



Architecting for Greater Security in AWS

Jonathan Desrocher

Security Solutions Architect, Amazon Web Services.

Guy Tzur

Director of Ops, Totango.



1) Why does security come first in cloud adoption?



AWS Job Zero



New Territory

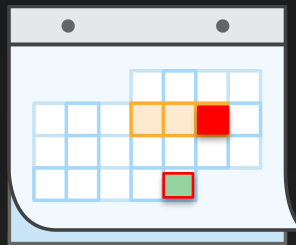


IT Security is
Traditionally Hard

2) Why is security traditionally so hard?



So much planning

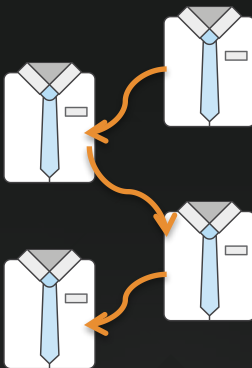


Slows down feature flow

3) Why so much planning which takes so long?



So many processes

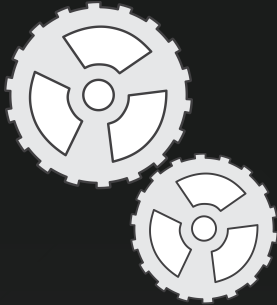


So many hand-offs



Built-in pauses

4) Why so many processes?



Processes detect
unwanted change



Visibility, control and
quality are
essential

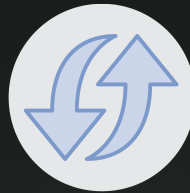


Reduce impact of failure

5) Why are change detection and low-risk changes so difficult?



Lack of visibility



No stimulus+response

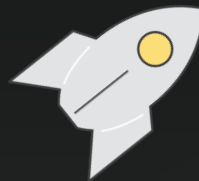


Low degree of automation

So where does AWS come in?



AWS makes security faster



Lets you move fast but stay safe

1) Secure, Sensible Defaults - Access

IAM Users, Groups, Roles

Managed and inline policies

Versioned IAM policies

Multi-factor authentication

Workforce lifecycle management (SAML Federation, Connected Directory)

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"
          ]
        }
      }
    }
  ]
}
```

[Create Policy](#)[Policy Actions](#) ▾

Filter: All Types ▾

	Policy Name ↕	Attached Entities ▾	Creation Time ↕	Edited Time ↕
☐	AmazonRDS-Prod-LogsOnly	0	2015-04-06 07:39 PDT	2015-04-06 07:39 PDT
☐	 AmazonRDSFullAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
☐	 AmazonRDSReadOnlyAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST

[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

The following managed policies are attached to this . You can attach up to Infinity managed policies.

[Attach Policy](#)

Policy Name	Actions
AmazonRDS-Prod-LogsOnly	Show Policy Detach Policy Simulate Policy

Inline Policies

▼ 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

1) Secure, Sensible Defaults - Access

IAM Users, Groups, Roles

Managed and inline policies

Versioned IAM policies

Multi-factor authentication

Workforce lifecycle management (SAML Federation, Connected Directory)

1) Secure, Sensible Defaults - Network

Virtual Private Cloud

DirectConnect & Virtual Private Gateway

Routing control – private and public subnets

IAM policies limit who can launch instances by trust zone

Security Groups

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 X

☐	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	Network ACL:	acl-26148f47
State:	available	Tenancy:	Default
VPC CIDR:	10.40.0.0/16	DNS resolution:	yes
DHCP options set:	dopt-c77d5ca9	DNS hostnames:	no
Route table:	rtb-29148f48		
ClassicLink:	Disabled		

[Create Subnet](#)[Delete Subnet](#)[Modify Auto-Assign Public IP](#)

☐	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](#)

☐	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](#)

☐	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

2) Improve Trust & Accountability with Better Visibility

AWS CloudTrail

AWS CloudWatch Logs

AWS Config

Tagging

Asset Management

API Activity History

Look up API activity captured for your AWS account in the last 7 days. Filter using one of the attributes to troubleshoot operational issues or security incidents.

Filter:	Event name ▾	PutRolePolicy ✕	Time range:	Select time range	📅
	Event time	User name	Event name	Resource type	Resource name
▼	2015-04-06, 07:02:30 AM	billshin_cli	PutRolePolicy	Role and 1 more	DBA and 1 more
AWS access key ASIAJMZ3GN43GVODHQ5A			Event source iam.amazonaws.com		
AWS region us-east-1			Event time 2015-04-06, 07:02:30 AM		
Error code			Request ID 9064a4fb-dc65-11e4-8847-c5d6598f6d95		
Event ID c407e827-975a-4200-b3c1-bce8d3d92917			Source IP address 72.21.196.64		
Event name PutRolePolicy			User name billshin_cli		
Resources Referenced (2)					
DBA		policygen-DBA-201309271307			
Role		Policy			

View Event

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAIL4BLJTMNQJVCCK56",
    "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",
```

