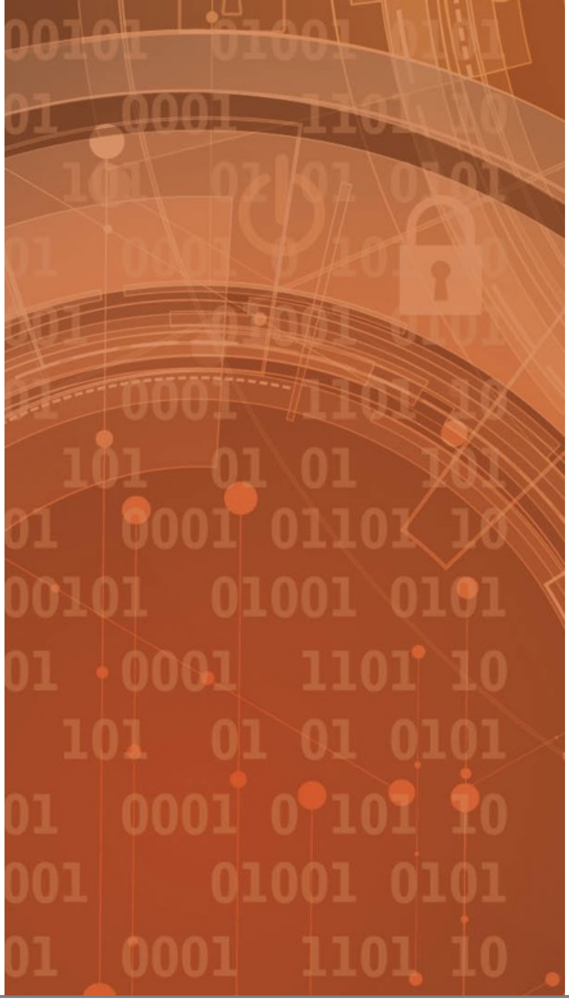
Volatility of cloud services

Methods to stay current

Translating to best practices and implementation

Implementing and Updating Cloud Computing Best Practices

Introduction

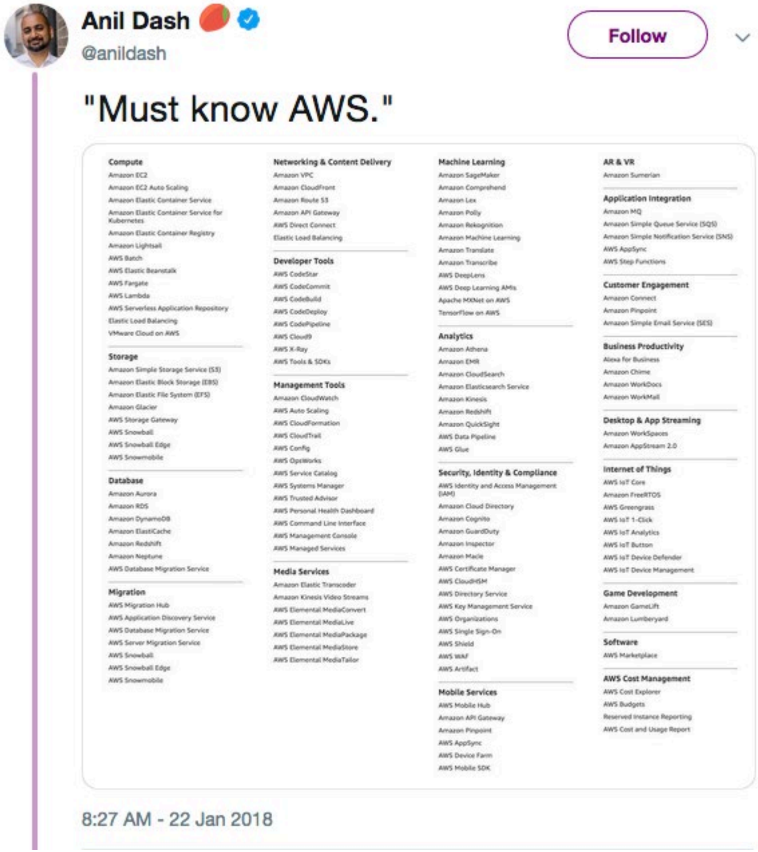


Introduction

- Read my bio if you want
  - Started in IT
  - Worked cybersecurity operations and incident response
  - Team lead, Security Solutions, part of Monitoring and Response within CERT.
    - Architecture
    - Cybersecurity operations
    - Transitioning research to practice

I do not consider myself an expert at cloud computing, so this presentation is an effort to show, in part, how I work towards the knowledge I need.

