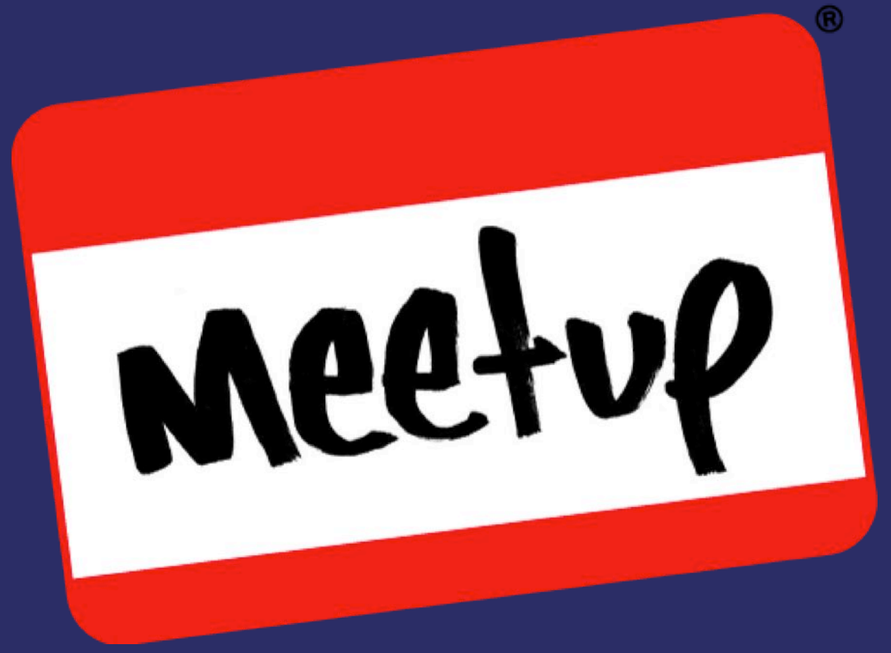
Survival Guide

Philipp Krenn

@xeraa

Electronic Data Interchange (EDI)

