

Developer Operations

Security Considerations

Security in Cloud / DevOps

- Security often considered an **inhibitor** to cloud deployment
 - Isolation failure (*nosy neighbour* problem)
 - Credential leakage
 - Legal & regulatory issues
 - Loss of control
 - Data loss
 - Transition of legacy applications / models
 - Punctured perimeter (so network security devices like firewalls and intrusion detection lose effectiveness)

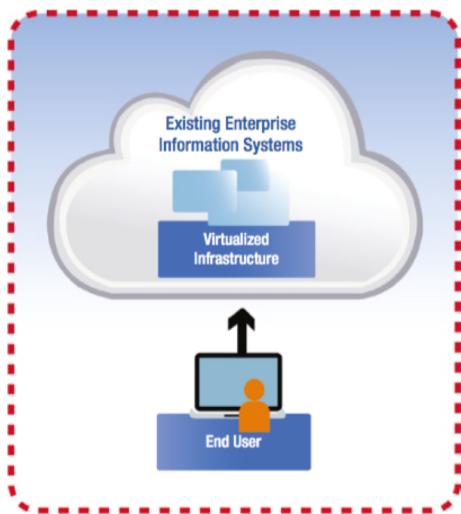
Security in Cloud / DevOps

- But security can also be an **enabler**
 - Security more easily outsourced to specialists
 - Especially relevant to PaaS and SaaS
 - New deployments allow security to be built in from the start
 - Specialist cloud security services (“security as a service”) can improve security – e.g.:
 - Encryption accelerators
 - Secure random number generators
 - Secure containers
 - Security monitoring
 - Online penetration testing

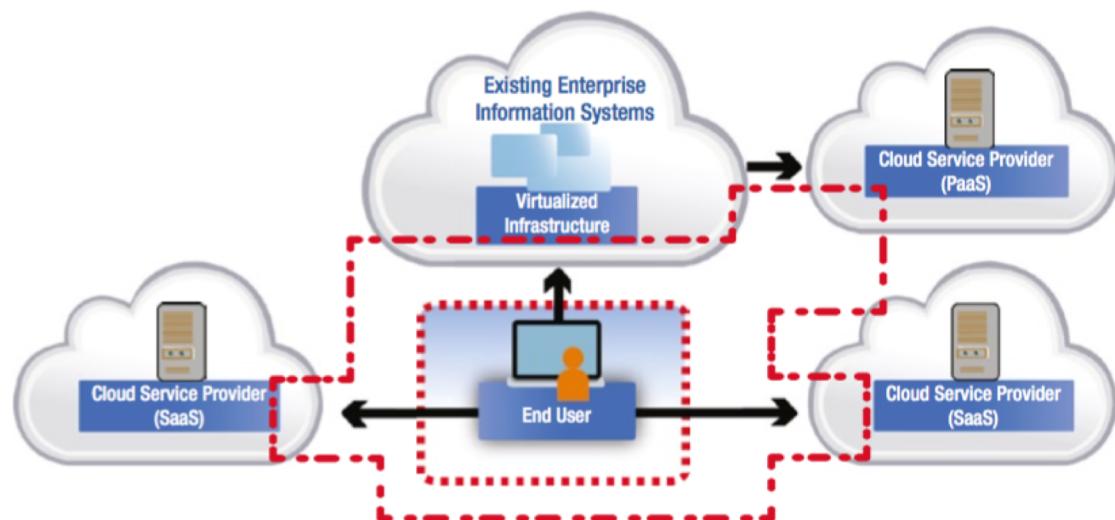
Trends impacting cloud security

- Virtualisation and cloud architectures
 - Multi-tenancy: hardware shared by different lines of business and even different businesses
- Increased attack sophistication
 - No longer just OS and system/application software
 - BIOS, firmware, hypervisor
 - Targeted attacks
 - More covert
- Legal and regulatory compliance
 - Increased regulation and audit of personally identifiable data, financial data, etc.

