Are You Sure Your AWS Cloud Is Secure?

Alan Williamson
Solution Architect at
TriNimbus

60 Second AWS Security Review

AWS Terminology

Identity and Access Management (IAM) - AWS Security Service to manage resources.

IAM User - An entity who authenticates. For example, people.

IAM Group - A collection of IAM Users

IAM Role - An entity that is assumed by an authenticated user.

IAM Policies - A set of granular permissions attached to an IAM User, Group, or Role to control access to AWS resources

Key Management Service(KMS) - Service providing Master Keys supporting envelope encryption of data keys, commonly used in storage encryption

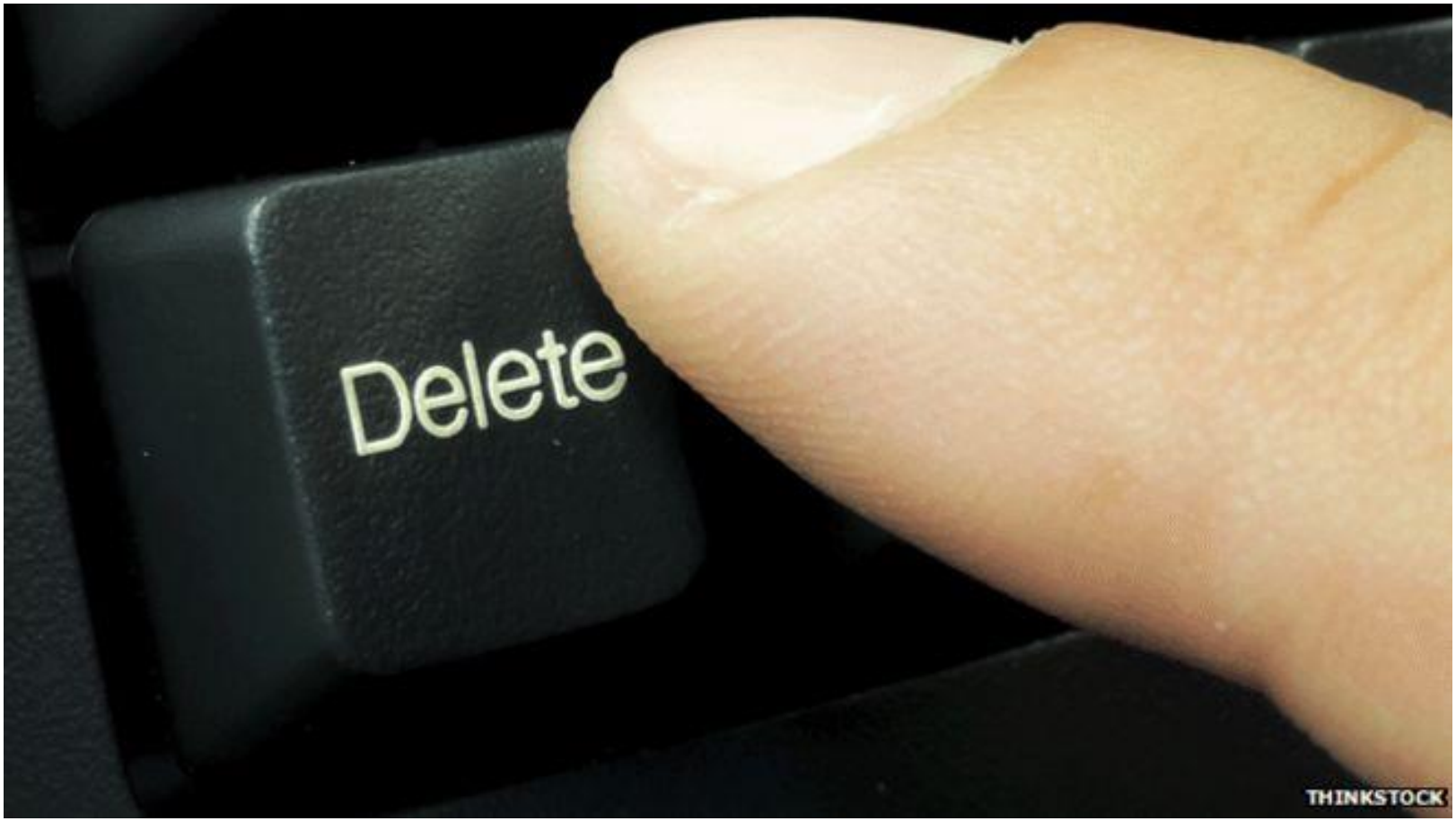
What this discussion is not

- An intro to AWS Security
- How to write IAM policies
- Comparing different authentication options
- Best practices for designing IAM
- A complete list of actions to secure your AWS Account

