

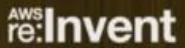
SID 314

AWS re:INVENT

IAM Policy Ninja

Brigid Johnson
Manager, Product Management – AWS Identity

November 27, 2017

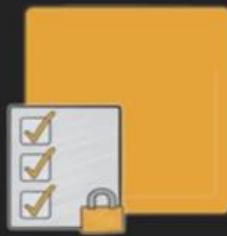


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Are you interested in learning **how to control access to your AWS resources**? Have you wondered how to best scope permissions to achieve least-privilege permissions access control? If your answer is "yes", this session is for you. We look at the **Identity & Access Management policy language**, starting with the basics of the **policy** language and how to create and attach policies to IAM **users**, **groups**, and **roles**. We explore policy variables, conditions, and tools to help you author least privilege policies. We cover common use cases, such as granting a user secure access to an Amazon **S3 bucket** or to launch an **Amazon EC2 instance** of a specific type.

Limit Amazon EC2 instance types Demo



We are going to build a policy to do the above

Limit Amazon EC2 instance types

Demo



- Goal: Limit a user from starting an instance unless the instance is t2.*
- Let's try to:
 - Create a managed policy that attempts to limit starting an EC2 instance except for these instance types.
 - Attach that policy to an IAM user.

We will start with a demo in the console as below

The screenshot shows the AWS Management Console with the EC2 Management Console selected. The main view is the Instances page. On the left, there's a sidebar with links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected), Spot Requests, Reserved Instances, Dedicated Hosts, Images, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Snapshots, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, and Network Interfaces. The main content area has a search bar and filters for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), IPv4 Public IP, and IPv6 IPs. A message at the top says, "An error occurred fetching instance data: You are not authorized to perform this operation." Below that, it says "Select an instance above". At the bottom, there are links for Feedback, English (US), and Mozilla Firefox seems slow.. To start. There are also links for Privacy Policy and Terms of Use, and a status bar at the bottom right showing the date and time.

Casey has no permissions at the moment and cannot do anything. We will start by creating a policy to start giving him the exact access he needs to do his job

Screenshot of the AWS IAM Management Console showing a list of customer-managed policies. The sidebar on the left shows navigation links for Dashboard, Groups, Users, Roles, Policies (selected), Identity providers, Account settings, Credential report, and Encryption keys. The main content area displays a table of policies with columns for Policy name, Type, Attachments, and Description. A search bar at the top right allows filtering by policy name.

	Policy name	Type	Attachments	Description
<input type="checkbox"/>	AWSCloudTrailAccessPolicy	Customer managed	1	
<input type="checkbox"/>	Cloudtrail-Access	Customer managed	2	This grants access to list and read actions in CloudTrail
<input type="checkbox"/>	EC2-Create-Tag-RunInstances	Customer managed	1	Grants access to create tags but only during runinstances
<input type="checkbox"/>	Ec2-CreateTag-withValues	Customer managed	1	Grants access to create and modify tags with specific values
<input type="checkbox"/>	EC2-launch-instance-T2	Customer managed	1	This policy allows developers to launch instances only in the T2 family
<input type="checkbox"/>	EC2-launch-instance-T2-withTag	Customer managed	1	Grants access to launch T2 instances, but requires project tag with poker or blackjack values
<input type="checkbox"/>	Ec2-manage-instances-tag	Customer managed	3	This policy allows access to manage instances with a specific tag
<input type="checkbox"/>	list-pass-role-reinvent-2017-mobile	Customer managed	2	This policy allows developers to pass the reinvent mobile role when they launch instances
<input type="checkbox"/>	s3-2017-reinvent-mobile-resource-access-dev	Customer managed	1	This policy grants access to list buckets and read from the mobile folder in the reinvent-2017-policy-ninja...
<input type="checkbox"/>	S3-reinvent-2017-dev	Customer managed	2	Access to read files from S3 bucket reinvent-2017-policy-ninja-dev

Screenshot of the AWS IAM Management Console showing the "Create policy" step. The top navigation bar includes links for IAM Management, EC2 Management, S3 Management, and other services. The main content area is titled "Create policy" and shows two steps: "Editor" (highlighted with a blue circle) and "Review". Below the steps, a note explains what a policy is and how it can be created. The "Visual editor" tab is selected, showing a form to define permissions. The "JSON" tab is also present. At the bottom, there are buttons for "Add additional permissions", "Cancel", and "Review policy".

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

Visual editor JSON Import managed policy

Use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service. Learn more

Expand all | Collapse all

Select a service

Service * Choose a service

Actions Choose a service before defining actions

Resources Choose actions before applying resources

Request Conditions Choose actions before specifying conditions

Add additional permissions

* Required

Feedback English (US)

We want to create a policy that will allow Casey to create and use instances of t1 type only

Screenshot of the AWS IAM Management Console showing the "Create policy" step. The URL is https://console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=edit.

The interface shows two steps: **1 Editor** and **2 Review**.

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

Visual editor (selected) | **JSON**

Use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service. Learn more

Expand all | Collapse all

Select a service

Service * Select a service below
close Q ec2| Enter service manually

EC2 EC2 Container Service
EC2 Container Registry EC2 Messages

Actions Choose a service before defining actions

Resources Choose actions before applying resources

* Required Cancel Review policy

Feedback English (US) Privacy Policy Terms of Use 10:49 AM

Screenshot of the AWS IAM Management Console showing the "Create policy" step, continuing from the previous screen. The URL is https://console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=edit.

The interface shows two steps: **1 Editor** and **2 Review**.

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

Visual editor (selected) | **JSON**

Use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service. Learn more

Expand all | Collapse all

EC2 (72 actions) 1 warning

Service * EC2

Actions * Specify the actions allowed in EC2 close Q Filter actions Switch to deny permissions

Manual actions (add actions)
 All EC2 actions (ec2:*)

Access level groups

List (60 selected)
 Read (12 selected)
 Write
 Tagging

Resources * There are actions in your policy that support the **instance** resource type.

* Required Cancel Review policy

Feedback English (US) Privacy Policy Terms of Use 10:49 AM

The screenshot shows the AWS IAM Policy Visual Editor. A warning message at the top states: "Use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service. Learn more." Below this, a section for the EC2 service is expanded, showing 73 actions. The "RunInstances" action is selected, indicated by a checked checkbox. Other visible actions include "RunScheduledInstances". The "Actions" section has a "Specify the actions allowed in EC2" input field and a "Switch to deny permissions" link. The "Resources" section lists supported resource types: image, instance, network-interface, security-group, subnet, and volume. At the bottom, there are "Required" and "Review policy" buttons.

In addition to the List and Read permissions, we also need to allow Casey to run instances

The screenshot shows the AWS IAM Policy Visual Editor with the EC2 service expanded. The "Actions" section displays a very long list of actions, starting with "List" and continuing with numerous other EC2-related actions such as "DescribeAccountAttributes", "DescribeAddresses", "DescribeAvailabilityZones", "DescribeBundleTasks", "DescribeClassicLinkInstances", "DescribeConversionTasks", "DescribeCustomerGateways", "DescribeDhcpOptions", "DescribeEgressOnlyInternetGateways", "DescribeExportTasks", "DescribeFlowLogs", "DescribeHostReservationOfferings", "DescribeHostReservations", "DescribeHosts", "DescribeInstanceProfileAssociations", "DescribeIdentityFormat", "DescribeImageFormat", "DescribeImageAttribute", "DescribeImages", "DescribeImportImageTasks", "DescribeImportSnapshotTasks", "DescribeInstanceAttribute", "DescribeInstances", "DescribeInstanceStatus", "DescribeInternetGateways", "DescribeKeyPairs", "DescribeMovingAddresses", "DescribeNatGateways", "DescribeNetworkAcls", "DescribeNetworkInterfaceAttribute", "DescribeNetworkInterfaces", "DescribePlacementGroups", "DescribePrefixLists", "DescribeRegions", "DescribeReservedInstances", "DescribeReservedInstancesListings", "DescribeReservedInstancesModifications", "DescribeReservedInstancesOfferings", "DescribeRouteTables", "DescribeSecurityGroups", "DescribeSnapshotAttribute", "DescribeSnapshots", "DescribeSpotDatafeedSubscription", "DescribeSpotFleetInstances", "DescribeSpotFleetRequestHistory", "DescribeSpotFleetRequests", "DescribeSpotInstanceRequests", "DescribeSpotPriceHistory", "DescribeSubnets", "DescribeVolumeAttribute", "DescribeVolumes", "DescribeVolumeStatus", "DescribeVpcAttribute", "DescribeVpcClassicLink", "DescribeVpcClassicLinkDnsSupport", "DescribeVpcEndpoints", "DescribeVpcEndpointServices", "DescribeVpcPeeringConnections", "DescribeVpcs", "DescribeVpnGateways". At the bottom, there are "Required" and "Review policy" buttons.

Secure | https://console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=edit

Apps Bookmarks Pin It Personal RoomFinder IAM READ_FUN PERKS CoolStuff Women AWS reInvent 2017 CP1-2018 ChristmasGifts PM Other bookmarks

AWS Services Resource Groups

RunInstances

Resources * Specific All resources

image Any resource of type = image Any

instance Any resource of type = instance Any

key-pair Any resource of type = key-pair Any

network-interface Any resource of type = network-interface Any

placement-group Any resource of type = placement-group Any

security-group Any resource of type = security-group Any

snapshot Any resource of type = snapshot Any

subnet Any resource of type = subnet Any

volume There are actions in your policy that support the volume resource type. Add ARN to restrict access

Request Conditions Specify request conditions (optional)

Add additional permissions Cancel Review policy

* Required

Feedback English (US)

© 2006–2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

IAM Management Console EC2 Management Console S3 Management Console

Secure | https://console.aws.amazon.com/iam/home?region=us-east-1#/policies\$new?step=edit

Apps Bookmarks Pin It Personal RoomFinder IAM READ_FUN PERKS CoolStuff Women AWS reInvent 2017 CP1-2018 ChristmasGifts PM Other bookmarks

AWS Services Resource Groups

RunInstances

Resources * Specific All resources

image Any

instance Any

key-pair Any

network-interface Any

placement-group Any

security-group Any

snapshot Any

subnet Any

volume Any

Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more.

Specify ARN for volume List ARNs manually

arn:aws:ec2:volume:/

Region Account Volume Id

Cancel Add

Request Conditions Specify request conditions (optional)

Add additional permissions Cancel Review policy

* Required

Screenshot of the AWS IAM Management Console showing the creation of a new policy. The policy is titled 'RunInstances' and has 'RunInstances' as its ARN. It is set to 'Specific' resources and includes actions for various AWS services like Image, Instance, Key-Pair, Network-Interface, Placement-Group, Security-Group, Snapshot, Subnet, and Volume. A note at the bottom says 'Request Conditions Specify request conditions (optional)'. A 'Request Conditions' section is shown with a 'Key' dropdown set to 'ec2:InstanceType', a 'Qualifier' dropdown set to 'Default', an 'Operator' dropdown set to 'StringLike', and a 'Value' input field containing 't1'. A note below says 'Requires users to authenticate with an MFA device to perform the specified actions.' A 'Source IP' section is also present. At the bottom right are 'Add additional permissions', 'Cancel', and 'Review policy' buttons.

