

How Empowering Your DevOps Teams Can Lead to Better Cloud Security

Shira Shamban
CEO and co-founder @ Solvo

**DEVOPS
WORLD**
by CloudBees



Hi, I'm Shira!

- CEO of Solvo
- Co-chair of OWASP Israel
- Founder of Security Diva
- Cloud security fan





Being a DevOps is the best job in the world!





How to be good at what we do?

ELITE PERFORMERS

Comparing the elite group against the low performers, we find that elite performers have...



208
TIMES MORE
frequent code deployments

106
TIMES FASTER
lead time from
commit to deploy



2,604
TIMES FASTER
time to recover from incidents

7
TIMES LOWER
change failure rate
(changes are $\frac{1}{7}$ as likely to fail)





The cloud is here to help

**On-demand
self-service**

**Broad network
access**

**Resource
pooling**

**Rapid
elasticity**

**Measured
services**



The cloud is here to help

On-demand
self-service

Broad network
access

Measured
services

Rapid
elasticity

Resource
pooling

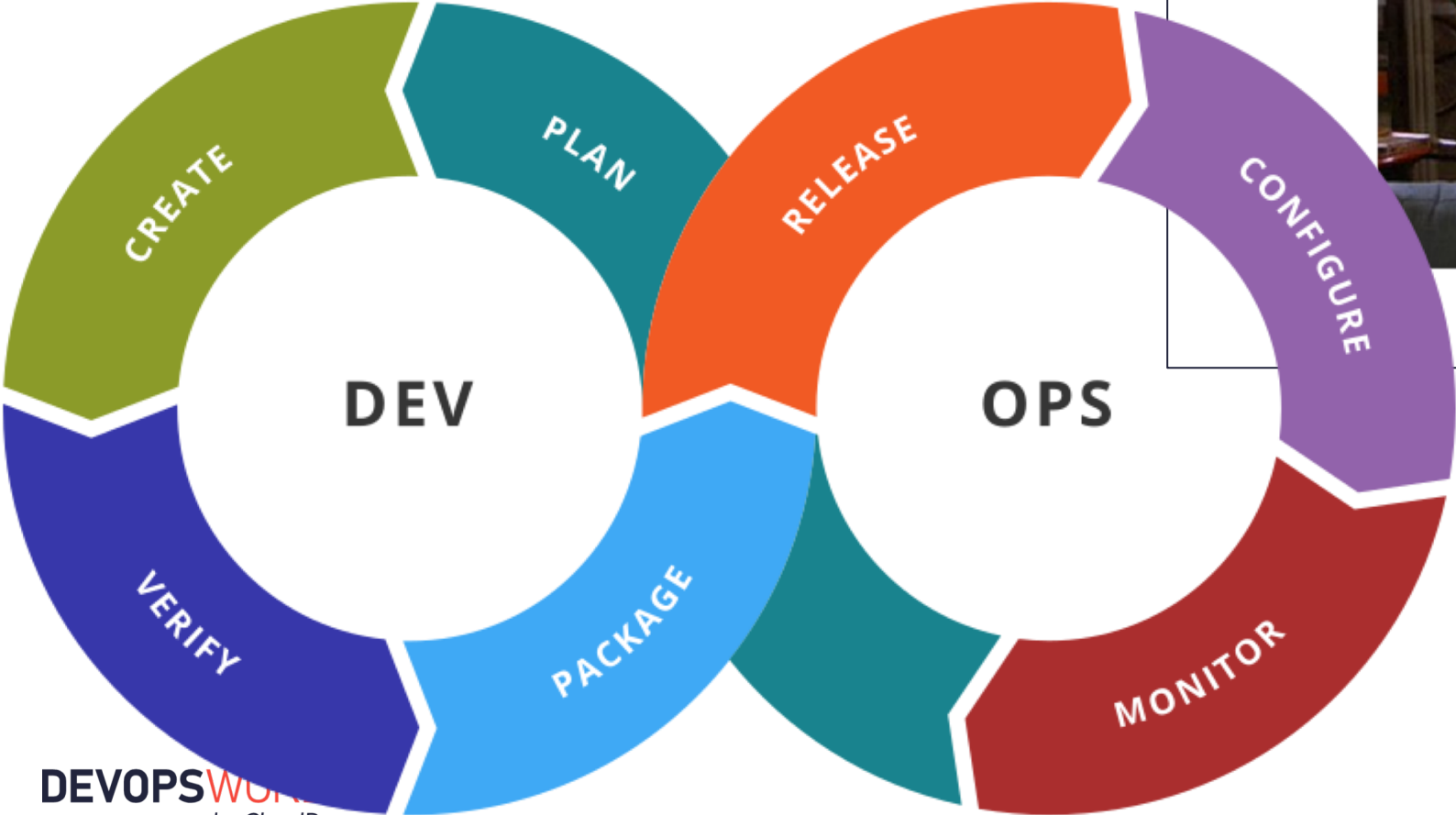
Templates
(infra as code)

Gold images

Logging and
monitoring

Automation and
enforcement

CI/CD



DEVOPS WORKFLOW
by CloudBees

© 2020 All Rights Reserved.