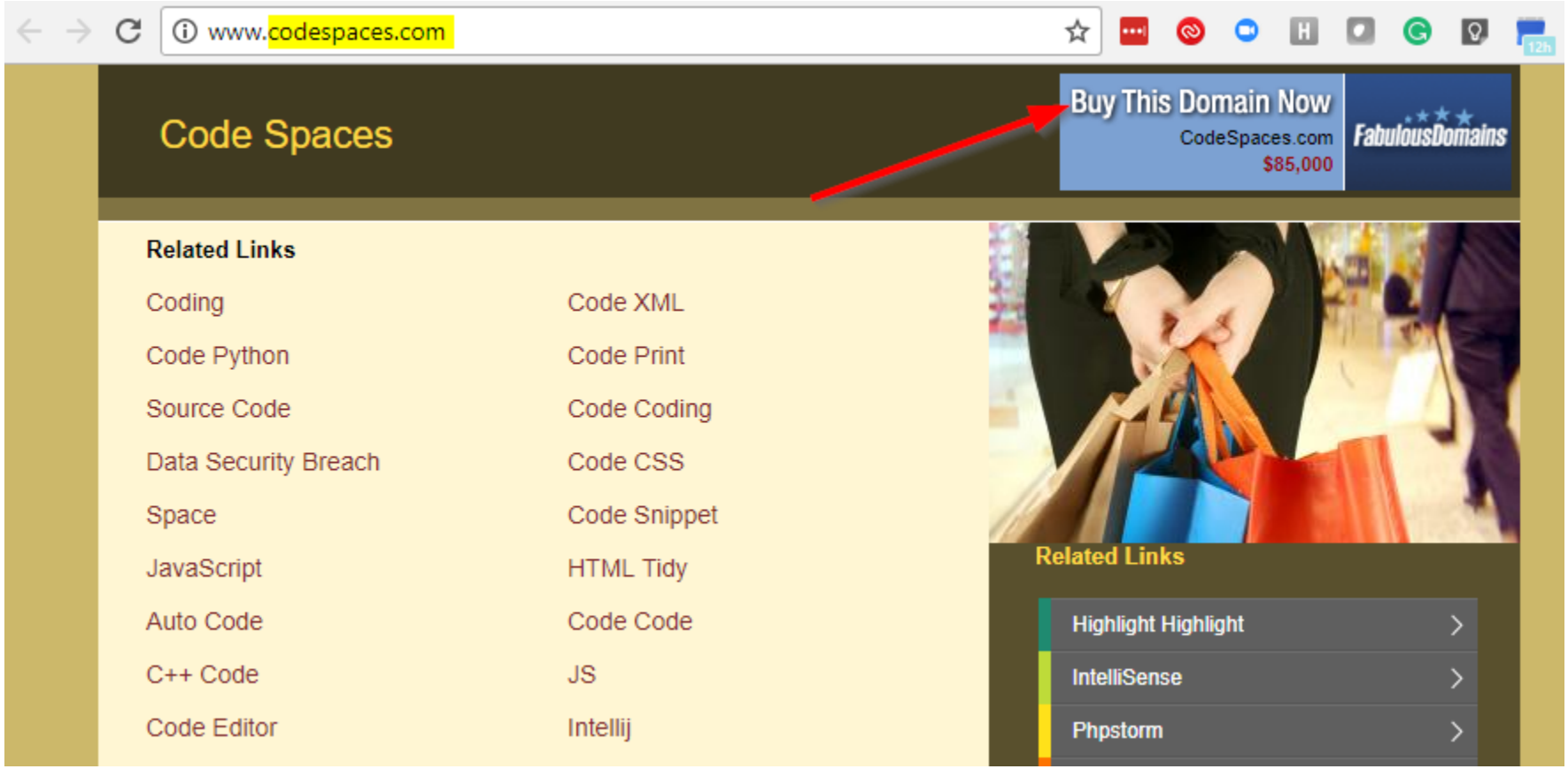
Disaster Proof?

Designed to tolerate this

What about this?



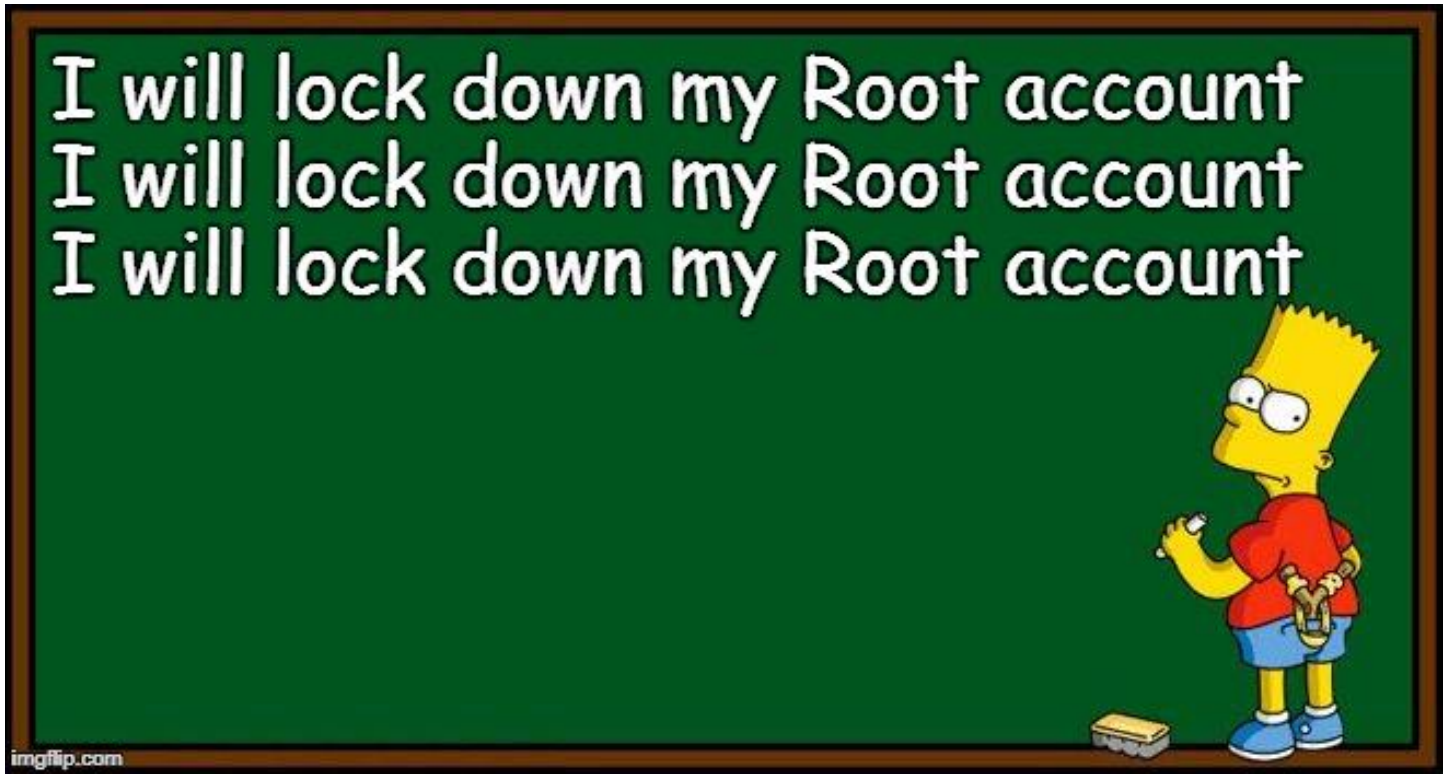
The Code Spaces Story



Lessons Learned

Root Account Lockdown

- MFA enabled
- Very complex password
- No access keys
- Email distro for visibility on reset requests
- Alert on use



Restrict Admin Usage

- Avoid IAM Roles and Groups for general admins
- Principle of least privilege
- Require MFA
- Example conditions:
  - Source IP Address
  - SAML Users only
  - AWS Services only
  - AWS Region

Credential Reports

- User creation time
- Is MFA enabled for user
- Monitor passwords and access keys for:
  - Is enabled
  - Last used time
  - Last changed time
  - Last used service (keys only)
  - Last used region (keys only)

Escrow Accounts

- Use a separate AWS account
- Save data in other AWS regions
- Pull data from the escrow account
- Re-encrypt data using escrow account keys

Escrow Accounts Continued

- No access to both general and escrow accounts
- Use physical MFA. Test logins quarterly.
- Replicate audit data with higher frequency
- Don't forget code, templates and important logs

Your IAM Users All Have **MFA** Enabled, it's All Good Right?

