
cloud
CSA
security
alliance®
aws
Using Encryption with Amazon Web Services
Cloud Security Alliance (CSA) Colorado Fall Summit 2018
November 8, 2018, Arvada, CO
GTRI®
IS NOW ZIVARO
Scott Hogg, CTO GTRI
CCIE #5133, CISSP #4610, CCSP, CCSK
AWS Certified Solutions Architect – Professional
AWS Certified Network and Security - Specialty (ANS & SCS)

Today’s Agenda

1. Importance of Encryption in Cloud Infrastructure
2. AWS Encryption Methods
3. Live Demonstration of AWS Encryption Techniques
4. Summary, Resources, and Q&A

Importance of Encryption in Cloud Infrastructure

“Encryption” in the Cloud

- Protecting the confidentiality of data
- “process of encoding a message or information in such a way that only authorized parties can access it” (wikipedia.org)
  - At rest: encrypting instance storage and object data
  - In transit: encryption of connectivity, VPNs, secure remote management
  - In use: instance roles allow access to encryption keys
- Encryption is a security compliance requirements
- Customer maintains the encryption keys => Crypto-shreading
- Other concepts for cloud-confidentiality
  - Data Dispersion, Storage Slicing, Information Dispersal Algorithms (IDAs)

CCSK Body of Knowledge Domains

CCSK™
Certificate of
Cloud Security Knowledge

- CCSK Guidance V4 has 14 domains
  1. Cloud Computing Concepts and Architectures
  2. Governance and Enterprise Risk
  3. Legal Issues, Contracts and Electronic Discovery
  4. Compliance and Audit
  5. Information Governance
  6. Management Plane and Business Continuity
  7. Infrastructure Security
  8. Virtualization and Containers
  9. Incident Response
  10. Application Security
  11. Data Security and Encryption
  12. Identity Entitlement, and Access Management
  13. Security-as-a-Service
  14. Related Technologies

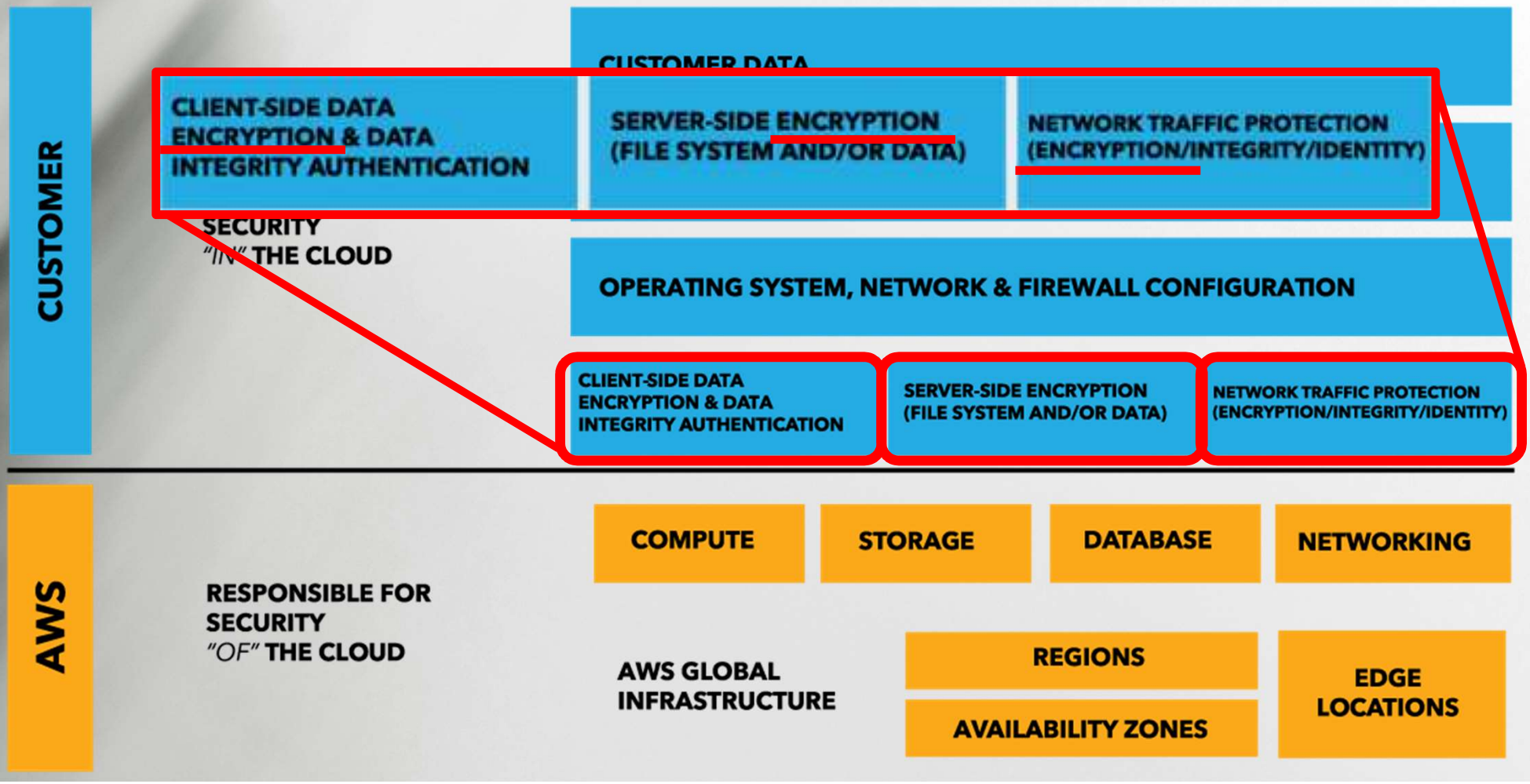
$(ISC)^2$ Certified Cloud Security Professional (CCSP)