Seinfeld Ops @SeinfeldOps · 05 Aug
The team when the deploy works and nothing is broken right away



↻ 1 ❤️ 12 🔗



Culture in successful teams



Seinfeld Ops

@SeinfeldOps

The build is red...

...and it's your fault.



20:19 · 19 Aug 20 · [Buffer](#)

Trust

Safety



DevOps as security enabler

On-demand
self-service

Infrastructure
as code

Feedback



Sam Coren

@samcoren

I did a [@SimpsonsOps](#) again



4:59 · 20 Aug 20 · Twitter for iPhone



The right tools for the job

Useful

Easy to use

Boost
productivity



Seinfeld Ops @SeinfeldOps · 12 Aug

When you try and copy the architecture from Google or Facebook



↻ 2

♡ 14



The IAM problem

By 2023, **75%** of security failures will result from inadequate management of identities, access, and privileges, up from 50% in 2020.



Seinfeld Ops

@SeinfeldOps

Two senior engineers convincing the junior engineer to take the pager for the weekend



17:59 · 19 Aug 20 · [Buffer](#)

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import man](#)[Expand all](#) | [Collapse all](#)

▼ S3

[Clone](#) |

► Service S3

▼ Actions Specify the actions allowed in S3 ?

close

🔍 Filter actions

Manual actions ([add actions](#))☐ All S3 actions (s3:*)**Access level**

- ☐ List
- ☐ Read
- ☐ Tagging
- ☐ Write
- ☐ Permissions management

[Switch to deny permis](#)[Expand all](#) | [Co](#)**Resources** Choose actions before applying resources

Character count: 39 of 6,144.

[Cancel](#)[Review](#)

Documentation

No automation,
no self-service,
no pooling

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

Import man

[Expand all](#) | [Collapse all](#)

▼ S3 (All actions) ⚠️ 4 warnings

Clone

► Service S3

▼ Actions Specify the actions allowed in S3 ?
[close](#)

[Switch to deny permis](#)

Q Filter actions

Manual actions [\(add actions\)](#)

☒ All S3 actions (s3:*)

Access level

- ☒ List (3 selected)
- ☒ Read (41 selected)
- ☒ Tagging (6 selected)
- ☒ Write (31 selected)
- ☒ Permissions management (11 selected)

[Expand all](#) | Co

► Resources Specify **accesspoint** resource ARN for the **DeleteAccessPointPolicy** and 5 more actions. ⓘ
Specify **bucket** resource ARN for the **GetBucketLocation** and 44 more actions. ⓘ

Cancel

Review

No automation,
no self-service,
no pooling

entation



The Office Ops @TheOfficeOps · 04 Aug
Adding one more should get us there!



  4  20 

No automation,
no self-service,
no pooling

Documentation

▼ S3 (All actions) ⚠ 4 warnings

Clone

► Service S3

► Actions Manual actions

*

▼ Resources ☒ Specific
[close](#) ☐ All resources

accesspoint ⓘ Specify **accesspoint** resource ARN for the **DeleteAccessPointPolicy** and 5 more actions. ⓘ
[Add ARN](#) to restrict access

bucket ⓘ Specify **bucket** resource ARN for the **GetBucketLocation** and 44 more actions. ⓘ
[Add ARN](#) to restrict access

job ⓘ Specify **job** resource ARN for the **DescribeJob** and 2 more actions. ⓘ
[Add ARN](#) to restrict access

object ⓘ Specify **object** resource ARN for the **PutObjectRetention** and 29 more actions. ⓘ
[Add ARN](#) to restrict access

► Request conditions [Specify request conditions \(optional\)](#)

+ Add additional permissions

Character count: 39 of 6,144.

Cancel

Review

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import man](#)[Expand all](#) | [Collapse all](#)

▼ S3 (All actions)

[Clone](#)

▶ Service S3

▶ Actions Manual actions

*

▼ Resources ☐ Specific
[close](#) ☒ All resources

▶ Request conditions [Specify request conditions \(optional\)](#)[+ Add additional perm](#)

Character count: 110 of 6,144.

