# **AWS Config - Hands-on Exercise**

er

- Introduction
- Part 1 IAM Users
  - Goal
    - Part 1A Login and get to Config
    - Part 1B Find "your" IAM user
    - Part 1C Whitelist "your" IAM user
- Part 2 S3 Buckets
  - ° Goal
    - Part 2A Login and go to Config
    - Part 2B Find "your" S3 bucket
    - Part 2C Whitelist "your" bucket
- Part 3 Wait for Config Rule re-evaluation
  - Goal
    - Part 3A Find "your" resources in Config again
    - Part 3B Be prepared for delayed gratification

## Introduction

This hands-on exercise shows how to work with non-compliant resources in AWS Config and how to whitelist them for Config.

## Part 1 – IAM Users

#### Goal

Although the use of IAM users in Cornell AWS accounts is discouraged in most situations, there are some valid use-cases where IAM users are necessary. The Cornell AWS Config rule **251-MED-no-iam-users-except-whitelist** labels all IAM users as non-compliant unless they are specifically whitelisted.

For this exercise, an IAM user was previously created in cu-training for each training participant. In this exercise, you will find "your" IAM user there and whitelist it for the 251-MED-no-iam-users-except-whitelist Config rule.

## Part 1A - Login and get to Config

- 1. Login to the cu-training AWS account using traditional Shibboleth login.
  - a. Use this link to initiate login: https://signin.aws.cucloud.net/
    - This will start the usual process for Cornell Two-Step Login process. Complete your two-step login.
  - Once you have finished with DUO, you will be in one of two places. Take your next steps based on where you end up.
     If you are given the option of selecting a role, select shib-training under the "cu-training" AWS account, and click on Sign in.

← → ♂ ŵ	🗴 🔟 🔒 https://signin.aws.amazon.com/saml	MISC 🔵 🚥 🖂	III\ 🗉 🗶 👜 😑
aws			0
	Select a role:		
	Account: ()		
	Account: cu-training ()		
	o shib-training		
	Sign in		
	English		
	Terms of Use Privacy Policy © 1996-2021, Amazon Web Services, Inc. or its	s affiliates.	

1. Once in the AWS Management Console, check which AWS region your console is pointed at. You want "N. Virginia". If your console is in any other region, change it to "US East (N. Virgina) us-east-1".





## Part 1B - Find "your" IAM user

- 1. Click on **Resources** from the left-hand navigation panel in the Config console.
- 2. Enter the "netid" form of your Cornell email address (e.g., netid@cornell.edu) in the **Resource identifier** search field and hit "enter" on your keyboard. This will start the search for "your" IAM user.

esource Inventory		
arch existing or deleted resources recor compliance timeline. The resource conf ecific resource. The resource compliance nfigurations, use the advanced SQL que	ded by AWS Config. For a specific resourc iguration timeline allows you to view all timeline allows you to view compliance ry editor.	e, view the resource details, configuration timeline the configuration items captured over time for a status changes. To query your resource
Resources		View details Resource Timeline
Resource category	Resource type	Compliance
All resource categories	<ul> <li>All resource types</li> </ul>	<ul> <li>Any compliance status</li> </ul>
Resource identifier - <i>optional</i>		X Include deleted resources
		< 1 > @
Resource identifier	Туре	Compliance

3. Config should show one search result, listing an IAM user named like "netid@cornell.edu". That IAM User resource will be labelled as noncompliant.