MFA Setup for User

Users > alan.test

Summary

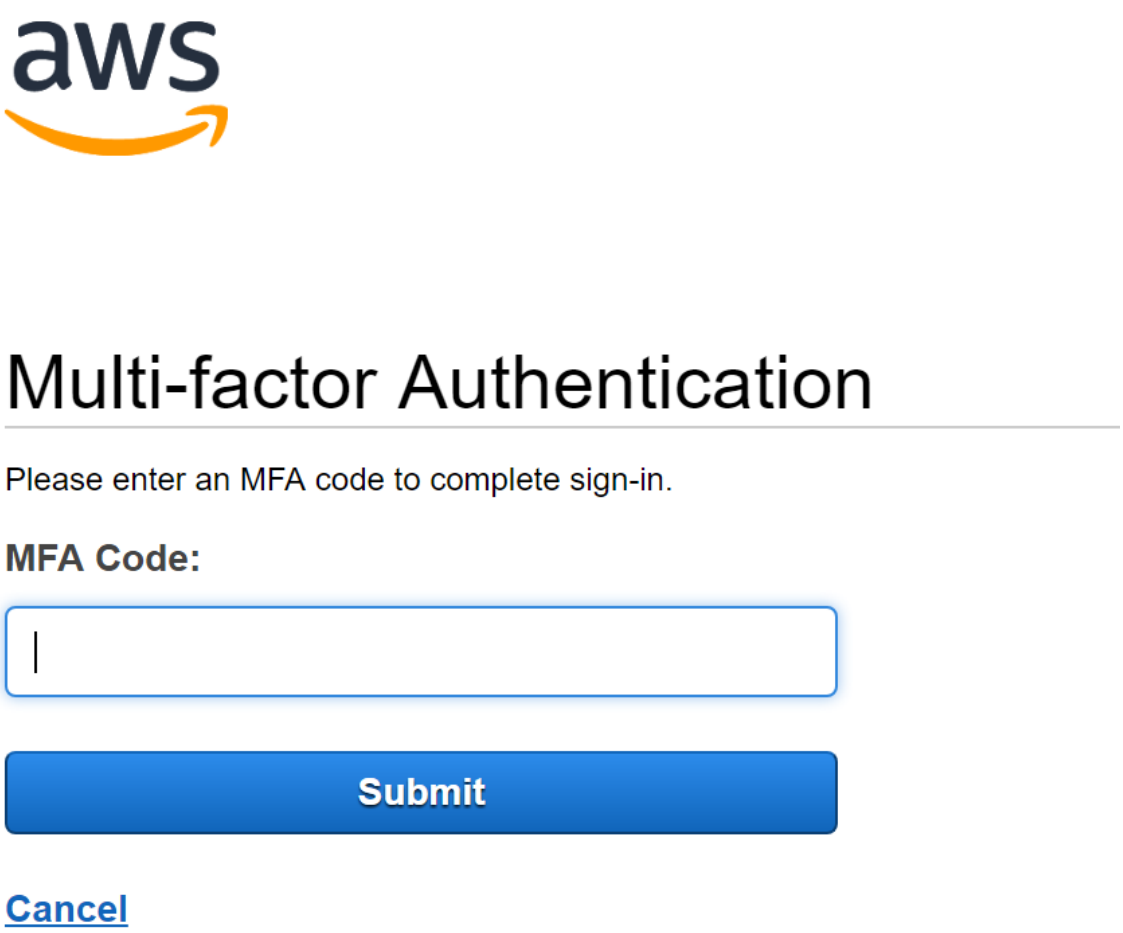
User ARN	arn:aws:iam::[redacted]:user/alan.test
Path	/
Creation time	2016-01-24 22:09 EST

Permissions | **Groups (1)** | **Security credentials** | **Access Advisor**

Sign-in credentials

Console password	Enabled Manage password
Console login link	https://trinimbus.signin.aws.amazon.com/console
Last login	2016-01-25 12:19 EST
Assigned MFA device	arn:aws:iam::[redacted]mfa/alan.test

AWS Console Login



Same User with CLI

```
C:\>aws ec2 describe-vpcs --profile trinimbus-test --region
 ca-central-1  --query "Vpcs[].[State,IsDefault]"
[
    [
        "available",
        true
    ]
]

C:\>_
```

No MFA Prompt

What?!? How do I fix that?

IAM Role Assumption Design

1. **IAM User** - Little to no access

2. **Power user role**- Day to day resources.
   Require: ✓MFA

3. **Admin role -** Everything but security controls or mission critical resources.
   Require: ✓MFA ✓trusted IP

4. **AWS SUDO role** - Access it all*
   Require: ✓MFA ✓trusted IP
   ✓Notifications on role assumptions

Other MFA Gotchas

ADFS - AWS MFA is enforced for IAM Users. If you use ADFS (SAML) look at RADIUS.