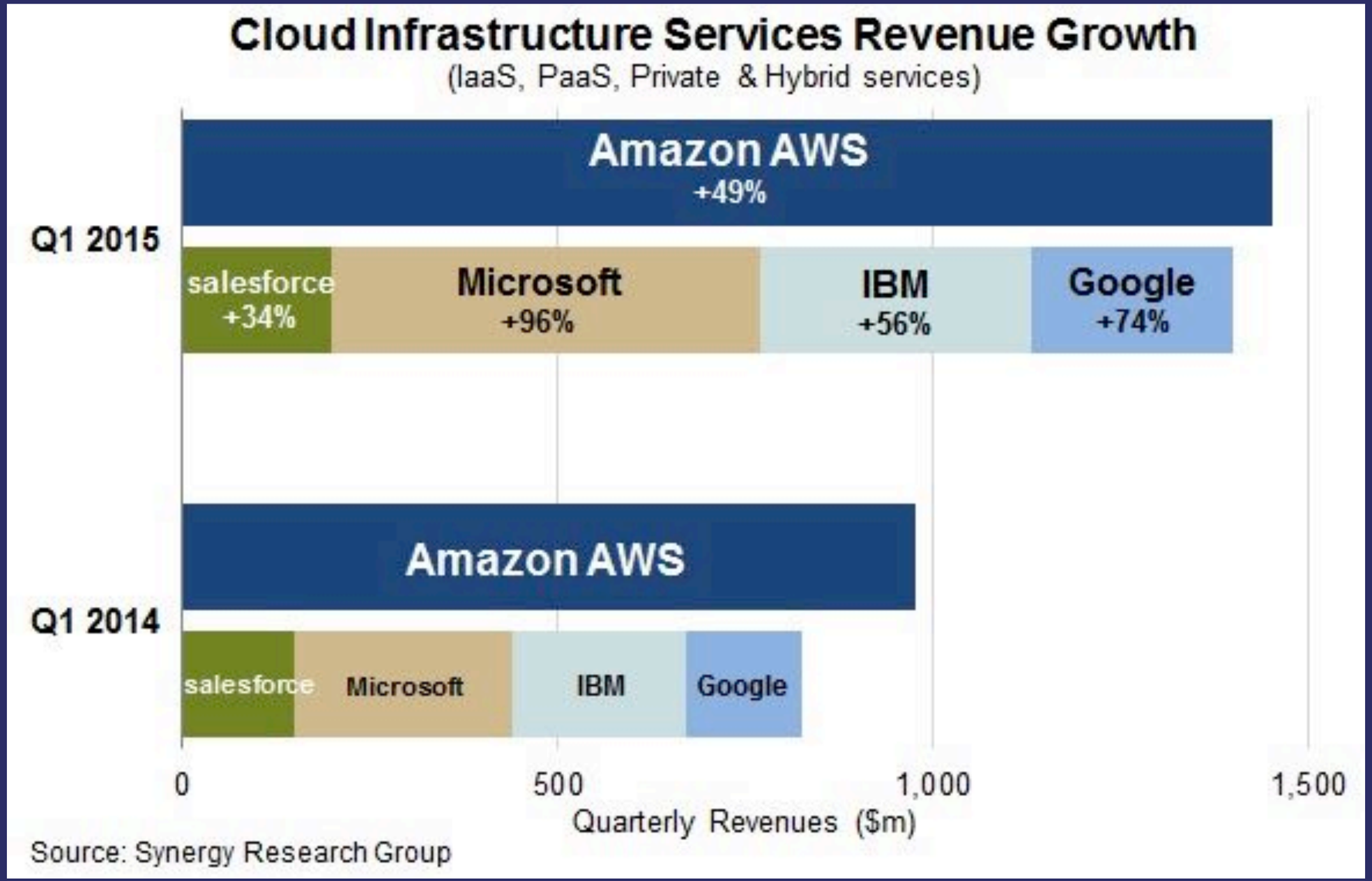


ViennaDB

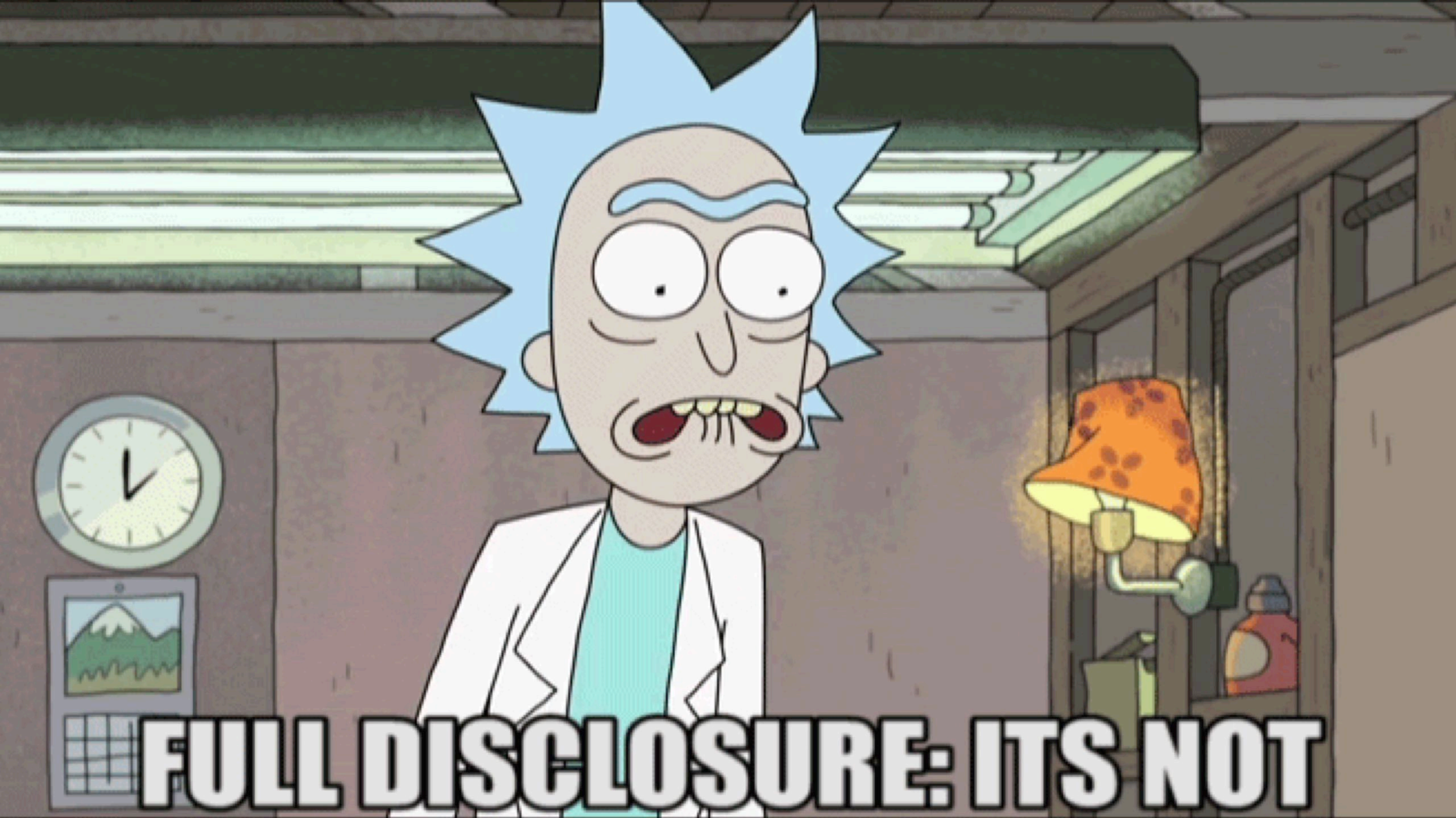
Papers We Love Vienna

Who uses

AWS, Azure,...?


Cloud Infrastructure Services Revenue Growth
(IaaS, PaaS, Private & Hybrid services)
Q1 2015
Amazon AWS
+49%
salesforce
+34%
Microsoft
+96%
IBM
+56%
Google
+74%
Q1 2014
Amazon AWS
salesforce
Microsoft
IBM
Google
0
500
1,000
1,500
Quarterly Revenues ($m)
Source: Synergy Research Group

Does the cloud solve all your security issues?


FULL DISCLOSURE: ITS NOT

"We can operate more securely on AWS than we can in our own data centers" Rob Alexander of CapitalOne #reinvent

— Adrian Cockcroft, https://twitter.com/adrianco/status/651788241557942272

AWS Security Bulletins

https://aws.amazon.com/security/security-bulletins/

Xen, Heartbleed,...