	Resource identifier	Туре	Compliance
0	pea1@cornell.edu	IAM User	▲ Noncompliant

- 4. Click on the IAM user name (i.e., netid@cornell.edu) to drill into that resource.
- 5. Review the Rules at the bottom to confirm that "your" IAM user is indeed non-compliant with respect to the 251-MED-no-iam-users-exceptwhitelist rule.

ws config > Resources > pear@cornett.edu			
ea1@cornell.edu		Resource Timeline	Manage Resource 🛽
▼ Details		/	
Resource name pea1@cornell.edu Resource type AWS:IAM:User Resource ID AID Amazon resource name propursionaria	Availability zone Not Applicable Created on April 12, 2021 8:16 AM	User Name pea1@cornell.edu Inline Policy Details -	
/deleteme/pea1@cornell.edu			
//deleteme/pea1@cornell.edu     View Configuration Item (JSON)  Rules applied Tags			
Anisarsaalit     User/example       /deleteme/pea1@cornelLedu       View Configuration Item (JSON)       Rules       Any status	View de	tails Edit rule Act	ions ▼ Add rule < 1 > ③
anitawstatility     Loser/example       /deleteme/peat@cornell.edu       View Configuration Item (JSON)       Rules       Any status       Name	View de	tails Edit rule Act	ions ▼ Add rule < 1 > ③ e Compliance
Anizars.ani     User/example       /deleteme/pea1@cornell.edu       View Configuration Item (JSON)       Rules       Any status       Name       OrgConfigRule-152-HIGH-no-lam-users-w	View de with-password-jwhckxhj	stails Edit rule Act Remediation action Typ Not set -	ions ▼ Add rule < 1 > @ e Compliance ⊘ Compliant
Any status     Image: Complexity of the status	View de with-password-jwhckxhj ad-credentials-check-ywaxmu8d	tails Edit rule Act Remediation action Typ Not set - Not set -	ions V Add rule < 1 > ③ e Compliance ③ Compliant ④ Compliant
Any status     Image: Status       Name     OrgConfigRule-152-HIGH-no-lam-users-unusers-       OrgConfigRule-252-MED-access-keys-rot	View de with-password-jwhckxhj ed-credentials-check-ywaxmu8d ated-jxtdpgwk	tails Edit rule Act Remediation action Typ Not set - Not set -	ions ▼ Add rule < 1 > ③ e Compliance ⊙ Compliant ⊙ Compliant

6. In the top right of that page, click on Manage Resource.

## Part 1C - Whitelist "your" IAM user

- 1. You should now be viewing "your" IAM user in the the IAM console.
- 2. Click on the Tags tab.

→ C' 🏠		🔒 🗣 https	s://console.aws.amazo	on.com/iam/home?#/use	rs/pea1@cornell.e cu-training 🔴 🛛 🚥 🖂	III\ 🗉 🖲 🐠
aws Services	▼ Q Se	arch for servic	ces, features, marketpl	lace product: [Option+S]	Shib-training/pea1@cornell.edu @ cu-trainin	ng 🔻 Global 🔻 Support
Users > pea1@c	ornell.edu					
Summary	/					Delete user
Us	er ARN arm	aws:lam::	:user/exar	mple/deleterne/pea1@co	rnell.edu 省	
	Path /ex	ample/deleter	me/			
Creati	on time 20	21-04-12 08:1	6 EDT			
oroun						
Permissions	Groups (1)	Tags	Security credentials	s Access Advisor		
Permissions	Groups (1)	Tags	Security credentials	s Access Advisor		
Permissions Permission Add permission	Groups (1) ONS policies sions	Tags (1 policy a	Security credentials	s Access Advisor		Add Inline policy
Permissions   Permissions  Add permission Policy r	Groups (1) ons policies sions	Tags (1 policy a	Security credentials	s Access Advisor	Policy type 👻	• Add inline policy
Permissions  Permissions Add pormissi Policy r Attached from	Groups (1) ons policies sions name • m group	Tags (1 policy a	Security credentials	S Access Advisor	Policy type 👻	O Add Inline policy

Click on Add tags.
 Add a tag with the following settings, and click Save changes:

)- C	🖸 👫 🔽 🖨 🖙 http	ps://console.aws. <b>amazon.com</b> /iam/home?#/users/pea1@corne cu-training 🔵 🛛 🚥 💟	II\ 🗉 🍭
aws	Services  Q Search for serv	vices, features, marketplace on [Option+S]	Global 🔻 Suppo
	Tags for pea1@cor	rnell.edu	
	Кеу	Value (optional)	Remove
	ED-no-iam-users-except-whitelist	t	×
	Add new key		
	You can add 49 more tags.		
		Cancel	ave changes
eedback	English (US) 🔻	© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of	f Use Cookie pre
••	MWS Config Console X 💡 IAM M	Management Console X +	
• • • → ♂	Image: AWS Config Console     X     Image: AWS Config Console     X     Image: AWS Config Console       Image: AWS Config Console     Image: AWS Config Console     X     Image: AWS Config Console     X		
● ● ) → C' aws	T AWS Config Console X ♀ IAM M	Management Console x +	
) → C aws	AWS Config Console     X     Image: I	Management Console x + el.e.ws.amazon.com/iam/home?#/users/pea1@corni: cu-training  …	
● → C <sup>4</sup> aws Users >	Image: Average Console     Image: Average Console     Image: Average Console       Image: Average Console     Image: Console     Image: Console	Management Console X + ele.aws.amazon.com/(am/home?#/lusers/pea1@cornic_cu-training	
) → ♂ aws users > Sumr	AWS Config Console      X     Y     LAMM      C     X     Y     LAMM      C     X     Y     X     Y     X     X     Y     X     Y     X     X     Y     X     Y     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X     X     Y     X	Management Console X + ile.aws.amazon.com/(am/home?#/users/pea1@cornic_cu-training • ••• ♥ III • ® • = urres, marketplace prod [Option+S] A sht-training/pea1@cornel.edu @ ou-training • Global • Support •	
) → C aws s Users > Sumr	AWS Centrig Consule     X      C      LAM M     C	Management Console X + lle.avs.amazon.com/lam/home?#/users/peo1@corr: cu-training • ···· ♥ II\ © ® ● = urns, marketplace prod [Option+S]	
→ C     aws     users >     Sumr     Tags u	AWS Centrig Consule     X      Consule     X      Consule     X     Consule     X     Consule     X     Consule     X     Consule     X     Consule     X     Consule     X     X     Consule     X	Managament Console × + le.aws.amazon.com/lam/home?#/users/pea1@corn: cu-training • ♥ II\ © ® ● = urns, markstplace prod [Option+S]	
● ● → C <sup>a</sup> users → Sumr Tags u	AWS Centrig Consule     X      Consule     X     X     Consule     X     Consule     X     Consule     X     Consule     X     Consule     X     X     Consule     X     X     Consule     X     X     Consule     X     X     X     Consule     X     X     X     X     Consule     X	Managament Console X + ble.aws.amazon.com/lam/home?#/users/pea1@corn: cu-training • v u lin u & • = ures, markstplace prod [Option+S]	
→ C' aws Users → Sumr Tags u	AWS Config Console	Managament Console X + ble.aves.amazon.com/lam/home?#/users/pea1@corn: cu-training • ♥ III\ © @ @ = ures, marketplace prod (Option+S)	
→ C <sup>4</sup> aws c Users → Sumr Tags u	AWS Config Console     Y     Y     AWS     Config Console     Y     Y     Y     Console     Y	Managament Console X + ble.aws.amazon.com/lam/home?#/users/pea1@corns: cu-training • v III. 0 • . = . urea, marketplace prod (Option+S)	
) → C' aws ( Users > Sumr Tags u	AWS Config Console	Managament Console X + ble.avas.amazon.com/lam/home?#/users/pea1@corns: cu-training • ♡ III\ © © urea, markatplace prod (Option+S)	
→ C' aws ( Users > Sumr Tags u	AWS Config Console     Y	Management Console X + ble.avis.amazon.com/lam/home?#/users/pea1@cornii: cu-training • V III. C & urea, markatplace prod [Option+S]	
→ C <sup>I</sup> aws c Users > Summ Tags u Permission IAM tag	AWS Config Console     Y	Management Consol	
→ C <sup>I</sup> aws c Users > Summ Tags u Permiss IAM tag can use	AWS Config Console     Y	Management Consol	
→ C' Ws C' Users > Summ Tags u I and tags u LAM tag can use Edit	AWS Centrig Console     AWS Centrig Console     C	Meragement Consol	
→ C' aws c Users > Summ Tags u Idata tags u LAM tag can use Edit 0 s	AWS Centrig Console     AWS Centrig Console     C	Management Console X + He aves a mazon.com/iam/home?#/users/pea1@corn: cu-training • V III • • • • = III • • • • • • • • • • •	
→ C' aws Users > Sumr Tags u Tags u	AWS Centrig Console     AWS Centrig Console     C	Meregement Consol	
→ C <sup>4</sup> dWS C <sup>4</sup> Users > Summ Tags u Permission can using Edition Cathering	AWS Config Console     AWS     Config Console	Management Consol	