[Cancel](#)[Review](#)

Documentation

No automation,
no self-service,
no pooling

We can try to do better



Create role









1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy



Filter policies ▾		Q full	Showing 175 results
	Policy name ▾	Used as	
<input type="checkbox"/>	▶  AlexaForBusinessFullAccess	None	
<input type="checkbox"/>	▶  AmazonAPIGatewayInvokeFullAccess	None	
<input type="checkbox"/>	▶  AmazonAppFlowFullAccess	None	
<input type="checkbox"/>	▶  AmazonAppStreamFullAccess	None	
<input type="checkbox"/>	▶  AmazonAthenaFullAccess	None	
<input type="checkbox"/>	▶  AmazonAugmentedAIFullAccess	None	
<input type="checkbox"/>	▶  AmazonAugmentedAIHumanLoopFullAccess	None	
<input type="checkbox"/>	▶  AmazonChimeFullAccess	None	

▶ Set permissions boundary

Identity and Access Management (IAM)

[Dashboard](#)

▼ Access management

[Groups](#)[Users](#)[Roles](#)

Policies

[Identity providers](#)[Account settings](#)

▼ Access reports

[Access analyzer](#)[Archive rules](#)[Analyzers](#)[Settings](#)[Credential report](#)[Organization activity](#)[Service control policies \(SCPs\)](#)

AWS account ID:

915018814527

[Policies](#) > AmazonDynamoDBReadOnlyAccess

Summary

Policy ARN arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess **Description** Provides read only access to Amazon DynamoDB via the AWS Management Console.[Permissions](#)[Policy usage](#)[Policy versions](#)[Access Advisor](#)[Policy summary](#)[{} JSON](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "application-autoscaling:DescribeScalableTargets",
7         "application-autoscaling:DescribeScalingActivities",
8         "application-autoscaling:DescribeScalingPolicies",
9         "cloudwatch:DescribeAlarmHistory",
10        "cloudwatch:DescribeAlarms",
11        "cloudwatch:DescribeAlarmsForMetric",
12        "cloudwatch:GetMetricStatistics",
13        "cloudwatch:ListMetrics",
14        "datapipeline:DescribeObjects",
15        "datapipeline:DescribePipelines",
16        "datapipeline:GetPipelineDefinition",
17        "datapipeline:ListPipelines",
18        "datapipeline:QueryObjects",
19        "dynamodb:BatchGetItem",
20        "dynamodb:Describe*",
21        "dynamodb:List*"
22      ]
23    }
24  ]
25 }
```

read-only 



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-
autoscaling:DescribeScalableTargets",
        "application-
autoscaling:DescribeScalingActivities",
        "application-
autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*",

```

[Apply](#)[Reset](#)

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

	Service	Action	Resource Type	Simulation Resource	Permission
▸	AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	DeleteGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	GetGroupQuery	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	ListGroupResources	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	SearchResources	not required	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸	AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-
autoscaling:DescribeSc
        "application-
autoscaling:DescribeScalingActivities",
        "application-
autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*",

```

Get function configuration[Apply](#)[Reset](#)

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

	Service	Action	Resource Type	Simulation Resource	Permission
▸	AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	DeleteGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	GetGroupQuery	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	ListGroupResources	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	SearchResources	not required	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸	AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPlans",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*"
      ]
    }
  ]
}
```

Get function configuration**List lambda functions**[Apply](#)[Reset](#)

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

	Service	Action	Resource Type	Simulation Resource	Permission
▸	AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
		DeleteGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
		GetGroupQuery	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	ListGroupResources	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	SearchResources	not required	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸	AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPlans",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeDashboards",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*"
      ]
    }
  ]
}
```

Get function configuration**List lambda functions****Describe security groups**[Apply](#)[Reset](#)

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

	Service	Action	Resource Type	Simulation Resource	Permission
▸	AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
		DeleteGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
		GetGroupQuery	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
		ListGroupResources	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	SearchResources	not required	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸	AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPlans",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeDashboards",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipeline",
        "datapipeline:GetPipeline",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*"
      ]
    }
  ]
}
```

Get function configuration**List lambda functions****Describe security groups****Describe subnets**[Apply](#)[Reset](#)

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

	Service	Action	Resource Type	Simulation Resource	Permission
▸	AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
		DeleteGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
		GetGroupQuery	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
		ListGroupResources	group	*	allowed 1 matching statements.
▸	AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
		SearchResources	not required	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸	AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸	AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸	AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPlans",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeDashboards",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipeline",
        "datapipeline:GetPipeline",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*"
      ]
    }
  ]
}
```

Get function configuration**List lambda functions****Describe security groups****Describe subnets**

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▸ AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
	DeleteGroup			denied Implicitly denied (no matching...
▸ AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
	GetGroupQuery	group	*	allowed 1 matching statements.
▸ AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
	ListGroupResources	group	*	allowed 1 matching statements.
▸ AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
	SearchResources	not required	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸ AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPlans",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeDashboards",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipeline",
        "datapipeline:GetPipeline",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*"
      ]
    }
  ]
}
```

