Vos applications sont plus en sécurité dans le cloud

Sébastien Stormacq, Training Manager EMEA
stormacq@amazon.com

© 2016, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

5 x Pourquoi ?

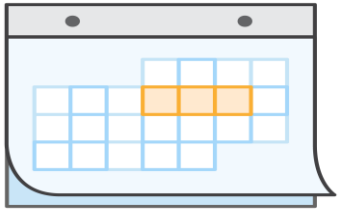
1. Pourquoi la sécurité est la priorité des entreprises qui adoptent AWS ?

Priorité d’AWS aussi

Un nouveau monde

Difficile

2. Pourquoi est-ce difficile ?

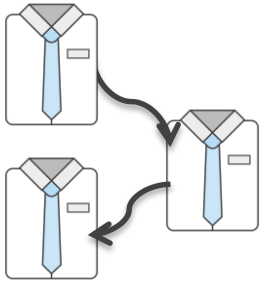


Anticipation des régulations

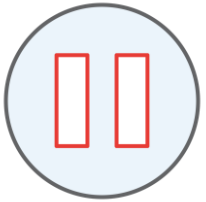
Contrôler les changements

3. Pourquoi est-ce si long ?

Beaucoup de processus

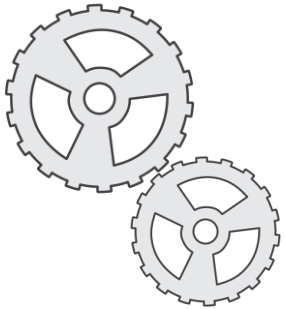


Plusieurs équipes



Beaucoup de dépendances

4. Pourquoi tant de processus ?



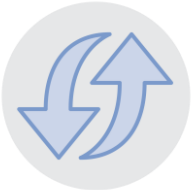
Détecter les changements

Visibilité et contrôle

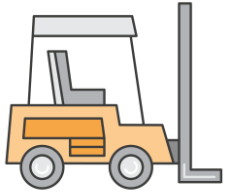
Réduire les risques d’erreurs

5. Pourquoi détecter les changements est difficile ?

Manque de visibilité

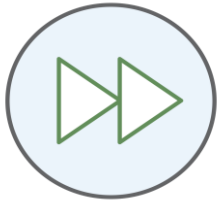


Pas de cycle déclencheur / réponse

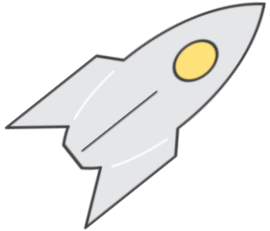


Peu d’automatisation

Comment AWS peut vous aider ?



Processus plus rapides



Permet l’innovation
en restant protégé

Responsabilité Partagée

Nous nous occupons de la sécurité **du** cloud.
Vous vous occupez de la sécurité **dans** le cloud

Principe du moindre privilège

Confiner les autorisations
au strict nécéssaire

AWS IAM

Identity & Access Management.
Contrôler **QUI** peut faire **QUOI** dans
votre compte et définir des politiques d’accès.

Dashboard

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

IAM > Roles > **DBA**

Summary

Role ARN	arn:aws:iam::663354267581:role/DBA
Instance Profile ARN(s)	arn:aws:iam::663354267581:instance-profile/DBA
Path	/
Creation Time	2013-09-27 11:32 PDT

Permissions

Managed Policies

There are no managed policies attached to this role.

Attach Policy

Inline Policies

This view shows all inline policies that are embedded in this role.