Perimeter evolution



Traditional perimeter



Cloud security perimeter

AWS Security

AWS Shared Responsibility Model

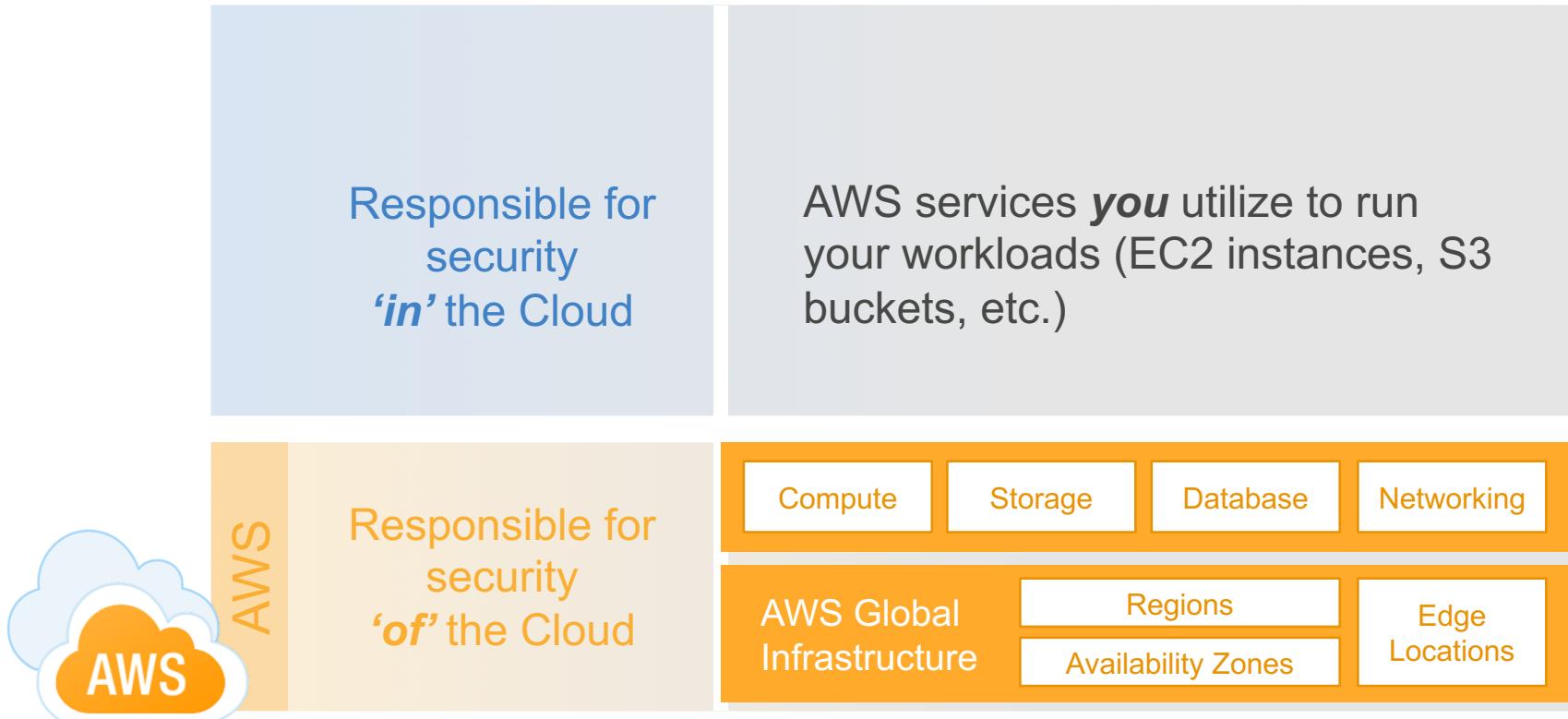
Responsible for
security
'in' the Cloud

AWS services ***you*** utilize to run
your workloads (EC2 instances, S3
buckets, etc.)