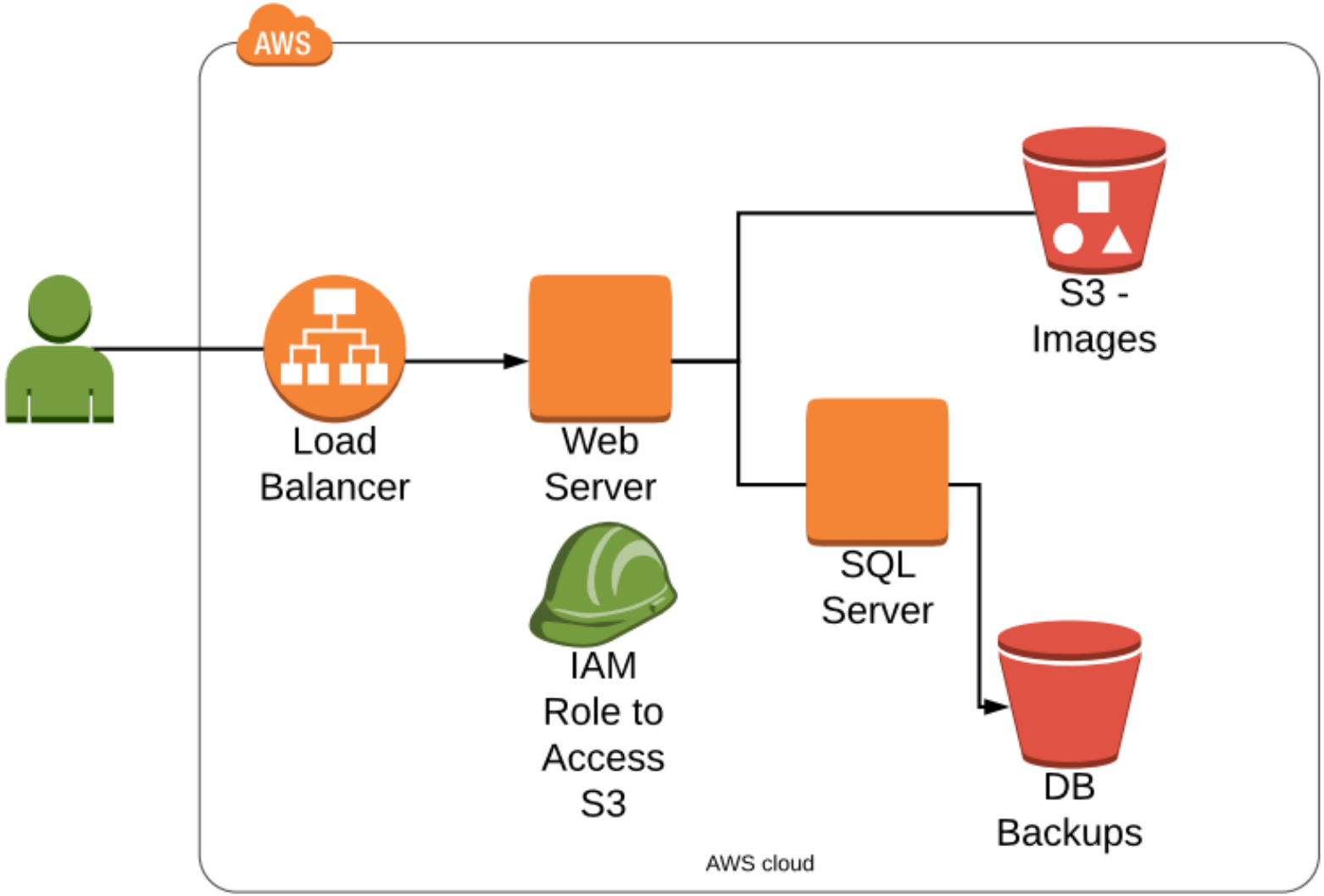
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/mfa.html

Time-based one-time password (TOTP) - If scripting, cache temp credentials. No code re-use within 30 seconds.

https://tools.ietf.org/html/rfc6238

Protecting Your Data in the Cloud.