Create Role Policy

Policy Name	Actions
policygen-DBA-201309271307	Show Policy | Edit Policy |

Show Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DownloadDBLogFilePortion"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "rds:db-tag/environment": [
            "prod",
            "dr"
          ]
        }
      }
    }
  ]
}
```

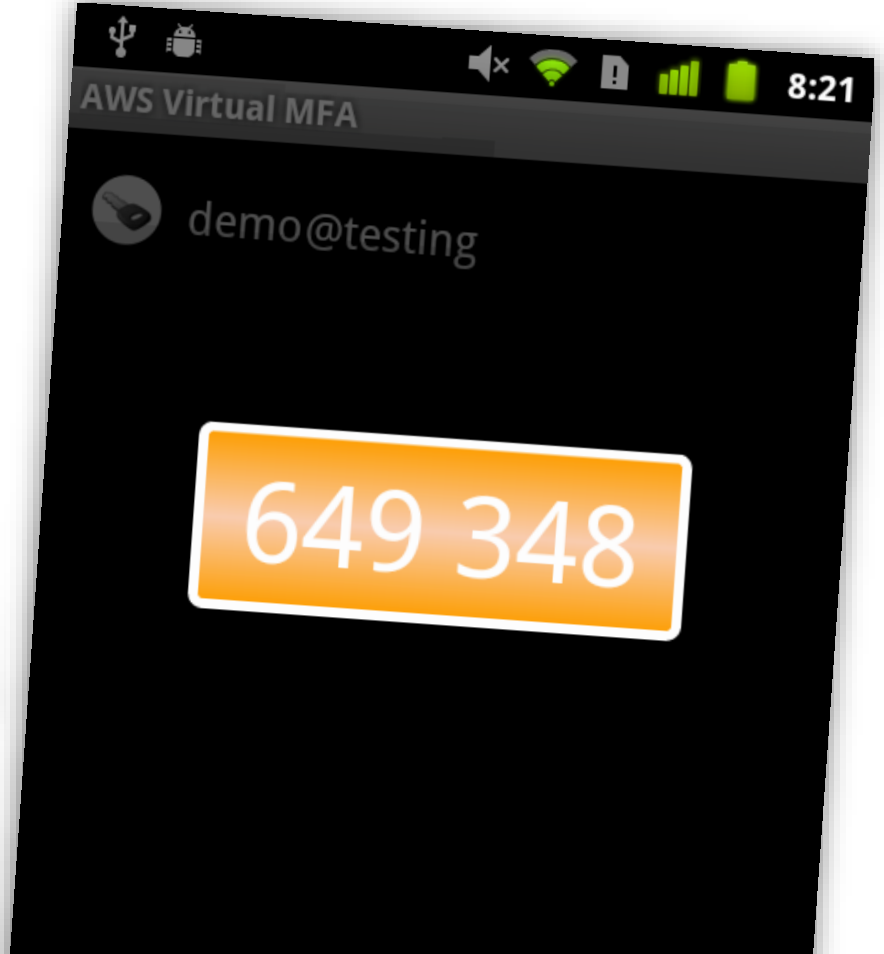
Policy Versions

Each time you update a policy, you create a new version. You can have up to 5 versions. Learn more.

Set as Default | Delete

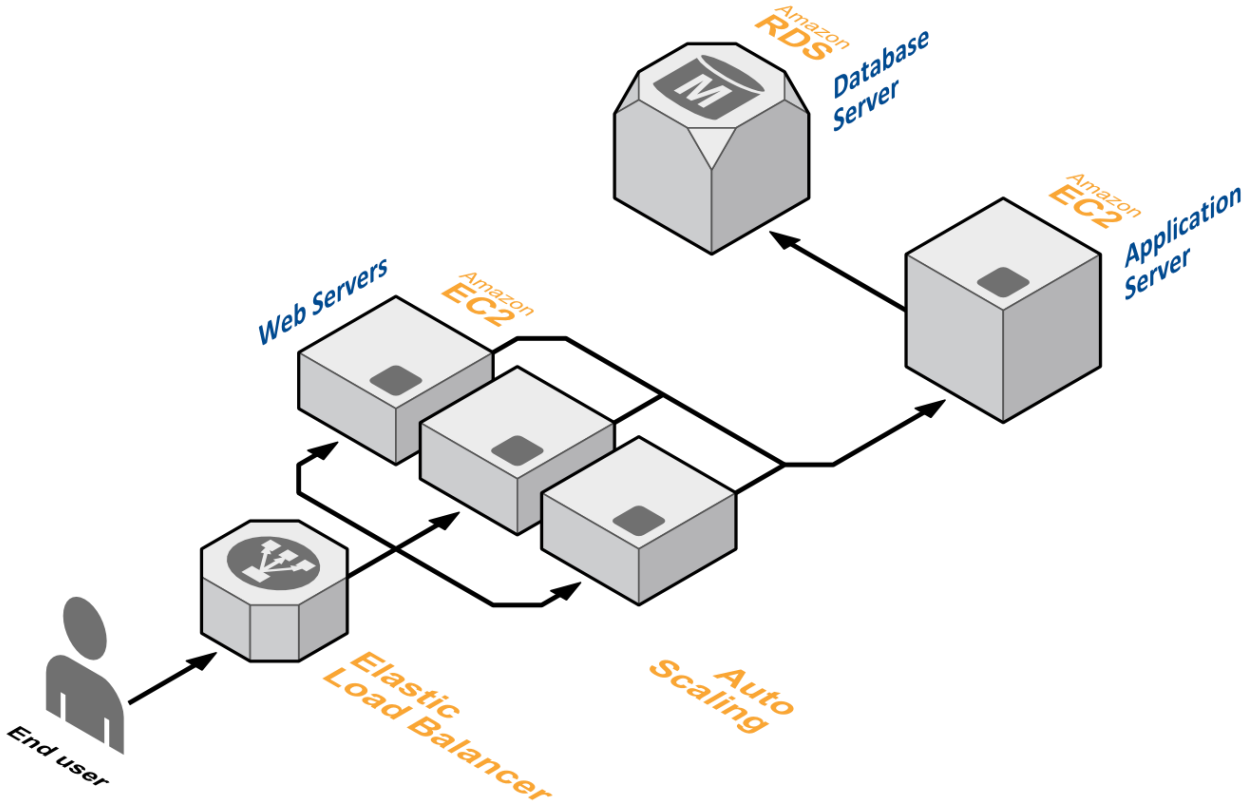
	Version	Creation Time
	Version 2 (default)	2015-04-06 07:07 PDT
☑	Version 1	2015-03-27 10:29 PDT

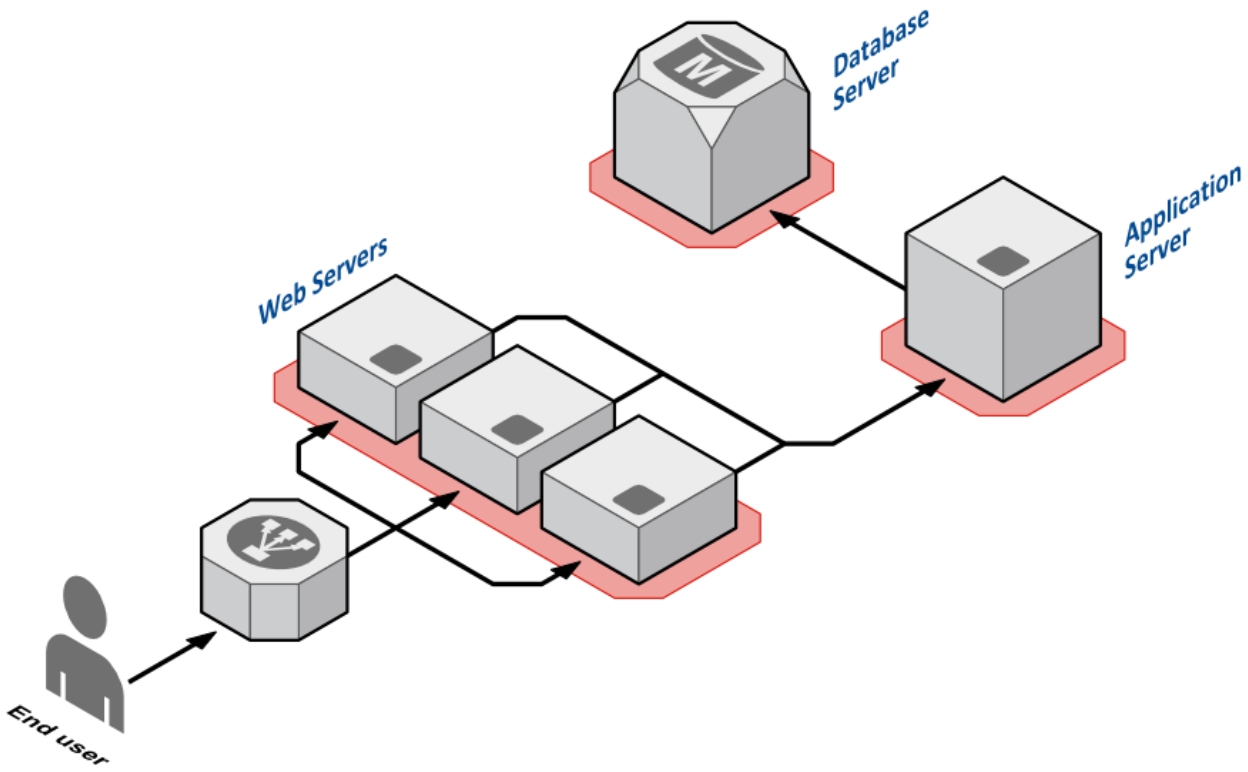
gemalto
production
gemalto
gemalto
prod
gemalto
infrastructure
gemalto
production

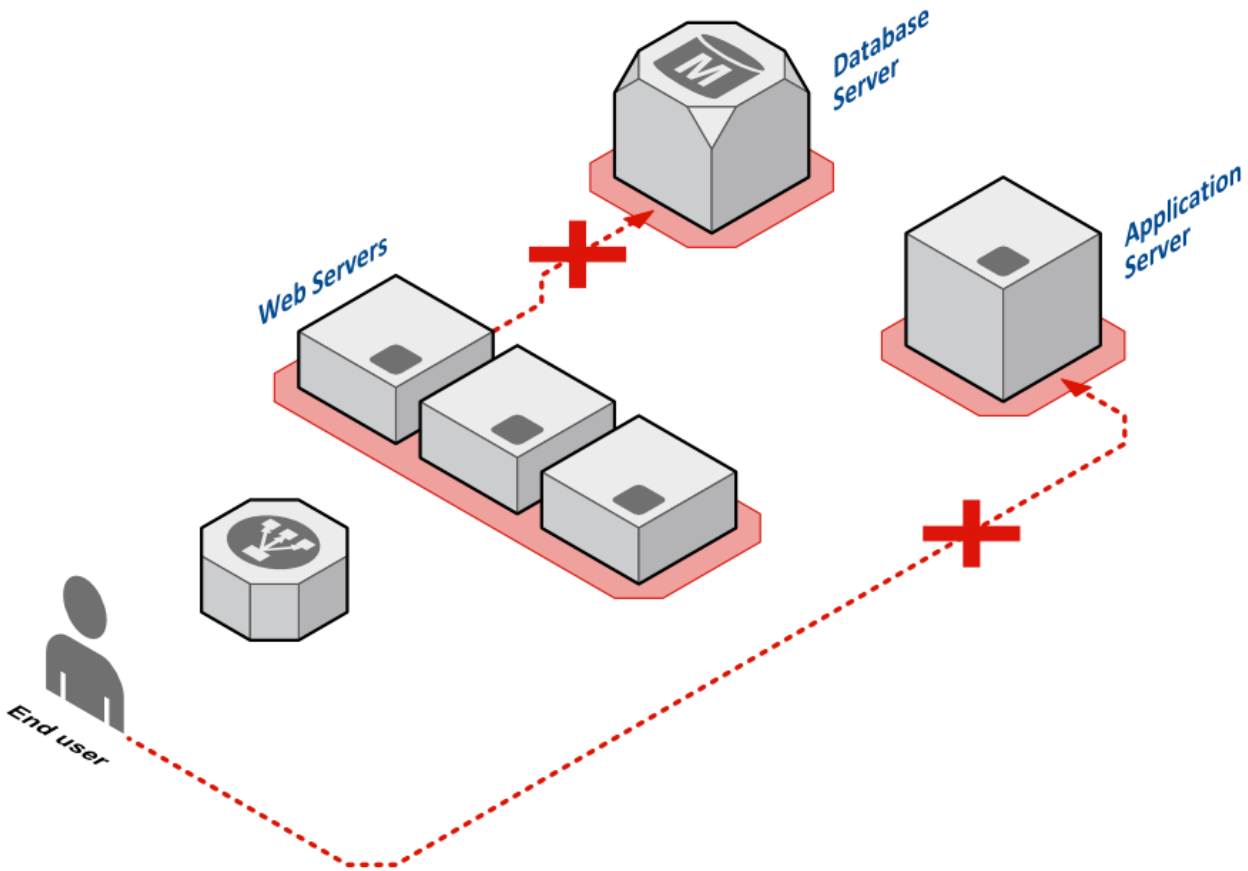

8:21
AWS Virtual MFA
demo@testing
649 348

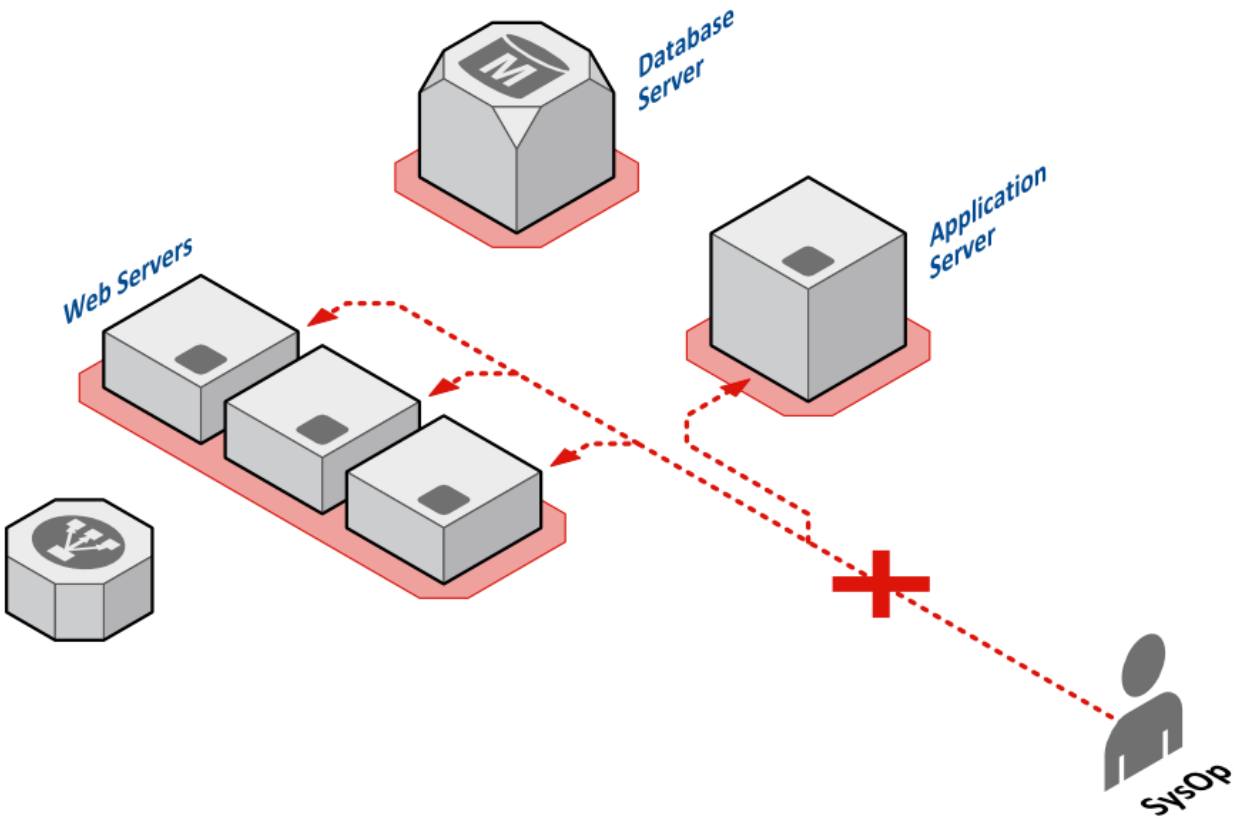
Principe du moindre privilège

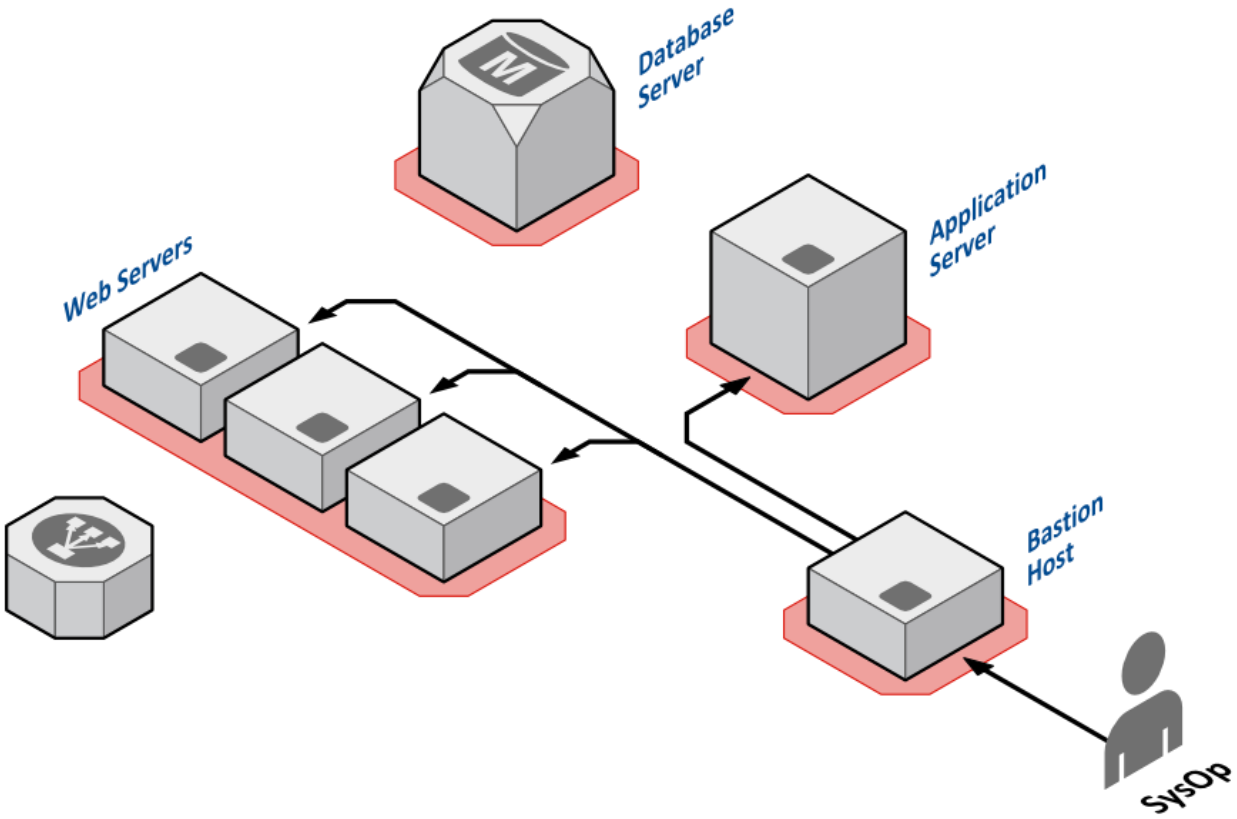
Restreindre les accès réseaux
aux noeuds qui en ont besoin

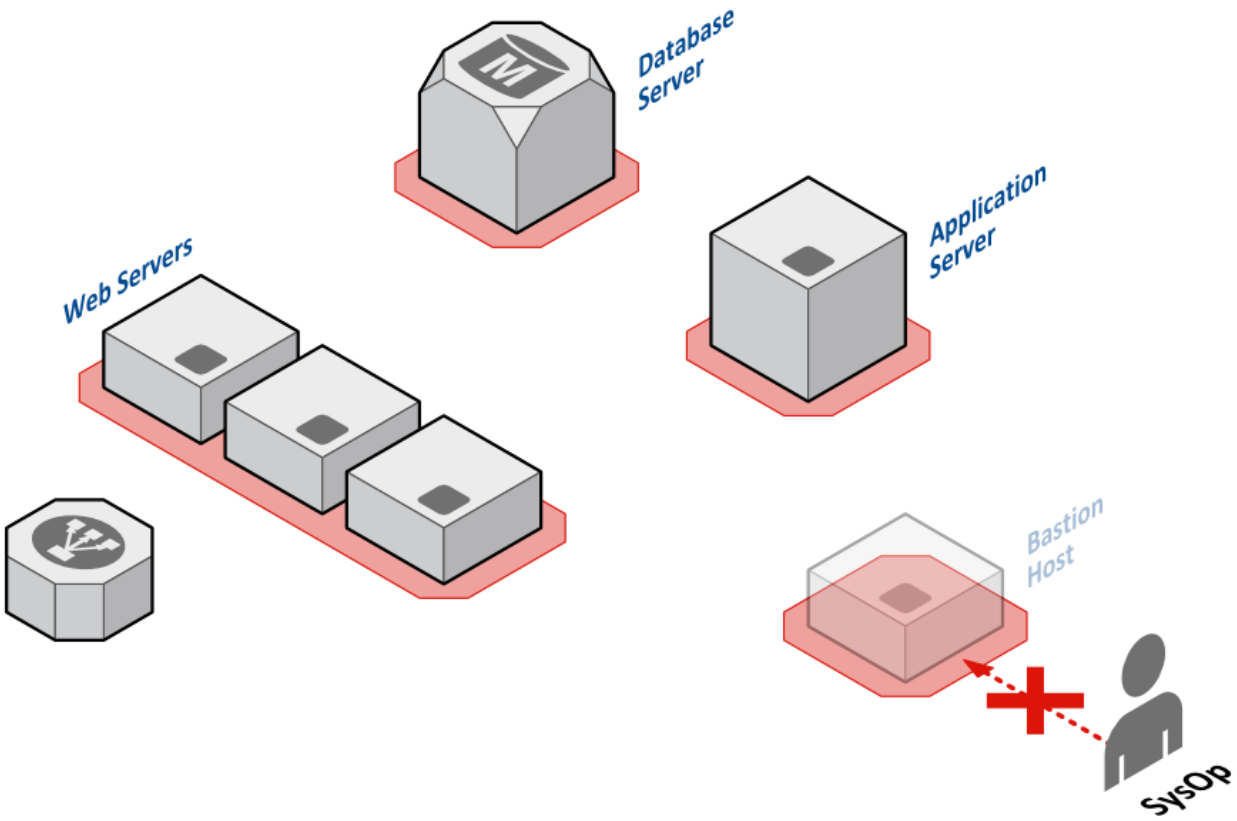

Amazon
RDS
Database
Server
Amazon
EC2
Application
Server
Web Servers
Amazon
EC2
End user
Elastic
Load Balancer