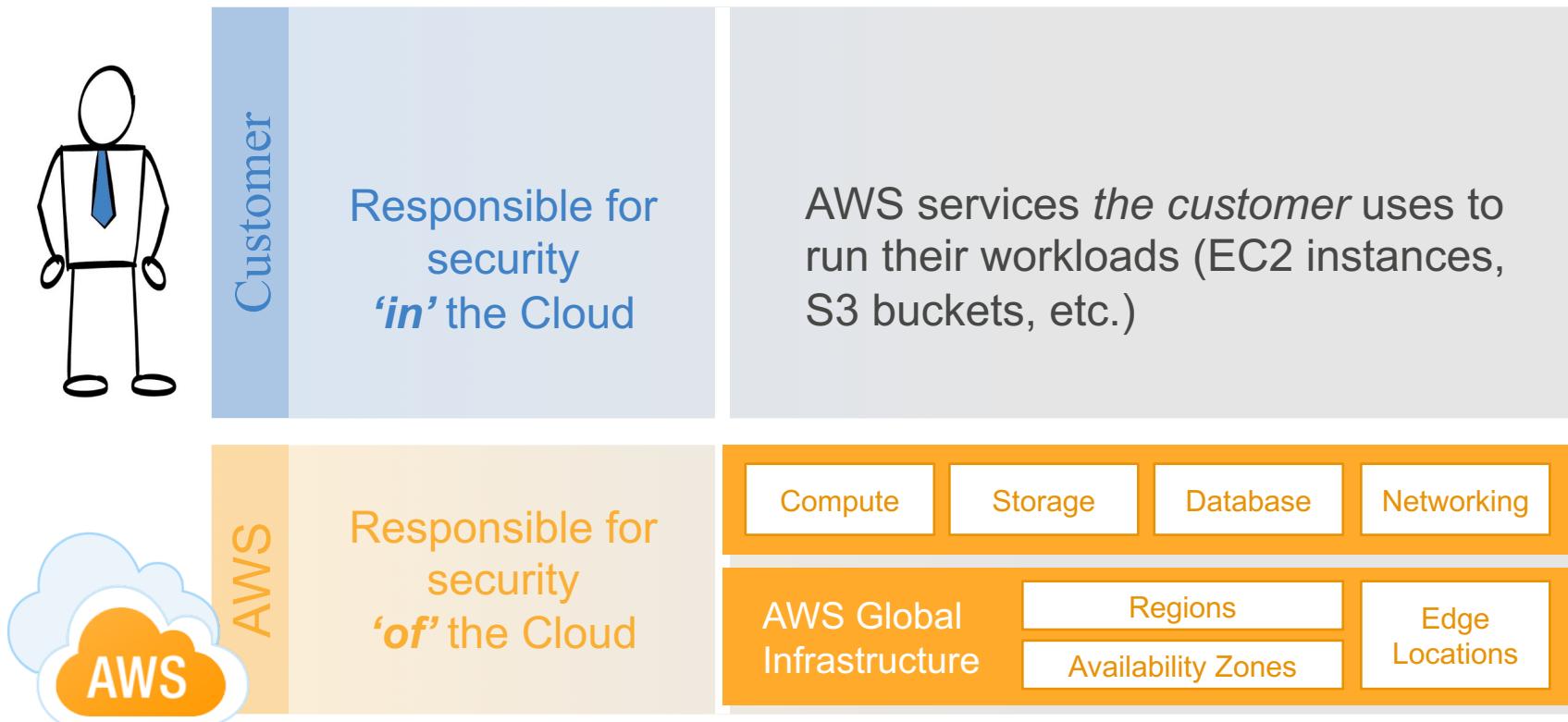
Responsible for
security
'of' the Cloud

Policies and mechanisms **AWS**
uses to protect the cloud itself

AWS Shared Responsibility Model



AWS Shared Responsibility Model



AWS Principal Services for Security

Areas	Key Services
Data protection	 Elastic Load Balancing  Amazon EBS  Amazon S3  Amazon RDS  AWS Key Management Service (KMS)
Privilege management	 AWS IAM  MFA token
Infrastructure protection	 Amazon VPC
Detective controls	 AWS CloudTrail  AWS Config  Amazon CloudWatch

AWS Data Protection

- Many AWS services include encryption capabilities to protect data in transit and at rest, such as:
 - Elastic Load Balancing
 - Elastic Block Store (EBS),
 - Simple Storage Service (S3)
 - Relational Database Service (RDS).
- AWS Key Management Service (KMS)
 - Secure key storage, creation, rotation, usage
- Cloud HSM
 - Cloud-based hardware security module – managed by customer

AWS Privilege Management

- Identity & Access Management (IAM)
 - Users & Groups
 - Roles
 - Permissions (policies)
 - Multi-factor authentication
 - API keys



IAM Authentication: Management Console

■ AWS Management Console

- User Name and Password
- MFA



Account:

User Name:

Password:

MFA users, enter your code on the next screen.

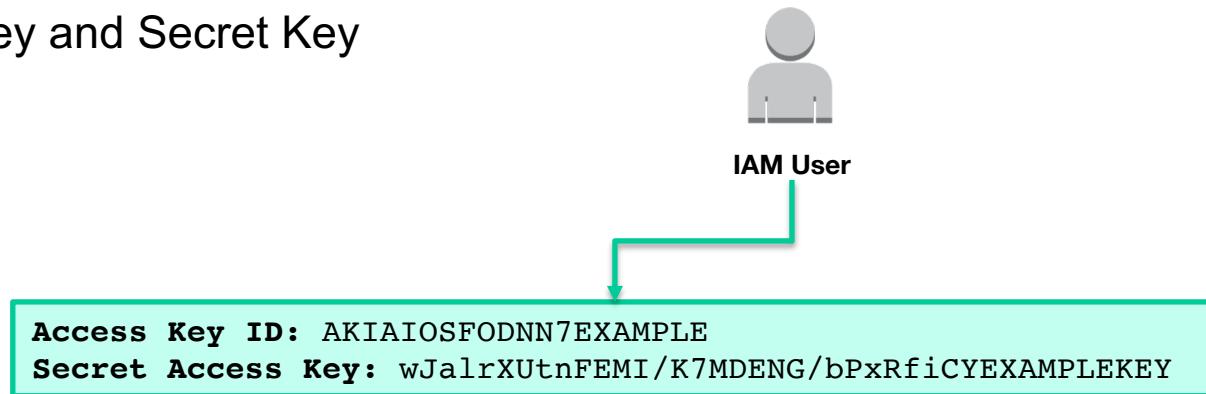
Sign In

The screenshot shows the AWS Management Console homepage. At the top, there's a search bar and navigation links for 'AWS', 'Services', and 'Edit'. Below the search bar is a large, light-gray navigation menu titled 'Amazon Web Services' that lists various AWS services. To the right of the menu, there are sections for 'Resource Groups', 'Getting Started', 'Additional Resources', 'AWS Marketplace', 'AWS re:Invent Announcements', and 'Service Health'. At the bottom right, there's a status bar with the message 'All services operating normally' and some footer links.