Securing your Infrastructure Account

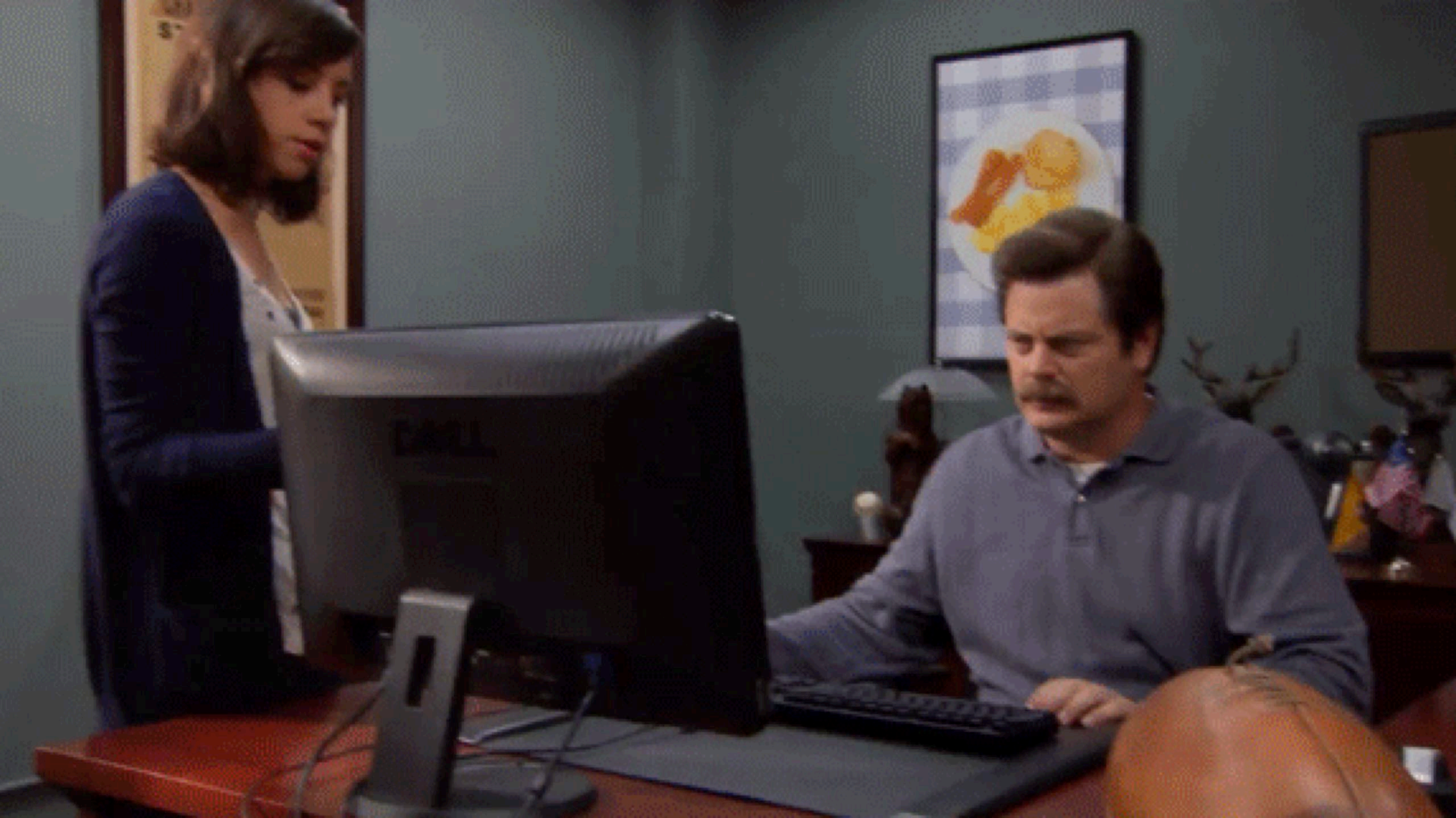
Infrastructure

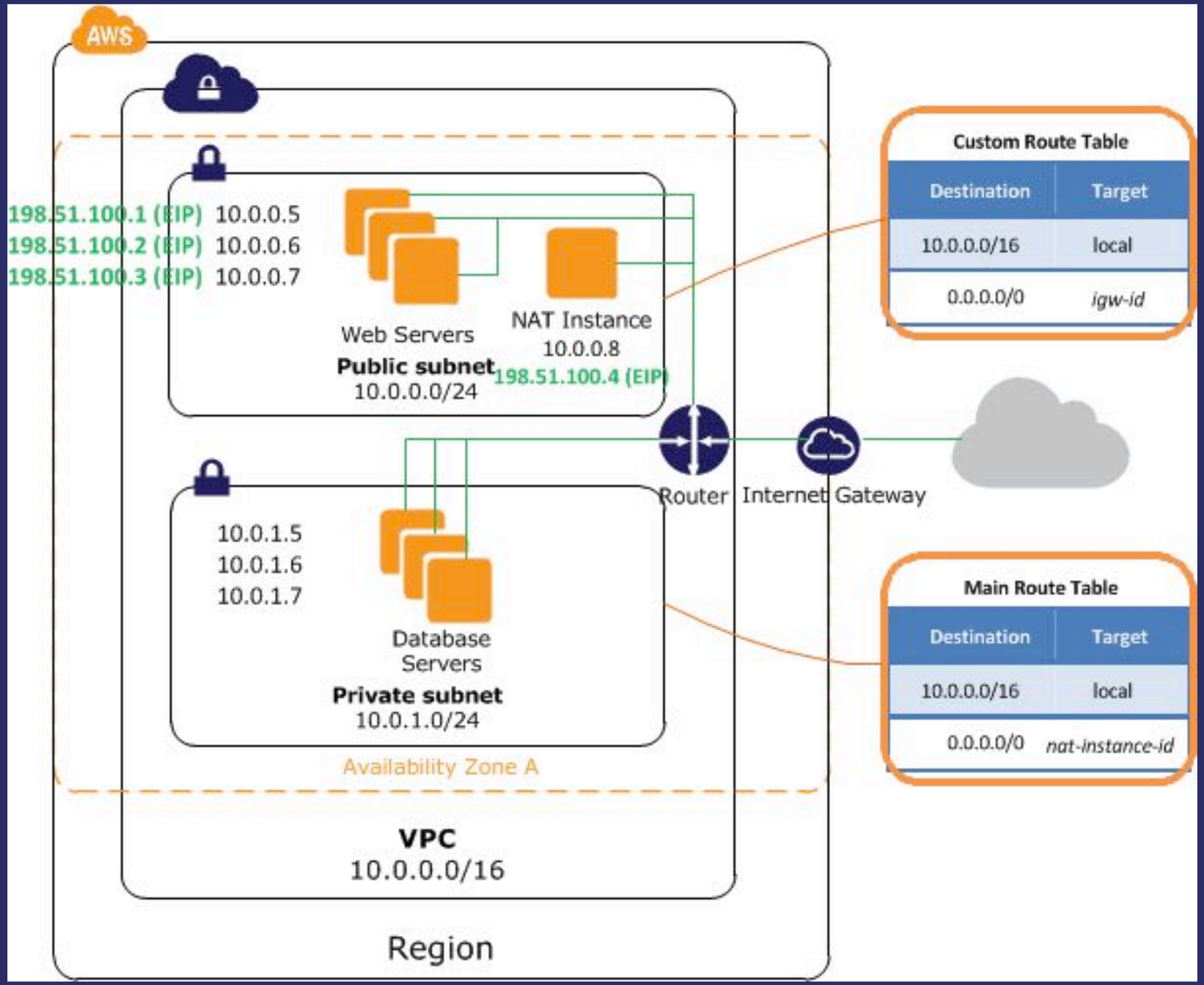
VPC

Virtual Private Cloud

EC2 Classic

Private and public IP on every instance




AWS
198.51.100.1 (EIP) 10.0.0.5
198.51.100.2 (EIP) 10.0.0.6
198.51.100.3 (EIP) 10.0.0.7
Web Servers
NAT Instance
10.0.0.8
198.51.100.4 (EIP)
Public subnet
10.0.0.0/24
Router
Internet Gateway
10.0.1.5
10.0.1.6
10.0.1.7
Database Servers
Private subnet
10.0.1.0/24
Availability Zone A
VPC
10.0.0.0/16
Region
Custom Route Table
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
igw-id
Main Route Table
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
nat-instance-id

Network /16

Production `10.0.*.*`

Development `10.1.*.*`

…

Availability Zones /18

A `10.*.0.0/18`

B `10.*.64.0/18`

Spare `10.*.128.0/18` **&** `10.*.192.0/18`

Subnets /20

A public `10.*.0.0/20`
A private `10.*.16.0/20`

A spare `10.*.32.0/20` **&** `10.*.48.0/20`

B public `10.*.64.0/20`
B private `10.*.80.0/20`

B spare `10.*.96.0/20` **&** `10.*.112.0/20`

PS: Networking

No broadcasts or multicasts

No IPv6 yet

Security Group

Per instance

Description | Inbound | **Outbound** | Tags

Edit

Type	Protocol	Port Range	Destination
HTTP	TCP	80	0.0.0.0/0
Custom TCP Rule	TCP	11371	0.0.0.0/0
SSH	TCP	22	10.1.0.0/16
Custom TCP Rule	TCP	27017	10.1.0.0/16
SMTPS	TCP	465	0.0.0.0/0
MYSQL/Aurora	TCP	3306	10.1.0.0/16
Custom UDP Rule	UDP	123	0.0.0.0/0
Custom TCP Rule	TCP	587	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
All ICMP	All	N/A	0.0.0.0/0

Network ACL

Per subnet (optional)