Auto
Scaling


Database Server
Application Server
Web Servers
End user


Database Server
Application Server
Web Servers
End user


Database Server
Application Server
Web Servers
SysOp


Database Server
Application Server
Web Servers
Bastion Host
SysOp


Database Server
Application Server
Web Servers
Bastion Host
SysOp

VPC Dashboard

Filter by VPC:

None

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Peering Connections

Security

- Network ACLs
- Security Groups

Create VPC | Actions

Search VPCs and their prop

Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL
	vpc-27148f46	available	10.40.0.0/16	dopt-c77d5ca9	rtb-29148f48	acl-26148f47

vpc-27148f46 (10.40.0.0/16)

Summary | Tags

VPC ID: vpc-27148f46
State: available
VPC CIDR: 10.40.0.0/16
DHCP options set: dopt-c77d5ca9
Route table: rtb-29148f48
ClassicLink: Disabled

Network ACL: acl-26148f47
Tenancy: Default
DNS resolution: yes
DNS hostnames: no

Create Subnet | Delete Subnet | Modify Auto-Assign Public IP

Search Subnets and their p

Name	Subnet ID	CIDR	Availability Zone	Route Table	Auto-assign Public IP
public-1a	subnet-cc3afee7	10.40.0.0/24	us-east-1a	rtb-5a3e583f | internet	No