Introduction: “Must know AWS”



Anil Dash
@anildash

Follow

"Must know AWS."

Compute
Amazon EC2
Amazon EC2 Auto Scaling
Amazon Elastic Container Service
Amazon Elastic Container Service for Kubernetes
Amazon Elastic Container Registry
Amazon Lightsail
AWS Batch
AWS Elastic Beanstalk
AWS Fargate
AWS Lambda
AWS Serverless Application Repository
Elastic Load Balancing
VMware Cloud on AWS

Storage
Amazon Simple Storage Service (S3)
Amazon Elastic Block Storage (EBS)
Amazon Elastic File System (EFS)
Amazon Glacier
AWS Storage Gateway
AWS Snowball
AWS Snowball Edge
AWS Snowmobile

Database
Amazon Aurora
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon Redshift
Amazon Neptune
AWS Database Migration Service

Migration
AWS Migration Hub
AWS Application Discovery Service
AWS Database Migration Service
AWS Server Migration Service
AWS Snowball
AWS Snowball Edge
AWS Snowmobile

Networking & Content Delivery
Amazon VPC
Amazon CloudFront
Amazon Route 53
Amazon API Gateway
AWS Direct Connect
Elastic Load Balancing

Developer Tools
AWS CodeStar
AWS CodeCommit
AWS CodeBuild
AWS CodeDeploy
AWS CodePipeline
AWS Cloud9
AWS X-Ray
AWS Tools & SDKs

Management Tools
Amazon CloudWatch
AWS Auto Scaling
AWS CloudFormation
AWS CloudTrail
AWS Config
AWS OpsWorks
AWS Service Catalog
AWS Systems Manager
AWS Trusted Advisor
AWS Personal Health Dashboard
AWS Command Line Interface
AWS Management Console
AWS Managed Services

Media Services
Amazon Elastic Transcoder
Amazon Kinesis Video Streams
AWS Elemental MediaConvert
AWS Elemental MediaLive
AWS Elemental MediaPackage
AWS Elemental MediaStore
AWS Elemental MediaTailor

Machine Learning
Amazon SageMaker
Amazon Comprehend
Amazon Lex
Amazon Polly
Amazon Rekognition
Amazon Machine Learning
Amazon Translate
Amazon Transcribe
AWS DeepLens
AWS Deep Learning AMIs
Apache MXNet on AWS
TensorFlow on AWS

Analytics
Amazon Athena
Amazon EMR
Amazon CloudSearch
Amazon Elasticsearch Service
Amazon Kinesis
Amazon Redshift
Amazon QuickSight
AWS Data Pipeline
AWS Glue

Security, Identity & Compliance
AWS Identity and Access Management (IAM)
Amazon Cloud Directory
Amazon Cognito
Amazon GuardDuty
Amazon Inspector
Amazon Macie
AWS Certificate Manager
AWS CloudHSM
AWS Directory Service
AWS Key Management Service
AWS Organizations
AWS Single Sign-On
AWS Shield
AWS WAF
AWS Artifact

Mobile Services
AWS Mobile Hub
Amazon API Gateway
Amazon Pinpoint
AWS AppSync
AWS Device Farm
AWS Mobile SDK

AR & VR
Amazon Sumerian

Application Integration
Amazon MQ
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
AWS AppSync
AWS Step Functions

Customer Engagement
Amazon Connect
Amazon Pinpoint
Amazon Simple Email Service (SES)

Business Productivity
Alexa for Business
Amazon Chime
Amazon WorkDocs
Amazon WorkMail

Desktop & App Streaming
Amazon WorkSpaces
Amazon AppStream 2.0

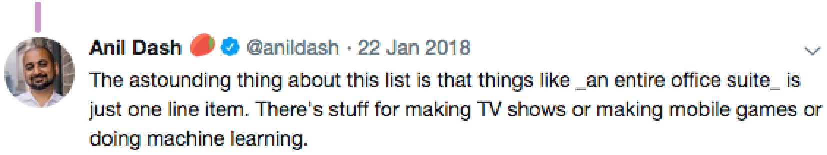
Internet of Things
AWS IoT Core
Amazon FreeRTOS
AWS Greengrass
AWS IoT 1-Click
AWS IoT Analytics
AWS IoT Button
AWS IoT Device Defender
AWS IoT Device Management