Dashboard

Alarms

ALARM

INSUFFICIENT

OK

Billing

Logs

Metrics

Selected Metrics

DynamoDB

EBS

EC2

ELB

RDS

SNS

Custom Metrics...



Your alarm [PutRolePolicy](#) has been saved.

Log Groups > Filters for CloudTrail/DefaultLogGroup

Add Metric Filter



Your filter **eventName-PutRolePolicy** has been created.

Filter Name: eventName-ListRoles
Filter Pattern: { (\$.eventName = ListRoles) }
Metric: [LogMetrics](#) / [ListRoles](#)
Metric Value: 1

Create Alarm  

Alarm: [ListRoles](#)



Filter Name: eventName-PutGroupPolicy
Filter Pattern: { (\$.eventName = PutGroupPolicy) }
Metric: [LogMetrics](#) / [PutGroupPolicy](#)
Metric Value: 1

Create Alarm  

Alarm: [PutGroupPolicy](#)



Filter Name: eventName-PutRolePolicy
Filter Pattern: { (\$.eventName = PutRolePolicy) }
Metric: [LogMetrics](#) / [PutRolePolicy](#)
Metric Value: 1

Create Alarm  

Alarm: [PutRolePolicy](#)



ALARM: "PutRolePolicy" in US-West-2

☐ AWS Notifications

Sent: Monday, April 6, 2015 at 7:05 AM

To:  Shinn, Bill

You are receiving this email because your Amazon CloudWatch Alarm "PutRolePolicy" in the US-West-2 region has entered the ALARM state, because "Threshold Crossed: 1 datapoint (1.0) was greater than or equal to the threshold (0.0)." at "Monday 06 April, 2015 14:05:11 UTC".

View this alarm in the AWS Management Console:

<https://console.aws.amazon.com/cloudwatch/home?region=us-west-2#s=Alarms&alarm=PutRolePolicy>

Alarm Details:

- Name: PutRolePolicy
- Description: Role Policy Changed
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint (1.0) was greater than or equal to the threshold (0.0).
- Timestamp: Monday 06 April, 2015 14:05:11 UTC
- AWS Account: 663354267581

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 0.0 for 60 seconds.

Monitored Metric:

- MetricNamespace: LogMetrics
- MetricName: PutRolePolicy
- Dimensions:
- Period: 60 seconds
- Statistic: Sum
- Unit: not specified

State Change Actions:

- OK:
- ALARM: [arn:aws:sns:us-west-2:663354267581:CloudTrailNotifier]

2) Improve Trust & Accountability with Better Visibility

AWS CloudTrail

AWS CloudWatch Logs

AWS Config

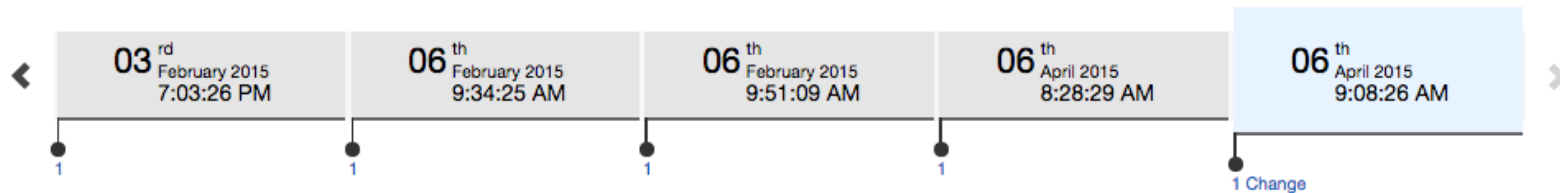
Tagging

Asset Management

[Create Subnet](#)[Delete Subnet](#)[Modify Auto-Assign Public IP](#)