Web App Serving Content from S3



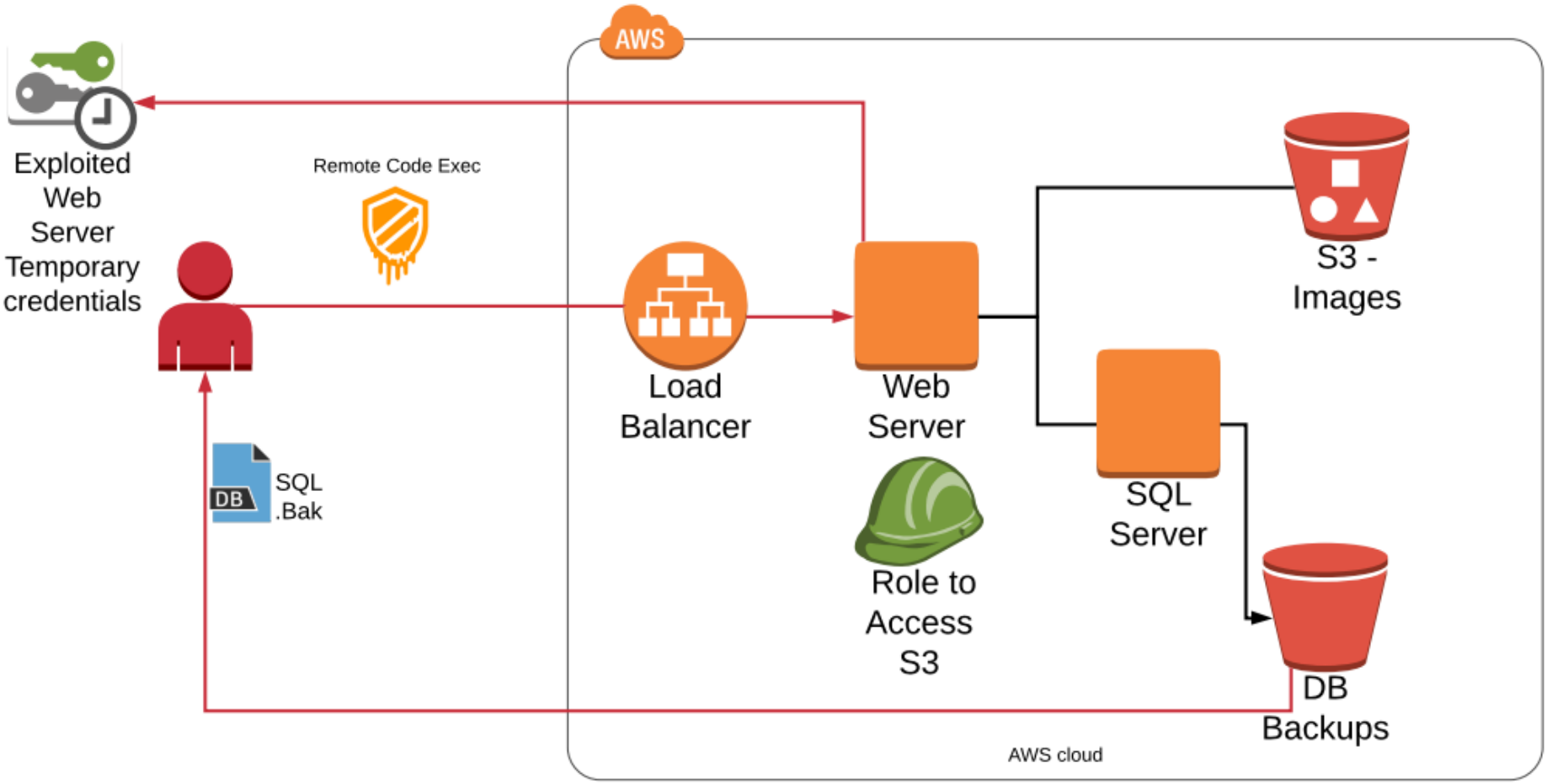
“AmazonEC2RoleforAWSCodeDeploy” Policy

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Action": [
6                  "s3:GetObject",
7                  "s3:GetObjectVersion",
8                  "s3:ListBucket"
9              ],
10             "Effect": "Allow",
11             "Resource": "*"
12         }
13     ]
14 }
```

Download

Any S3 Bucket

Unscoped IAM policy on Web Server

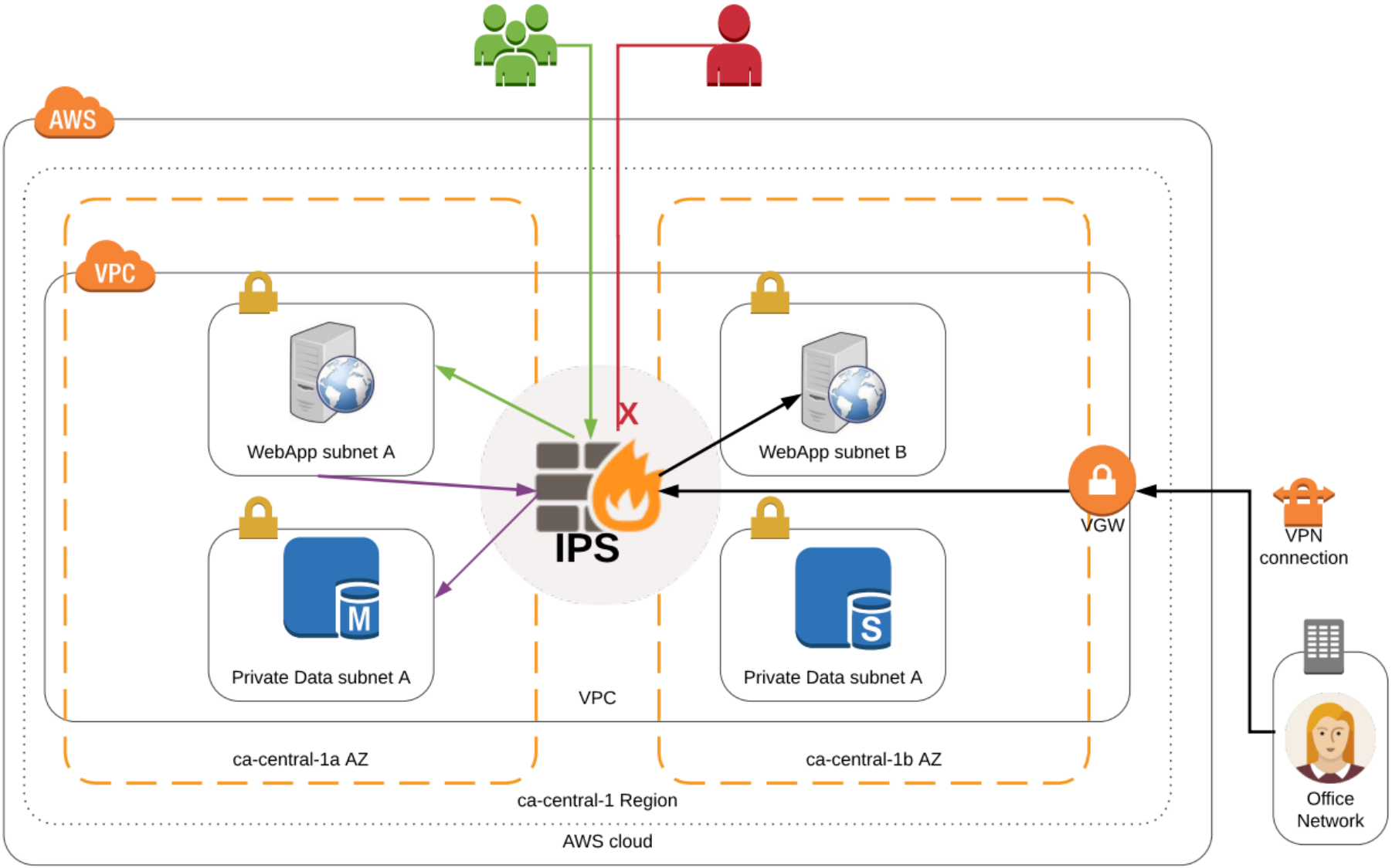


Customer Managed Policies

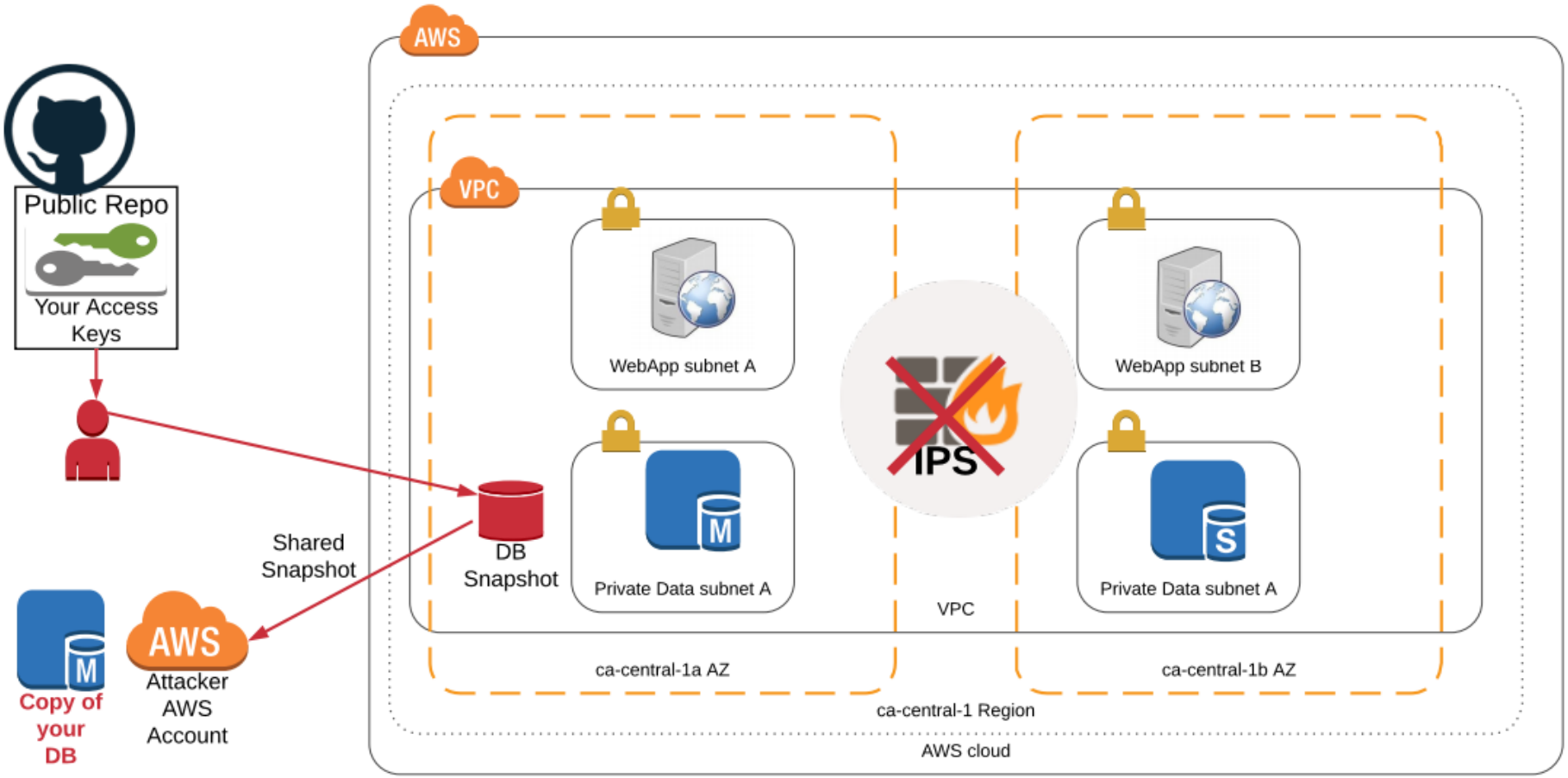
Resource Policy Lockdown

- Supported by some AWS Services
- Explicit denies help prevent access problems from unscoped IAM policies
- Use S3 Bucket Policies to lock down data stores, audit logs, etc.
- Reminder: KMS Master Keys require a Key Policy or Key Grant in addition to IAM
- Use KMS Key Grants on Master Keys for more granular controls than key policies

Traditional IPS Solution in AWS



Bypassing the Network With APIs




We scan your prior GitHub commits for access keys
DO YOU?
imgflip.com

Reducing the Impacts From Attacks

A $1843 USD Lesson

Misconfigured .gitignore file uploaded access keys in error

Within hours unusual activity was noticed on a weekend.

9 * c4.8xlarge

3 * m4.16xlarge

$23.92 USD / HR Compute in us-west-2

Could Have Been Worse!

$23.92 USD / hr / region

* 16 regions

$383 USD / hr

* 24 hours / day

$9,185 USD / day

Service Limits

Set appropriate service limits:

- Set low limits (i.e. 0) in unused regions
- Set limit to 0 for high cost unused instance types
- Use Trust Advisor to monitor service limits

Use Service Control Policies

- Use AWS Organizations
- Manage groups of related AWS accounts in OUs
- Apply Service Control Policies to whitelist or blacklist AWS Services

Reminder: Can limit Root account service usage on member accounts, but doesn't prevent all actions (for example closing accounts).