- The CCSP Common Body of Knowledge (CBK) emphasized the use of encryption as a way to preserve confidentiality and avoid vendor lock-in (exit strategy):
  - 1. Architectural Concepts & Design Requirements
  - 2. Cloud Data Security
  - 3. Cloud Platform & Infrastructure Security
  - 4. Cloud Application Security
  - 5. Operations
  - 6. Legal & Compliance

CCSP Domains Covering Encryption

- 1. Architectural Concepts & Design Requirements
  - 1.3 Understand Security Concepts Relevant to Cloud Computing
    - Cryptography (e.g. encryption, in motion, at rest, key management)
- 2. Cloud Data Security
  - 2.2 Design and Implement Cloud Data Storage Architectures
    - Technologies Available to Address Threats (e.g., encryption)
  - 2.3 Design and Apply Data Security Strategies
    - Encryption
    - Application of Technologies (e.g., time of storage vs. encryption needs)
    - Emerging Technologies (e.g., bit splitting, data obfuscation, homomorphic encryption)

AWS Shared Responsibility Model



Concerns About AWS Security

- A breach of the Cloud Service Provider's infrastructure can lead to a "Hyperjacking" event whereby many customer's data is exposed
- Examples of CSP Data Breaches:
  - Code Spaces goes out of business in June 2014 after AWS infrastructure hack
  - Dropbox breach in October 2014, compromising 7M passwords held for Bitcoin ransom
  - Worcester Polytechnic Institute (WPI) claims cross-VM RSA key recovery in AWS, October 2015
  - Datadog password breach for their AWS customers in July 2016
  - OneLogin breach of AWS infrastructure due to insecure keys in May 2017
  - RNC leaks 1.1TB of data on 200M people via Deep Root Analytics on S3 bucket June 2017
  - World Wrestling Entertainment leaked 3M customer info unprotected AWS S3 bucket July 2017
  - Verizon leaked 14M customer data by Nice Systems on weak AWS S3 bucket July 2017
  - Alteryx breached AWS infrastructure, 123M U.S. households in October 2017