public-1b	subnet-f9148f98	10.40.1.0/24	us-east-1b	rtb-5a3e583f | internet	No
private-1a	subnet-b046fec7	10.40.2.0/23	us-east-1b	rtb-29148f48	No
private-1b	subnet-a246fed5	10.40.4.0/23	us-east-1b	rtb-29148f48	No
private-1c	subnet-f969d8a0	10.40.6.0/23	us-east-1c	rtb-29148f48	No
public-egress-1a	subnet-804480ab	10.40.250.0/24	us-east-1a	rtb-5a3e583f | internet	No
public-egress-1b	subnet-d83880af	10.40.251.0/24	us-east-1b	rtb-5a3e583f | internet	No
public-bastion-1a	subnet-ed3bffc6	10.40.252.0/23	us-east-1a	rtb-5a3e583f | internet	No
public-bastion-1b	subnet-eb47ff9c	10.40.254.0/23	us-east-1b	rtb-5a3e583f | internet	No

Create Route Table | Delete Route Table | Set As Main Table

Search Route Tables and th

Name	Route Table ID	Associated With	Main	VPC
internet	rtb-5a3e583f	6 Subnets	No	vpc-27148f46 (10.40.0.0/16)
	rtb-29148f48	0 Subnets	Yes	vpc-27148f46 (10.40.0.0/16)

rtb-29148f48

Summary | Routes | Subnet Associations | Route Propagation | Tags

Edit

Destination	Target	Status	Propagated
10.40.0.0/16	local	Active	No

Create Subnet | Delete Subnet | Modify Auto-Assign Public IP

Search Subnets and their p

Name	Subnet ID	CIDR	Availability Zone	Route Table	Auto-assign Public IP