Game Development
Amazon GameLift
Amazon Lumberyard

Software
AWS Marketplace

AWS Cost Management
AWS Cost Explorer
AWS Budgets
Reserved Instance Reporting
AWS Cost and Usage Report

8:27 AM - 22 Jan 2018



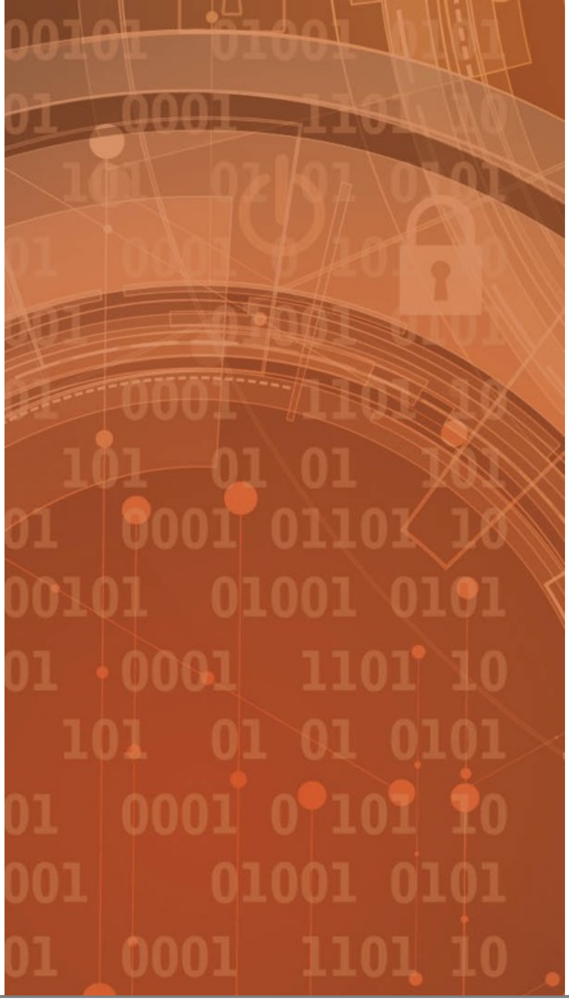
Anil Dash @anildash · 22 Jan 2018

The astounding thing about this list is that things like _an entire office suite_ is just one line item. There's stuff for making TV shows or making mobile games or doing machine learning.

https://twitter.com/anildash/status/955476924402487296

Implementing and Updating Cloud Computing Best Practices

Recap of previous work



Previous Work: Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud

1. Consumers Have Reduced Visibility and Control
2. On-Demand Self Service Simplifies Unauthorized Use
3. Internet-Accessible Management APIs can be Compromised
4. Separation Among Multiple Tenants Fails
5. Data Deletion is Incomplete
6. Credentials are Stolen
7. Vendor Lock-In Complicates Moving to Other CSPs
8. Increased Complexity Strains IT Staff
9. Insiders Abuse Authorized Access
10. Stored Data is Lost
11. CSP Supply Chain is Compromised
12. Insufficient Due Diligence Increases Cybersecurity Risk

Previous Work: Cloud Security Best Practices

- Due Diligence
  - Planning
  - Development and Deployment
  - Operation
  - Decommissioning
  - Multiple-CSP Strategy
- Managing Access
  - Identify and Authenticate Users
  - Assign User Access Rights
  - Create and Enforce Resource Access Policies
- Protect Data
  - Protect From Unauthorized Access
  - Ensure Availability of Critical Data
  - Prevent Disclosure of Deleted Data
- Monitor and Defend
  - Monitor Cloud-Deployed Resources
  - Analyze Both Cloud and On-Premise Monitoring
  - Coordinate with CSP

Previous Work: Operation Cloud Hopper Case Study

A blog post to try and show how one could use the guidance from the previous two documents to identify and mitigate risk.