IAM Authentication: CLI / API

- AWS CLI or SDK API

- Access Key and Secret Key



AWS CLI

```
:~ $ aws configure
AWS Access Key ID [*****022A]:
AWS Secret Access Key [*****4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

AWS SDK & API



Java



Python



.NET

IAM Authorisation

Policies:

- ✓ Are JSON documents to describe permissions.
- ✓ Are assigned to users, groups or roles.



IAM
User



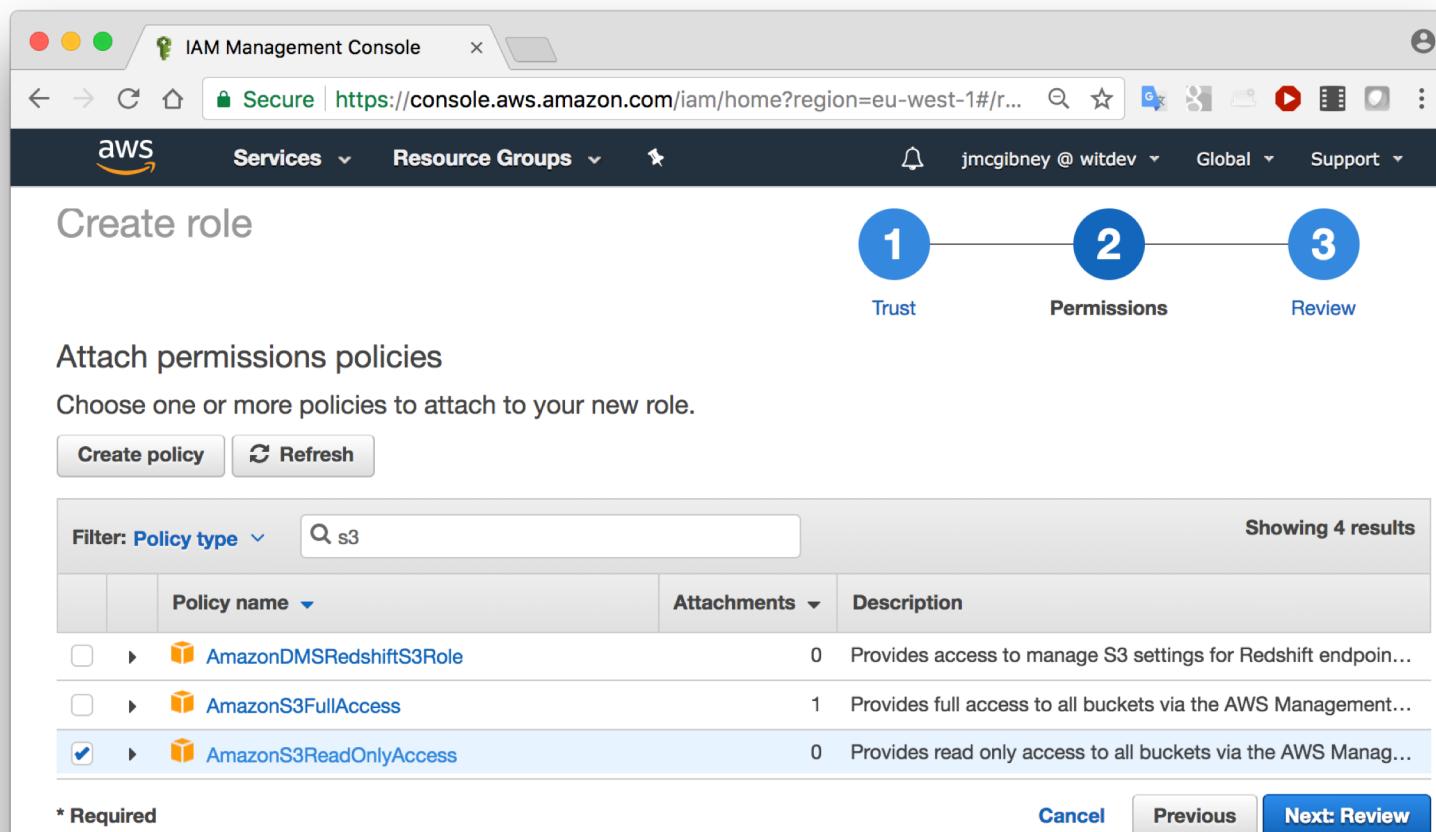
IAM
Group



IAM
Roles

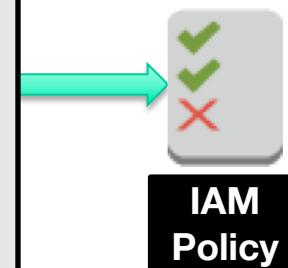
IAM Authorisation: Roles

- IAM roles are a secure way to grant permissions to specific entities
 - e.g. application code running on an EC2 instance that needs to perform some actions on AWS resources