public-1a	subnet-cc3afee7	10.40.0.0/24	us-east-1a	rtb-5a3e583f | internet	No
public-1b	subnet-f9148f98	10.40.1.0/24	us-east-1b	rtb-5a3e583f | internet	No
private-1a	subnet-b046fec7	10.40.2.0/23	us-east-1b	rtb-29148f48	No
private-1b	subnet-a246fed5	10.40.4.0/23	us-east-1b	rtb-29148f48	No
private-1c	subnet-f969d8a0	10.40.6.0/23	us-east-1c	rtb-29148f48	No
public-egress-1a	subnet-804480ab	10.40.250.0/24	us-east-1a	rtb-5a3e583f | internet	No
public-egress-1b	subnet-d83880af	10.40.251.0/24	us-east-1b	rtb-5a3e583f | internet	No
public-bastion-1a	subnet-ed3bffc6	10.40.252.0/23	us-east-1a	rtb-5a3e583f | internet	No
public-bastion-1b	subnet-eb47ff9c	10.40.254.0/23	us-east-1b	rtb-5a3e583f | internet	No

Web Application Firewall

Protège vos applications web
contre les attaques les plus fréquentes

Principe de protection des données

Protégez vos données en transit et au repos

Chiffrez vos données

AMAZON EMR
AMAZON S3
AMAZON GLACIER
AMAZON REDSHIFT
AMAZON RDS
…

Choisissez un modèle adapté

Automatique – AWS se charge du chiffrement
Activé – vous utilisez les outils AWS pour le chiffrement
Côté Client – vous utilisez vos propres outils et procédures

Gestion des clés privées sur AWS

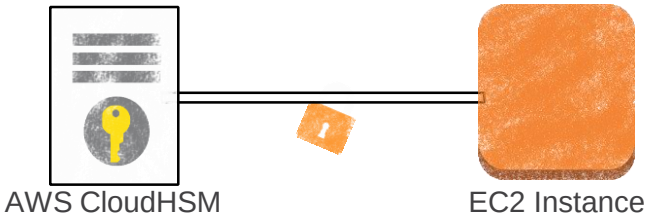