AWS Encryption Methods

AWS Encryption Methods

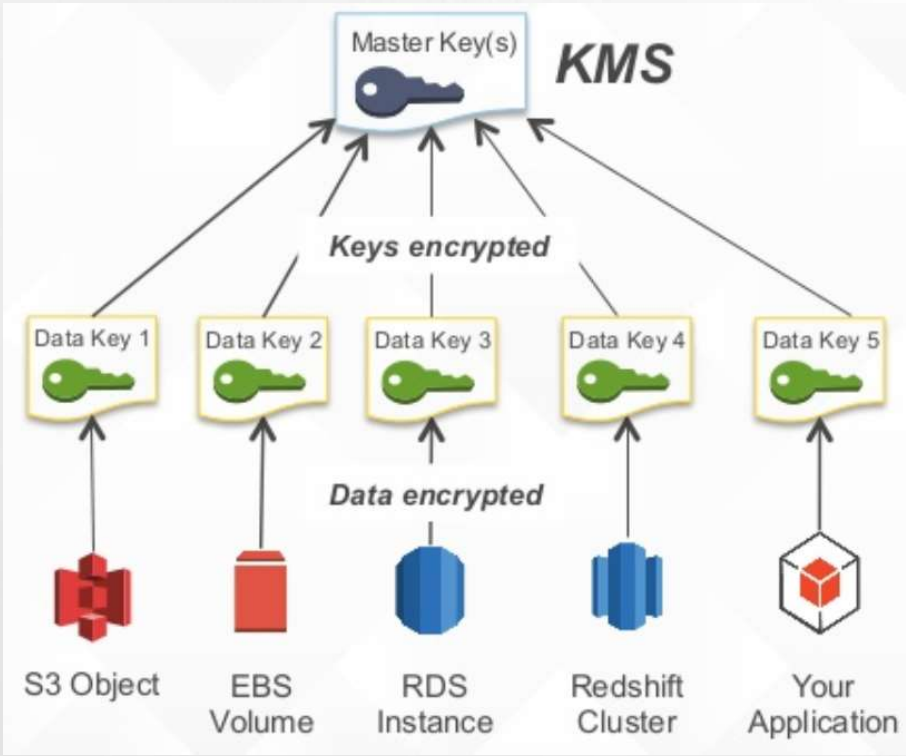
- Encryption services are provided by AWS, but it is up to the customer to operate them securely and protect the confidentiality of the keys
- Keeping the keys separated from the encrypted data is a best practice
- Customers can manage and control the keys themselves or let AWS handle it on their behalf
- Remember the “Shared Responsibility Model”
- Client Side Encryption (CSE) is where the customer encrypts the data and then upload it to AWS
- Server Side Encryption (SSE) is when AWS encrypts the data
  - SSE is freely available for many AWS storage services (S3, EBS, Snapshots, RDS)

AWS Key Management Service (KMS)

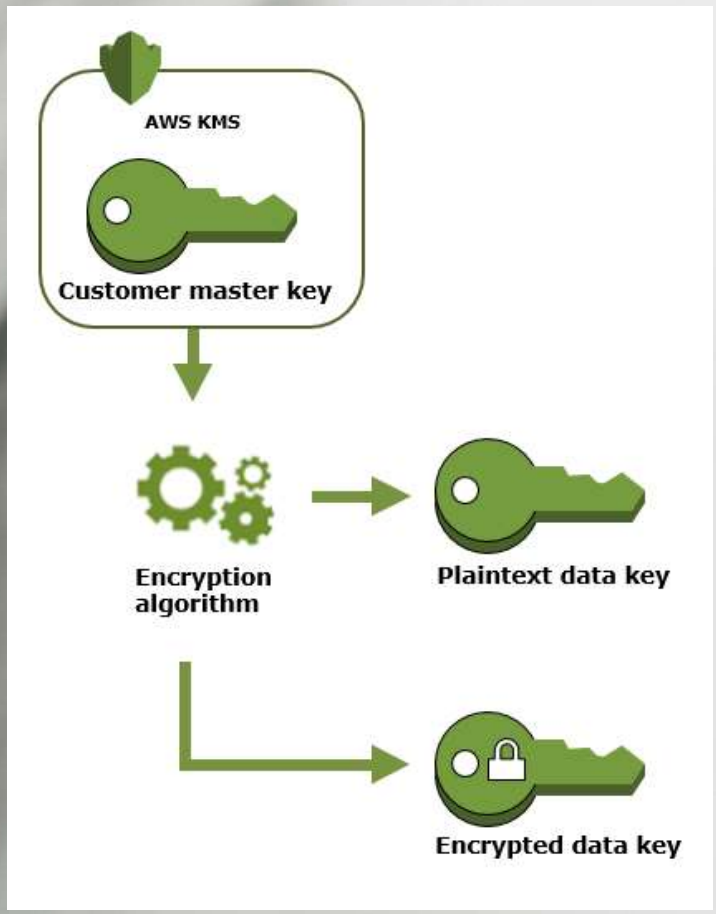
- AWS Key Management Service (KMS) is a managed symmetric key service
  - Customer-managed Customer Master Keys (CMKs): customer creates and manages the keys(upload their own key material)
  - AWS managed CMKs: are created, managed and used on customer's behalf with KMS
  - KMS securely stores (FIPS 140-2 Level 2/3), tracks, rotates and protects your CMKs (CMKs never leave KMS)
- AWS can manage the automatic key rotation or customer can expire and rotate their own keys and control key access
- https://aws.amazon.com/kms/