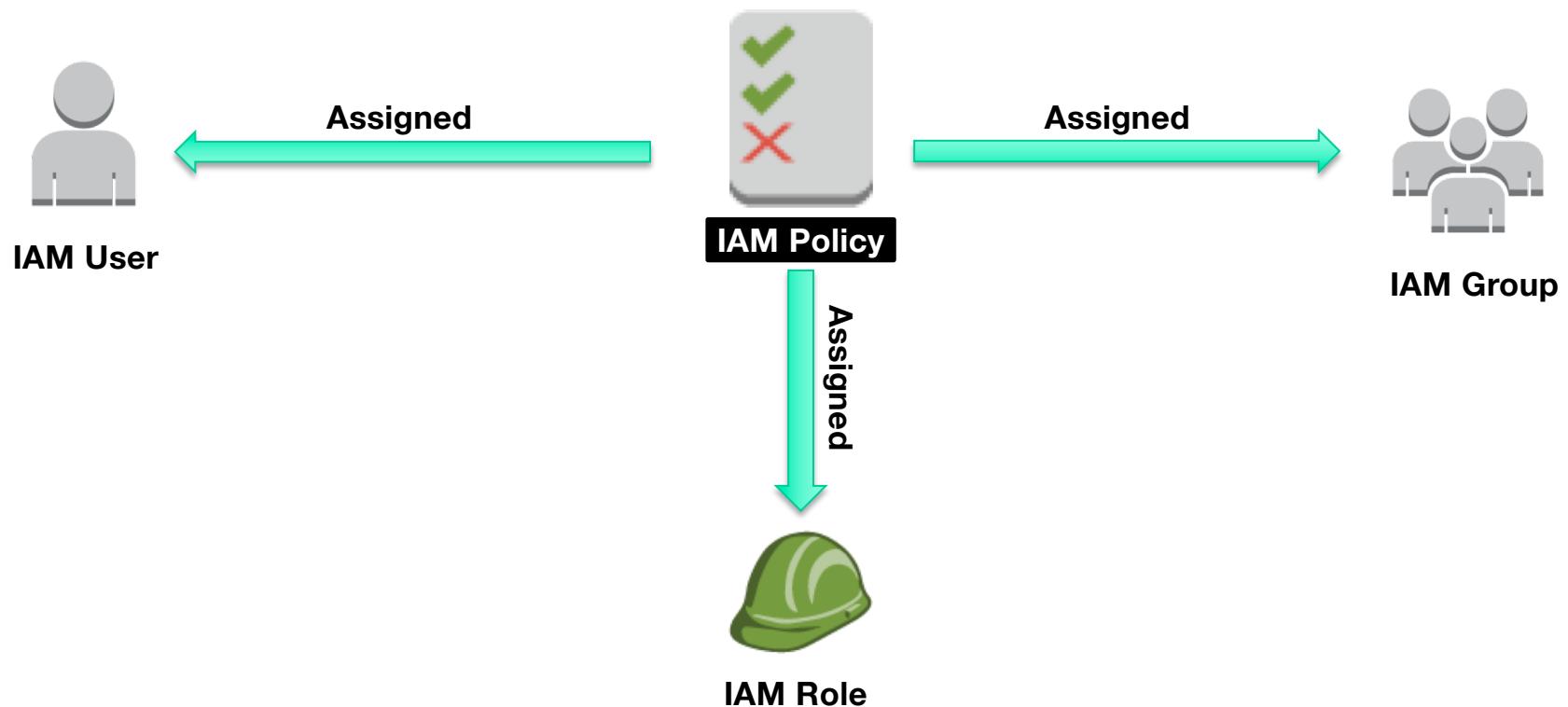


IAM Authorisation: Policy elements

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1453690971587",  
            "Action": [  
                "ec2:Describe*",  
                "ec2:StartInstances",  
                "ec2:StopInstances"  
            ],  
            "Effect": "Allow",  
            "Resource": "*",  
            "Condition": {  
                "IpAddress": {  
                    "aws:SourceIp": "54.64.34.65/32"  
                }  
            }  
        },  
        {  
            "Sid": "Stmt1453690998327",  
            "Action": [  
                "s3:GetObject*"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:s3:::example_bucket/*"  
        }  
    ]  
}
```