But where does the t1 instance type come into the policy? That is a condition that we need to specify as below

Screenshot of the AWS IAM Management Console showing the addition of a request condition. A modal dialog box is open with the title 'Add request condition'. It contains fields for 'Key' (set to 'ec2:InstanceType'), 'Qualifier' (set to 'Default'), 'Operator' (set to 'StringLike'), and 'Value' (set to 't1'). Below the Value field is a link 'Add another condition value'. At the bottom of the dialog are 'Cancel' and 'OK' buttons. The background shows the IAM policy editor with the 'RunInstances' policy and its conditions. A note at the bottom of the policy editor says 'Requires users to authenticate with an MFA device to perform the specified actions.' A 'Source IP' section is also present. At the bottom right are 'Add additional permissions', 'Cancel', and 'Review policy' buttons.

Screenshot of the AWS IAM Management Console showing the creation of a new policy named "EC2-launch-instance-T2-new".

Policy Document:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeTags",
                "ec2:DescribeVolumeModifications",
                "ec2:DescribeVpnConnections",
                "ec2:GetConsoleOutput"
            ],
            "Resource": [
                "arn:aws:ec2:*:image/*",
                "arn:aws:ec2:*:instance/*",
                "arn:aws:ec2:*:key-pair/*",
                "arn:aws:ec2:*:network-interface/*",
                "arn:aws:ec2:*:placement-group/*",
                "arn:aws:ec2:*:security-group/*",
                "arn:aws:ec2:*:snapshot/*",
                "arn:aws:ec2:*:subnet/*",
                "arn:aws:ec2:*:volume/*"
            ]
        }
    ]
}

```

Request Conditions:

- MFA required**: Requires users to authenticate with an MFA device to perform the specified actions.
- Source IP**: Allow access to the specified actions only when the request comes from the specified IP address range.
- ec2:InstanceType** (If exists, StringLike | `I2.*`) ([Edit](#) | [Remove](#))

[Add another condition](#)

[Add additional permissions](#)

* Required

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

We now have the policy, we can review it and click the button

Screenshot of the AWS IAM Management Console showing the "Review policy" step for the "EC2-launch-instance-T2-new" policy.

Review policy

Before you create this policy, provide the required information and review this policy.

Name: EC2-launch-instance-T2-new
Maximum 64 characters. Use alphanumeric and '-' characters.

Description: This policy allows developers to launch instances only in the `I2` family.
Maximum 1000 characters. Use alphanumeric and '-' characters.

Summary

Service	Access level	Resource	Request condition
EC2	Full: List, Read Limited: Write	Multiple	<code>ec2:InstanceType string like I2.* (If Exists)</code>

* Required

[Cancel](#) [Previous](#) [Create policy](#)

Screenshot of the AWS IAM Management Console showing a success message: "EC2-launch-instance-T2-new has been created." The left sidebar shows the navigation menu with "Policies" selected. The main content area displays a list of AWS managed policies, filtered by "Policy type".

Success Message: EC2-launch-instance-T2-new has been created.

Policies List:

Policy name	Type	Attachments	Description
AdministratorAccess	Job function	3	Provides full access to AWS services and resources.
AmazonAPIGatewayAdministrator	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management C...
AmazonAPIGatewayInvokeFullAccess	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	0	Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess	AWS managed	0	Provides full access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamReadOnlyAccess	AWS managed	0	Provides read only access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamServiceAccess	AWS managed	0	Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess	AWS managed	0	Provide full access to Amazon Athena and scoped access to the dependencies needed to enable qu...
AmazonChimeFullAccess	AWS managed	0	Provides full access to Amazon Chime Admin Console via the AWS Management Console.
AmazonChimeReadOnly	AWS managed	0	Provides read only access to Amazon Chime Admin Console via the AWS Management Console.
AmazonChimeUserManagement	AWS managed	0	Provides user management access to Amazon Chime Admin Console via the AWS Management Co...
AmazonCloudDirectoryFullAccess	AWS managed	0	Provides full access to Amazon Cloud Directory Service.
AmazonCloudDirectoryReadOnlyAccess	AWS managed	0	Provides read only access to Amazon Cloud Directory Service.
AmazonCoiotoolsDeveloperAuthenticatedT	AWS managed	0	Provides access to Amazon Coiotools APIs to support developer authenticated identities from your au...

we then attach the policy for Casey

Screenshot of the AWS IAM Management Console showing the "Attached policies" section for the user "Casey". The user summary shows ARN, Path, and Creation time. The "Attached policies" tab is selected, displaying four managed policies attached directly to the user.

User Summary:

- User ARN: arn:aws:iam::094697565664:user/Casey
- Path: /
- Creation time: 2017-11-20 19:21 PST

Attached policies:

Policy name	Policy type	Actions
S3-reinvent-2017-dev	Managed policy	X
list-pass-role-reinvent-2017-mobile	Managed policy	X
CloudTrail-Access	Managed policy	X
Ec2-manage-instances-tag	Managed policy	X

IAM Management Console X IAM Management Console X EC2 Management Console X S3 Management Console X

Secure | https://console.aws.amazon.com/iam/home?region=us-east-1#/users/Casey\$addPermissions?step=permissions&permissionType=policies

Apps Bookmarks Pin It Personal RoomFinder IAM READ_FUN PERKS CoolStuff Women AWS ReInvent 2017 CP1-2018 ChristmasGifts PM Other bookmarks

Services Resource Groups

Add permissions to Casey

1 2

Permissions Review

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group Copy permissions from existing user Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Create group Refresh

Search Group Attached policies

Admins AdministratorAccess

Feedback English (US)

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

IAM Management Console X IAM Management Console X EC2 Management Console X S3 Management Console X

Secure | https://console.aws.amazon.com/iam/home?region=us-east-1#/users/Casey\$addPermissions?step=permissions&permissionType=policies

Apps Bookmarks Pin It Personal RoomFinder IAM READ_FUN PERKS CoolStuff Women AWS ReInvent 2017 CP1-2018 ChristmasGifts PM Other bookmarks

Services Resource Groups

Attach one or more existing policies directly to the users or create a new policy. Learn more

Create policy Refresh

Filter: Customer managed Search Showing 7 results

Policy name	Type	Attachments	Description
AWSCloudTrailAccessPolicy	Customer managed	1	
EC2-Create-Tag-RunInstances	Customer managed	1	Grants access to create tags but only during runInstances
EC2-CreateTag-withValues	Customer managed	1	Grants access to create and modify tags with specific values
EC2-launch-instance-T2	Customer managed	1	This policy allows developers to launch instances only in the T2 family
EC2-launch-instance-T2-new	Customer managed	0	This policy allows developers to launch instances only in the T2 family
EC2-launch-instance-T2-withTag	Customer managed	1	Grants access to launch T2 instances, but requires project tag with poker or blackjack values
s3-2017-reinvent-mobile-resource-access-dev	Customer managed	1	This policy grants access to list buckets and read from the mobile folder in the reinvent-2017-policy-ninja-dev

Cancel Next: Review

Feedback English (US)

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

IAM Management Console X IAM Management Console X EC2 Management Console X S3 Management Console X

Secure https://console.aws.amazon.com/iam/home?region=us-east-1#/users/Casey\$addPermissions?step=review&permissionType=policies&policies=arn:aws:iam::094097565664:policy%2F...

Apps Bookmarks Pin It Personal RoomFinder IAM READ_FUN PERKS CoolStuff Women AWS reInvent 2017 CP1-2018 ChristmasGifts PM Other bookmarks

AWS Services Resource Groups Admin-2017-Reinvent-Dev 0... Global Support

Add permissions to Casey

1 2

Permissions Review

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	EC2-launch-instance-T2-new

Cancel Previous Add permissions

Next, we need to go and see what Casey can do below

AWS Management Console X EC2 Management Console X CloudTrail Management ... X

https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#instanceshort=instanceId

Casey @ 0940-9756-5664 Ohio Support

Services Resource Groups

EC2 Dashboard

- Events
- Tags
- Reports
- Limits
- INSTANCES**
- Instances**
- Spot Requests
- Reserved Instances
- Dedicated Hosts
- IMAGES**
- AMIs
- Bundle Tasks
- ELASTIC BLOCK STORE**
- Volumes
- Snapshots
- NETWORK & SECURITY**
- Security Groups
- Elastic IPs
- Placement Groups
- Key Pairs
- Network Interfaces

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
i-0570761992dca44ce	t2.micro	us-east-2c	running	2/2 checks	None	ec2-18-217-49-19.us-ea...	18.217.49.19	-	
i-06cfa2425ac65f6f7	t2.micro	us-east-2c	stopped	None	None	ec2-18-217-49-19.us-ea...	-	-	
i-08bc000b615a05ef0	t2.micro	us-east-2c	running	2/2 checks	None	ec2-13-58-248-46.us-ea...	13.58.248.46	-	
i-0d3a531b3c9d32e1d	m1.large	us-east-2c	running	2/2 checks	None	ec2-13-58-13-147.us-ea...	13.59.13.147	-	
i-0de003593c3b62a0	t2.micro	us-east-2c	running	2/2 checks	None	ec2-18-221-184-55.us-e...	18.221.184.55	-	

Select an instance above

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Mozilla Firefox seems slow... to... start. Learn How to Speed it Up Don't Tell Me Again

Casey can now see some instances

AWS Management Console EC2 Management Console CloudTrail Management ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Warning: Your instance configuration is not eligible for the free usage tier. To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about free usage tier eligibility and usage restrictions.

Don't show me this again Edit AMI

AMI Details

amzn-ami-hvm-2017.09.1.20171103-x86_64-gp2 - ami-aaf1b34cf
Amazon Linux AMI 2017.09.1.20171103 x86_64 HVM GP2
Root Device Type: ebs Virtualization type: hvm

Edit instance type

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m4 large	6.5	2	8	EBS only	Yes	Moderate

Edit security groups

Security Groups

Security Group ID	Name	Description
sg-099ec061	default	default VPC security group

All selected security groups include inbound rules.

Cancel Previous Launch

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Learn How to Speed It Up Don't Tell Me Again

Mozilla Firefox seems slow... to... start.

AWS Management Console EC2 Management Console CloudTrail Management ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Services Resource Groups

1. Choose AMI 2. Choose instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Warning: Your instance configuration is not eligible for the free usage tier. To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about free usage tier eligibility and usage restrictions.

Don't show me this again Edit AMI

AMI Details

amzn-ami-hvm-2017.09.1.20171103-x86_64-gp2 - ami-aaf1b34cf
Amazon Linux AMI 2017.09.1.20171103 x86_64 HVM GP2
Root Device Type: ebs Virtualization type: hvm

Edit instance type

Instance Type

Instance Type	ECUs	vCPUs	Memory
m4 large	6.5	2	8

Security Groups

Security Group ID	Name	Description
sg-099ec061	default	default VPC security group

All selected security groups include inbound rules.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair
Select a key pair
reinvent2017

I acknowledge that I have access to the selected private key file (reinvent2017.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Learn How to Speed It Up Don't Tell Me Again

Mozilla Firefox seems slow... to... start.

AWS Management Console < EC2 Management Console < CloudTrail Management ... < +

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Services Resource Groups

Casey @ 0946-9756-5664 Ohio Support

Launch Status

Launch Failed

You are not authorized to perform this operation. Encoded authorization failure message: yJkXaCkG6PL34BjH0yWGMHPcqisBsMQM-WTbIz7P3h0KB-AFMnnd0k-UDFVt9coobp5aJcE3unhRVMZlBPK41owf9Gx0L_HyQU1ipTm4B0xKSSDnyvdDKhME9zJnLjvEsme9rQPhcPW1QJaKeatzlf30fGrnlExRFEL_4RA/WUflfJxmfIfhb5bkGvd45sstmFFKdyA4Q-f9d1phc-RfOfJn_P5h0k1UQbz2PzvBdw0e0mpfQk7c1QqMTDc6bt4_n2C0x7V0RgKQ3Q2CSKxYbdsdbImY_3e8CBPb-e4zLW4f2jZjCD99ow2Gbkv21k0x4_uXyBEjgYgsqpl5KhwZZK8Ge5al-WsJyAddQPZCmrgfQVhBeYnOB1BdsKu8TT6B7sMmrfGFQoAdtp61Ok8a_GyFYdfLxmfv5qp_RChE4_vgoxVXDBKTh0ka469p0bxSW_LQxObIRuc58k0le-s_mphJloMFnP4k4dsL1wjk0h6AouzZqcUl923P4js1MdxTwR63q55UOThvEds1alujtvpPP2mS53SfQNEjhypo3cdKdCrrD961qLOMKwh9Akpa1ek/b0e7QaaMRm2vL3C0_rRka7FmneZeye0wB69qgkG3mG8v2bhH7o3M40yJdDvqIAr90fCn0ggs3adg

Hide launch log

Initiating launches Failure Retry

Cancel Back to Review Screen Retry Failed Tasks

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Services Resource Groups

Casey @ 0946-9756-5664 Ohio Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details Edit AMI

amzn-ami-hvm-2017.09.1.20171103-x86_64-gp2 - ami-aa1b34cf

Amazon Linux AMI 2017.09.1.20171103 x86_64 HVM GP2

Root Device Type: ebs Virtualization type: hvm

Instance Type Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups Edit security groups

Security Group ID	Name	Description
sg-099ecb61	default	default VPC security group

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-099ecb61 (default)	

Cancel Previous Launch

Feedback English (US) © 2009-2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Learn How to Speed It Up Don't Tell Me Again

Mozilla Firefox seems slow... to... start.

AWS Management Console EC2 Management Console CloudTrail Management ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Casey @ 0946-9756-5664 Ohio Support

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Edit instance type

Security Groups

Security Group ID	Name	Description
sg-099ecb61	default	default VPC security group

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-099ecb61 (default)	

Instance Details

Storage

Tags

Cancel Previous Launch

Feedback English (US)

© 2009 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Mozilla Firefox seems slow... to... start.

AWS Management Console EC2 Management Console CloudTrail Management ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Casey @ 0946-9756-5664 Ohio Support

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)
t2.micro	Variable	1	1

Edit instance type

Security Groups

Security Group ID	Name
sg-099ecb61	default

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-099ecb61 (default)	

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair
Select a key pair
reinvent2017

I acknowledge that I have access to the selected private key file (reinvent2017.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Instance Details

Storage

Tags

Feedback English (US)

© 2009 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Mozilla Firefox seems slow... to... start.

AWS Management Console < EC2 Management Console < CloudTrail Management ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard

Services Resource Groups

Casey @ 0946-9756-5664 Ohio Support

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0e332859ad8fa9e2b View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can [connect](#) to them from the instances screen. [Find out how to connect to your instances.](#)

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Amazon EC2 User Guide
- Learn about AWS Free Usage Tier
- Amazon EC2 Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

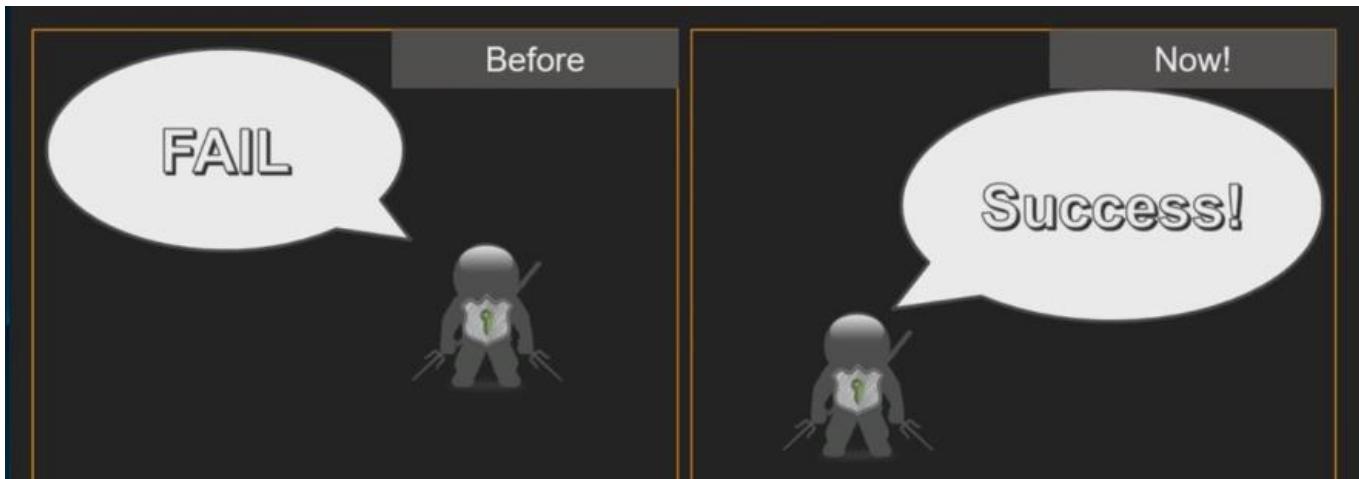
Feedback English (US) © 2006 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Mozilla Firefox seems slow... to... start. Learn How to Speed It Up Don't Tell Me Again

Casey can only use the t2 instance types

Limit Amazon EC2 instance types Demo



- Goal: Limit a user from starting an instance unless the instance is `t2.*`
- Let's try to:
 - Create a managed policy that attempts to limit starting an EC2 instance except for these instance types.
 - Attach that policy to an IAM user.



What to expect from this session

Learn the **policy language** to control access to your AWS resources

Understand the different **types of policies**, why to use them, and how they work together

Get to know the **tools** available to help you with policies

Become a **policy ninja!**



The policy language

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:Get*", "s3>List*"],
            "Resource": "*"
        }
    ]
```