Logging Into EC2 Instances With Your EC2 Key Pairs.

EC2 Key Pairs on Linux

- 2048-bit RSA keys pair
- Public key copied to instance for SSH access at launch
- Applied to known users with root access
- Can't be changed / revoked

EC2 Key Pairs on Windows

- **Administrator password reset** at instance launch
- Password is **encrypted** with public part of key pair and sent to EC2 service
- Private key **decrypts** the new password accessible from the EC2 service
- Password data is not kept in **sync** with Windows.

EC2 Keypair Alternatives

Centralized Auth

- Launch with a secured break glass key
- Use a tool like Active Directory

Configuration Management

- Launch without a key pair
- Use dynamic config management tool to maintain users

Avoid Logging In

- Run Command for ad hoc operations
- Configuration Management tool for changes
- Enable users via Run Command as needed

AWS System Manager - Run Command

Select Command

Owned by Me or Amazon | Filter by attributes

	Name	Owner	Platform type
○	AWS-ConfigureCloudWatch	Amazon	Windows
○	AWS-ConfigureWindowsUpdate	Amazon	Windows
○	AWS-FindWindowsUpdates	Amazon	Windows
○	AWS-InstallApplication	Amazon	Windows
○	AWS-InstallMissingWindowsUpdates	Amazon	Windows
○	AWS-InstallPowerShellModule	Amazon	Windows
○	AWS-InstallSpecificWindowsUpdates	Amazon	Windows
○	AWS-JoinDirectoryServiceDomain	Amazon	Windows
○	AWS-ListWindowsInventory	Amazon	Windows
●	AWS-RunPowerShellScript	Amazon	Windows
○	AWS-RunShellScript	Amazon	Linux
○	AWS-UpdateEC2Config	Amazon	Windows
○	AWS-UpdateSSMAgent	Amazon	Windows,Linux

Choose Targets

Target instances

i-09

Select instances

Where are my instances?

Filter by attributes

1 to 2 of 2

	Name	Instance ID	Instance State	Availability Zon	Ping Status	L
■	Windows Run ...	i-09	running	us-east-1a	Online	M
☐	Windows Run ...	i-0a	running	us-east-1a	Online	M

Close

Enter Command Parameters

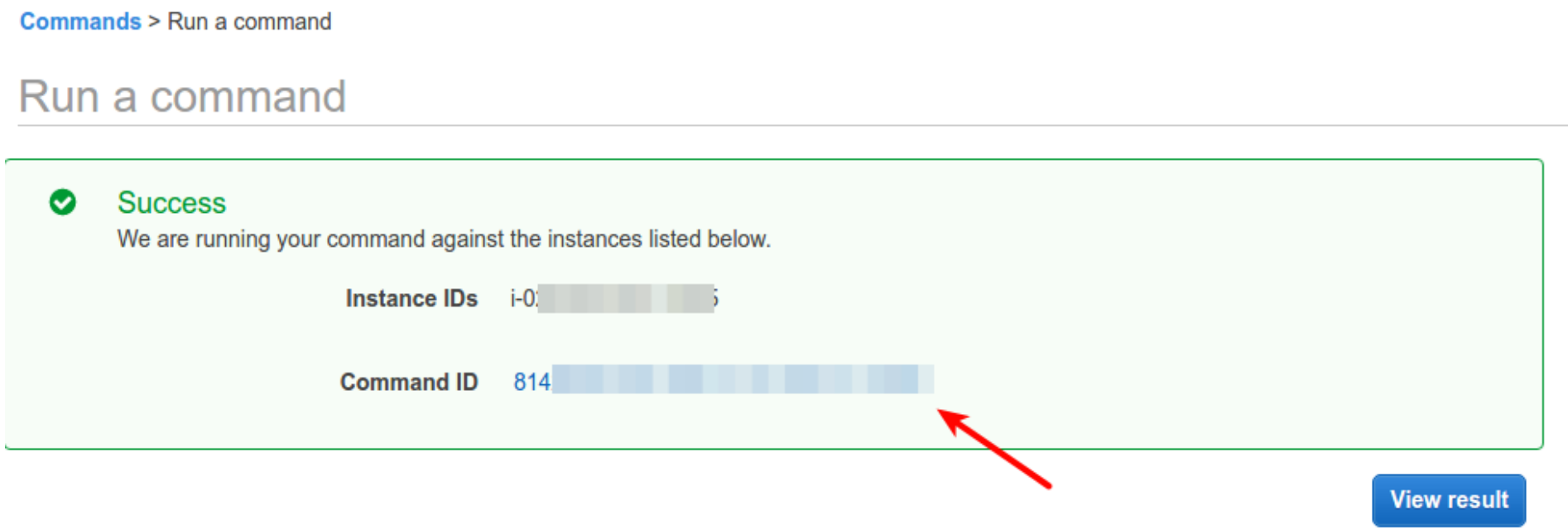
Commands*