Gèré par AWS
mais **vous** gèrez les clés

Plus de performance pour
l’accès aux clés et le chiffrement

Conforme à des règles strictes
adoptées par l’industrie

AWS CloudHSM

Service HSM dédié

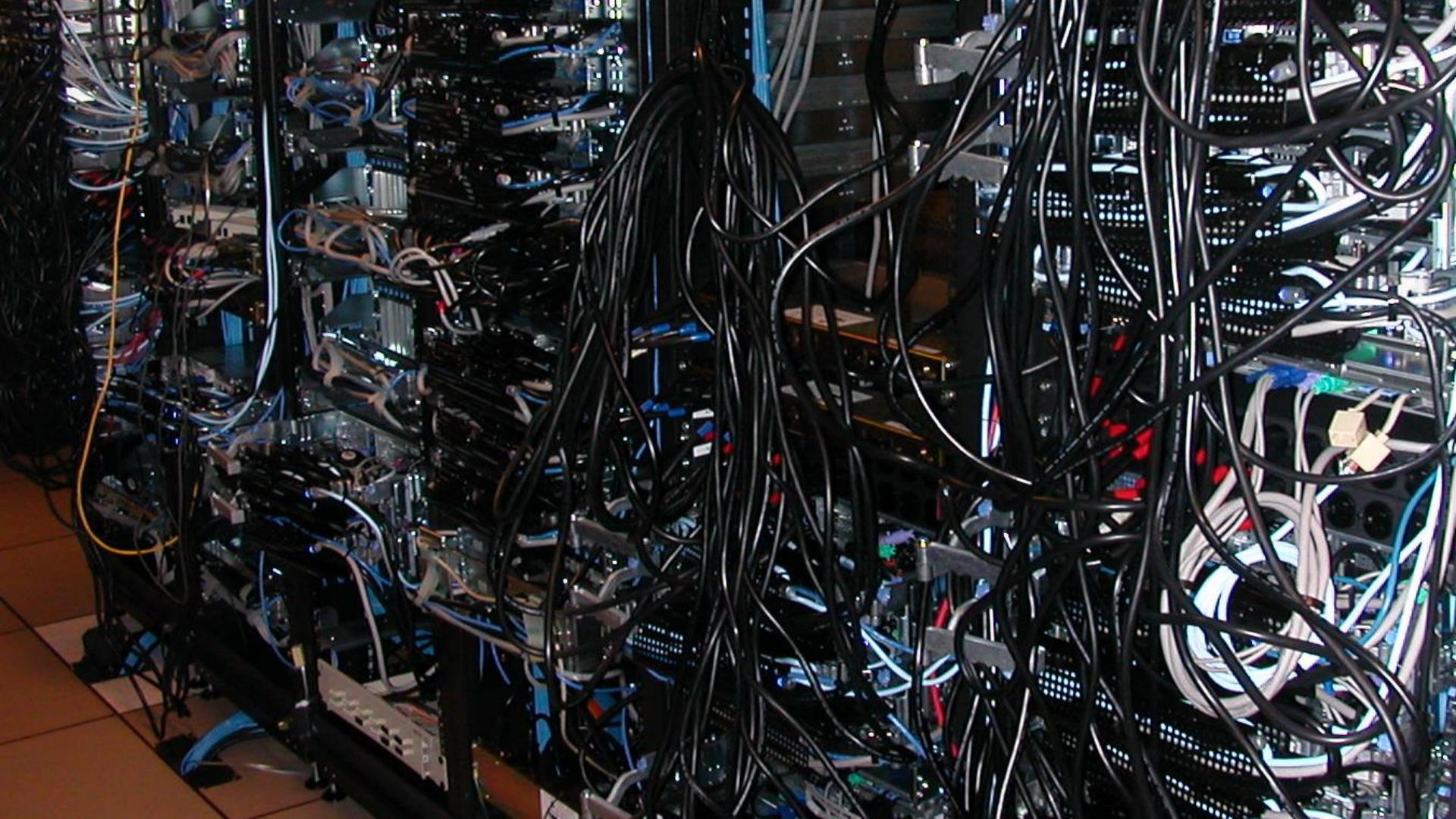


Key Management Service

Simplifie la création, le contrôle, la rotation et l’utilisation de clés de chiffrement dans vos applications

Principe de visibilité

Vous ne protégez pas ce que vous ignorez



EC2 Management Console

https://eu-west-1.console.aws.amazon.com/ec2/v2/home?region=eu-west-1#SecurityGroups:sort=groupId

AWS | Services | Edit | powuser @ 6709-3476-2290 | Ireland | Support

- 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

Create Security Group | Actions

Filter by tags and attributes or search by keyword

1 to 12 of 12

Name	Group ID	Group Name	VPC ID	Description
	sg-1f1d0173	default	vpc-5c96e435	default VPC secu
	sg-33e7fd47	ElasticMapReduce-master		Master group for
	sg-3de7fd49	ElasticMapReduce-slave		Slave group for E
	sg-6620aa03	d-9367354752_controllers	vpc-18d31b7d	AWS created sec
	sg-8a4175fe	default		default group
	sg-9823a9fd	default	vpc-18d31b7d	default VPC secu

Security Group: sg-6620aa03