The policy language

- Provides authorization
- Two parts:
 - **Specification:** *Defining* access policies
 - **Enforcement:** *Evaluating* policies

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:Get*", "s3>List*"],
            "Resource": "*"
        }
    ]
```

Your job is to define and attach the policies to Users or Roles, make sure that you have granted the right permissions that are correctly scoped down. AWS will evaluate the policies by giving Yes or No to access requests.

Policy specification basics

- JSON-formatted documents
- Contain a statement (permissions) that specifies:
 - Which actions a principal can perform
 - Which resources can be accessed

```
{  
  "Statement": [  
    {  
      "Effect": "effect",  
      "Principal": "principal",  
      "Action": "action",  
      "Resource": "arn",  
      "Condition": {  
        "condition": {  
          "key": "value"  
        }  
      }  
    }  
  ]  
}
```

Principal
Action
Resource
Condition

You can have multiple statements and each statement is comprised of PARC

Principal: Examples

- An entity that is allowed or denied access to a resource
- Indicated by an Amazon Resource Name (ARN)
- With IAM policies, the principal element is implicit (i.e., the user, group, or role attached)

```
<!-- Everyone (anonymous users) -->  
"Principal": "AWS": "*.*"  
  
<!-- Specific account or accounts -->  
"Principal": {"AWS": "arn:aws:iam::123456789012:root"}  
"Principal": {"AWS": "123456789012"}  
  
<!-- Individual IAM user -->  
"Principal": {"AWS": "arn:aws:iam::123456789012:user/username"}  
  
<!-- Federated user (using web identity federation) -->  
"Principal": {"Federated": "accounts.google.com"}  
  
<!-- Specific role -->  
"Principal": {"AWS": "arn:aws:iam::123456789012:role/rolename"}  
  
<!-- Specific service -->  
"Principal": {"Service": "ec2.amazonaws.com"}
```

Replace with your account number

Action: Examples

- Describes the type of access that should be allowed or denied
- You can find actions in the docs or use the policy editor to get a drop-down list
- Statements must include either an Action or NotAction element

Principal
Action
Resource
Condition

```
<!-- EC2 action -->
"Action":"ec2:StartInstances"

<!-- IAM action -->
"Action":"iam:ChangePassword"

<!-- Amazon S3 action -->
"Action":"s3:GetObject"

<!-- specify multiple values for the Action element-->
"Action":["sns:SendMessage","sns:ReceiveMessage"]

<-- Wildcards (*) or (?) in the action name. Below covers create/delete/list/update-->
"Action":"iam:*AccessKey"
```

Every policy statement must have an Action or a NotAction.

Resource: Examples

- The object or objects being requested
- Statements must include either a Resource or a NotResource element

Principal
Action
Resource
Condition

```
<-- S3 bucket -->
"Resource":"arn:aws:s3:::my_corporate_bucket/*"

<-- All S3 buckets, except this one -->
"NotResource":"arn:aws:s3:::security_logging_bucket/*"

<-- Amazon SQS queue-->
"Resource":"arn:aws:sqs:us-west-2:123456789012:queue1"

<-- Multiple Amazon DynamoDB tables -->
"Resource":["arn:aws:dynamodb:us-west-2:123456789012:table/books_table",
           "arn:aws:dynamodb:us-west-2:123456789012:table/magazines_table"]

<-- All EC2 instances for an account in a region -->
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Replace
with your
account
number

Condition example

Principal
Action
Resource
Condition

What if you wanted to restrict access to a time frame and IP address range?

```
"Condition" : {  
    "DateGreaterThan" : {"aws:CurrentTime" : "2017-12-25T08:00:00Z"},  
    "DateLessThan": {"aws:CurrentTime" : "2017-12-26T08:00:00Z"},  
    "IpAddress" : {"aws:SourceIp" : ["192.0.2.0/24", "203.0.113.0/24"]}  
}
```

OR

Allows a user to access a resource under the following conditions:

- Anytime on Christmas day 2017 GMT from a source IP in the range
 - The time is after 8 A.M. GMT on 12/25/2017 AND
 - The time is before 8 A.M. GMT on 12/26/2017 AND
- The request comes from an IP address in the 192.0.2.0 /24 OR 203.0.113.0 /24 range
- All of these conditions must be met for the statement to evaluate to TRUE.