Related risks, threats, and vulnerabilities from previous report:

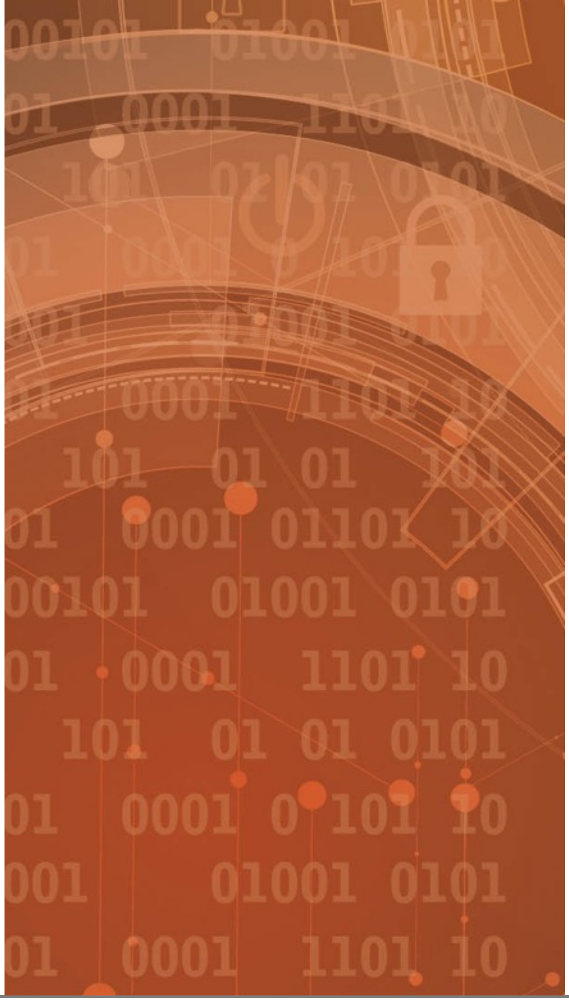
- Consumers have reduced visibility and control
- Credentials are stolen – Easy example of something that can be mitigated, i.e. multi-factor auth (MFA)
- Increased complexity strains IT staff
- Insiders abuse authorized access
- Insufficient due diligence increases risk

Additional potential for risks, threats, or vulnerabilities

- Risk from one customer can transfer to another
- Traditional risks, threats, and vulnerabilities

Implementing and Updating Cloud Computing Best Practices

Volatility of cloud services



Example of Industry Volatility

The following are just a couple key examples that have changed since the previous papers were written.

1. AWS Site-toSite VPN now supports certificate authentication instead of just pre-shared keys: https://aws.amazon.com/about-aws/whats-new/2019/08/aws-site-to-site-vpn-now-supports-certificate-authentication/
2. Azure Kubernetes Service (AKS) supports egress filtering (or maybe not?): https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic
3. Don’t forget cost forecasting

Volatility Examples – Continued

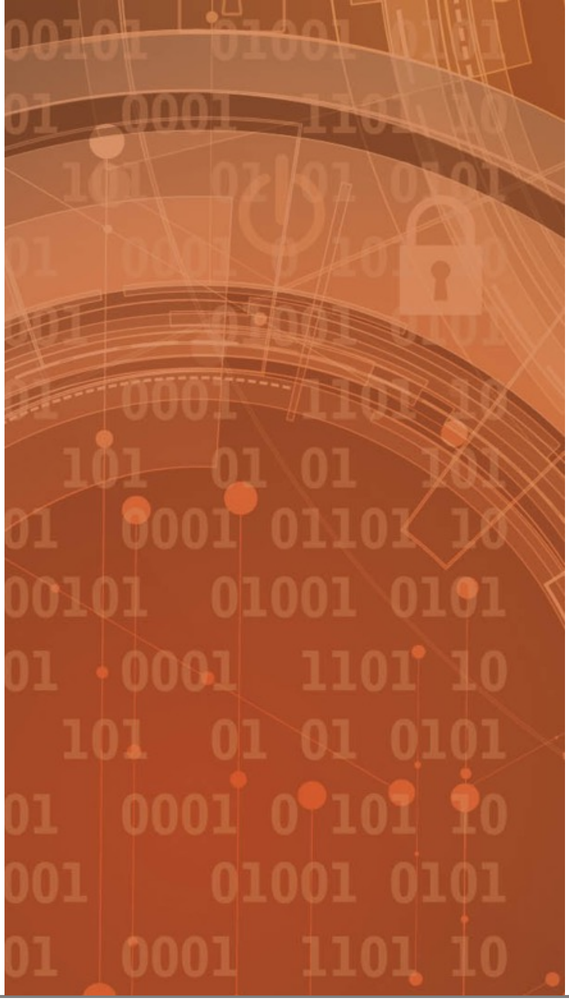
Government clouds are different than the commercial offerings, both at a high level and sometimes in the details. Some services behave differently, some are released at different times, and more.

