Welcome to the jungle!
Alfresco on Amazon Web Services

Robin Bramley
Chief Scientific Officer, Ixxus
• A Global Platinum-level Alfresco partner
• Working with Alfresco since Alfresco v0.6
• Over 140 Alfresco implementations
• Alfresco & WCM Architecture Design Patterns
• First worldwide implementation of the first Alfresco WCM product in 2007
• Excellent Alfresco knowledge and highly trained and experienced staff
  – Alfresco Certified Engineers and Alfresco Certified Administrators
  – Authoring of leading Alfresco books
  – Multiple speaking engagements at the Alfresco Conferences (2011-2014) and Alfresco Days
• Alfresco Million $ Club (May 2012) – Only 2 companies awarded
• Alfresco Solution Partner of the Year 2013 and 2014
• Alfresco Best Solution 2015 and Partner of the Year 2015 (Northern Europe)
Cloud
Cloud computing was inevitable... (a side-note on evolution)
IaaS

https://xkcd.com/908/
A quick AWS primer

https://www.flickr.com/photos/exfordy/2865944969/sizes/l
VPC

• Foundation of security
• Uses Software-Defined Networking (SDN)
• Allows definition of zones using subnets
Cloud Formation

- The AWS way of treating *Infrastructure as Code*
- Template your stack
- Describes the resources used

```json
"Ec2Instance" : {
    "Type" : "AWS::EC2::Instance",
    "Properties" : {
        "BlockDeviceMappings" : [
        ...
```
Elastic Compute Cloud (EC2)

- Virtual Server Hosting with resizable compute capacity
- Instance families are optimised for different use cases
  - M3 class (Ivy Bridge / Sandy Bridge) has SSD storage
  - M4 class (Haswell) is EBS only
  - xlarge has 4 vCPU → Alfresco Enterprise unit
- Load balance with ELB
Storage

• Ephemeral
• EBS
• EFS (preview)
• S3
• Glacier
RDS

- Managed Databases

- Multi-AZ (Availability Zone)
SES

• Simple Email Service
• Don’t bother with your own SMTP relays
CloudHSM

• **Hardware** Security Module
  – Appliances wired into a VPC
  – Not instantly provisioned

• Useful for master keys
  – E.g. RSA Private Key

• SafeNet Luna SA
  – JCE provider
  – Keys do not leave the hardware
Direct Connect

• Leased line connectivity
  – E.g. for England
    • Leased line to Docklands
    • Backhaul to AWS Ireland

• Reduced contention with Internet traffic!
Import/Export

• Introduced in 2009
• Send your 2TB disk packs to AWS
• Can be encrypted using TrueCrypt
• Contents copied to S3
• Returned by Courier
Snowball

- 50TB rugged, luggable disk pack
- Encrypted
- Copied to S3
- Amazon-owned
- Wiped to NIST SP 800-88 guidelines

October 2015
Case study
Migrating to Alfresco on AWS

• Top 20 global publisher
  – $1.5 billion revenue (2014)
  – 5,500 employees across 20 countries worldwide

• Programme involved several streams
  1. Major on-premises DAM replacement
  2. Rich Media
  3. Encryption at rest
  4. Reconciliation
Migration
Migration

- Higher Education print archive contained:
  - 85,000 products
  - ~1.8 million assets
  - ~35 TB of files
Encryption at rest
Symmetric encryption

Plain text

Key

Algorithm

Cipher text
Public-key cryptography

Encryption

Plain text → Public key → Cipher text → Cipher text

Decryption

Cipher text → Private key → Plain text

BeeCon 2016
S3 Connector classes
S3 encryption options

- **Unencrypted**
  - Alfresco Enterprise S3 Connector

- **Server-Side Encryption (SSE)**
  - Encryption: AWS
  - Key management: AWS
  - Alfresco Enterprise S3 Connector

- **SSE-C**
  - Encryption: AWS
  - Key management: Customer

- **Client-Side Encryption (CSE)**
  - Encryption: Customer
  - Key management: Customer
  - No offering!
  - Alfresco Cryptodoc

BeeCon 2016
OWASP Cryptographic Storage rules

① Only use **strong** cryptographic algorithms
② Store keys away from the encrypted data
③ Use **independent keys** when multiple keys are required
④ Protect keys in a key vault
⑤ Key substitution
   i. Build support for **changing keys** periodically
   ii. Rekey data at least every one to three years
Envelope Encryption

- **Symmetric (secret key) encryption** is fast
  - More suitable for encrypting content
- **Asymmetric (public key) encryption** is strong
  - Decryption is slower
- **Envelope encryption** uses separate keys
  - Envelope (data) keys
  - Master keys
S3 Connector modifications

- S3ServiceAdapterFactory
- S3ServiceAdapter
- S3ContentStore
- S3ContentReader
- S3ContentWriter
- S3StreamListener
- CryptoS3ServiceAdapterImpl
- KeyOperationsService
- S3Service
Encryption at rest
Encryption at rest
Closing comments

• The S3 Connector encryption modifications have been contributed back to Alfresco
• Any questions? Come find me afterwards...

• References
  – https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
  – http://www.ixxus.com/content-encryption-alfresco/

Robin Bramley @rbramley
• http://www.ixxus.com
• http://leanjavaengineering.com
Welcome to the jungle!
Alfresco on Amazon Web Services

Robin Bramley
Chief Scientific Officer, Ixxus