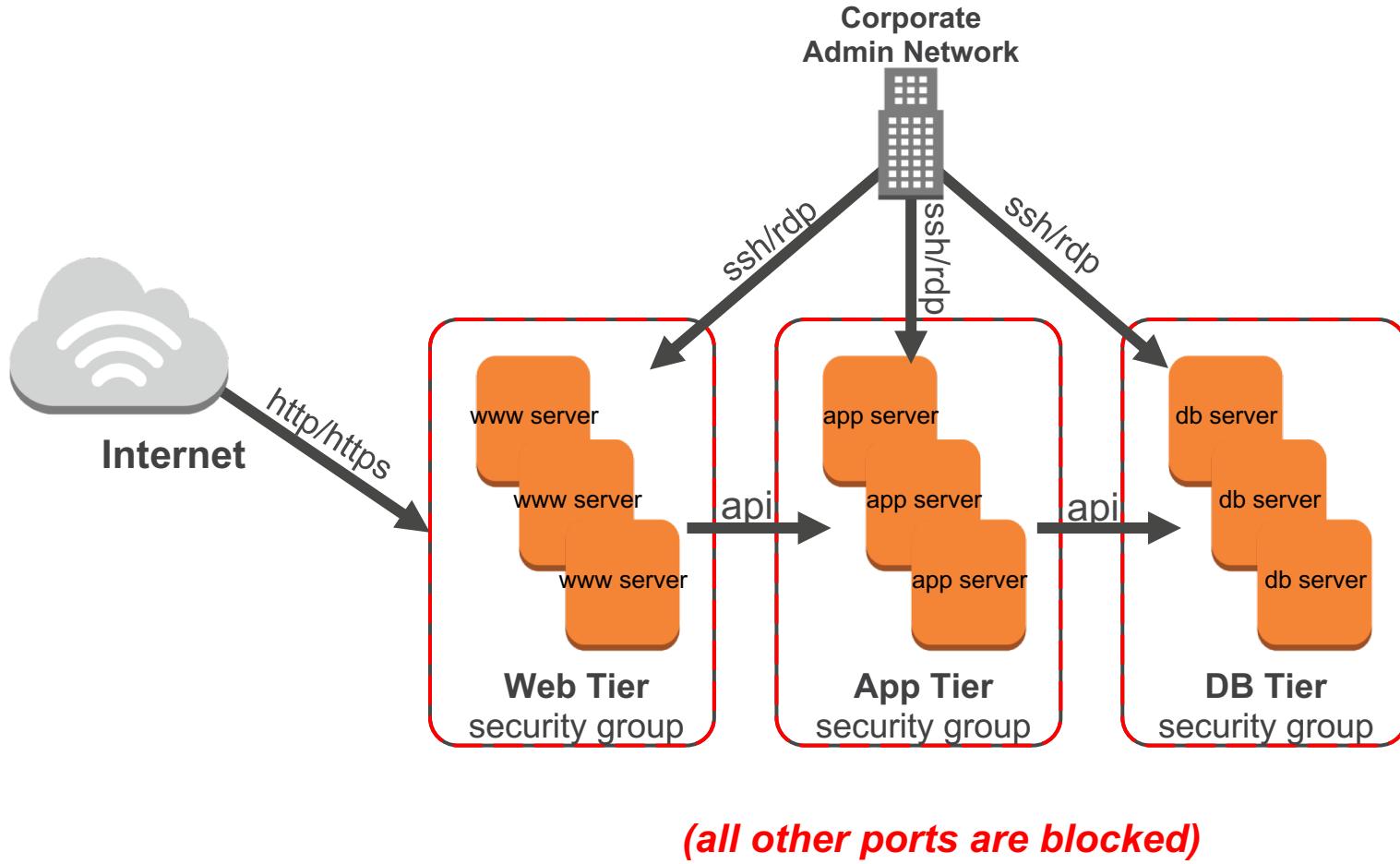
IAM Authorisation: Policy assignment



AWS Infrastructure protection

- Amazon Virtual Private Cloud (VPC) lets you provision a private, isolated section of the AWS cloud where you can launch AWS resources in a virtual network
- Public and private subnets
- NAT
- Security Groups
 - Control traffic to/from EC2 instances and RDS databases
- Network Access Control Lists (NACLs)
 - Control traffic to/from subnets
- VPN connections – for connecting to other networks, e.g. customer on-premises network