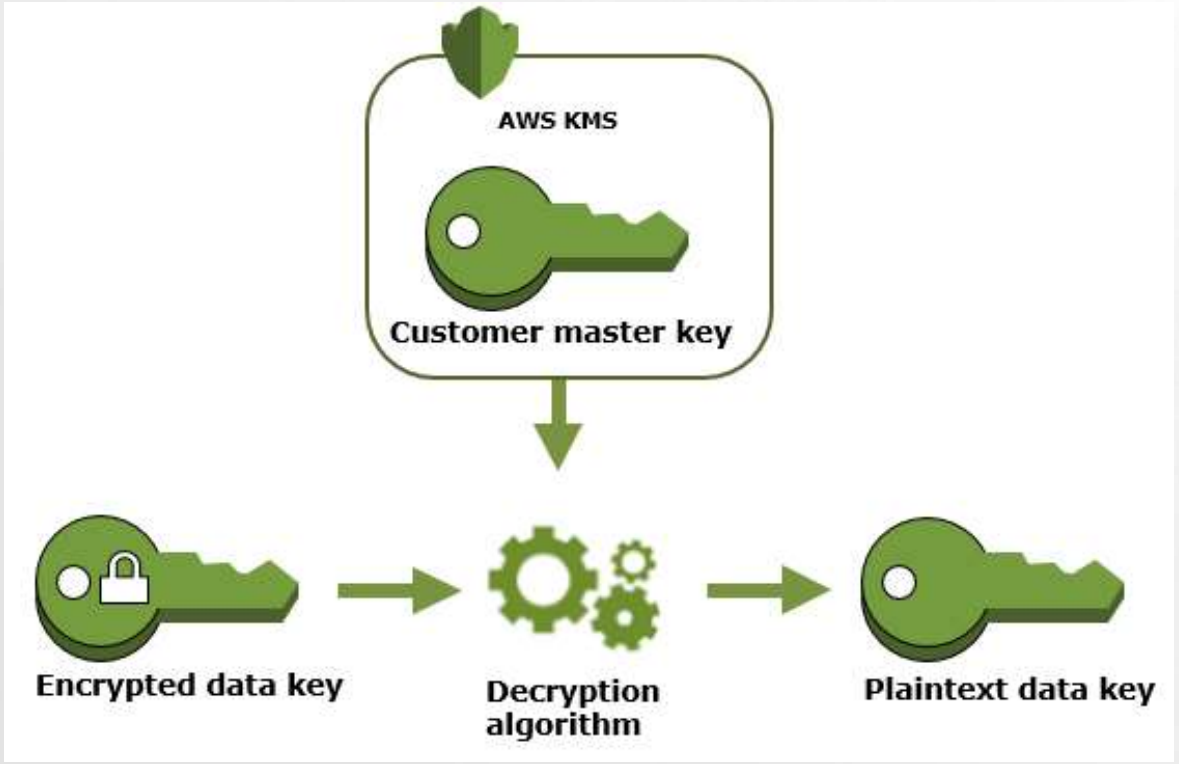
AWS Key Management Service (KMS)

- KMS uses two-tiered key hierarchy using envelope encryption, creates a unique data key to encrypt the customer data.
- The CMK creates, encrypts, and decrypts the data keys.
- KMS does not store, manage, or track customer data keys.
- Easier to manage few CMKs than many data keys.