If you have a complex condition, you should break it out into multiple conditions that must all evaluate to be true.

Policy enforcement



This is what AWS has responsibility to enforce

Policy enforcement



It's not just IAM policies



AWS Organizations
Service control policies (SCPs)



AWS Identity and Access Management
Inline policies
Managed policies



AWS Security Token Service (STS)
Scoped-down policies



Specific AWS services
Resource-based policies

Example: Amazon S3 bucket policies

All use the
same policy
language

What is AWS Organizations?



When to use each type of permission policy



AWS Organizations
Service control policies (SCPs)

*Guardrails on the account
to disable access to
services*



AWS IAM
Inline policies
Managed policies

*Set granular permissions
based on functions that
users or applications need
to perform*



AWS STS
Scoped-down policies

*Reduce general shared
permissions further*

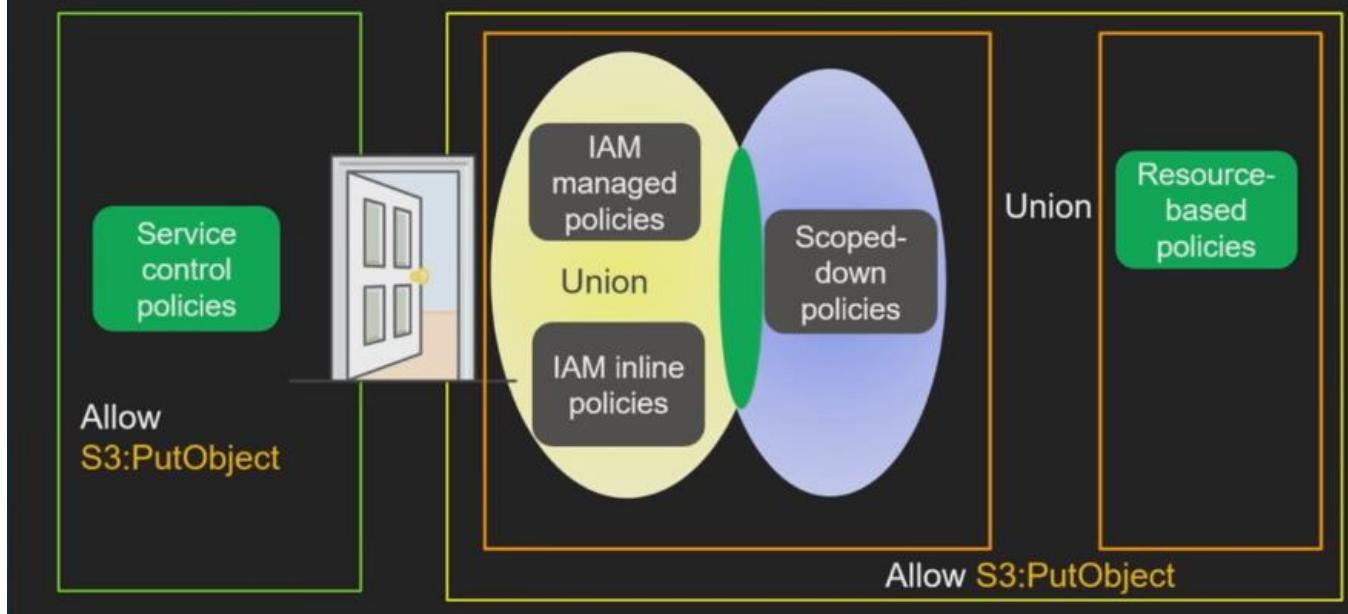


Specific AWS services
Resource-based policies

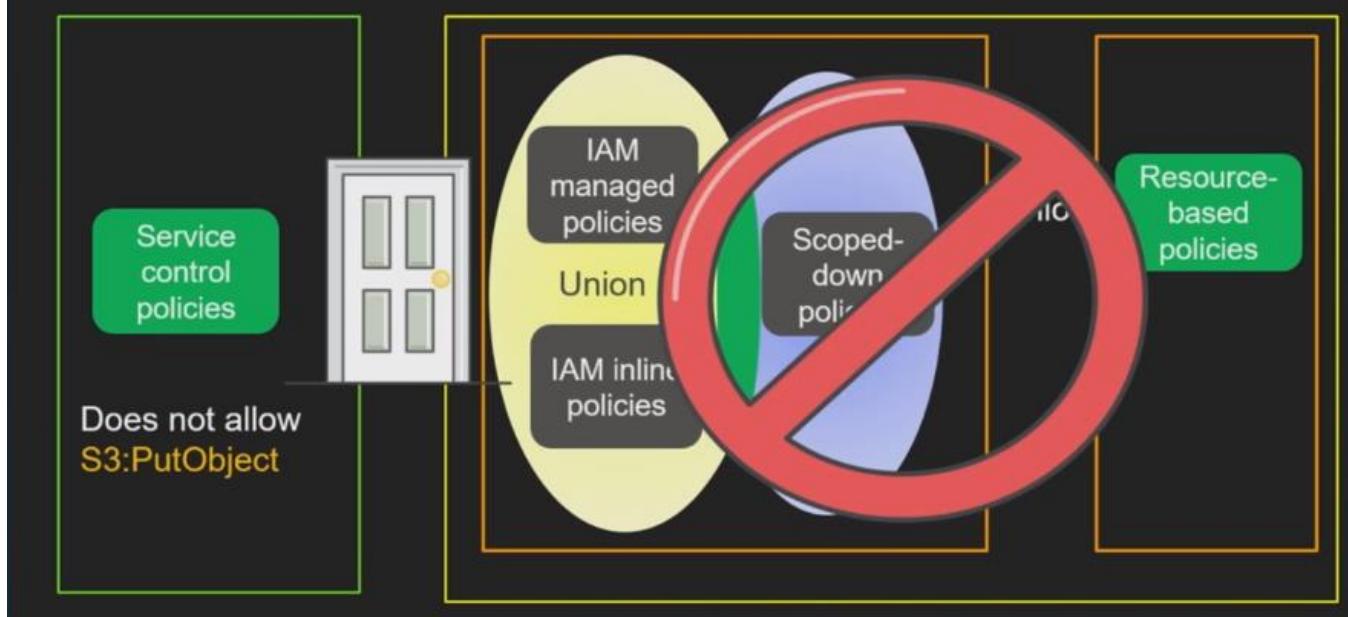
*Cross-account access and
to control access from the
resource*

Example: S3 bucket policies

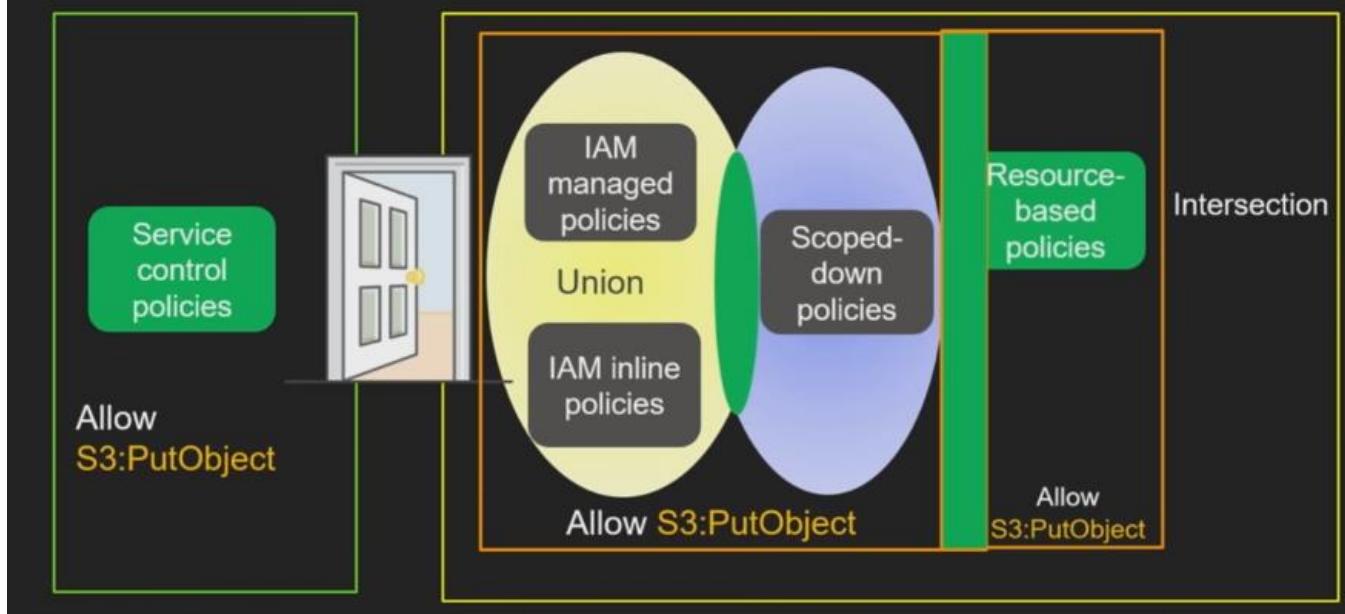
How they work together—for an account



How they work together—for an account



How they work together—across account



Enough already –
Let's look at some examples

Demo with SCPs and IAM policies

SCP

- Allows `*` (all services and actions)
- Denies all AWS **Directory Service** and **Amazon Polly**
- Denies AWS **CloudTrail** to stop trail logging

IAM policy—Attached to Casey

- Allows **Amazon S3** read to a specific bucket
- Allows **AWS CloudTrail** stop trail logging (oops!)