☐	Name ^	Subnet ID v	CIDR v	Availability Zone v	Route Table v
☐	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

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



► Configuration Details

► Relationships

▼ Changes (1)

Configuration Changes (0)

Relationship Changes (1)

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

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

06th
April 2015
9:08:26 AM06th
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

2) Improve Trust & Accountability with Better Visibility

AWS CloudTrail

AWS CloudWatch Logs

AWS Config

Tagging

Asset Management

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



Totango And Dome9

Success Story

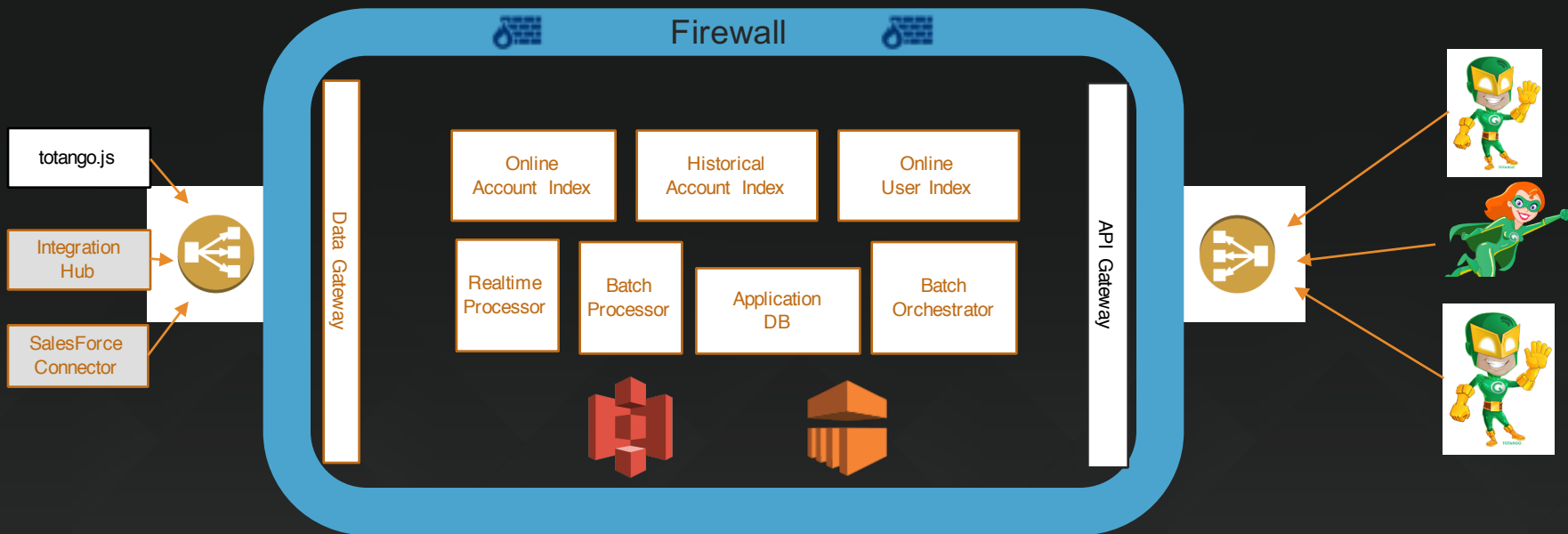
Guy Tzur
Director of OPS @ Totango



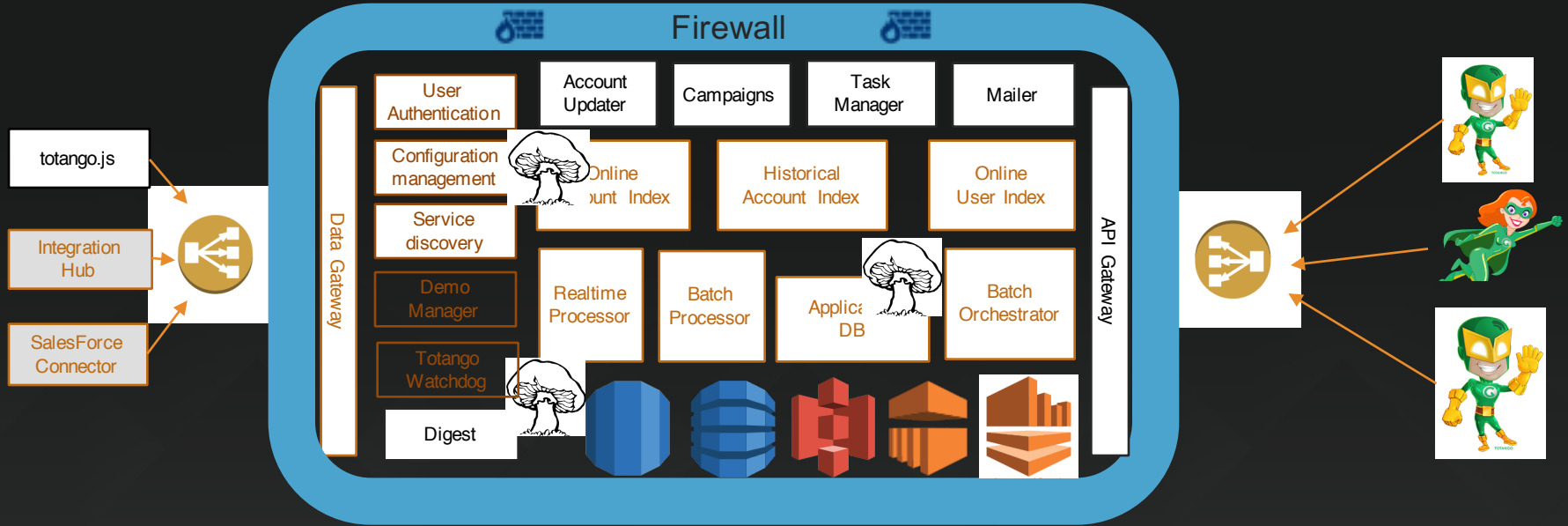
About Totango

- A Customer Success platform
- What is Customer Success?
- A SaaS solution that provides analytics for SaaS companies
- About 150 Customers

Totango's Architecture In the Past



Then Came The “Microservices”



The Problem

- P: Service creation/removal becomes a daily process – heavy load on OPS team
- S: OPS team enables automated service creation (powered by AWS
 - CLI, Fabric and Chef)

That leads to a bigger problem...

The Problem!!!

- Configuration mistakes can lead to severe security risks.
 - What happens if a service created is unsecured to the internet?



- Security Visualization, Monitoring and Management for AWS
 - Agentless; SaaS; Security focused UI; Made in Israel



The solution by Dome9

- Simplified Security State Visualization
 - Unified Security UI for multiple AWS accounts
 - Developer logins for self-service dynamic access
- Continues Alerting and Monitoring
 - “Alert when Instance tagged PROD has RDP/SSH open to new external IPs”
 - “Alert and Revert network changes, that are NOT done through Dome9 UI”
 - “Alert and Revert changes to non-active AWS regions”

Summery

3) Inherit compliance and controls

Map AWS certifications into your enterprise GRC

Recognized industry audit standards

Jurisdiction

Regulatory and contractual options (FedRAMP, HIPAA Business Associate Addendum, EU DPD Data Protection Addendum, PCI Attestation of Compliance)

4) Ride the pace of innovation

Find projects in your 3-year strategy where we are innovating and let us do it

Most companies do not encrypt content internally

Encryption is built into EBS, S3, RDS, Redshift, Glacier, Elastic MapReduce, and more