Second layer of defense

Default allow incoming & outgoing

Allow and deny

Order matters

Stateless

IAM

Identity and Access Management

Users are managed in Groups

AWS services are assigned Roles

Policies define permissions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::EXAMPLE-BUCKET-NAME"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::EXAMPLE-BUCKET-NAME/*"
    }
  ]
}
```

Create an IAM user / role for every person, service, and action

https://awspolicygen.s3.amazonaws.com/policygen.html

Encryption

at rest

S3, EBS, RDS,...

Transparent key management


REC
www.zalando.de

Microservices

Technologies & AWS account per team

OAuth for internal & external communication

Account

We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.

Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An **unauthorised** person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Reaching out to the address started a chain of events that revolved arount the person trying to extort a large fee in order to resolve the DDOS.

Upon realisation that somebody had access to our control panel we started to investigate how access had been gained and what access that person had to the data in our systems, it became clear that so far **no** machine access had been achieved due to the intruder not having our Private Keys

[…] our data, backups, machine configurations and offsite backups were either partially or completely deleted.

— http://www.codespaces.com

Important announcement: A recent security breach and the end of DrawQuest

DrawQuesters,

It is with great sadness and heavy hearts that we must share two unfortunate pieces of news.

1. We were recently made aware of a security breach that affected all of our servers hosted with Amazon, which comprises the entirety of DrawQuest. The person(s) used our account to order hundreds of expensive servers, likely to mine Bitcoin or other cryptocurrencies. When we detected this activity, we immediately locked down the account.

Unfortunately we have no way of knowing what, if any, information was accessed by the attacker(s). It's possible they only used our account to order servers, however it's also possible they accessed our database, and thus user e-mail addresses, encrypted passwords, and other information.

2. As a result of this breach, we will be shutting down DrawQuest *effective immediately*. With no full-time employees on staff to repair our infrastructure and ensure its integrity, we feel the only

The person(s) used our account to order hundreds of expensive servers, likely to mine Bitcoin or other cryptocurrencies.

— http://blog.drawquest.com

Service-wide outage

Incident Report for Bonsai

On Wednesday, June 19th, One More Cloud's services Websolr.com and Bonsai.io suffered a major extended outage. This outage was the result of an attack on our systems using a compromised API key.

We are so sorry for the severe impact to our customers and their businesses, and we regret the circumstances which made it possible.

Timeline

This outage was the result of an attack on our systems using a compromised API key.

— *http://status.bonsai.io/incidents/qt70mqtjbf0s*


IMPERIALBEDROOMS

1001 easy steps

0000

Lock away your root account and never use it

0001

Always use an IAM account

0010

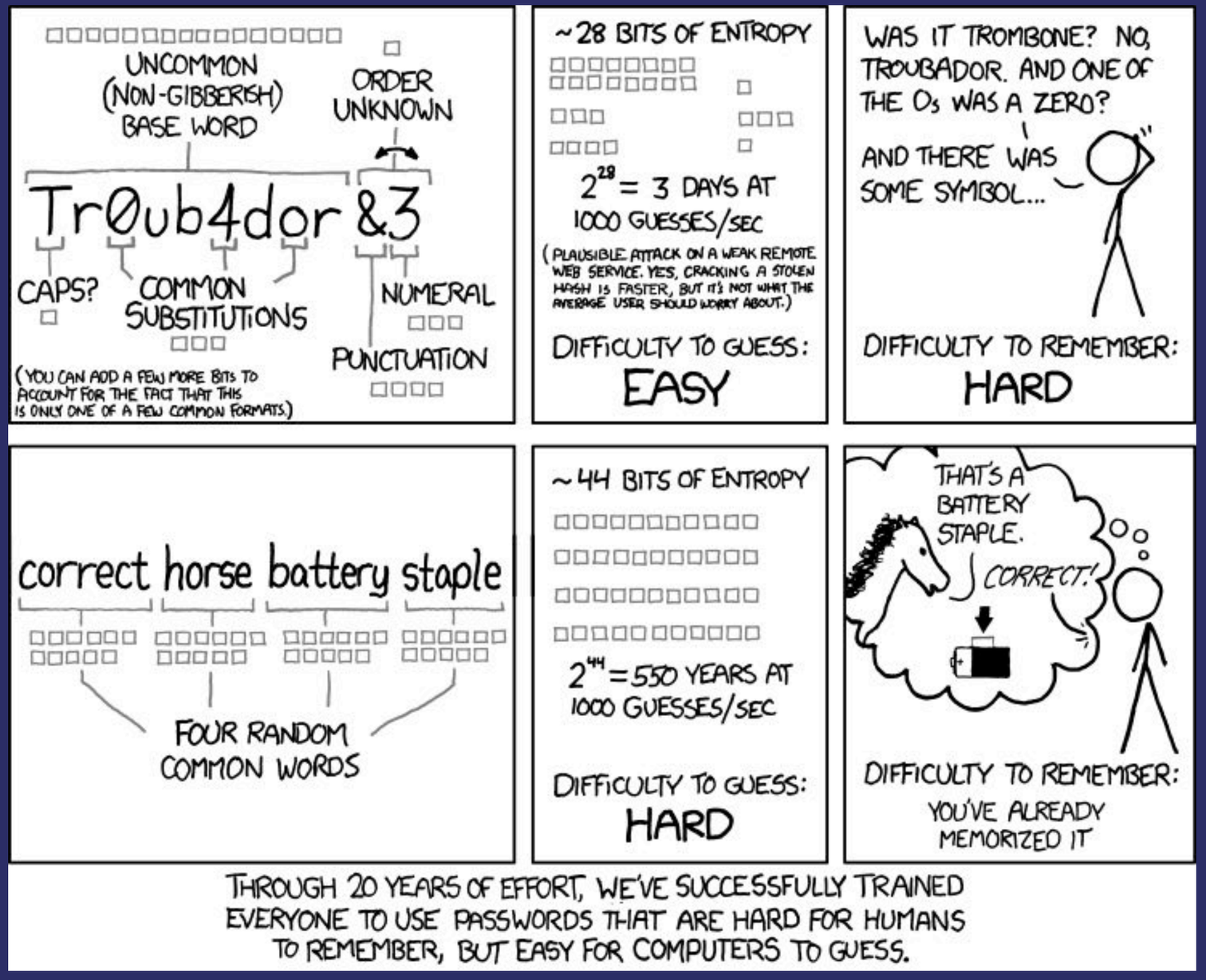
Only allow what is necessary

Principle of the least access