SCP

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Sid": "DenyUnapprovedActions",  
        "Effect": "Deny",  
        "Action": ["polly:*",  
                  "ds:*",  
                  "cloudtrail:StopLogging"]  
    },  
    {"Resource": ["*"]}  
]}  
}
```



Don't Forget!

We also have
an Allow *.*
policy attached
to this OU

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

This is what the policy looks like.

IAM policy – Attached to Casey – S3

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": ["s3:GetObject", "s3>ListBucket"],  
        "Resource": [  
                    "arn:aws:s3::::reinvent-2017-policy-ninja-dev/*",  
                    "arn:aws:s3::::reinvent-2017-policy-ninja-dev"]  
    }, {  
        "Effect": "Allow",  
        "Action": ["s3>ListAllMyBuckets", "s3:HeadBucket", "s3>ListObjects"],  
        "Resource": "*"  
    }]  
}
```

IAM policy – Attached to Casey – CloudTrail

```
"Version": "2012-10-17",
"Statement": [
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "cloudtrail:LookupEvents",
            "cloudtrail:StopLogging",
            "cloudtrail>ListPublicKeys",
            "cloudtrail>ListTags",
            "cloudtrail:GetTrailStatus",
            "cloudtrail:GetEventSelectors",
            "cloudtrail:DescribeTrails"
        ],
        "Resource": "*"
    }
]
```

What is the outcome?

Situation 1

Developer Casey turns off CloudTrail logging



The screenshot shows the AWS CloudTrail Management Console interface. On the left, there's a sidebar with options like CloudTrail, Dashboard, Event history, and Trails. The 'Trails' option is selected. In the main area, there's a list of trails, with one named 'reinvent2017' currently selected. A modal dialog box is open over the trail settings page. The dialog contains the following text:
Are you sure you want to stop logging?
You will no longer collect log files in your S3 bucket and CloudWatchLogs log group.
Previous log files will still be accessible.
At the bottom of the dialog, there are 'Cancel' and 'Continue' buttons. To the right of the dialog, there's a 'Logging' toggle switch which is currently set to 'ON'. Below the switch, there are links for 'Learn more', 'Pricing', 'Documentation', 'Forums', and 'FAQs'.

AWS Management Console < EC2 Management Console < CloudTrail Management ... < https://console.aws.amazon.com/cloudtrail/home?region=nvl-east-1#configuration/armawecloudtrails-east-1094697565664-trail@reln

You don't have the necessary CloudTrail permissions to turn off CloudTrail. [Learn more](#)

CloudTrail Services Resource Groups +

CloudTrail Dashboard Event history Trails

Trails > Configuration

relinvent2017

Logging **ON**

Learn more Pricing Documentation Forums FAQs

Trail settings

When a trail applies to all regions, the trail exists in all regions and delivers log files for all regions to one Amazon S3 bucket and an optional CloudWatch Logs log group. To see all of your trails, click Trails.

Apply trail to all regions Yes

Management events

Management events provide insights into the management operations that are performed on resources in your AWS account. [Learn more](#)

ReadWrite events All

Data events

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional charges apply. [Learn more](#)

Configure

Feedback English (US)

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Mozilla Firefox seems slow... to... start. Learn How to Speed It Up! Don't Tell Me Again

What is the outcome?

Situation 1

Developer Casey turns off CloudTrail logging



Casey can't do anything with CloudTrail

What is the outcome?

Situation 2

Developer Casey reads an object from a bucket



We are going to use the command line for this as below

```
C:\Users\brightj\Documents\Presenting\reinvent\PolicyNinja2017\CommandsForReInvent.txt - Notepad++  
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?  
AWS re:Invent 2017 Accounts & Identity AWS Lambda Policies CommandsForReInvent.txt  
1 EC2-launch-instance-T2-new  
2  
3 This policy allows developers to launch instances only in the T2 family.  
4  
5 aws s3api get-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/SurfAttack.JPG SurfAttack.JPG --region us-east-2  
6  
7 aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
8  
9 aws s3api put-object --bucket reinvent-2017-policy-ninja-stage --key home/Casey/Casey.txt --body Casey.txt --region us-east-2
```

```
1 aws s3api get-object --bucket reinvent-2017-policy-ninja-dev  
2  
3 C:\Users\brightj\Desktop\reInvent-Casey>aws s3api get-object --bucket reinvent-2017-policy-ni  
4 bytes 138240 image/jpeg "f83ie38d1d69d0621da5d1a33ddd473" Tue, 21 Nov 2017 03:3  
5 aws s3api put-object --bucket reinvent-2017-policy-ninja-stage  
6  
7 C:\Users\brightj\Desktop\reInvent-Casey>SurfAttack.JPG  
8
```



Casey can download/read a file from the bucket

What is the outcome?

Situation 2

Developer Casey reads an object from a bucket



Situation 3

Developer Casey adds an object to the same bucket



```
C:\Users\brightj\Documents\Presenting\reinvent\PolicyNinja2017\CommandsForReInvent.txt - Notepad++  
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?  
AWS re:Invent 2017 Accounts & Identity AWS Lambda Policies CommandsForReInvent.txt  
1 EC2-launch-instance-T2-new  
2  
3 This policy allows developers to launch instances only in the T2 family.  
4  
5 aws s3api get-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/SurfAttack.JPG SurfAttack.JPG --region us-east-2  
6  
7 aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
8  
9 aws s3api put-object --bucket reinvent-2017-policy-ninja-stage --key home/Casey/Casey.txt --body Casey.txt --region us-east-2
```

```

1 aws s3api get-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/NurfAttack.JPG NurfAttack.JPG --region us-east-2
2 bytes 188240 image/jpeg "F831e33bd1d69d0021da5d1a33dd473" Tue, 21 Nov 2017 03:02:40 GMT
3 C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey.txt --body Casey.txt --region us-east-2
4 An error occurred (AccessDenied) when calling the PutObject operation: Access Denied
5 C:\Users\brigidj\Desktop\reInvent-Casey>

```

What is the outcome?

Situation 2

Developer Casey reads an object from a bucket



Situation 3

Developer Casey adds an object to the same bucket



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



No PutObject permission is granted to Casey

The screenshot shows the AWS S3 Management Console with the 'Permissions' tab selected for the 'reinvent-2017-policy-ninja-dev' bucket. The 'Bucket Policy' tab is active. The interface is divided into several sections for managing access:

- Access for your AWS account:** Contains tabs for 'Account', 'List objects', 'Write objects', 'Read bucket permissions', and 'Write bucket permissions'. The 'Write objects' tab is highlighted.
- Access for other AWS accounts:** Contains tabs for 'Account', 'List objects', 'Write objects', 'Read bucket permissions', and 'Write bucket permissions'. The 'Write objects' tab is highlighted.
- Public access:** Contains tabs for 'Group', 'List objects', 'Write objects', 'Read bucket permissions', and 'Write bucket permissions'. The 'Write objects' tab is highlighted.
- S3 log delivery group:** Contains tabs for 'Group', 'List objects', 'Write objects', 'Read bucket permissions', and 'Write bucket permissions'. The 'Write objects' tab is highlighted.

```
1 {
2     "Version": "2012-10-17",
3         "Statement": [
4             {
5                 "Sid": "AllowPutObjectToBucket",
6                 "Effect": "Allow",
7                 "Principal": "*",
8                 "Action": "s3:PutObject",
9                 "Resource": "arn:aws:s3:::reinvent-2017-policy-ninja-dev/*"
10            }
11        ]
12    }
```

Bucket policy editor ARN: arn:aws:s3:::reinvent-2017-policy-ninja-dev
Type to add a new policy or edit an existing policy in the text area below.

Documentation Policy generator

Demo with SCP, IAM, and bucket policy

SCP policy

- Allows ***.***
- Denies all **Directory Service** and **Amazon Polly**
- Denies **CloudTrail** to stop trail logging

IAM policy – Attached to Casey

- Allows **S3** read to a specific bucket

S3 bucket policy

- Allows **S3** write for Casey

Now we add a bucket policy

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Sid": "AllowPutObject",  
         "Effect": "Allow",  
         "Principal": {  
             "AWS": "arn:aws:iam::123456789123:user/Casey"  
         },  
         "Action": "s3:putobject",  
         "Resource": "arn:aws:s3:::reinvent-2017-policy-ninja-dev/*"  
    ]  
}
```

The screenshot shows the AWS S3 console with a bucket named 'reinvent-2017-policy-ninja-dev'. In the 'Bucket Policy' tab, a JSON policy document is displayed:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Sid": "AllowPutObject",  
         "Effect": "Allow",  
         "Principal": {  
             "AWS": "arn:aws:iam::123456789123:user/Casey"  
         },  
         "Action": "s3:putobject",  
         "Resource": "arn:aws:s3:::reinvent-2017-policy-ninja-dev/*"  
    ]  
}
```

Below the policy, a command prompt window shows the execution of AWS commands:

```
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api get-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/NurfAttack.JPG --region us-east-2  
bytes 118248 image/jpeg "F831e33d1d69d0021da5d1a33dd473" Tue, 21 Nov 2017 03:12:40 GMT  
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
C:\Users\brigidj\Desktop\reInvent-Casey>
```

Now Casey can put images into the S3 bucket

The screenshot shows a Windows Notepad window containing a script of AWS commands:

```
1 C:\Users\brigidj\Documents\Presenting\reInvent\PolicyNinja2017\CommandsForReinvent.txt - Notepad++  
2 File Edit Search View Encoding Language Settings Tools More Run Plugins Window I  
3 EC2-launch-instance-T2-new  
4 This policy allows developers to launch instances only in the T2 family.  
5 aws s3api get-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/NurfAttack.JPG NurfAttack.JPG --region us-east-2  
6 aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
7 aws s3api put-object --bucket reinvent-2017-policy-ninja-stage --key home/Casey/Casey.txt --body Casey.txt --region us-east-2
```

We can let Casey try to put the image into the Staging account and not the Dev account

The screenshot shows a Windows Command Prompt window executing the AWS commands from the Notepad file:

```
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api get-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/NurfAttack.JPG NurfAttack.JPG --region us-east-2  
bytes 118248 image/jpeg "F831e33d1d69d0021da5d1a33dd473" Tue, 21 Nov 2017 03:12:40 GMT  
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-dev --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
C:\Users\brigidj\Desktop\reInvent-Casey>aws s3api put-object --bucket reinvent-2017-policy-ninja-stage --key home/Casey/Casey.txt --body Casey.txt --region us-east-2  
An error occurred (AccessDenied) when calling the PutObject operation: Access Denied  
C:\Users\brigidj\Desktop\reInvent-Casey>
```

Casey is denied access to put objects into the staging S3 bucket, the only way to fix this is to grant access via IAM or a new policy.

AWS Organizations

console.aws.amazon.com/organizations/home?region=us-east-1#/accounts

Admin-2017-Reinvent-Master

Support

Invitations

Settings

Add account Remove account Hide Failed account creation requests Filter

Account name	Email	Account ID	Status
reinvent-2017-master	brigid+master2017@amazon.com	390493669640	Joined on 11/20/2017
reinvent-2017-dev	brigid+dev2017@amazon.com	094597565664	Joined on 11/20/2017
reinvent-2017-stage	brigid+stage2017@amazon.com	364850286996	Joined on 11/21/2017
reinvent-2017-prod	brigid+prod2017@amazon.com	578497455434	Joined on 11/21/2017

No selection

Please select an account to see more details

AWS Organizations

console.aws.amazon.com/organizations/home?region=us-east-1#/browse/ou/qf1h

Admin-2017-Reinvent-Master

Support

Invitations

Settings

Root

Tree View Filter

ORGANIZATIONAL UNITS (1)

- + New organizational unit reinvent-2017

ACCOUNTS (1)

- reinvent-2017-mas... brigid+master2017@...