AWS Key Management Service (KMS)





Source: https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html

AWS Services Integrated with KMS

Alexa for Business*
Athena
Aurora
CloudWatch Logs
Comprehend*
Connect
DynamoDB*
DynamoDB Accelerator (DAX)*
EBS
EFS
Elastic Transcoder
Elasticsearch Service
EMR
Glacier
Kinesis Data Streams
Kinesis Firehose
Kinesis Video Streams
Lex
Lightsail*
SES
SQS
Neptune
RDS
Redshift
SageMaker
S3
WorkMail
WorkSpaces
ACM*
Cloud9*
CloudTrail
CodeBuild
CodeCommit*
CodeDeploy
CodePipeline
Database Migration Service
Lambda
Secrets Manager
Systems Manager
Snowball
Snowmobile
Snowball Edge
Storage Gateway
X-Ray

*AWS-managed KMS keys only

Source: https://aws.amazon.com/kms/details/#integration

AWS CloudHSM

- Cloud Hardware Security Modules (HSMs) are AWS managed physical tamper-resistant cryptography hardware appliances available for storing your self-managed symmetric and asymmetric keys
- CloudHSM is single tenancy (dedicated to 1 AWS customer) connected to a Private subnet in a VPC
- Create IAM role for the HSM and install CloudHSM SafeNet client application/libraries on EC2 “control instance” (used for HSM key replication)
- HSM Users: Precrypto Officer (PRECO), Crypto Officer (CO, PCO), Crypto User (CU), Appliance User (AU)
- FIPS 140-2 Level 3 (1 = low, 4 = highest) and Common Criteria EAL4+ compliant

SafeNet Luna SA7000 HSM appliance

AWS Encryption with S3 Object Storage

- AWS S3 Server Side Encryption (SSE) Methods
- SSE-C
  - Server-Side Encryption with Customer-Provide Keys option, customer manages the keys
  - AWS Encryption SDK, S3 Encryption Client EMRFS Client, DynamoDB Encryption Client
- SSE-S
  - AWS maintains the master key and rotates it automatically, uses AES-256
- SSE-KMS
  - S3 SSE-KMS encryption of objects leverages KMS and your CMK and envelope encryption to create a symmetric data key for S3 objects

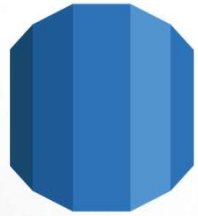
AWS EC2 Instance Encryption - EBS

- Encryption of EBS Volumes mounted by EC2 instances can be encrypted using KMS
- EBS Root Volume of default AMIs cannot be encrypted (instance storage is not encrypted) but can be encrypted with the OS with, for example Linux dm-crypt
  - https://aws.amazon.com/blogs/aws/new-encrypted-ebs-boot-volumes/
- Snapshots that are taken from encrypted volumes are automatically encrypted
- You can share an encrypted snapshot within a region and only with specific AWS accounts, you can't publicly share encrypted snapshots
- To use your shared, encrypted snapshot, you must also share the CMK key that was used to encrypt it.
- EBS volumes can be transferred between AZs (within a region), but only if they are un-encrypted
  - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

AWS Elastic File System (EFS) Encryption

- Amazon Elastic File System (EFS) allows you to encrypt your data at rest using data keys managed by KMS.
- Encryption and decryption are handled seamlessly, so you don't have to modify your applications to access your data.
- Encryption with KMS is configured when creating the EFS
  - Click "Create File System" and click the checkbox to enable encryption.
- Data is encrypted in-transit (TLS 1.2) with the EFS Mount Helper
  - sudo mount -t efs -o tls fs-12345678:/ /mnt/efs
- http://docs.aws.amazon.com/efs/latest/ug/encryption.html
- https://aws.amazon.com/efs/faq/#encryption