```
{ "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ec2:ReleaseAddress",
                "route53:DeleteHostedZone"
            ],
            "Resource": "*"
        }
] }
```

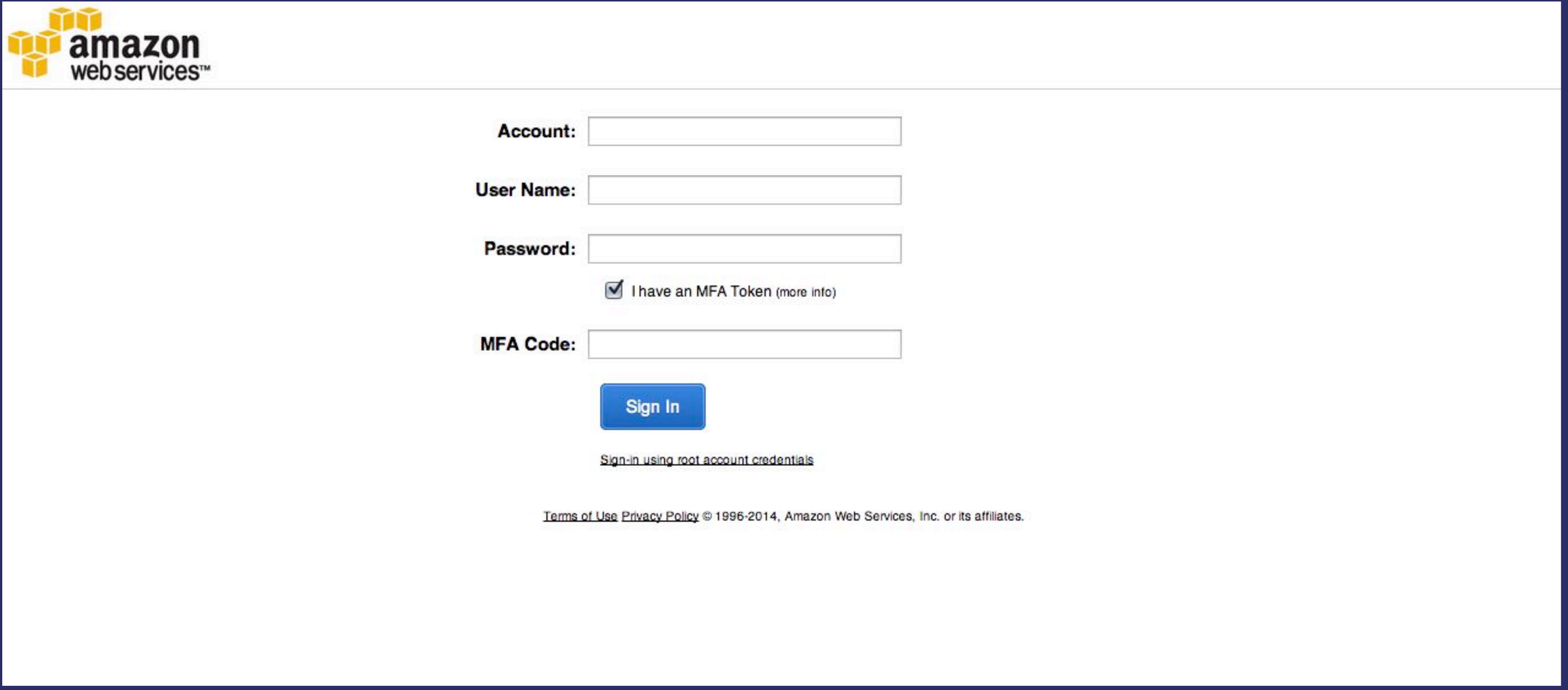
0011

Use strong passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

0100

Use Multi Factor Authentication (MFA)


amazon
web services™
Account:
User Name:
Password:
I have an MFA Token (more info)
MFA Code:
Sign In
Sign-in using root account credentials
Terms of Use Privacy Policy © 1996-2014, Amazon Web Services, Inc. or its affiliates.


10:45
Saturday, 11 January

0101

Never commit your credentials

Where to keep your secrets?

1. Environment variables
2. Encrypted files in SCM
3. Fancy tools

http://ejohn.org
/blog/keeping-passwords-in-source-control/


jQuery
write less, do more.

```
#!/bin/sh

FILE=$1
FILENAME=$(basename "$FILE")
EXTENSION="${FILENAME##*.}"
NAME="${FILENAME%.*}"

if [[ "$EXTENSION" != "aes256" ]]
then
     echo "Encrypting $FILENAME and removing the plaintext file"
     openssl aes-256-cbc -e -a -in $FILENAME -out ${FILENAME}.aes256
     rm $FILENAME
else
then
     echo "Decrypting $FILENAME"
     openssl aes-256-cbc -d -a -in $FILENAME -out $NAME
fi
```

```
$ ls
truststore.jks.aes256

$ encrypt-decrypt.sh truststore.jks.aes256
Contact operations@ecosio.com for the password
Decrypting truststore.jks.aes256
enter aes-256-cbc decryption password:

$ ls
truststore.jks      truststore.jks.aes256
```

Tools

Ansible Vault, HashiCorp Vault,...

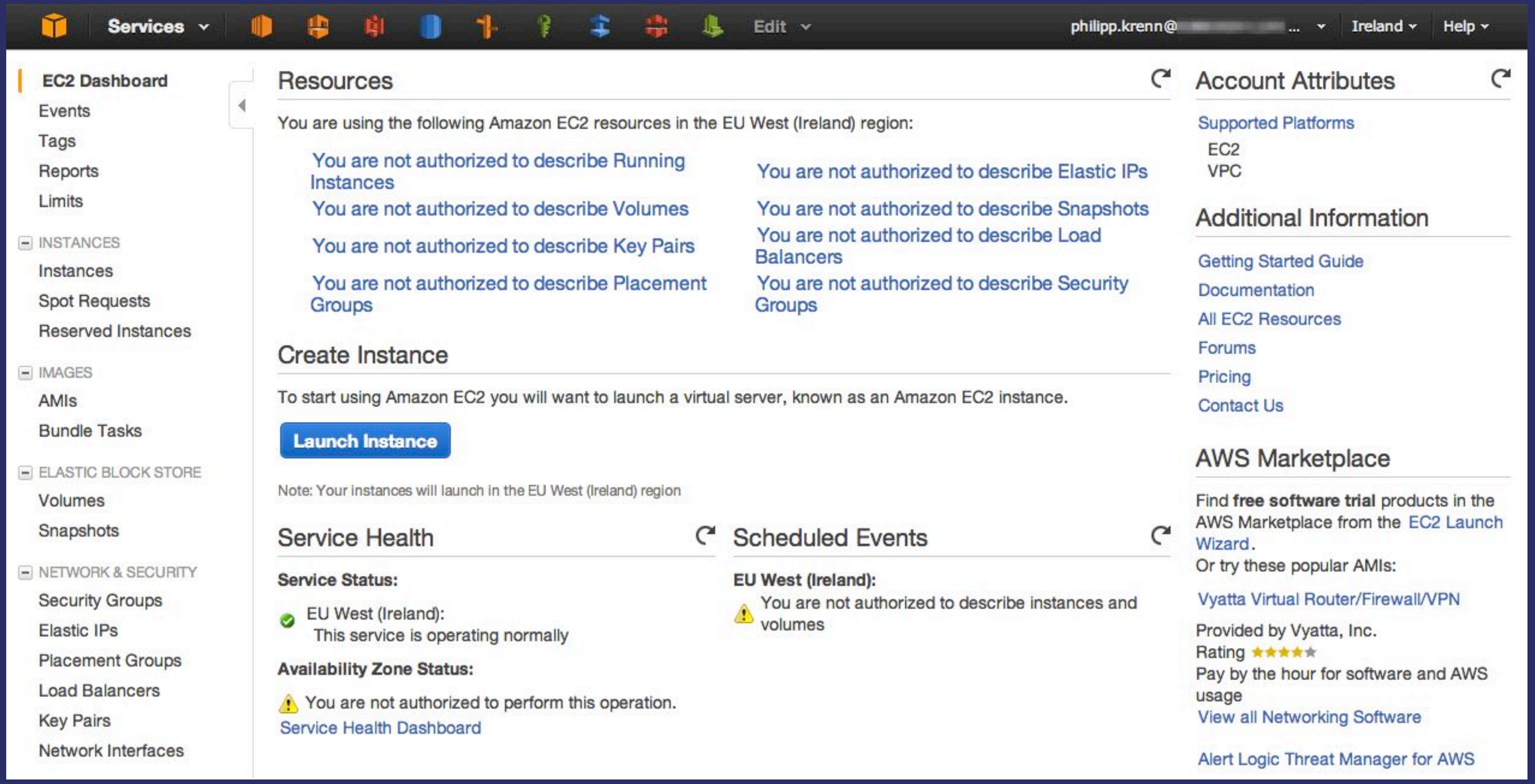
Check your code

https://github.com/michenriksen/gitrob

0110

Enable IP restrictions