Root

Arn: arn:aws:organizations:390493669640:root/o-leafunit-kv/r-qf1h

POLICIES

Service control policies >

ENABLE / DISABLE POLICY TYPES

Service control policies Disable

AWS Organizations

console.aws.amazon.com/organizations/home?region=us-east-1#/browse/ou/qf1h-t0lykeyj

Admin-2017-Reinvent-Master

Support

Invitations

Settings

reinvent-2017

reinvent-2017

Root

reinvent-2017

Loading

Tree View Filter

ORGANIZATIONAL UNITS (0)

- + New organizational unit

No organizational units are present in the current OU

ACCOUNTS (3)

- reinvent-2017-stage brigid+stage2017@...
- reinvent-2017-prod brigid+prod2017@...
- reinvent-2017-dev brigid+dev2017@...

Arn: arn:aws:organizations:390493669640:ou/o-hj0umkv/e/ou-qf1h-b5hylegg

ID: ou-qf1h-b5hylegg

Accounts >

POLICIES

Service control policies >

reinvent-2017

reinvent-2017

Organizational Units (0)

No organizational units are present in the current OU

Accounts (3)

- reinvent-2017-stage
- reinvent-2017-prod
- reinvent-2017-dev

Deny-Unapproved-Services Detach
This policy denies services that are not approved

FullAWSAccess Detach

Policies Inherited

FullAWSAccess
Allows access to every operation
Source: Root

Create policy Delete policy

Policy name	Policy type	Description
FullAWSAccess	Service control	Allows access to every operation
Deny-Unapproved-S...	Service control	This policy denies services that are not approved.

Arn: arn:aws:organizations::396493669640:policy/o-lqf0ulmkve/service_control_policy/p-8ar95xz

Description: This policy denies services that are not approved.

Policy editor —

Accounts >

Organizational units >

Roots >

This is how you can go and create the multi-account setup and allow or deny access as needed.

Bucket policy at play – New outcome!

Situation 2 – Same account
Developer Casey adds an object to the same bucket

What about cross-account?

SCP policy

- Allows `*.*`
- Denies all **Directory Service** and **Amazon Polly**.
- Denies **CloudTrail** to stop trail logging

IAM policy – Attached to Casey

- Allows **S3** read to a specific bucket

S3 bucket policy in a different account

- Allows **S3** write for Casey

Cross-account S3 bucket

Situation 2 – Different account

Developer Casey adds an object to a bucket in a different account



Recap

★ Review of IAM policy language

★ Review of how policies work together to control access

Policy tools – Create, test, and correct policies

Policy Foo – Ninja moves with Amazon EC2

Additional resources

Policy Tools – Policy summaries

An easier way to understand the permissions your policies grant

- Summary of service and access level
- Four types of access levels for actions
 - List – See a list of resources
 - Read – Read the content in resources
 - Write – Create, delete, or modify resources
 - Permissions – Grant or modify permissions to resources
- Show remaining services and actions
- Identify and correct errors in your policies



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Policy tools – Visual policy editor

Point and click your way through granting permissions in AWS

- Create and modify IAM policies
- Select from a list of AWS services
- Select from a list of available actions
- Explore services and actions with inline documentation
- Understand the resources you can specify for service actions
- Select from a list of available conditions for actions you select
- Easily include dependent actions required to perform tasks in AWS
- Import existing policies and modify

Demo: Correct an Existing Policy

Goal: You have an existing policy that enables developers to use the EC2 console to:

- Start, stop, and terminate instances with a specific tag

Situation: It does not work (oh, bother!)

Pro tip! Use policy summaries and the editor to correct your existing policies



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Existing policy – Does not work

```
{ "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "arn:aws:ec2:region:account-id:security-group/sg-12345678"
    },
    {
      "Effect": "Allow",
      "Action": ["elasticloadbalancing:Describe*", "cloudwatch>ListMetrics",
                 "cloudwatch:GetMetricStatistics", "cloudwatch:Describe*",
                 "autoooooooscaling:Describe*"
               ],
      "Resource": "*"
    }, <continued>
```



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Proposed policy – Does not work

```
...{  
    "Effect": "Allow",  
    "Action": ["ec2:StartInstances", "ec2:StopInstances"],  
    "Condition": {  
        "StringEquals": {  
            "ec2:CrazyTags/project": "poker"  
        }  
    },  
    "Resource": "*"  
}  
]  
}
```

The screenshot shows the AWS IAM Management Console interface. On the left, a sidebar navigation bar includes links for Dashboard, Groups, Users, Roles, Policies (which is selected), Identity providers, Account settings, and Credential report. The main content area displays a success message: "EC2-launch-instance-T2-new has been created." Below this, there are tabs for "Create policy" and "Policy actions". A search bar and filter dropdown are present. The main table lists 11 customer-managed policies, with columns for Policy name, Type, Attachments, and Description. One policy, "Ec2-manage-instances-tag", is highlighted with a blue background and a cursor arrow pointing to its "Edit" icon.

Policy name	Type	Attachments	Description
AWSCloudTrailAccessPolicy	Customer managed	1	
Cloudtrail-Access	Customer managed	2	This grants access to list and read actions in CloudTrail
EC2-Create-Tag-RunInstances	Customer managed	1	Grants access to create tags but only during runInstances
EC2-CreateTag-withValues	Customer managed	1	Grants access to create and modify tags with specific values.
EC2-launch-instance-T2	Customer managed	1	This policy allows developers to launch instances only in the T2 family.
EC2-launch-instance-T2-new	Customer managed	0	This policy allows developers to launch instances only in the T2 family.
EC2-launch-instance-T2-withTag	Customer managed	1	Grants access to launch T2 instances, but requires project tag with poker or blackjack values
Ec2-manage-instances-tag	Customer managed	3	This policy allows access to manage instances with a specific tag
list-pass-role-reinvent-2017-mobile	Customer managed	2	This policy allows developers to pass the reinvent mobile role when they launch instances.
s3-2017-reinvent-mobile-resource-access-dev	Customer managed	1	This policy grants access to list buckets and read from the mobile folder in the reinvent-2017-policy-ninja-dev
S3-reinvent-2017-dev	Customer managed	2	Access to read files from S3 bucket reinvent-2017-policy-ninja-dev

There is an error, we can edit to fix each warning

We can remove the last faulty policy and add a new correct one in its place as below

Screenshot of the AWS IAM Management Console showing the policy editor for the EC2-manage-instances-tagEdit policy. The 'Actions' section is expanded, showing various actions under 'EC2' and 'Auto Scaling'. Under 'Auto Scaling', the 'Service' dropdown is set to 'Auto Scaling'. The 'Actions' dropdown is set to 'Specify the actions allowed in Auto Scaling'. The 'Manual actions' section contains a checkbox for 'All Auto Scaling actions (autoscaling:*)'. The 'Access level groups' section shows two groups: 'List (17 selected)' and 'Read (1 selected)'. A warning message at the top right says 'Switch to deny permissions'. At the bottom right are 'Cancel' and 'Review policy' buttons.

Screenshot of the AWS IAM Management Console showing the policy editor for the EC2-manage-instances-tagEdit policy. The 'Actions' section is expanded, showing various actions under 'EC2'. Under 'EC2', the 'Service' dropdown is set to 'EC2'. The 'Actions' dropdown is set to 'Manual actions'. The 'Resources' section contains a note: 'The actions in your policy do not support resource-level permissions and require you to choose All resources.' followed by the ARN 'arn:aws:ec2:region:account-id:security-group:sg-12345678'. The 'Request Conditions' section is collapsed. Below the actions are sections for 'ELB v2', 'ELB', 'CloudWatch', 'EC2', and 'Auto Scaling'. At the bottom right are 'Cancel' and 'Review policy' buttons.

We need to fix this also

The screenshot shows the AWS IAM Management Console with a policy editor for the EC2 service. The policy has 66 actions under the EC2 service. The actions listed are:

- ELB v2 (9 actions)
- ELB (6 actions)
- CloudWatch (5 actions)
- EC2 (2 actions) ! 1 warning
- Auto Scaling (18 actions)

The EC2 actions are:

- StartInstances
- StopInstances

The policy also includes a 'Request Conditions' section with the condition `ec2:CrazyTags/project`. The condition details state: "There are no actions in your policy that support this condition key."

At the bottom right, there are 'Clone' and 'Remove' buttons, and a blue 'Review policy' button.

This screenshot shows the same policy editor as the first one, but with a different configuration. The EC2 actions listed are:

- ELB v2 (9 actions)
- ELB (6 actions)
- CloudWatch (5 actions)
- EC2 (2 actions) ! 1 warning
- Auto Scaling (18 actions)

The EC2 actions are:

- Write
- StartInstances
- StopInstances

The policy includes a 'Request Conditions' section with the condition `ec2:CrazyTags/project`. The condition details state: "There are no actions in your policy that support this condition key."

At the bottom right, there is a blue 'Add additional permissions' button, a 'Cancel' button, and a blue 'Review policy' button.

We need to fix this too

Screenshot of the AWS IAM Management Console showing the policy editor for the 'Ec2-manage-instances-tag' policy. The policy grants 'Write' actions on EC2 resources. A specific condition is being added: 'ec2:ResourceTag:StringEquals project'. The 'Review policy' button is visible at the bottom right.

CloudWatch (5 actions) EC2 (2 actions) 1 warning Auto Scaling (18 actions)

Service * EC2

Actions * Write

StartInstances StopInstances

Resources * All resources

Request Conditions

- MFA required
- Close Requires users to authenticate with an MFA device to perform the specified actions
- Source IP
- ec2:ResourceTag:StringEquals project (Edit | [Remove](#))
There are no actions in your policy that support this condition key.

Add another condition

Clone Remove Add additional permissions Review policy

Screenshot of the AWS IAM Management Console showing the 'Add request condition' dialog. The condition being added is 'ec2:ResourceTag:StringEquals project'. The 'Add' button is highlighted with a cursor.

ELB (5 actions) CloudWatch (5 actions) EC2 (2 actions)

Service * EC2

Actions * Write

StartInstances StopInstances

Resources * All resources

Request Conditions

Key * ec2:ResourceTag

Tag key * project

Qualifier Default

Operator StringEquals

If exists

Value * blackjack

Add another condition value

Cancel Add

Auto Scaling (18 actions)

Clone Remove Add additional permissions Review policy

Screenshot of the AWS IAM Management Console showing the policy editor for the 'Ec2-manage-instances-tag' policy. The policy grants 'Write' actions on EC2 resources. It includes conditions for MFA required, Source IP, and a specific tag condition: 'ec2:ResourceTag/project StringEquals blackjack'. The 'Review policy' button is highlighted.