AWS RDS Encryption



- RDS Encryption only supported on MySQL, Oracle, MS SQL Server, PostgreSQL, MariaDB, (NOT Aurora)
- RDS must be encrypted when DB created, encryption cannot be disabled once enabled, can't encrypt already running RDS
  - If RDS is encrypted, then read replicas also must be encrypted (using the same key)
  - Backups become automatically encrypted too
- RDS with MS SQL Server and Oracle encryption uses Transparent Data Encryption (TDE)
- TDE encrypts the data before it is written to storage and automatically decrypts data when it is read from storage
- Encryption of the data at rest uses AWS Key Management Service (KMS)
- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

AWS DynamoDB Encryption and Security

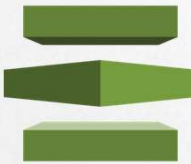
- DynamoDB encryption uses KMS for encryption of data at rest
  - https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html
- DynamoDB can be accessed using TLS (SSL) connections - to protect data in transit
- Fine Grained Access Control (FGAC) = table owner has control over data (items), controls which user/caller can access which items and attributes, uses IAM policies
- JSON policies can restrict access to a specific table
- Authentication and Access Control restrictions, including Web Identity Federation with Identity Provider authentication

AWS SQS Encryption

- Simple Queueing Service (SQS) message queue service is used to decouple application components, but sensitive data exchanged (data in use) between modules should be confidential.
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS
- SQS messages can be encrypted with your KMS keys in an SSE method, messages are encrypted as they wait in the queue to be pulled.

AWS Certificate Manager (ACM)

- Using secure web connections using TLS 1.3/1.2 is a best practice
- Whether you are creating your own private keys, generating a CSR, then obtaining a commercial certificate via CA or using Let's Encrypt
- AWS Certificate Manager (ACM) helps easily create and manage public certs (using Domain Validation (DV) or e-mail validation)
  - Certificates can be assigned to an ALB, CloudFront distribution or API Gateway endpoint
- Validate your SSL/TLS configurations using Qualys SSLLabs.com or open source SSL scanning utility (ssllabs-scan, testssl.sh, sslyze, SSLScanner, etc.)
- AWS also offers s2n, open source TLS library



AWS Connectivity Using Encryption

- Securely establish connectivity to your AWS Management VPC
  - Use encryption and control source IP addresses connecting to your VPC
  - Establish IPsec tunnel-mode VPN connection to your Virtual Private Gateway (VGW)
  - IKE v1 *(No IKE v2),* AES-256, SHA-1, DH Group 2, PFS, DPD (Enhanced AWS VPN AES-256, SHA2(256), DH 14-18, 22, 23, 24, NAT-T)
  - Supports static routes or eBGP dynamic routing (propagated)
- Direct Connect is unencrypted and partially exposed within DX partner to AWS connectivity
  - Use a VGW with Direct Connect to encrypt traffic traversing the DX Link