Examples:

- AWS
  - GovCloud S3 namespaces are regional, not global
  - Three GovCloud S3 endpoints, two for ITAR and one for FIPS
- Azure
  - User activity in Security Center not logged in Azure Government
  - URLs for API Management are different

Implementing and Updating Cloud Computing Best Practices

Methods to stay current



Methods to stay current: Vendors

OUR HERO PAINFULLY POINTS TO WHAT IS CLEARLY UNDERSTOOD BY EVERYONE ELSE !!!
CAPTAIN OBVIOUS
IT'S A BIRD!
THIS IS A SUPER-HERO STANCE!!!
PLANE
IT'S A PLANE!!
IT'S A PANEL BORDER !!!!
IT'S A WORD BUBBLE !!!

Most vendors have multiple ways to propagate information about changes to their services, including:

- Website
- Twitter and other social media

They will usually notify customers of:

- New products and services
- End of life products and services
- Changes to products and services

Methods to stay current: Hands-on

There is no substitute to use a product or service day-to-day. Your knowledge will always be better, all other things being equal.

- Work lab
- Customer lab
- Production
- Other (personal projects or experimentation, class-based, etc)

Note that, if you have the opportunity for hands-on work, that also means you likely have potential mentors at your organization that could help you learn. I have a number of colleagues across the CERT Division and SEI that I know can help me at the strategic level down to the technical details.

Methods to stay current: Formal training

Formal training generally has a few positives and a few negatives compared to self-taught or on-the-job training.

Potential positives:

1. Some people learn better in a classroom environment
2. It removes you from the day-to-day to allow focus
3. Usually includes a mix of lecture and hands-on lab material – you should probably avoid anything without labs
4. Could cover material that you don’t get to use as much in practice

Potential negatives:

1. Usually expensive
2. Easy to lose what you learned if you don’t use it afterward

Methods to stay current: Industry experts, policies and regulations, government resources

Industry Experts:

- Research firms
- Companies (for profit and non-profit)
- Individuals and other resources like flaws.cloud and flaws2.cloud

Policies and regulations:

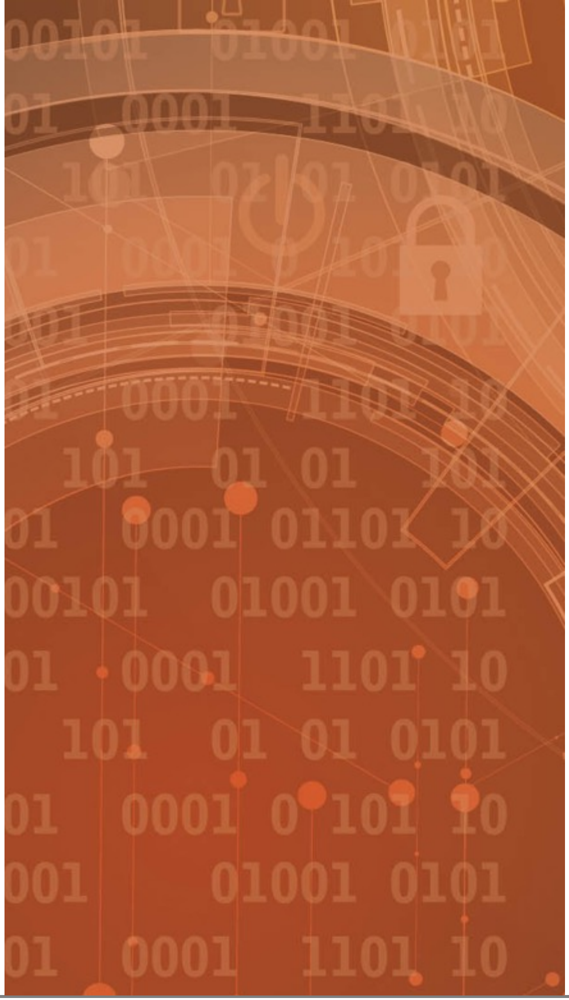
- FIPS
- ITAR
- GDPR

Government resources

- FedRAMP

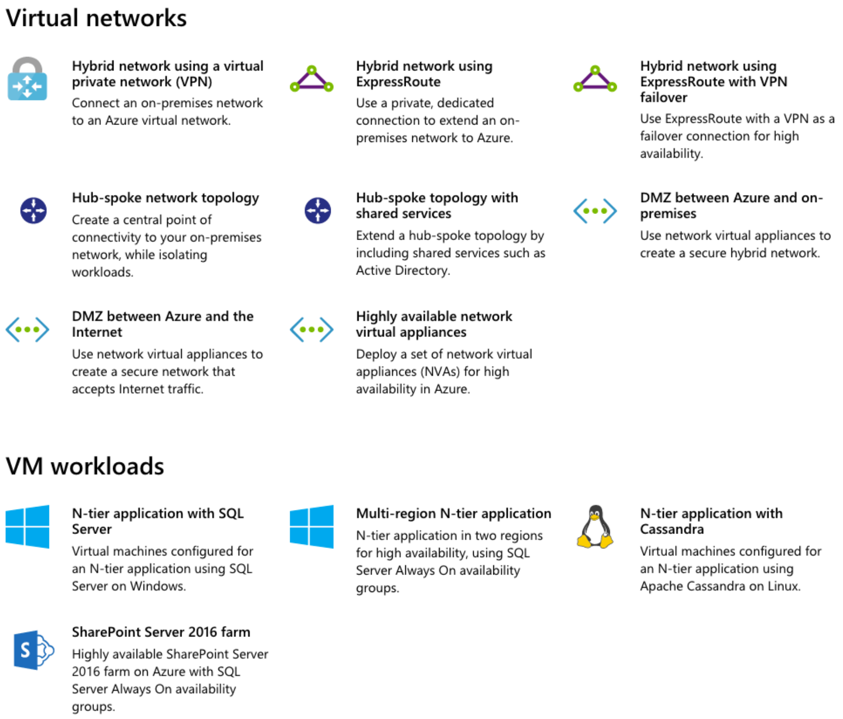
Implementing and Updating Cloud Computing Best Practices

Translating to best practices and implementation



Transitioning best practices: Industry and vendor examples

- Reference models, frameworks, and other examples help you break down the problem based on vendor guidance
- Reference architecture examples:
  - AI/ML
  - Big data
  - IoT
  - Serverless
  - Virtual networks
  - VM workloads
  - Web applications
  - More…



Virtual networks

Hybrid network using a virtual private network (VPN)
Connect an on-premises network to an Azure virtual network.

Hybrid network using ExpressRoute
Use a private, dedicated connection to extend an on-premises network to Azure.

Hybrid network using ExpressRoute with VPN failover
Use ExpressRoute with a VPN as a failover connection for high availability.

Hub-spoke network topology
Create a central point of connectivity to your on-premises network, while isolating workloads.

Hub-spoke topology with shared services
Extend a hub-spoke topology by including shared services such as Active Directory.

DMZ between Azure and on-premises
Use network virtual appliances to create a secure hybrid network.

DMZ between Azure and the Internet
Use network virtual appliances to create a secure network that accepts Internet traffic.

Highly available network virtual appliances
Deploy a set of network virtual appliances (NVAs) for high availability in Azure.

VM workloads

N-tier application with SQL Server
Virtual machines configured for an N-tier application using SQL Server on Windows.