AWS Infrastructure protection



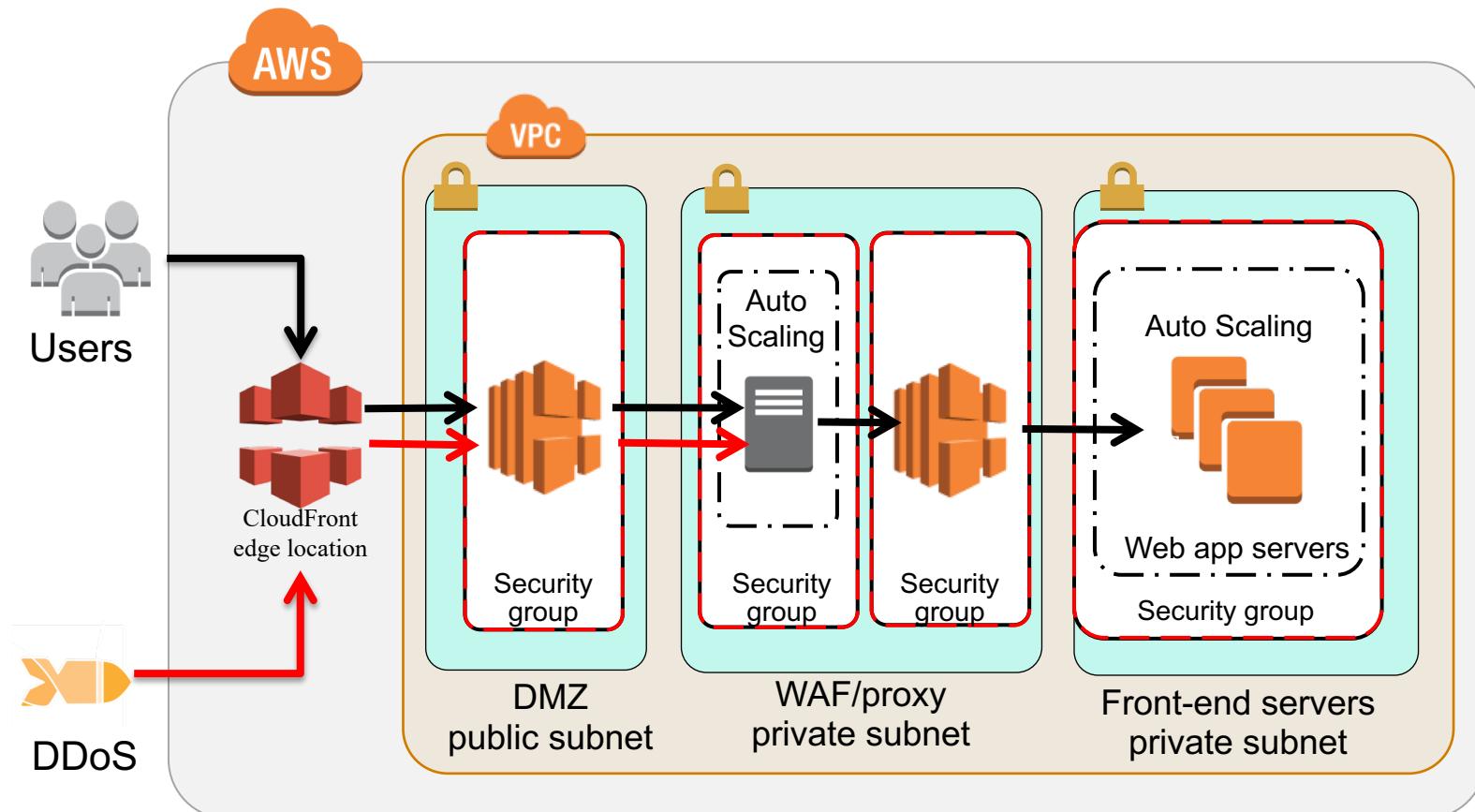
Security Group configuration

Edit inbound rules

Protocol	Port	Source IP
HTTP	80	Custom IP 193.1.34.15/
HTTP	80	Custom IP 193.1.34.0/2
HTTP	80	Custom IP 176.61.0.0/1
HTTP	80	Custom IP 46.7.0.0/16
Custom TCP Rule	8080	Custom IP 193.1.184.2/
Custom TCP Rule	8080	Custom IP 109.76.0.0/1
Custom TCP Rule	8080	Custom IP 89.100.0.0/1
Custom TCP Rule	8080	Custom IP 193.1.184.0/
Custom TCP Rule	8080	Custom IP 86.40.0.0/13
Custom TCP Rule	8080	Custom IP 79.97.0.0/16
Custom TCP Rule	8080	Custom IP 188.141.0.0/
Custom TCP Rule	8080	Custom IP 178.73.195.0/
Custom TCP Rule	8080	Custom IP 95.83.192.0/
Custom TCP Rule	8080	Custom IP 109.125.0.0/
Custom TCP Rule	8080	Custom IP 193.1.184.2/
Custom TCP Rule	8080	Custom IP 193.1.34.15/
Custom TCP Rule	8080	Custom IP 193.1.34.0/2
Custom TCP Rule	8080	Custom IP 176.61.0.0/1
Custom TCP Rule	8080	Custom IP 46.7.0.0/16
SSH	22	Anywhere 0.0.0.0/0

Add Rule Cancel Save

DDoS Mitigation with AWS



DDoS = Distributed Denial of Service

AWS Detective Controls

- AWS CloudTrail
 - records AWS API calls
- AWS Config
 - provides a detailed inventory of AWS resources and configuration
- Amazon CloudWatch
 - monitoring service for AWS resources

Some other AWS Security Features

- EC2 authentication
 - Key pair for Linux instances; username & password for Windows
- Web application firewall (WAF)
 - Monitors and filters HTTP/HTTPS requests to protect web apps
- Inspector
 - Application behaviour monitoring (installed on instances)
- Certificate Manager
 - TLS certificates deployment, management, renewal
- AWS Shield
 - Protection against DDoS (distributed denial of service)
- Trusted Advisor
 - Dashboard for monitoring AWS resources; includes security

Web Application Firewall

The screenshot shows the AWS WAF console interface. The top navigation bar includes 'AWS WAF', the URL 'https://console.aws.amazon.com/waf/home?region=eu-west-1#/wizard/', and user information 'jmcgilbney @ witdev'. Below the navigation is a menu bar with 'Services' (selected), 'Resource Groups', and links for 'Global' and 'Support'.

The main content area has a title 'Set up a web access control list (web ACL)' and a sidebar with steps: 'Concepts overview', 'Step 1: Name web ACL', **Step 2: Create conditions** (selected), 'Step 3: Create rules', 'Step 4: Choose AWS resource', and 'Step 5: Review and create'.

The central panel is titled 'Create conditions' and contains two sections: 'Cross-site scripting match conditions' and 'IP match conditions'. The 'Cross-site scripting match conditions' section has a button 'Create condition' and a note: 'You don't have any cross-site scripting match conditions. Choose **Create XSS match condition** to get started.' Below it is a detailed description of what a XSS match condition does. The 'IP match conditions' section also has a 'Create condition' button and a similar note.