```
{ "Statement": [
      {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
      },
      {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                  "NotIpAddress": {
                        "aws:SourceIp": ["1.2.3.4/24", "5.6.7.8/28"]
                  }
            }
      }
] }
```


Services
Edit
philipp.krenn@ ...
Ireland
Help
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Load Balancers
Key Pairs
Network Interfaces
Resources
You are using the following Amazon EC2 resources in the EU West (Ireland) region:
You are not authorized to describe Running Instances
You are not authorized to describe Elastic IPs
You are not authorized to describe Volumes
You are not authorized to describe Snapshots
You are not authorized to describe Key Pairs
You are not authorized to describe Load Balancers
You are not authorized to describe Placement Groups
You are not authorized to describe Security Groups
Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.
Launch Instance
Note: Your instances will launch in the EU West (Ireland) region
Service Health
Service Status:
EU West (Ireland):
This service is operating normally
Availability Zone Status:
You are not authorized to perform this operation.
Service Health Dashboard
Scheduled Events
EU West (Ireland):
You are not authorized to describe instances and volumes
Account Attributes
Supported Platforms
EC2
VPC
Additional Information
Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us
AWS Marketplace
Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard.
Or try these popular AMIs:
Vyatta Virtual Router/Firewall/VPN
Provided by Vyatta, Inc.
Rating
Pay by the hour for software and AWS usage
View all Networking Software
Alert Logic Threat Manager for AWS

0111

Enable billing alerts

ALARM: "BillingAlert" in US - N. Virginia

You are receiving this email because your estimated charges are greater than the limit you set for the alarm "BillingAlert" in AWS Account [redacted].

The alarm limit you set was $ 2000.00 USD. Your total estimated charges accrued for this billing period are currently $ [redacted] USD as of Friday 01 August, 2014 01:54:21 UTC. The actual charges you will be billed in this statement period may differ from the charges shown on this notification. For more information, view your estimated bill at:
https://console.aws.amazon.com/billing/home#/bill?year=2014&month=8

More details about this alarm are provided below:

Amazon CloudWatch Alarm "BillingAlert" in the US - N. Virginia region has entered the ALARM state, because "Threshold Crossed: 2 datapoints were greater than or equal to the threshold (2000.0). The most recent datapoints: [redacted]." at "Friday 01 August, 2014 01:54:21 UTC".

View this alarm in the AWS Management Console:
https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#s=Alarms&alarm=BillingAlert

Alarm Details:
- Name: BillingAlert
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 2 datapoints were greater than or equal to the threshold (2000.0). The most recent datapoints: [redacted].
- Timestamp: Friday 01 August, 2014 01:54:21 UTC
- AWS Account: [redacted]

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 2000.00 for 3600 seconds.

Monitored Metric:
- MetricNamespace: AWS/Billing
- MetricName: EstimatedCharges

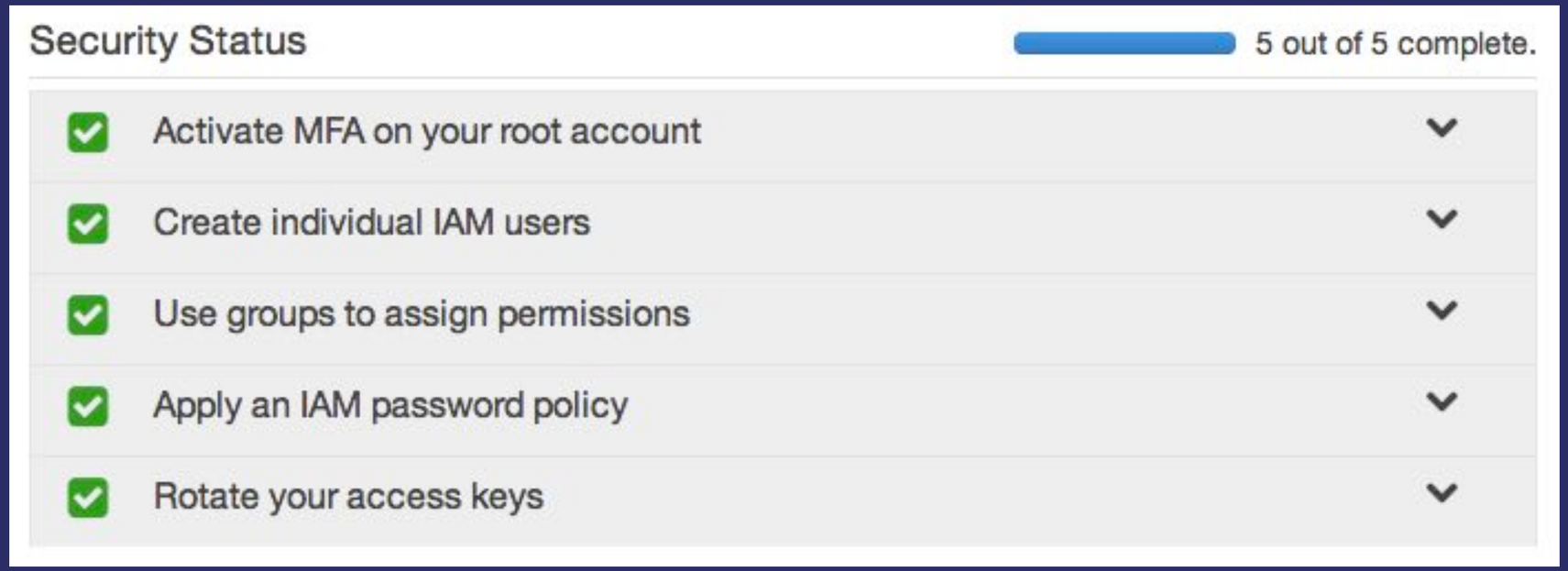
1000

Enable CloudTrail

```
{ "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
        },
        "eventTime": "2015-09-09T19:01:59Z",
        "eventSource": "ec2.amazonaws.com",
        "eventName": "StopInstances",
        "awsRegion": "eu-west-1",
        "sourceIPAddress": "205.251.233.176",
        "userAgent": "ec2-api-tools 1.6.12.2",
        "requestParameters": {
            "instancesSet": {
                "items": [
                    { "instanceId": "i-ebeaf9e2" }
                ]
            },
            "force": false
        },
        ...
    },
    ...
] }
```

1001

Check Your Security Status


Security Status
5 out of 5 complete.
Activate MFA on your root account
Create individual IAM users
Use groups to assign permissions
Apply an IAM password policy
Rotate your access keys

Bonus

Premium Support: Trusted Advisor *Security*

- **Dashboard**
  - Cost Optimization
  - Performance
  - Security
  - Fault Tolerance
- Preferences

Trusted Advisor Dashboard

Cost Optimization	Performance	Security	Fault Tolerance
			
4 ✓ 3 ⚠ 0 !	5 ✓ 3 ⚠ 0 !	5 ✓ 4 ⚠ 2 !	9 ✓ 5 ⚠ 1 !
0 excluded items	0 excluded items	7 excluded items	1 excluded items
$1,292.42 Potential monthly savings			

Recent Changes

✓	Idle Load Balancers	5/12/15
⚠	CloudFront Content Delivery Optimization	5/12/15
✓	Amazon EC2 Reserved Instances Optimization	5/12/15

What's New

Checks: Trusted Advisor adds four new checks for Elastic Load Balancing
Features: Introducing Trusted Advisor Action Links
Checks: Service Limits check improvements
Checks: AWS CloudTrail and 4 Amazon Route 53 checks

Conclusion

No Magic

Just do your homework

140 servers running on my AWS account. What? How? I only had S3 keys on my GitHub and they where gone within 5 minutes!

— http://www.devfactor.net/2014/12/30/2375-amazon-mistake/

If a key is compromised, rotate it!

How a bug in Visual Studio 2015 exposed my source code on GitHub and cost me $6,500 in a few hours

— https://www.humankode.com/security/how-a-bug-in-visual-studio-2015-exposed-my-source-code-on-github-and-cost-me-6500-in-a-few-hours

And never commit your credentials!

Thank you!

Questions?

@xeraa