Screenshot of the AWS IAM Management Console showing the 'Edit Ec2-manage-instances-tag' page. The policy has been reviewed and saved. A numbered diagram shows step 1 (Editor) and step 2 (Review). The 'Save changes' button is highlighted.

Service	Access level	Resource	Request condition
Auto Scaling	Full: List, Read	All resources	None
CloudWatch	Full: List Limited: Read	All resources	None
EC2	Full: List Limited: Read, Write	All resources	ec2:ResourceTag/project = blackjack
ELB	Full: List, Read	All resources	None
ELB v2	Full: List, Read	All resources	None

No more errors

Screenshot of the AWS IAM Management Console showing the 'Edit Ec2-manage-instances-tag' policy. A modal dialog box is displayed, stating 'You've currently reached the maximum number of versions for this policy'. It contains two options: 'Remove oldest non-default policy version (version v7 - created 2 days ago)' (selected) and 'Select versions to remove'. Below the modal, there is a 'Review policy' section with a 'Save as default' checkbox checked. At the bottom right of the review section is a 'Delete version and save' button, which is highlighted with a mouse cursor.

Screenshot of the AWS IAM Management Console showing the 'Ec2-manage-instances-tag' policy summary. The policy ARN is listed as 'arn:aws:iam:094697565664:policy/Ec2-manage-instances-tag'. The description is 'This policy allows access to manage instances with a specific tag'. The 'Permissions' tab is selected, showing the following permissions:

Service	Access level	Resource	Request condition
Auto Scaling	Full: List, Read	All resources	None
CloudWatch	Full: List Limited: Read	All resources	None
EC2	Full: List Limited: Read, Write	All resources	ec2:ResourceTag/project = blackjack
ELB	Full: List, Read	All resources	None
ELB v2	Full: List, Read	All resources	None

The left sidebar shows the navigation path: Policies > Ec2-manage-instances-tag. Other tabs include 'Attached entities (3)', 'Policy versions', and 'Access Advisor'. The bottom of the page includes standard AWS footer links: Feedback, English (US), Privacy Policy, and Terms of Use.

Screenshot of the AWS Management Console EC2 Management Console showing the Instances page. The sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Dedicated Hosts, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Snapshots, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, and Feedback.

The main content shows a table of EC2 instances:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
i-057f61992dce44ce	t2.micro	us-east-2c	running	2/2 checks	None	None	ec2-18-217-49-19.us-ea...	18.217.49.19	-
i-06c0a2625ac65e697	t2.micro	us-east-2c	stopped	2/2 checks	None	None	ec2-13-58-248-46.us-ea...	13.58.248.46	-
i-08c000b615e0fe0	t2.micro	us-east-2c	running	2/2 checks	None	None	ec2-13-59-13-147.us-ea...	13.59.13.147	-
i-0d3a531b3c3d32e1d	m4.large	us-east-2c	running	2/2 checks	None	None	ec2-18-221-184-65.us-e...	18.221.184.65	-
i-0de003ff0c3602a0	t2.micro	us-east-2c	running	2/2 checks	None	None	ec2-18-216-97-133.us-e...	18.216.97.133	-
i-0e32869adffafab	t2.micro	us-east-2c	running	2/2 checks	None	None	ec2-18-216-97-133.us-e...	18.216.97.133	-

A modal window for instance i-06c0a2625ac65e697 is open, showing the 'Tags' tab. It contains one tag: project/blackjack. The 'Start Instances' button is visible at the bottom of the modal.

Casey can now see an EC2 instance tagged with the key/value of project/blackjack. Casey can then start an instance

Screenshot of the AWS Management Console EC2 Management Console showing the Instances page. The sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Spot Requests, Reserved Instances, Dedicated Hosts, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Snapshots, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, and Feedback.

The main content shows a table of EC2 instances. A modal window titled 'Start Instances' is displayed over the table, asking 'Are you sure you want to start these instances?'. The instance i-06c0a2625ac65e697 is listed in the modal.

The modal has 'Cancel' and 'Yes, Start' buttons. The 'Yes, Start' button is highlighted with a cursor.

Casey can indeed start this kind of specific instance

Trying to start a different instance results in the above error screen due to no permissions for that action

Demo: Correct an existing policy

We found four issues:

1. Typo in our services
2. Mismatch of supported resource and action
3. Condition key not supported
4. Missing actions

Recap

- ★ Review of IAM policy language
 - ★ Review of how policies work together to control access
 - ★ Policy tools – Create, test, and correct policies
 - ★ Policy Foo – Ninja moves with EC2 
- Additional resources

Policy Foo – Access control with tags

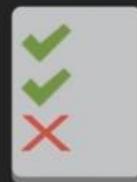
Control how users can add tags



Control which resources users can tag

Tags and EC2

Control which tags users can create



Control access to resources based on tags ✓

Tags are very useful as metadata on your EC2 Resources that are key/values pairs for ***discovering your resources***, ***organizing your resources***, ***cost allocation for auditing***, and ***access control to your resources***. As an admin, you can control how users can add a tag and also which tags users can create.

Demo: Permissions with tags

Goal: Allow Casey to launch instances only if he specifies a project tag with values ***blackjack*** or ***poker***.



Permissions overview

Allow adding tags only during instance launch

Require specific tags with values at instance launch

Bonus: Allow modify and create specific tags and resources

Policy: Create tag with RunInstances

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:CreateAction": "RunInstances"  
                }  
            }  
        }  
    ]  
}
```

Allows creation of tags

But only during RunInstances calls

Policy: Require tags at launch

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": ["ec2:RunInstances"], "Resource": ["arn:aws:ec2:::subnet/*", "arn:aws:ec2:::key-pair/*", "arn:aws:ec2:::instance/*", "arn:aws:ec2:::snapshot/*", "arn:aws:ec2:::volume/*", "arn:aws:ec2:::security-group/*", "arn:aws:ec2:::placement-group/*", "arn:aws:ec2:::network-interface/*", "arn:aws:ec2:::image/*"] }, { "Condition": { "StringLikeIfExists": { "ec2:InstanceType": "t2.*" } } } ] }
```

Previous

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": ["ec2:RunInstances"], "Resource": ["arn:aws:ec2:::subnet/*", "arn:aws:ec2:::key-pair/*", "arn:aws:ec2:::snapshot/*", "arn:aws:ec2:::volume/*", "arn:aws:ec2:::security-group/*", "arn:aws:ec2:::placement-group/*", "arn:aws:ec2:::network-interface/*", "arn:aws:ec2:::image/*"] }, { "Effect": "Allow", "Action": ["ec2:RunInstances"], "Resource": ["arn:aws:ec2:::instance/*"], "Condition": { "ForAllValues:StringEquals": { "aws:TagKeys": ["project", "name"]}, "StringEquals": { "aws:RequestTag/project": ["blackjack", "poker"], "ec2:InstanceType": "t2.micro" } } } ] }
```

Updated



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



We have now broken up the Previous Condition into 2 separate conditions statements in the Updated part.

Policy: Closer look at tagging conditions

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": ["ec2:RunInstances"], "Resource": ["arn:aws:ec2:::subnet/*", "arn:aws:ec2:::key-pair/*", "arn:aws:ec2:::snapshot/*", "arn:aws:ec2:::volume/*", "arn:aws:ec2:::security-group/*", "arn:aws:ec2:::placement-group/*", "arn:aws:ec2:::network-interface/*", "arn:aws:ec2:::image/*"] }, { "Effect": "Allow", "Action": ["ec2:RunInstances"], "Resource": ["arn:aws:ec2:::instance/*"], "Condition": { "ForAllValues:StringEquals": { "aws:TagKeys": ["project", "name"]}, "StringEquals": { "aws:RequestTag/project": ["blackjack", "poker"], "ec2:InstanceType": "t2.micro" } } } ] }
```

Allows project and/or name

Requires project with one of these values

Requires instance to be one of these sizes



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Screenshot of the AWS Management Console EC2 Management Console showing the 'Add/Edit Tags' dialog box. The dialog box is centered over the instance details page for instance i-08bc0000b615e05ef0. The dialog box has a search bar at the top and a table below it with columns 'Key' and 'Value'. A 'Create Tag' button is at the bottom right. The main page shows a list of instances with their public DNS and IP addresses.

Key	Value
project	poker

Screenshot of the AWS Management Console EC2 Management Console showing the 'Add/Edit Tags' dialog box. The dialog box is centered over the instance details page for instance i-08bc0000b615e05ef0. The dialog box has a search bar at the top and a table below it with columns 'Key' and 'Value'. A 'Create Tag' button is at the bottom right. The main page shows a list of instances with their public DNS and IP addresses. A long error message is displayed in the center of the screen.

Key	Value
project	poker

Casey can't create a tag

AWS Management Console > EC2 Management Console > CloudTrail Management ... > Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Amazon Linux AMI 2017.09.1.20171103-x86_64-gpu-1

Instance Type

Instance Type	ECUs	vCPUs	Mem
t2.micro	Variable	1	1

Security Groups

Security Group ID	Name	Description
sg-009ecb61	default	sg-009ecb61 (default)

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-009ecb61 (default)	

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair
Select a key pair
reinvent2017

I acknowledge that I have access to the selected private key file (reinvent2017.pem), and that without this file, I won't be able to log into my instance.

Launch Instances

AWS Management Console > EC2 Management Console > CloudTrail Management ... > Step 7: Review Instance Launch

Launch Status

Launch Failed

You are not authorized to perform this operation. Encoded authorization failure message:
 7whcN02icP4dlnlwmjh1OJ3lnlgemAz2nnx8QaICzPhNyX_ch3L2ZP9WnBeiytp56109pblw0Tu0o_hR9TWuTL35MyhCSh7ghlD890bP1WhlofAQQ0x7h26T-Rz1dmY7kH-T2CrjsfB0sbIVcgIgMAtSgb69daAyl7EgjgjtKgRy2BK8LU0h0pVujj0i0tGwHPqDTERBh5BHdhftQbzQHtzCMFq-h1buUC1_scy-BPaleOfaleo2m2QLOMgm-ixAOB1y0Lb02_pcY0dr9tayMcKwZZacst4HFqocZ50a0iz_k65SmruEty31ofakc750shb64t3e-VkuUkrntZsToA27gP9WyrpcQbQJ5hUdpkbyvpzlflj.9xF1qe-5ZFdd-8g5mqe5CJ-Xegdt4V8B7t7p1NKAuv/vphZrprnt_oWqlfmpHH0_e9U000ibk0gbe3HPYsdft5tsqHeVUKQqifYn8sQRNM8/yP_LukQ2B-KQ4M0JU2TAhQ9f5GdQ1ZRGGVJUKDeMdwwcztU-9QOUwRYEcovSWG7QdJsoBJThsiyvhG72Yhe3qPjd9ZOhmMDsRgv5CBOnqPl0DIBRQoK8p9DYaCg3zOQc2WA1sMGhkhpuC8UqshWTYelUICja1YFNm25_LDsITuyFYAmGRG5TvAxe2-JDg
 Hide launch log

Initiating launches Failure Retry

Retry Failed Tasks

Casey also does not have permissions to launch instances at the moment. Let us go and add those permissions below

Screenshot of the AWS IAM Management Console showing the user summary for 'Casey'.