Secure AWS Management Console Access

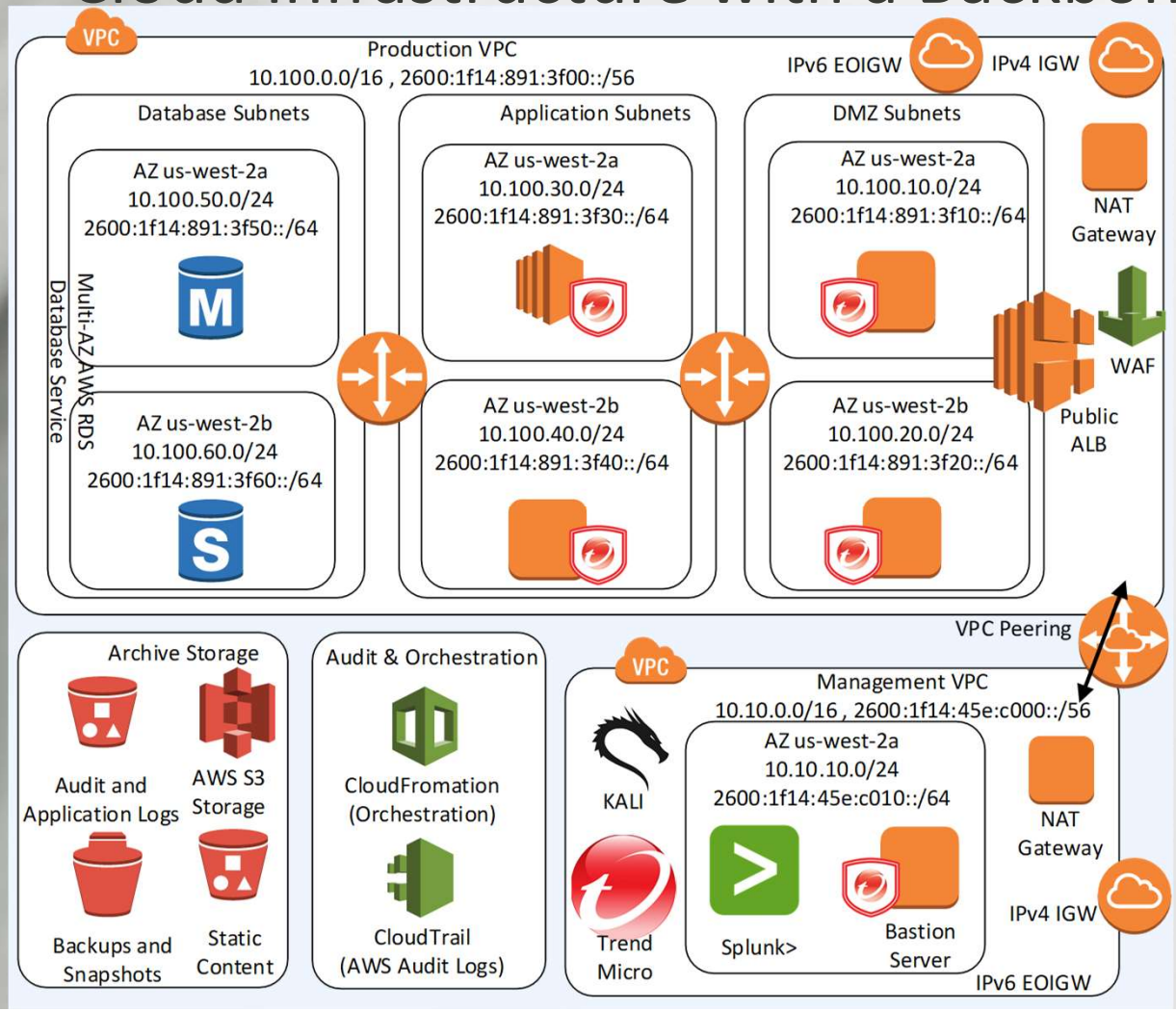
- Using MFA for secure administrative access is a best practice
  - In addition to your username and password, you are asked for a six-digit numeric code based upon a time-synchronized one-time password algorithm.
  - https://aws.amazon.com/iam/details/mfa/
- Hardware MFA (e.g. Gemalto, Yubico U2F, SurePassID for GovCloud)
- Virtual MFA (e.g. TOTP (RFC 6238) with Google Authenticator, Authy on your mobile device)
- Google Chrome and Mozilla Firefox work with U2F
  - Firefox: about:config, search for u2f, toggle security.webauth.u2f = true