Key Management Service give you more control and visibility at cloud scale

We launched ~190 security-related features last year

5) Much Smaller Batch, Faster Changes

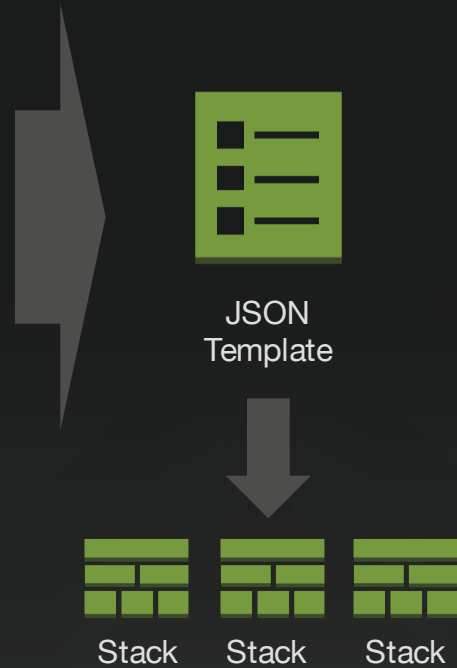
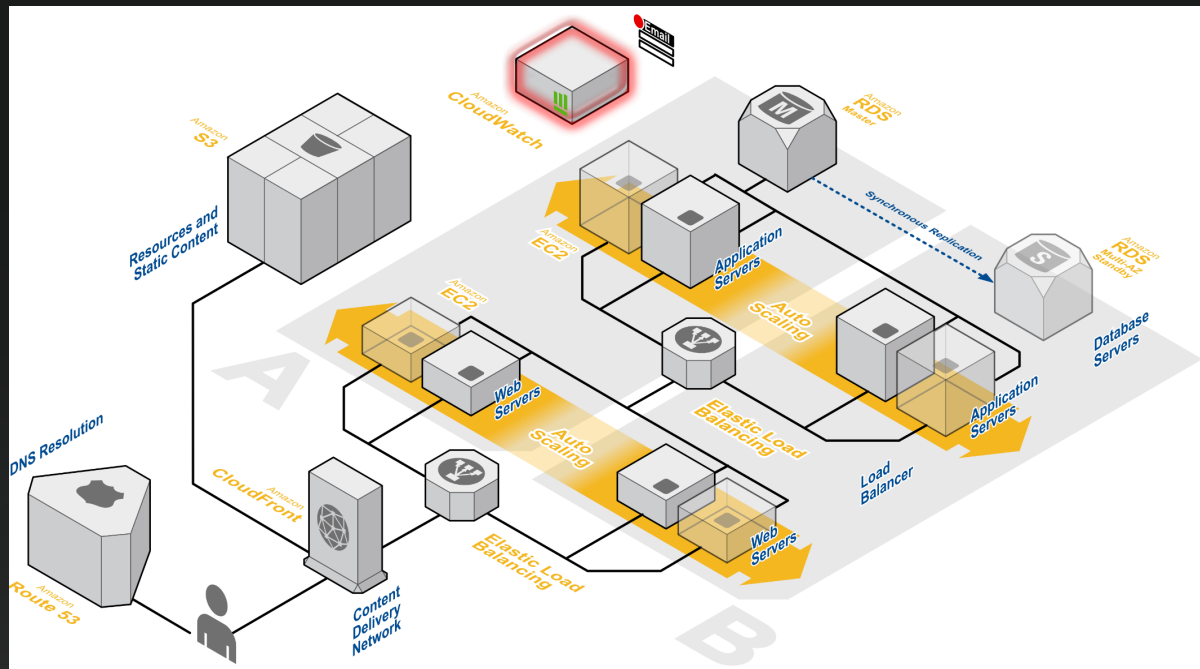
CloudFormation