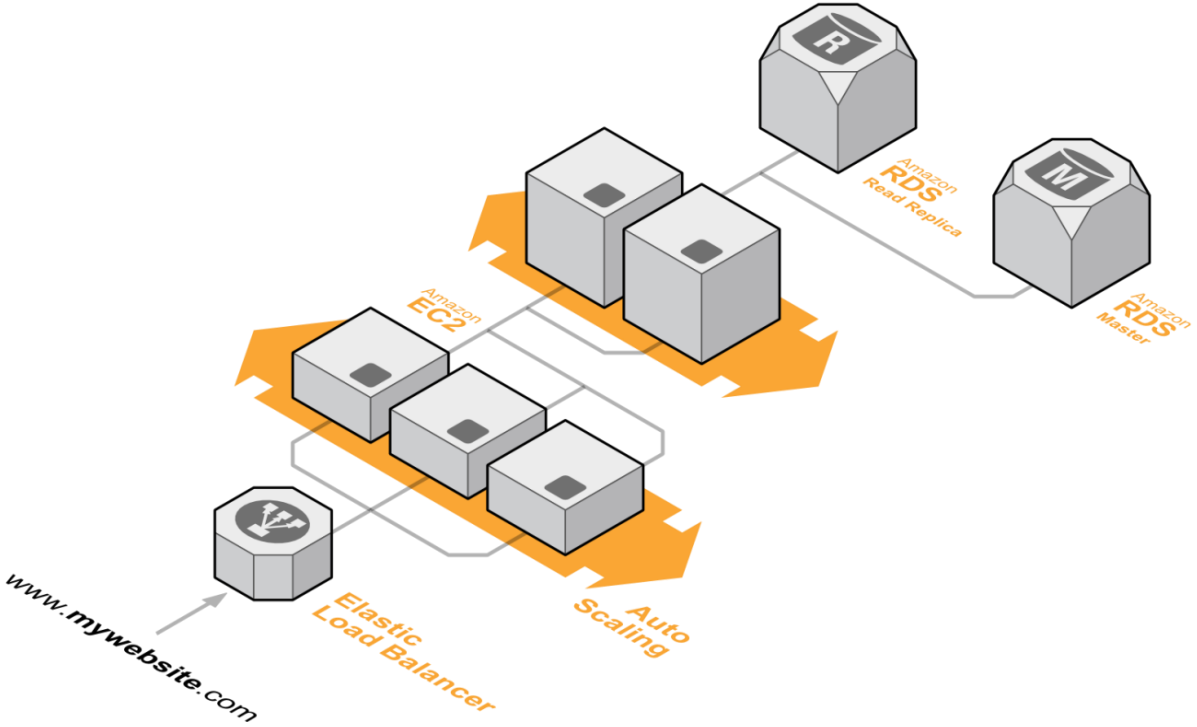
Description | Inbound | Outbound | Tags

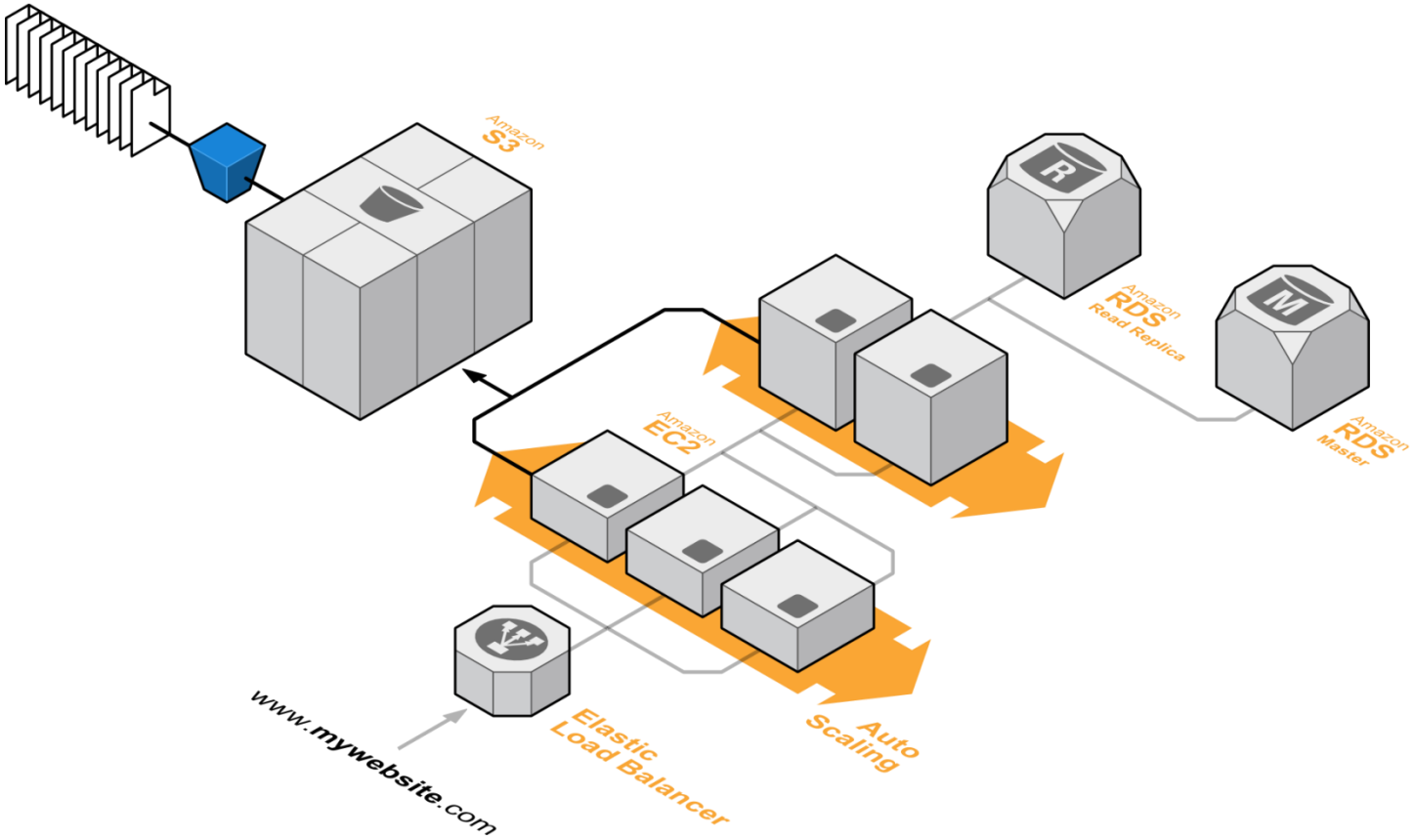
Group name	d-9367354752_controllers	Group description	AWS created security group for d-9367354752 directory controllers
Group ID	sg-6620aa03	VPC ID	vpc-18d31b7d

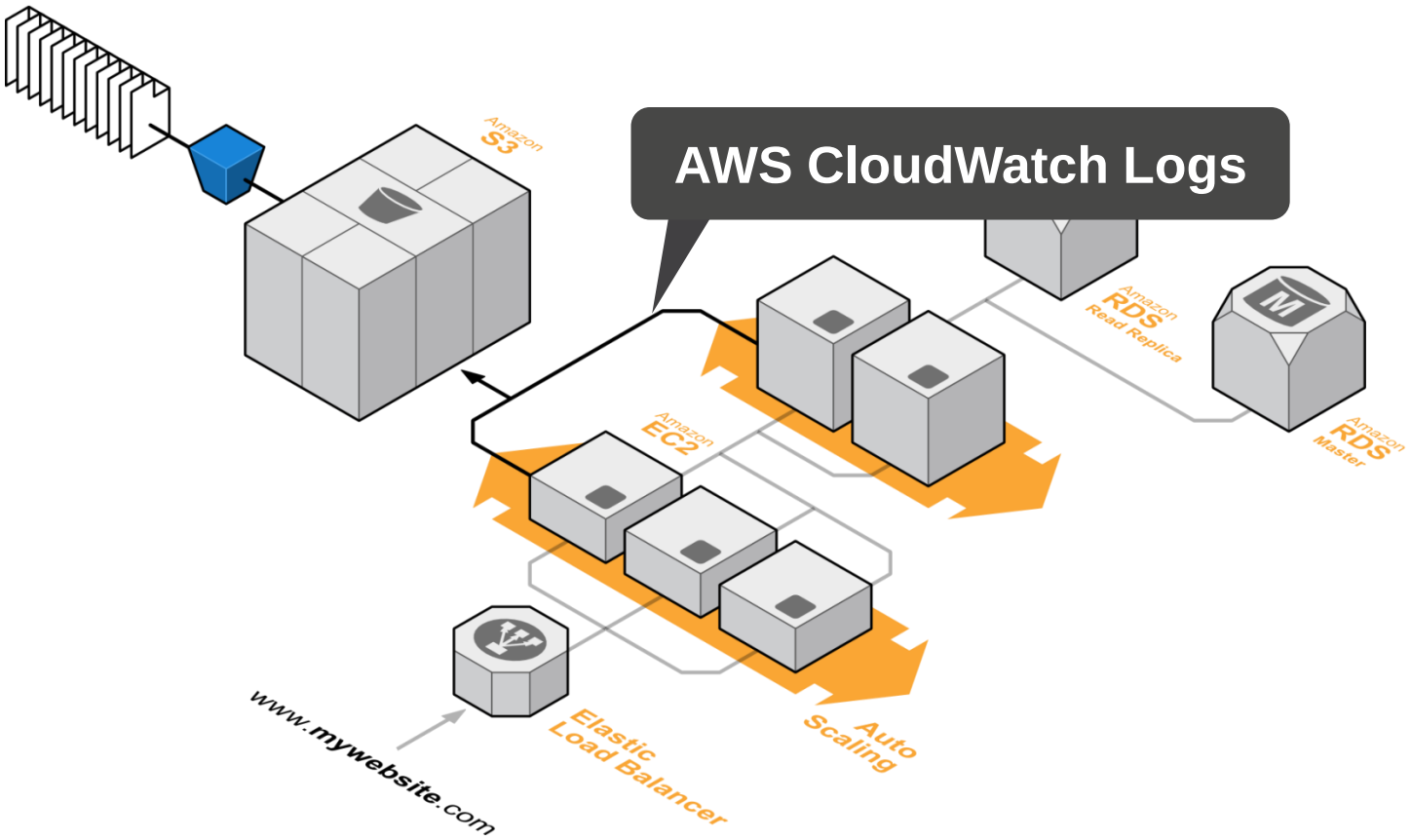
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use | Feedback

Journaux d’audit

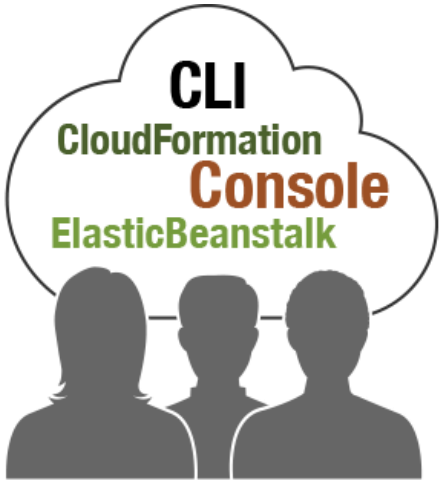
Acquérir, Analyser et Archiver


www.mywebsite.com
Elastic Load Balancer
Auto Scaling
Amazon EC2
Amazon RDS Read Replica
Amazon RDS Master


Amazon
S3
Amazon
RDS
Read Replica
Amazon
RDS
Master
Amazon
EC2
Elastic
Load Balancer
Auto
Scaling
www.mywebsite.com


AWS CloudWatch Logs
Amazon S3
Amazon RDS Read Replica
Amazon RDS Master
Amazon EC2
Elastic Load Balancer
Auto Scaling
www.mywebsite.com

AWS CloudTrail



Vos appels d'API

Sur de nombreux services dans plusieurs régions

Sont enregistrés continuellement par CloudTrail

User	Action	Time
Tim	Created	1:30pm
Sue	Deleted	2:40pm
Kat	Created	3:30pm

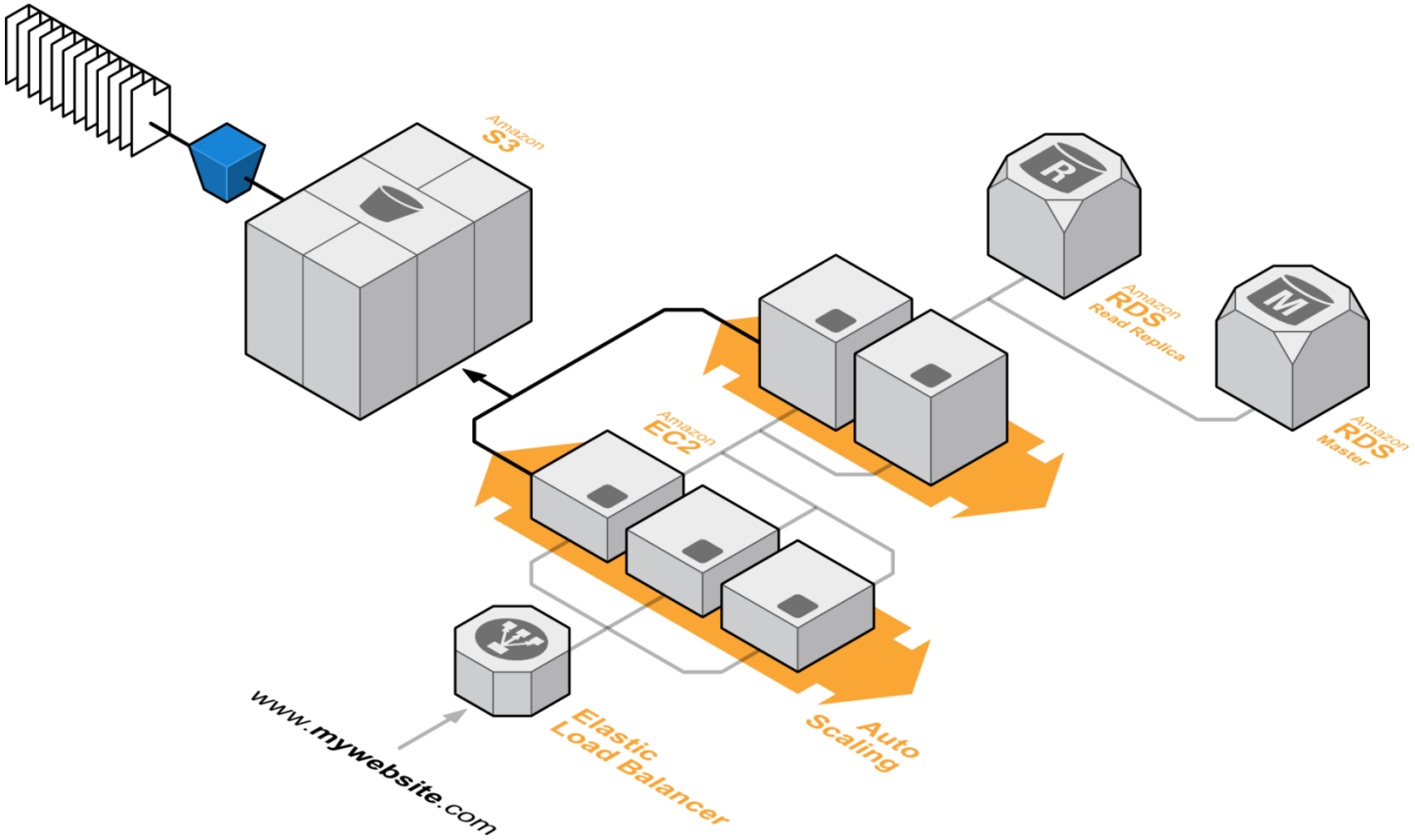
Et mis à vore disposition dans des journaux d'audit

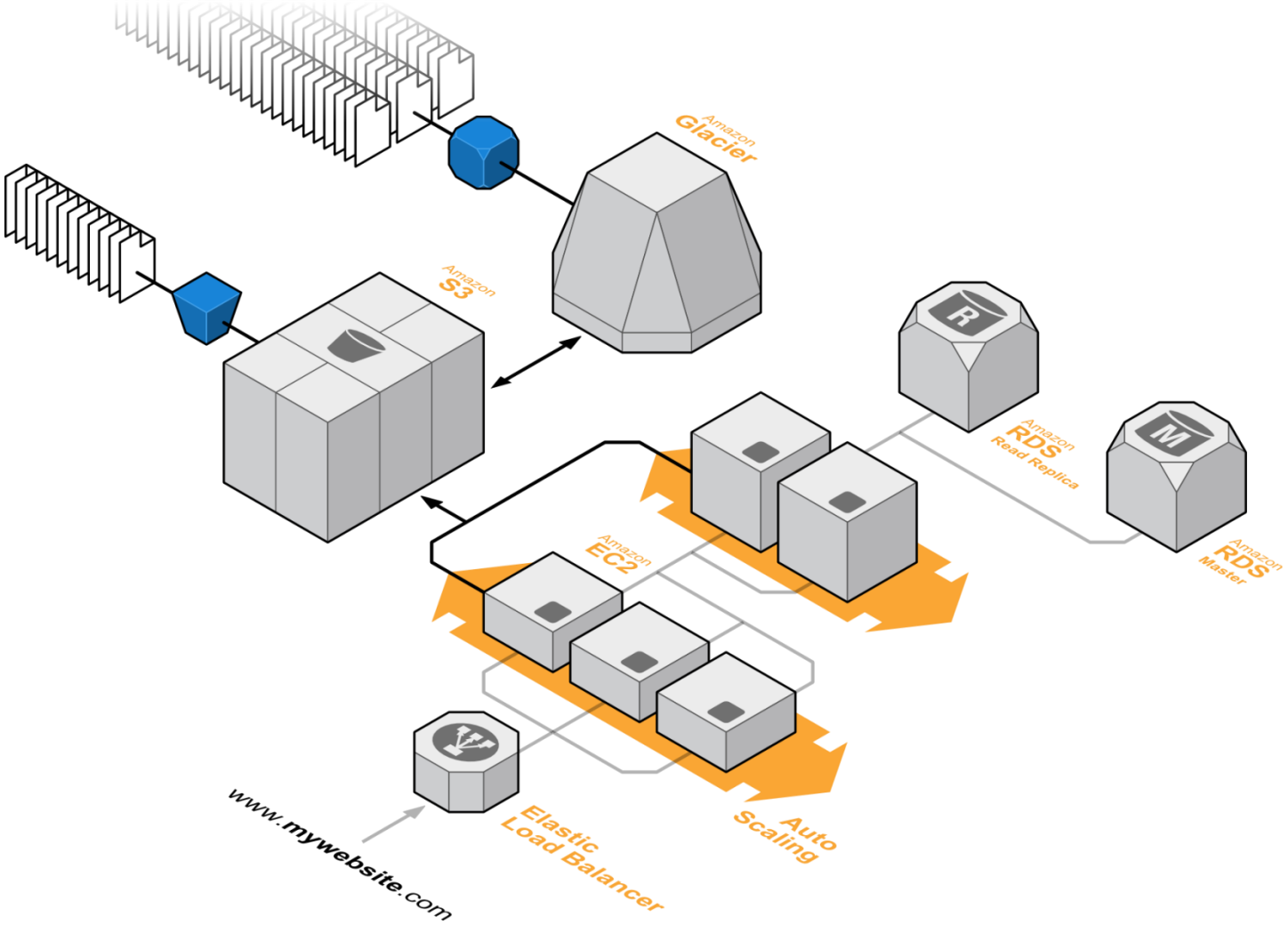
View Event