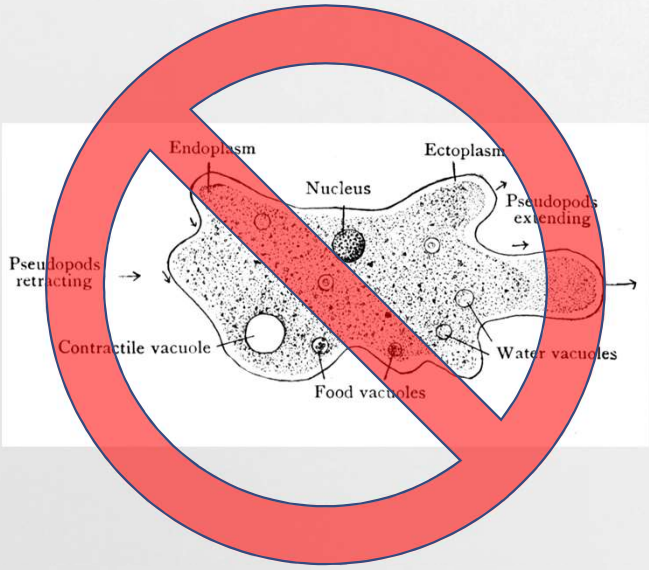
AWS Encrypted Instance Access

- Bastion Servers in Management VPCs are used as jump-hosts to administer other EC2 instances in VPCs
- SSH uses public-key cryptography to authenticate and encrypt CLI connections
- SSH can also be used to “tunnel” other protocols (e.g. X-Windows, RDP, etc.)
- Use TLS to secure your RDP connections to Windows Bastion Servers
- Apache Guacamole is clientless HTML5 remote desktop gateway for VNC, RDP, and SSH
- AWS Systems Manager (Session Manager) is an alternative to using bastion servers for CLI access

Live Demonstration of AWS Encryption

Cloud Infrastructure with a Backbone

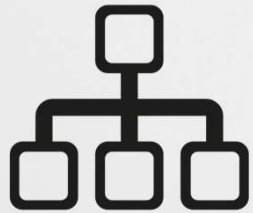




Summary, Resources, and Q&A

Final Thoughts & Recommendations

- Start off your cloud deployment with the best InfoSec hygiene
- Encrypting everything should be your default method
- All things being equal, choose the more secure option – Snyder's Razor
- Use automation methods whenever possible to eliminate human error and make repeatable best practices
- Use built-in AWS security features and services rather than trying to build-your-own
- Leverage No||Low-cost resources available, AWS FREE-Tier account to learn and test security and encryption methods



Valuable (but FREE) AWS Security Resources

- AWS Security Whitepapers – AWS Security Center
  - http://aws.amazon.com/security/
- Introduction to AWS Security - July 2015
  - https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
- AWS: Overview of Security Processes – May 2017
  - https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
- AWS Well Architected Framework Security Pillar – July '18
  - https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf
- AWS Security Best Practices – August 2016
  - https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf
- AWS: Risk and Compliance, May 2017
  - https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- AWS Cloud Adoption Framework Security Perspective – June 2016
  - https://d1.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf
- AWS Security by Design
  - https://aws.amazon.com/compliance/security-by-design/

Valuable (but FREE) AWS Security Resources (Cont.)

- AWS re:Invent 2017: A Deep Dive into AWS Encryption Services (SID329)
  - https://www.youtube.com/watch?v=gTZgxsCTfbk
- AWS re:invent 2017: Best Practices for Implementing AWS Key Management Service (SID330)
  - https://www.youtube.com/watch?v=X1eZjXQ55ecAWS
- AWS Key Management Service Best Practices – April 2017
  - https://d0.awsstatic.com/whitepapers/aws-kms-best-practices.pdf
- AWS Key Management Service Cryptographic Details – August 2018
  - https://d1.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf
- Encrypting Data at Rest – November 2014
  - https://d1.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf
- Encrypting File Data with Amazon Elastic File System - April 2018
  - https://d1.awsstatic.com/whitepapers/Security/amazon-efs-encrypted-filesystems.pdf
- Amazon Virtual Private Cloud Connectivity Options – January 2018
  - https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-vpc-connectivity-options.pdf

Questions and Answers

- Are there any questions?
- Thank you very much for your time.
- Presentation will be posted to: https://github.com/ScottHogg/
- Feel free to contact me if ever I can ever be of service to you.
  - Scott@HoggNet.com 303-949-4865 @ScottHogg