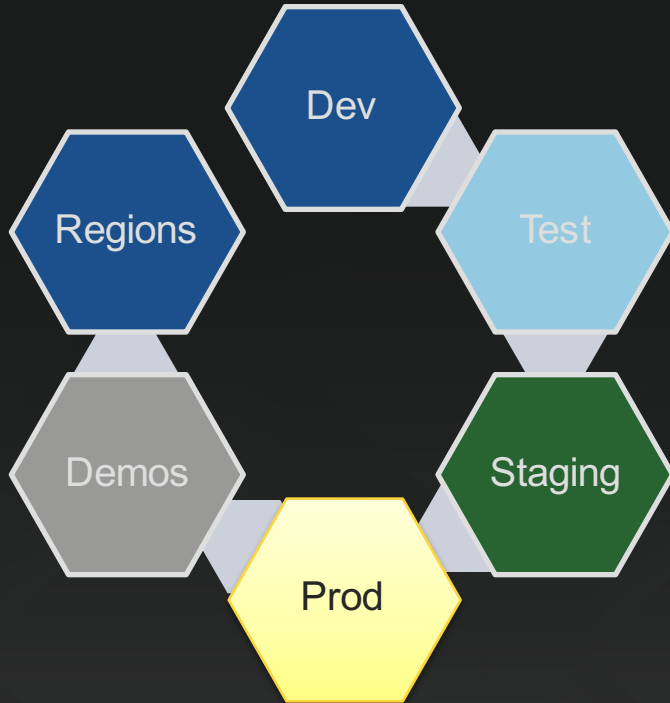
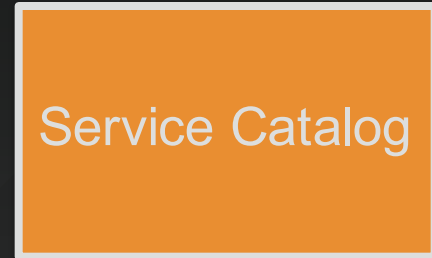
Infrastructure as code, checked into source code control

Route53 or ELB cutover in deployments

Elastic Beanstalk application versions

Integrate teams across functions - less hand-offs between teams, but far greater awareness and control of lower-risk changes





Proposed Change 1 #3

Edit

New issue

Merged root merged 1 commit into `root:master` from `root:proposed_change_1` 20 hours ago

Conversation 3

Commits 1

Files Changed 1

Showing 1 changed file

Unified

Split

cloudformation.template.erb			Ignore Space	Show notes	View
8	8	"Type" : "AWS::SQS::Queue"			
9	9	},			
10	10	"MuQueue2" : {			
11	11	"Type" : "AWS::SQS::Queue"			
12		},			
13		"MuQueue3" : {			
14		"Type" : "AWS::SQS::Queue"			
15	12	}			
16	13	},			
17	14	"Outputs" : {			
18	15	}			

Proposed Change 1 #3

Edit New Issue

Open root wants to merge 1 commit into `root:master` from `root:proposed_change_1`

Conversation **1** Commits **1** Files Changed **1**



root commented 27 seconds ago

Comment Here - this will be the audit trail of the proposed change



root commented just now

Notes and discussion from the change approver.

This pull request can be automatically merged.
You can also merge branches on the [command line](#).

Merge pull request



Write Preview

Leave a comment

Attach images by dragging & dropping, or selecting them.

Labels

None yet

Milestone

No milestone

Assignee

No one

1 participant



[Create VPC](#)

Actions ▾

☐	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

You can add tags to your resources to help you organize them. For more information, see [Tagging Your Resources](#).

[Edit](#)

Key	Value
-----	-------

Name

Application	stack-1381256732
-------------	------------------

Network	Public
---------	--------

Project	ArchHIPAA
---------	-----------

aws:cloudformation:logical-id	VPC
-------------------------------	-----

aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:663354267581:stack/stack-1381256732/04ed03e0-3047-11e3-8a8b-50e2416294a8
-----------------------------	---

aws:cloudformation:stack-name	stack-1381256732
-------------------------------	------------------

Create Stack

Update Stack

Delete Stack

Filter: Active ▾

By Name:

	Stack Name	Created Time	Status	Description
☒	stack-1381256732	2013-10-08 11:25:33 UTC-0700		VPC - Architecting for HIPAA

Overview

Outputs

Resources

Events

Template

Parameters

Tags

Stack Policy

Logical ID	Physical ID	Type
VPC	vpc-27148f46	AWS::EC2::VPC
InternetGateway	igw-24148f45	AWS::EC2::InternetGateway
PublicRouteTable	rtb-f2148f93	AWS::EC2::RouteTable
PrivateSubnet4	subnet-f4148f95	AWS::EC2::Subnet
PrivateRouteTable	rtb-f5148f94	AWS::EC2::RouteTable
BastionHostSecurityGroup	sg-6b69d504	AWS::EC2::SecurityGroup
PrivateSubnet5	subnet-fa148f9b	AWS::EC2::Subnet
PublicSubnet2	subnet-c1148fa0	AWS::EC2::Subnet
ELBSecurityGroup	sg-6969d506	AWS::EC2::SecurityGroup
PublicSubnet1	subnet-f9148f98	AWS::EC2::Subnet
PrivateSubnet6	subnet-c3148fa2	AWS::EC2::Subnet
PrivateSubnet3	subnet-d2148fb3	AWS::EC2::Subnet
NATSecurityGroup	sg-6a69d505	AWS::EC2::SecurityGroup
AttachGateway	stack-Attac-1MAL878JV8U2T	AWS::EC2::VPCGatewayAttachment
PrivateSubnet4RouteTableAssoci...	rtbassoc-9b148ffa	AWS::EC2::SubnetRouteTableAssociation
PublicRoute	stack-Publi-BLNPL14KNUHM	AWS::EC2::Route