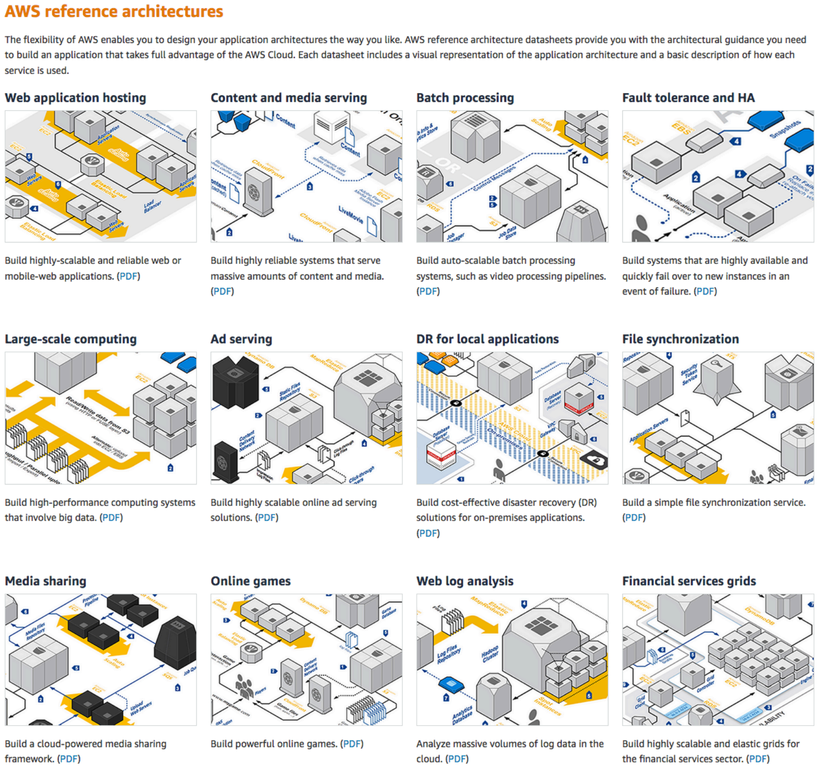
Multi-region N-tier application
N-tier application in two regions for high availability, using SQL Server Always On availability groups.

N-tier application with Cassandra
Virtual machines configured for an N-tier application using Apache Cassandra on Linux.

SharePoint Server 2016 farm
Highly available SharePoint Server 2016 farm on Azure with SQL Server Always On availability groups.

Transitioning best practices: Industry and vendor examples

- Working templates and implementations
  - AWS Quick Starts with CloudFormation
  - GCP Deployment Manager samples on Github
  - Azure Resource Manager Quickstart Templates
  - Some vendors can use this as a differentiator from competition



AWS reference architectures

The flexibility of AWS enables you to design your application architectures the way you like. AWS reference architecture datasheets provide you with the architectural guidance you need to build an application that takes full advantage of the AWS Cloud. Each datasheet includes a visual representation of the application architecture and a basic description of how each service is used.

Web application hosting

Build highly-scalable and reliable web or mobile-web applications. (PDF)

Content and media serving

Build highly reliable systems that serve massive amounts of content and media. (PDF)

Batch processing

Build auto-scalable batch processing systems, such as video processing pipelines. (PDF)

Fault tolerance and HA

Build systems that are highly available and quickly fail over to new instances in an event of failure. (PDF)

Large-scale computing

Build high-performance computing systems that involve big data. (PDF)

Ad serving

Build highly scalable online ad serving solutions. (PDF)

DR for local applications

Build cost-effective disaster recovery (DR) solutions for on-premises applications. (PDF)

File synchronization

Build a simple file synchronization service. (PDF)

Media sharing

Build a cloud-powered media sharing framework. (PDF)

Online games

Build powerful online games. (PDF)

Web log analysis

Analyze massive volumes of log data in the cloud. (PDF)

Financial services grids

Build highly scalable and elastic grids for the financial services sector. (PDF)

Transitioning best practices: Manageable chunks

It can be difficult to take a high-level best practice like, "Protect data from unauthorized access," and implement it. Decompose the practice into manageable chunks.

An example of breaking this one into a few steps:

1. Identify data types and sensitivity
2. Determine mechanisms for authentication and access control, which will change depending on cloud model (hybrid, native) and how it is integrated with local infrastructure
3. Determine roles for different levels of access, put users in appropriate roles
4. Make sure defaults are secure!
5. Feed into risk management, vulnerability, and other processes (e.g. identify a potential issue like SSRF and mitigate if possible)
6. Iterate through steps to identify what is missing or further decompose into actions

Transitioning best practices: CI/CD and DevOps

DevOps

“DevOps is a software development approach that brings development and operations staff (IT) together.” Focuses on agility and automation.

https://insights.sei.cmu.edu/sei_blog/2014/11/a-new-weekly-blog-series-to-help-organizations-adopt-implement-devops.html

SEI DevOps blog contains a wealth of information going back years.