```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIL4BLJTMNQJVCGK56",
        "arn": "arn:aws:iam::663354267581:user/billshin_cli",
        "accountId": "663354267581",
        "accessKeyId": "ASIAJMZ3GN43GVODHQ5A",
        "userName": "billshin_cli",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "true",
                "creationDate": "2015-04-06T04:35:08Z"
            }
        },
        "invokedBy": "signin.amazonaws.com"
    },
    "eventTime": "2015-04-06T14:02:30Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "PutRolePolicy",
    "awsRegion": "us-east-1",
```

Protégez vos journaux avec IAM

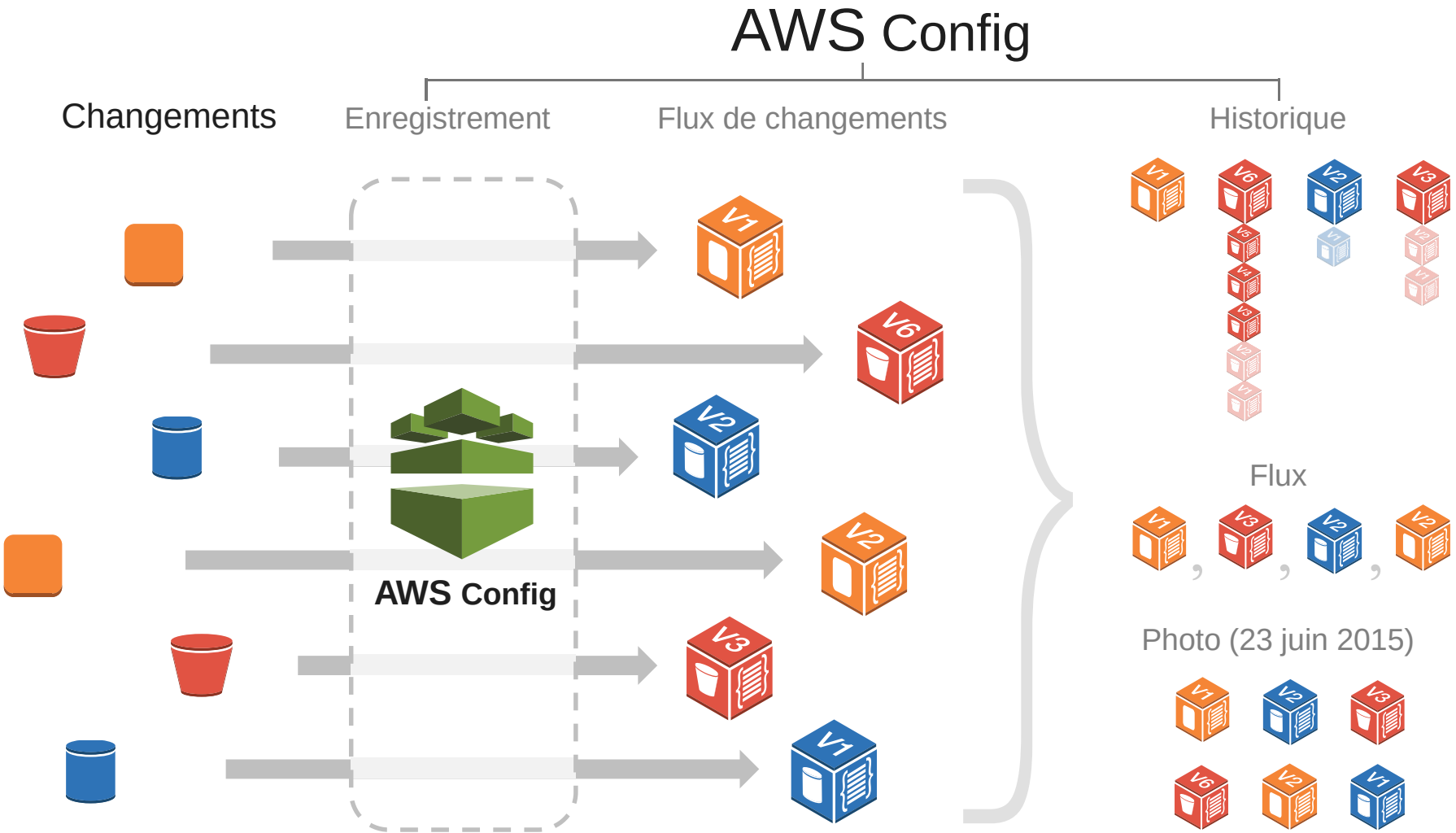
Archivez vos journaux


Amazon
S3
Amazon
RDS
Read Replica
Amazon
RDS
Master
Amazon
EC2
Elastic
Load Balancer
Auto
Scaling
www.mywebsite.com


Amazon
Glacier
Amazon
S3
Amazon
RDS
Read Replica
Amazon
RDS
Master
Amazon
EC2
Elastic
Load Balancer
Auto
Scaling
www.mywebsite.com

AWS Config

Tracez les changements de votre configuration


AWS Config
Changements
Enregistrement
Flux de changements
Historique
AWS Config
Flux
Photo (23 juin 2015)

Create Subnet | Delete Subnet | Modify Auto-Assign Public IP

Search Subnets and their p

Name	Subnet ID	CIDR	Availability Zone	Route Table
private-1a	subnet-b046fec7	10.40.2.0/23	us-east-1b	rtb-29148f48
private-1b	subnet-a246fed5	10.40.4.0/23	us-east-1b	rtb-29148f48
private-1c	subnet-f969d8a0	10.40.6.0/23	us-east-1c	rtb-29148f48
public-1a	subnet-cc3afee7	10.40.0.0/24	us-east-1a	rtb-5a3e583f | internet
public-1b	subnet-f9148f98	10.40.1.0/24	us-east-1b	rtb-5a3e583f | internet
public-1c	subnet-df59d786	10.40.8.0/24	us-east-1c	rtb-5a3e583f | internet
public-bastion-1a	subnet-ed3bffc6	10.40.252.0/23	us-east-1a	rtb-5a3e583f | internet
public-bastion-1b	subnet-eb47ff9c	10.40.254.0/23	us-east-1b	rtb-5a3e583f | internet
public-egress-1a	subnet-804480ab	10.40.250.0/24	us-east-1a	rtb-5a3e583f | internet
public-egress-1b	subnet-d83880af	10.40.251.0/24	us-east-1b	rtb-5a3e583f | internet

AWS Config

EC2 VPC vpc-27148f46 at April 06, 2015 9:08:26 AM PDT (UTC-07:00)

03 rd February 2015 7:03:26 PM	06 th February 2015 9:34:25 AM	06 th February 2015 9:51:09 AM	06 th April 2015 8:28:29 AM	06 th April 2015 9:08:26 AM
1	1	1	1	1 Change

Configuration Details

Relationships

Changes (1)

Configuration Changes (0)

Relationship Changes (1)

Field	From	To
AWS::EC2::Subnet	`null`	`"subnet-df59d786"`

AWS Config

EC2 Subnet subnet-df59d786 at April 06, 2015 9:40:15 AM PDT (UTC-07:00)

06th April 2015 9:08:26 AM

06th April 2015 9:08:27 AM

2

Configuration Details

Relationships

Changes (2)

Configuration Changes (0)

Relationship Changes (2)

Field	From	To
AWS::EC2::NetworkAcl	"acl-26148f47"	null
AWS::EC2::RouteTable	"rtb-5a3e583f"	null

Launch Instance | Connect | Actions

Filter by tags and attributes or search by keyword

DataClassific	Instance ID	Instance State	Public IP	Security Groups	Image ID	Elastic IP	Private IP Addr
Red	i-c881c3c1	running		ActiveDirectoryDo...	ami-c61678f6		10.0.3.66
Red	i-fa7e8df2	running		ActiveDirectoryDo...	ami-c61678f6		10.0.2.178
Yellow	i-605bd96a	running		svc9-SecSvcSecu...	ami-b5a7ea85		10.0.3.27
Yellow	i-25cc6d29	running		svc9-SecSvcSecu...	ami-b5a7ea85		10.0.2.31
Yellow	i-cf7bf9c5	running		svc9-WebTierSec...	ami-b5a7ea85		10.0.3.209
Yellow	i-6aab0a66	running		svc9-WebTierSec...	ami-b5a7ea85		10.0.2.136
Red	i-7d59f670	running		vpc_AppTier	ami-d1ad83e1		10.0.3.39
Red	i-c57a9ff1	running		vpc_AppTier	ami-0358ce33		10.0.3.18
Red	i-28da7ade	stopped		vpc_AppTier	ami-e7527ed7		10.0.2.147
Red	i-8637cfb4	running		vpc_AppTier	ami-2a31bf1a		10.0.2.98
Red	i-c6af0d30	running		vpc_AppTier	ami-d1ad83e1		10.0.2.73
Red	i-9bf86b96	running		vpc_AppTier	ami-d13845e1		10.0.2.81
Yellow	i-f5dd27f9	running		vpc_AppTier	ami-b5a7ea85		10.0.2.66
	i-76ce827f	running	54.186.23.194	vpc_MgmtTier	ami-c61678f6		10.0.254.36
	i-fc53a0f4	running	54.187.14.70	vpc_MgmtTier	ami-c61678f6		10.0.253.186
	i-eef119dc	running	50.112.160.119	vpc_MgmtTier	ami-2a31bf1a	50.112.160.119	10.0.253.68
Yellow	i-6d21c259	running	54.244.16.232	vpc_NATTier	ami-0358ce33	54.244.16.232	10.0.4.219
	i-45ab4f71	running	50.112.166.95	vpc_NATTier	ami-0358ce33	50.112.166.95	10.0.5.149

Votre configuration de sécurité devient un déclencheur

Analyse de journaux avec AWS Lambda.
Terminez les resources non-conformes.
Validez les changements.
Retour en arrière automatique si non-conforme.

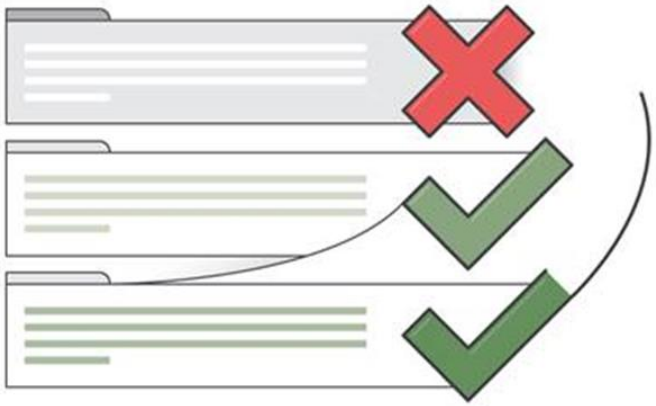
Config Rule

Des règles vérifient la conformité des changements

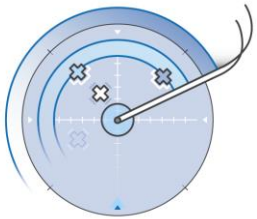
- Fournies par AWS

  ”Pas besoin de coder”

- Crées et hébergées par vous-même



AWS Inspector



Service de vérification de la sécurité

Agent au niveau du système

Test Manuel ou automatique

Donne des recommandations d’après les failles trouvées

Déployez en permanence

Les déploiements continu améliorent la sécurité.
Interdisez “SSH” en production.
Amenez vos patchs de sécurité en production rapidement.
Utilisez **AWS CodeDeploy**.

AWS Compliance & Certification

aws.amazon.com / **compliance**

“… We’ll also see organizations adopt cloud services for the improved security protections and compliance controls that they otherwise could not provide as efficiently or effectively themselves.”

Security’s Cloud Revolution is Upon Us
Forrester Research, Inc., August 2, 2013

“Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own data centers”

Tom Soderstrom – CTO – NASA JPL

“We work closely with AWS to develop a security model, which we believe enables us to operate more securely in the public cloud than we can in our own data centers.”

Rob Alexander, CIO, Capital One

Meilleur **Audit**

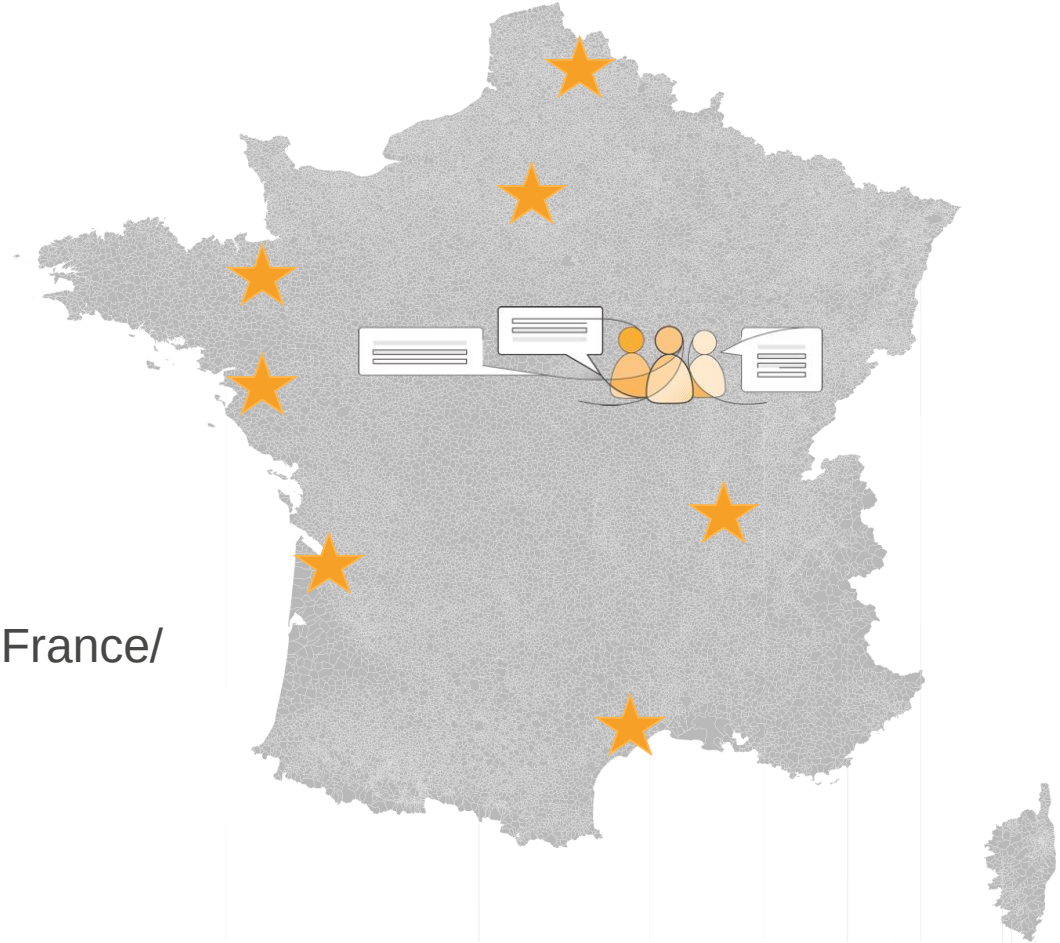
Meilleure **Visibilité**

Meilleur **Contrôle**

aws.amazon.com/**security**

AWS User Groups

Lille
Paris
Rennes
Nantes
Bordeaux
Lyon
Montpellier



facebook.com/groups/AWSFrance/

@aws_actus

Merci !

amazon web services