6) Reduce the impact of failure

Multi-Availability Zone deployments

Use multiple regions

Replicate data – S3, EBS, RDS

Lifecycle policies

Auto-scaling

Auto-recovery

7) Further improve automation

Access and deployments are no longer performed by people

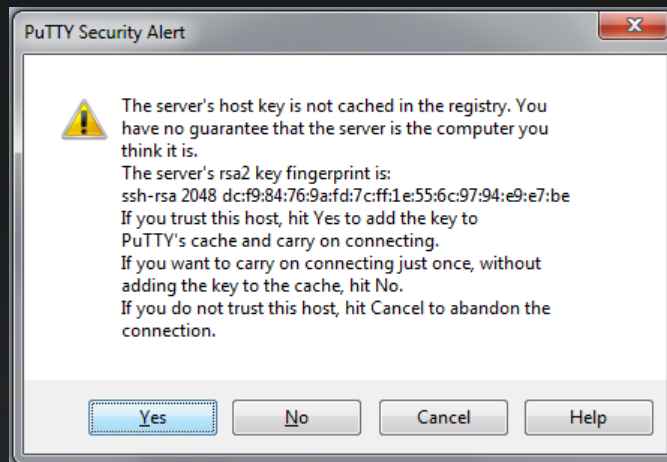
EC2 Instance Profiles and service roles (Security Token Service)

AWS CodeDeploy

Amazon EC2 Container Service

Continuous Integration & Deployment

Extends to on-premises workloads



CodeDeploy package specification

```
os: linux
files:
  - source: Config/config.txt
    destination: webapps/Config
  - source: source
    destination: /webapps/myApp
hooks:
  BeforeInstall:
    - location: Scripts/UnzipResourceBundle.sh
    - location: Scripts/UnzipDataBundle.sh
  AfterInstall:
    - location: Scripts/RunResourceTests.sh
      timeout: 180
  ApplicationStart:
    - location: Scripts/RunFunctionalTests.sh
      timeout: 3600
  ValidateService:
    - location: Scripts/MonitorService.sh
      timeout: 3600
    runas: codedeployuser
```

Amazon EC2 Container Service Task Definition

```
{
  "containerDefinitions": [
    {
      "name": "wordpress",
      "links": [
        "mysql"
      ],
      "image": "wordpress",
      "essential": true,
      "portMappings": [
        {
          "containerPort": 80,
          "hostPort": 80
        }
      ],
      "memory": 500,
      "cpu": 10
    },
    {
      "environment": [
        {
          "name": "MYSQL_ROOT_PASSWORD",
          "value": "password"
        }
      ],
      "name": "mysql",
      "image": "mysql",
      "cpu": 10,
      "memory": 500,
      "essential": true
    }
  ],
  "family": "hello_world"
}
```

Automate security operations

- Secret and configuration management.
- Test backup and restore
- Perform intrusion detection on launch/retire
- Validate running deployments against expectations and human approvals

On success: retire instance.

On failure: call a human.

8) Make security actionable

Review what matters

- Internet Gateway
- Identity and Access Management
- VPC – Subnet and NACL changes
- Security Groups

Shut things down automatically

Assess what changes

Roll-back automatically

Use Lambda for event-driven security

Benefits of IT Security on AWS

Higher degree of visibility, transparency and accountability (secure and can prove it)

Higher degree of trust and autonomy

Significant reductions in long-term, privileged access

Focus a greater portion of limited security resources toward application security

Have a much higher rate of successful change and changes are delivered more quickly

Thank you!