https://insights.sei.cmu.edu/devops/

Secure DevOps

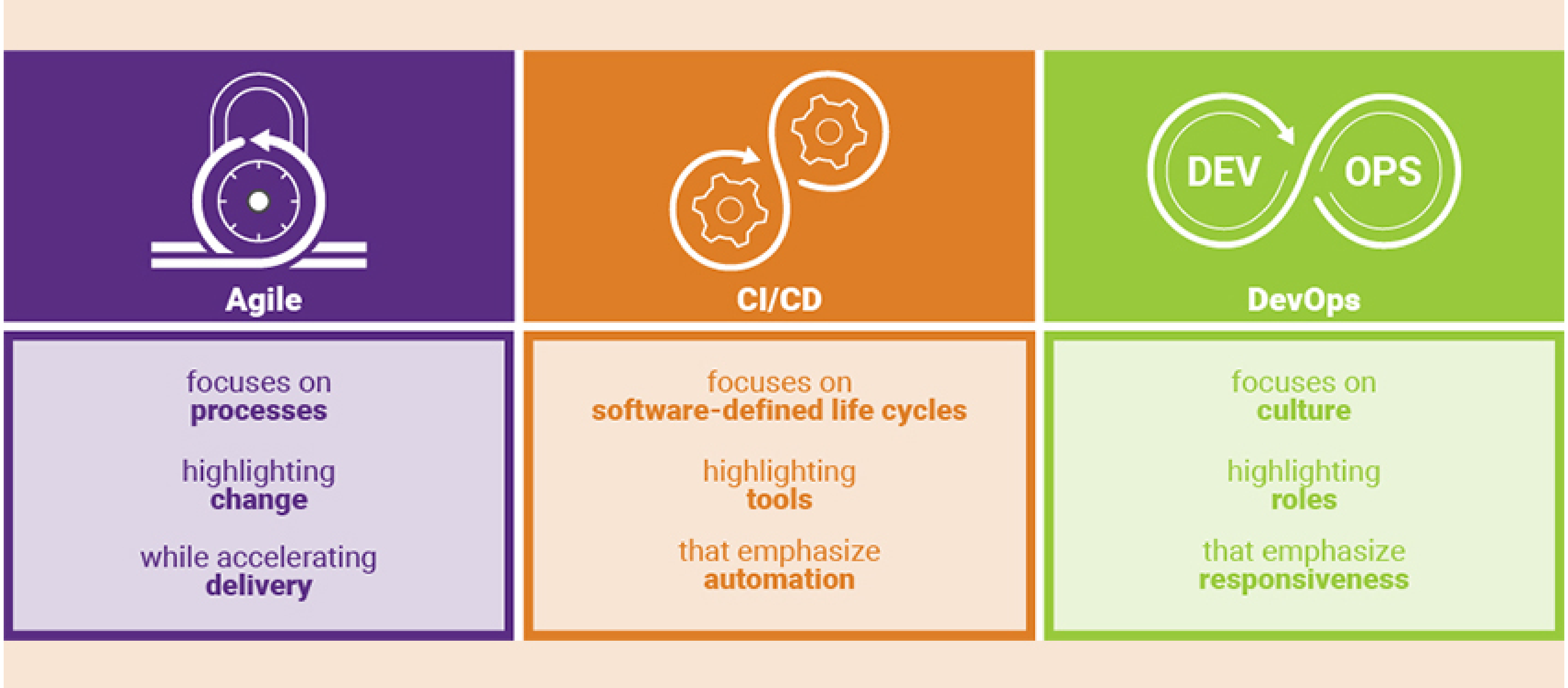
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=465551

Continuous Integration/Continuous Delivery (CI/CD)

CI is frequent build and test, CD is delivering the code from one environment to another.

https://insights.sei.cmu.edu/devops/2015/09/-a-devops-a-day-keeps-the-auditors-away-and-helps-organizations-stay-in-compliance-with-federal-regu.html

Transitioning best practices: CI/CD and DevOps



Agile

focuses on **processes**

highlighting **change**

while accelerating **delivery**

CI/CD

focuses on **software-defined life cycles**

highlighting **tools**

that emphasize **automation**

DevOps

focuses on **culture**

highlighting **roles**

that emphasize **responsiveness**

https://www.synopsys.com/blogs/software-security/agile-cicd-devops-difference/

Conclusion

Contact Information

Presenter / Point of Contact match to Information Sheets

Nathaniel Richmond

Senior Team Lead

Telephone: +1 703.247.1395

Email: nr@cert.org