User ARN: arn:aws:iam::094697565664:user/Casey

Path: /

Creation time: 2017-11-20 19:21 PST

Permissions tab selected. Attached policies: 4

Policy name	Policy type
S3-reinvent-2017-dev	Managed policy
Ist-pass-role-reinvent-2017-mobile	Managed policy
CloudTrail-Access	Managed policy
Ec2-manage-instances-tag	Managed policy

Add inline policy button.

Screenshot of the AWS IAM Management Console showing the 'Add permissions to Casey' step.

Step 1: Permissions (highlighted with a blue circle)

Step 2: Review (highlighted with a grey circle)

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Options:

- Add user to group
- Copy permissions from existing user
- Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Create group Refresh

Search: Showing 1 result

Group	Attached policies
Admins	AdministratorAccess

Screenshot of the AWS IAM Management Console showing the "Add permissions" step. The user is selecting policies to attach directly to the user "Casey".

Filter: Customer managed

Policy name	Type	Attachments	Description
AWSCloudTrailAccessPolicy	Customer managed	1	
EC2-CREATE-Tag-RunInstances	Customer managed	1	Grants access to create tags but only during runInstances
EC2-CreateTag-withValues	Customer managed	1	Grants access to create and modify tags with specific values.
EC2-launch-instance-T2	Customer managed	1	This policy allows developers to launch instances only in the T2 family.
EC2-launch-instance-T2-new	Customer managed	0	This policy allows developers to launch instances only in the T2 family.
EC2-launch-instance-T2-withTag	Customer managed	1	Grants access to launch T2 instances, but requires project tag with poker or blackjack values
s3-2017-reinvent-mobile-resource-access-dev	Customer managed	1	This policy grants access to list buckets and read from the mobile folder in the reinvent-2017-policy-ninja-dev...

Showing 7 results

Next: Review

Screenshot of the AWS IAM Management Console showing the "Review" step of adding permissions to user "Casey".

Add permissions to Casey

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	EC2-CREATE-Tag-RunInstances
Managed policy	EC2-launch-instance-T2-withTag

1 2

Permissions Review

Cancel Previous Add permissions

Screenshot of the AWS IAM Management Console showing the user summary for 'Casey'.

User ARN: arn:aws:iam::094697565664:user/Casey

Path: /

Creation time: 2017-11-20 19:21 PST

Attached policies: 6

Policy name	Policy type
S3-reinvent-2017-dev	Managed policy
EC2-Create-Tag-RunInstances	Managed policy
list-pass-role-reinvent-2017-mobile	Managed policy
CloudTrail-Access	Managed policy
Ec2-manage-instances-tag	Managed policy
EC2-launch-instance-T2-withTag	Managed policy

Add inline policy

Screenshot of the AWS IAM Management Console showing the policy summary for 'EC2-Create-Tag-RunInstances'.

Policy ARN: arn:aws:iam::094697565664:policy/EC2-Create-Tag-RunInstances

Description: Grants access to create tags but only during runInstances

Attached entities (2)

```
1: {
2:     "Version": "2012-10-17",
3:     "Statement": [
4:         {
5:             "Sid": "VisualEditor0",
6:             "Effect": "Allow",
7:             "Action": "ec2:CreateTags",
8:             "Resources": "*",
9:             "Condition": {
10:                 "StringEquals": {
11:                     "ec2:CreateAction": "RunInstances"
12:                 }
13:             }
14:         }
15:     ]
16: }
```

AWS Management Console > EC2 Management Console > CloudTrail Management ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Services > Resource Groups >

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Spot Requests

Reserved Instances

Dedicated Hosts

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Launch Instance Connect Actions

Get Windows Password

Launch My - Like This

Name Instance ID

Instance State

Instance Settings

Image Networking

CloudWatch Monitoring

Availability Zone

Instance State

Status Checks

Alarm Status

Public DNS (IPv4)

IPv4 Public IP

IPv6 IPs

1 to 6 of 6

Instance: i-057f761992dce44ce Public DNS: ec2-18-217-49-19.us-east-2.compute.amazonaws.com

Description Status Checks Monitoring Tags

Add/Edit Tags

Key Value

This resource currently has no tags.

Feedback English (US)

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

AWS Management Console > EC2 Management Console > CloudTrail Management ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Services > Resource Groups >

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (1-255 characters maximum) Value (255 characters maximum) Instances Volumes

This resource currently has no tags.

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Feedback English (US)

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

AWS Management Console > EC2 Management Console > CloudTrail Management ... > LaunchInstanceWizard:

Services > Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key	(127 characters maximum)	Value	(256 characters maximum)	Instances	Volumes
project	slot			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

AWS Management Console > EC2 Management Console > CloudTrail Management ... > LaunchInstanceWizard:

Services > Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

amzn-ami-hvm-2017.09.1.20171103-x86_64-gp2 - ami-aa1b34cf	Amazon Linux AMI 2017.09.1.20171103 x86_64 HVM GP2
Root Device Type: ebs	Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Security Group ID	Name	Description
sg-099ecb61	default	default VPC security group

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-099ecb61 (default)	

Cancel Previous Launch

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

AWS Management Console > EC2 Management Console > CloudTrail Management ... > Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.

Step 7: Review Instance Launch

1. Choose AMI 2. Choose instance type 3. Configure instance 4. Add storage 5. Add tags 6. Configure security group 7. Review

AMI Details

Amazon Linux AMI 2017.09.1.20171103-x86_64-gpu2

Instance Type

Instance Type	ECU	vCPUs	Mem
micro	Variable	1	1

Security Groups

Security Group ID: sg-099ecb61

All selected security groups inbound rules:

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-099ecb61 (default)	

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair: Select a key pair: reinvent2017

I acknowledge that I have access to the selected private key file (reinvent2017.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Edit AMI Edit instance type Performance Moderate Edit security groups Cancel Previous Launch

AWS Management Console > EC2 Management Console > CloudTrail Management ... > Step 7: Review Instance Launch

Casey @ 0946-9756-5664 > Ohio > Support

Launch Status

Launch Failed

You are not authorized to perform this operation. Encoded authorization failure message: MzQD0f51OT5Q0gu7y94kEHGlg3Gnt0_w8kpOr9HjG2jcnalLR0rz9Lp992rlSc0qh0YFu-Ch5ajtM0eSL0FIFOtaop-VcRALyljbGMf7oJy_A2fbzB-WfIMl5NvHtzikkdeaccfCqzQNLPA8d0pkqbsR2Emsu77ibTrGAv/qGM3-VVn0hY-aluUcmZQ1_QqWZRCsm-AHijctonsAU9jOFBSe0kw4tampptBtTAUUL4LMNg95Bdt0TLbAmkTCb330hn2rbYmQltcm_SP56Am{)jDp7puyPa6UFaw9Psu5DDs4oAdshpvcRCITN14WNzJ0jHdd6_Mg01AZTIBiu-IGU0azjp0fWdahfrR1Chf7gQby5MuGoMa603su0tbWh-KCT-FY7ELf_leCIORYYYgo64nlaQ425SYYSQWmda7To6MgpeCG8m6m7Rrzvu42vsfZSf1BUKU0dthy2VTeHETMsOkNyJueJasuRmkkeRZstE6J2adarhB7dg0uSnLdVPGJpmUQxaAJAwPKUxHm0GLMS45AamQbkdy72H9K6XhpKVb-bwAob-TAT33oV2dMh3fz2rnk2HE633d40Qm6OGGVKh8V9WVPv8fBZQyMBJmciDwri1aqbm;_ya8Xg3t;koM8VTgal21Ufkpq-zg

Hide launch log

Initiating launches Failure Retry

Cancel Back to Review Screen Retry Failed Tasks

Casey can't launch instances with tags that are not blackjack

AWS Management Console < **EC2 Management Console** < **CloudTrail Management** ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Casey @ 0946-9756-5664 Ohio Support

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
project	blackjack			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
name	imhungry			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Feedback English (US) © 2008–2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

AWS Management Console < **EC2 Management Console** < **CloudTrail Management** ...

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

Casey @ 0946-9756-5664 Ohio Support

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.

AMI Details

amzn-ami-hvm-2017.09.1.20171103-x86_64-gp2

Amazon Linux AMI 2017.09.1.20171103 x86_64 HVM GP2

Root Device Type: /dev/sda1 Virtualization Type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Mem
t2.micro	Variable	1	1

Security Groups

Security Group ID: sg-099ecb61 Name: default

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-099ecb61 (default)	

Select an existing key pair or create a new key pair

A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair Select a key pair reinvent2017

I acknowledge that I have access to the selected private key file (reinvent2017.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Cancel Previous Launch

Feedback English (US) © 2008–2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

AWS Management Console | EC2 Management Console | CloudTrail Management ... | +

https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:

Casey @ 0946-9756-5664 | Ohio | Support

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0d1787c6bf34c88d6 View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can [connect](#) to them from the Instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Amazon EC2 User Guide
- Learn about AWS Free Usage Tier
- Amazon EC2 Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Casey can launch instances having the project/blackjack and name/<anything> tags as seen above

Policy Foo – Challenge

“But how do I let Casey update tags on existing instances without also allowing crazy tags?”

Goal: Allow Casey to create tags on resources tagged with one of his projects and a name tag with any value.

Pro tip! Look at the conditions that EC2:CreateTags supports.

project=poker
name=vegas

project=slots
name=vegas

Policy: Control tags using EC2

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": "ec2:CreateTags",  
        "Resource": "*",  
        "Condition": {  
            "StringEquals": {  
                "ec2:ResourceTag/project": ["blackjack", "poker"]  
            },  
            "ForAllValues:StringEquals": {  
                "aws:TagKeys": ["project", "name"]  
            },  
            "StringEqualsIfExists": {  
                "aws:RequestTag/project": ["blackjack", "poker"]  
            }  
        }  
    }]
```

Only tag resources with these tags

Tag with either of these keys

For *project*, you specify only these values

Allow users to create tags on resources tagged with project=blackjack or project=poker and only tag with project or name. If they use project, they must use blackjack or poker.

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Additional resources

AWS Security Blog: Announcements, use cases, and best practices

<https://aws.amazon.com/blogs/security/>

Other Sessions:

SID303 - How You can use AWS' Identity Services to be Successful on Your AWS Cloud Journey

SID309 - Credentials, Credentials, Credentials, Oh My!

SID321 - How Capital One uses AWS Organizations



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