```
fsutil volume diskfree c:
```

Commands*

```
df -h
```

Less Than a Second Later



Example Results

Commands > Output

Output for aws:runPowerShellScript

```
Total # of free bytes          : 11892555776
Total # of bytes               : 31843151872
Total # of avail free bytes    : 11892555776
```

Commands > Output

Output for aws:runShellScript

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        488M   56K  488M   1% /dev
tmpfs           498M     0  498M   0% /dev/shm
/dev/xvda1      7.8G  987M  6.7G  13% /
```

Custom Commands

```
1  {
2    "schemaVersion": "2.0",
3    "description": "Reset Local User Password.",
4    "parameters": {
5      "Username": {
6        "type": "String",
7        "description": "Name of the local user account to reset"
8      },
9      "NewPassword": {
10       "type": "String",
11       "description": "The new password to use"
12     }
13   },
14   "mainSteps": [{
15     "action": "aws:runPowerShellScript",
16     "name": "ChangeLocalUserPassword",
17     "inputs": [{
18       "runCommand": ["net user {{ Username }} {{ NewPassword }}"]
19     }]
20   }]
21 }
```

Limited User Input

Command parameters

Description

Reset Local User Password.

Username

Name of the local user account to reset

Bob

New Password

The new password to use

Bob'sNewP@ssword

Other parameters

Comment

(Optional) Type a note about the command

Resetting Bob's password on the inventory application's SQL Server

CloudTrails Audit Record


```
"eventSource": "ssm.amazonaws.com",
"eventName": "SendCommand",
"awsRegion": "us-east-1",
"sourceIPAddress": "[redacted]",
"userAgent": "aws-cli/1.11.66 Python/2.7.6 Linux/4.4.0-64-generic botocore/1.5.29",
"requestParameters": {
  "targets": [{
    "key": "tag:Role",
    "values": ["WebServer"]
  }],
  "documentName": "ExampleChangeHTTPDPassword",
  "maxConcurrency": "20%",
  "maxErrors": "2"
},
"responseElements": null,
"requestID": "05[redacted]",
"eventID": "d7[redacted]",
"resources": [{
  "ARN": "arn:aws:ssm:us-east-1:[redacted]:document/ExampleChangeHTTPDPassword",
```