To the right, a 'Concepts overview' sidebar provides examples of how conditions can be combined:

- Web ACL example**: if requests match
 - Rule 1**, Bad User-Agents, then block
 - IP match condition**: Suspicious IPs
 - and**
 - String match condition**: Bad bots
- or if requests match
 - Rule 2**, Detect SQLi, then block

Inspector

The screenshot shows the Amazon Inspector console home page within the AWS Management Console. The browser tab is titled "Amazon Inspector". The URL in the address bar is <https://eu-west-1.console.aws.amazon.com/inspector/home?region=eu-west-1#/home>. The top navigation bar includes links for "Services", "Resource Groups", and user information "jmcgibney @ witdev · Ireland · Support".

The main content area features a large circular icon with a green downward-pointing arrow. Below it is the title "Amazon Inspector". A descriptive text block states: "Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues." A blue "Get started" button is positioned below this text.

The page is divided into three main sections:

- Install:** Shows an icon of a computer monitor displaying binary code and a gear, with an orange circle containing a cursor pointing at the gear. Below the icon is the text "Install" and the subtext "Install the AWS agent on your EC2 instances." A "Learn more" link is provided.
- Run:** Shows an icon of a computer monitor displaying a clock and a gear, with an orange circle containing a gear. Below the icon is the text "Run" and the subtext "Run an assessment for your assessment target." A "Learn more" link is provided.
- Analyze:** Shows an icon of a person's silhouette looking at a document with an eye icon, with an orange circle containing an eye. Below the icon is the text "Analyze" and the subtext "Review your findings and remediate security issues." A "Learn more" link is provided.

Certificate Manager

AWS Certificate Manager

https://eu-west-1.console.aws.amazon.com/acm/home?region=eu-west-1#/importwizard/

Import a certificate

Step 1: Import certificate

You can use AWS Certificate Manager certificates only with Elastic Load Balancing. Learn more.

Step 2: Review and import

Select certificate

Paste the PEM-encoded certificate body, private key, and certificate chain below. [Learn more](#).

Certificate body*

```
-----BEGIN CERTIFICATE-----
MIIDiDCCAnACCQCcVeY9yDWDazANBkakhiG9w0BAQsFADC BhTELMAkGA1UEBhMC
SjUxEDAOBgNVBAgTB0lyZWxhbmQxEjAQBgNVBAcTCVdhdGVyZm9vZDELMakGA1UE
ChMCU1cxCzAJBgNVBAsTAINXMTYwNAYDVQQDEy10ZW1wLWxiLTk1NTQxMzA5My5l
dS13ZXN0LTEuZWxilMftYXpvbmF3cy5ib20wHhcNMTYxMTE2MiI1MilzWhcNMTCx
-----
```

Certificate private key*

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpaIBAAKCAQEArNo1A0rrDuOnewEcl.8aK3Tc1Z.I4S9hizsfI07./iICFLUTGFv
eQ4/CeccHrwzm01s
```

Certificate chain

```
-----BEGIN TRUSTEE-----
MIIDMDCCAhgCCC
RTEQMA4GA1UEC
EwJDQTELMAkGA1
```

* Required

Create Listener

Protocol: HTTPS (Secure HTTP)

Port: 443

Default target group: temp-tg

Select Certificate

An SSL Certificate allows you to configure the HTTPS/SSL listeners of your load balancer. You may select an existing SSL certificate or create a new one below. [Learn more](#) about setting up HTTPS load balancers and certificate management.

Certificate type

- Choose an **existing** certificate from AWS Certificate Manager (ACM)
- Choose an **existing** certificate from AWS Identity and Access Management (IAM)
- Upload a **new** SSL certificate to AWS Identity and Access Management (IAM)

Request a new certificate from ACM

AWS Certificate Manager provides a simple way to request a new SSL certificate for your domain. You can choose a certificate for your application or service, or request a certificate for a specific platform. ACM manages the certificate issuance process on your behalf.

Certificate name

Choose a certificate

52.17.134.20 (arn:aws:acm:eu-west-1:808146113457:certificate/7255fdb4-f069-46a3-960e-
temp-lb-955413093.eu-west-1.elb.amazonaws.com (arn:aws:acm:eu-west-1:808146113457:
temp-lb-955413093.eu-west-1.elb.amazonaws.com (arn:aws:acm:eu-west-1:808146113457:
✓ temp-lb-955413093.eu-west-1.elb.amazonaws.com (arn:aws:acm:eu-west-1:808146113457:

EC2
(load balancer config)

Finally ... protect credentials!

sign in  become a supporter | subscribe  search

find a job dating more ▾ International edition ▾

theguardian

UK world sport football opinion culture business lifestyle fashion environment tech travel  all sections

home > tech

Uber

Uber concealed massive hack that exposed data of 57m users and drivers

- Firm paid hackers \$100,000 to delete data and keep breach quiet
- Chief security officer Joe Sullivan fired for concealing October 2016 breach

     5357 **Julia** Ca
in San I
 Advertisement

According to Bloomberg, the breach occurred when two hackers obtained login credentials to access data stored on Uber's Amazon Web Services account. Paul Lipman, CEO of cybersecurity firm BullGuard, said that the fact that the data was being stored unencrypted was “unforgivable”.

Wednesday 22 November 2017 11.16 GMT



BOMGAR 