Get function configuration**List lambda functions****Describe security groups****Describe subnets**

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▸ AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
	DeleteGroup			denied Implicitly denied (no matching...
▸ AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
	GetGroupQuery			allowed 1 matching statements.
▸ AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
	ListGroupResources	group	*	allowed 1 matching statements.
▸ AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
	SearchResources	not required	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸ AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPlans",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeDashboards",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipeline",
        "datapipeline:GetPipeline",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*"
      ]
    }
  ]
}
```

Get function configuration**List lambda functions****Describe security groups****Describe subnets**

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▸ AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
	DeleteGroup			denied Implicitly denied (no matching...
▸ AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
	GetGroupQuery			allowed 1 matching statements.
▸ AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
	ListGroupResources	group		allowed 1 matching statements.
▸ AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
	SearchResources	not required	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸ AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...

Describe VPCs**Describe key****Get role**[Apply](#)[Reset](#)



Policies

[Back](#)

Policy name: tempgb1fec

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPlans",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeDashboards",
        "cloudwatch:ListMetrics",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipeline",
        "datapipeline:GetPipeline",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dax:Describe*",
        "dax:List*"
      ]
    }
  ]
}
```

Get function configuration**List lambda functions****Describe security groups****Describe subnets**

Policy Simulator

Identity And Ac... ▾

141 Action(s) se... ▾

[Select All](#)[Deselect All](#)[Reset Contexts](#)[Clear Results](#)[Run Simulation](#)

▸ Global Settings ⓘ

Action Settings and Results [200 actions selected. 0 actions not simulated. 8 actions allowed. 192 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▸ AWS Resource Groups	CreateGroup	group	*	denied Implicitly denied (no matching...
	DeleteGroup			denied Implicitly denied (no matching...
▸ AWS Resource Groups	GetGroup	group	*	allowed 1 matching statements.
	GetGroupQuery			allowed 1 matching statements.
▸ AWS Resource Groups	GetTags	group	*	denied Implicitly denied (no matching...
	ListGroupResources	group		allowed 1 matching statements.
▸ AWS Resource Groups	ListGroups	group	*	allowed 1 matching statements.
	SearchResources	not		denied Implicitly denied (no matching...
▸ AWS Resource Groups	Tag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	Untag	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroup	group	*	denied Implicitly denied (no matching...
▸ AWS Resource Groups	UpdateGroupQuery	group	*	denied Implicitly denied (no matching...
▸ AWS Accounts	DisableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	EnableRegion	not required	*	denied Implicitly denied (no matching...
▸ AWS Accounts	ListRegions	not required	*	denied Implicitly denied (no matching...

Describe VPCs**Describe key****Get role****List roles**[Apply](#)[Reset](#)



Reality vs. Expectations

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": ["dynamodb:*", "s3:*"],  
6       "Effect": "Allow",  
7       "Resource": "*"   
8     }  
9   ]  
10 }
```



Reality vs. Expectations

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": "dynamodb:GetItem",
6       "Effect": "Allow",
7       "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/ORDERS-TABLE"
8     },
9     {
10      "Action": [
11        "s3:GetObject"
12      ],
13      "Effect": "Allow",
14      "Resource": "arn:aws:s3:::app-bucket/receipts/*"
15    }
16  ]
17 }
```




Reality vs. Expectations

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": "dynamodb:GetItem",  
6       "Effect": "Allow",  
7       "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/ORDERS-TABLE"  
8     },  
9     {  
10      "Action": [  
11        "s3:GetObject"  
12      ],  
13      "Effect": "Allow",  
14      "Resource": "arn:aws:s3:::app-bucket/receipts/*"  
15    }  
16  ]  
17 }
```

Specific action



Reality vs. Expectations

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": "dynamodb:GetItem",  
6       "Effect": "Allow",  
7       "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/ORDERS-TABLE"  
8     },  
9     {  
10      "Action": [  
11        "s3:GetObject"  
12      ],  
13      "Effect": "Allow",  
14      "Resource": "arn:aws:s3:::app-bucket/receipts/*"  
15    }  
16  ]  
17 }
```

Specific resource



Reality vs. Expectations

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": "dynamodb:GetItem",  
6       "Effect": "Allow",  
7       "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/ORDERS-TABLE"  
8     },  
9     {  
10      "Action": [  
11        "s3:GetObject"  
12      ],  
13      "Effect": "Allow",  
14      "Resource": "arn:aws:s3:::app-bucket/receipts/*"  
15    }  
16  ]  
17 }
```

Scaled to the entire components of the application

Let us take care of
cloud security for you.
Just Code.



Thank you!
come visit us at solvo.cloud

Shira Shamban
CEO and co-founder @ Solvo

**DEVOPS
WORLD**
by CloudBees