Command Specific Access Policy

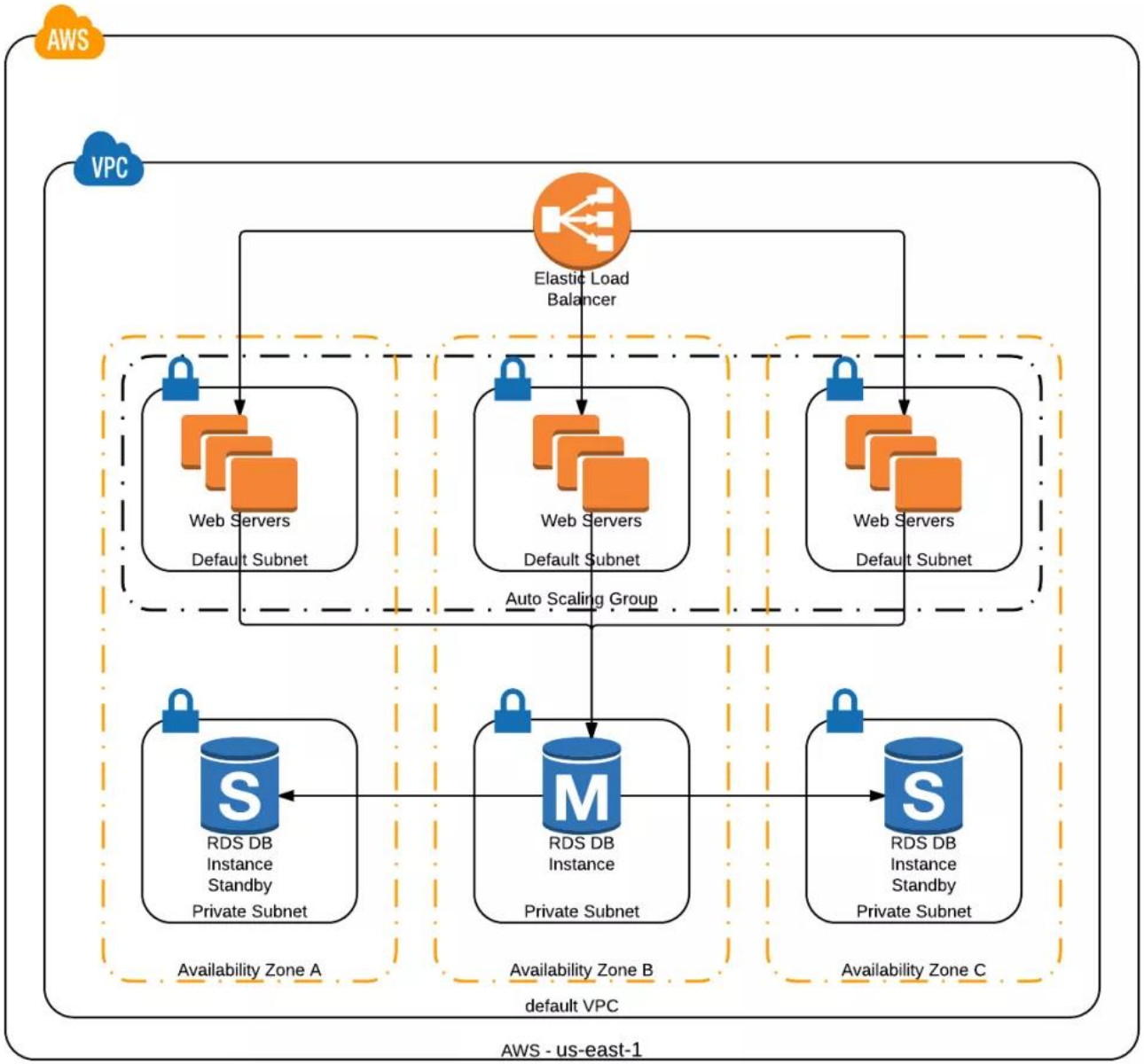
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": "arn:aws:ssm:us-east-1:123456789012:document/ResetUserPassword"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [...
            "Resource": "*"
        }
    ]
}
```

Run Command Advantage

1. ✓ **No network ingress rules** - Outbound requests to service
2. ✓ **Controlled executions** - Can use fixed commands vs unrestricted SSH access
3. ✓ **Audited -** Know who, what and when for each command, including comments
4. ✓ **No OS Users** - No need manage OS access for users

Outscaling Denial of Service Attacks

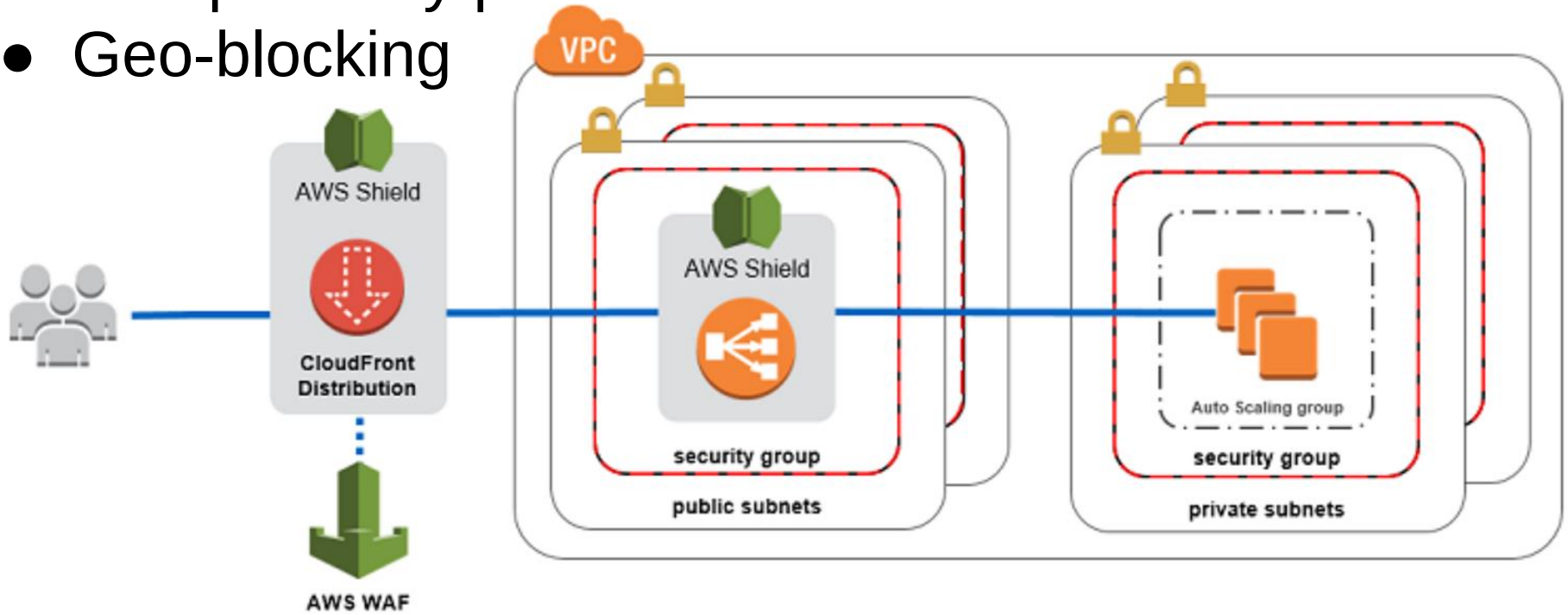
Typical Scalable Architecture



But Does Your Wallet Scale?

Network Layer Defense

- Layer 3 & 4 protection
- Multiple entry points
- Geo-blocking



Layer 7 protection

Avoid Unlimited Scaling

- Limit scaling policies to reasonable amounts for your applications
- Alert for excessive scaling (short and long term)

The Cost of Defense

AWS Shield Advanced

- **DDoS Cost Protection** - service credits for EC2, ELB, CloudFront and Route 53 cost spikes from DDoS attacks
- **AWS DDoS Response Team (DRT)** AWS team who can write rules on your behalf to mitigate application layer DDoS attacks

Monitor your AWS costs and alert when exceeding significant thresholds.

A Few Shout Outs to Some Interesting Security Services.

Amazon GuardDuty

- Continuous threat detection
- Machine learning to detect unusual behaviour and communications with known malicious IPs
- Analyzes AWS CloudTrail, VPC Flow Logs, and AWS DNS logs
- Identifies:
  - Reconnaissance patterns
  - Instance compromise
  - Account compromise

Honourable Mentions

- **Amazon Macie** - AI to classify data and detect unusual behaviour
- **AWS CloudTrail** - Transaction Auditing
- **AWS Config** - Resource tracking and compliance
- **Amazon Inspector** - Agent-based EC2 Security Assessment service
- **AWS Certificate Manager** - Free Domain Validated TLS certificates

THANK YOU

TriNimbus.com

Alan Williamson
alan@trinimbus.com