At this point in a typical Config workflow, you would find the **251-MED-no-iam-users-except-whitelist** Config Rule and trigger re-evaluation of the rule to confirm that your whitelisting had the desired effect (i.e. making the IAM user compliant for that rule). However, the Config API has a very, very threshold for the number of times that you can invoke revaluations. Therefore, the exercise leader will trigger re-evaluation just a few ≙ times during this hands-on session.

## Part 2 – S3 Buckets

#### Goal

To be conservative, the Cornell **153-HIGH-s3-bucket-public-read-prohibited** Config Rule flags any S3 buckets that are publicly readable. However, there are valid use cases where you want S3 bucket contents to be publicly readable (e.g., public web resources).

For this exercise, an S3 bucket was previously created in cu-training for each training participant. In this exercise, you will find "your" S3 web site bucket and whitelist it for the **153-HIGH-s3-bucket-public-read-prohibited** Config rule.

## Part 2A - Login and go to Config

1. If you aren't logged in to the cu-training account with role **shib-training**, follow the instructions in **Part 1A** above to login and navigate to the Config console.

## Part 2B - Find "your" S3 bucket

- 1. Click on **Resources** from the left-hand navigation panel in the Config console.
- In the Resource identifier search field, enter "your" S3 bucket name using this pattern my-public-web-site-NETID, and hit "enter" on your keyboard.

Resources			/iew details Resource Timeline
Resource category	Resource type		Compliance
All resource categories	<ul> <li>Multiple Selected</li> </ul>	•	Any compliance status
AWS S3 Bucket X Resource identifier - <i>optional</i> Q my-public-web-site-nl85			X Include deleted resource
			$\langle 1 \rangle$
Resource identifier		Туре	Compliance

- 3. Config should show one search result, listing an S3 bucket user named like **my-public-web-site-NETID**. That bucket will be labelled as non-compliant.
- 4. Click on the bucket name to drill into the Config details for that resource.
- 5. Review the Rules at the bottom of the page. They will show that the bucket is
  - a. compliant with respect to the **003-CRIT-s3-bucket-public-write-prohibited** rule, but b. non-compliant with respect to the **153-HIGH-s3-bucket-public-read-prohibited** rule.

VS Config > Resources > my-public-web-site-m	nl85			
וy-public-web-site-nl85		Resource Time	eline	Manage Resource
▶ Details				
View Configuration Item (JSON)				
Rules applied Tags				
Rules applied Tags Rules	View det	ails Edit rule	Actions	Add rule
Rules appled Tags Rules Any status	View det	ails Edit rule	Actions	Add rule
Rules Any status Name	View det	ails Edit rule	Actions	Add rule     Compliance
Rules applied     Tags       Rules	View det	ealls Edit rule Remediation action	Actions Type -	Add rule

6. In the top right of the details page, click on Manage Resource. This will take you to the S3 console for that bucket.

Part 2C - Whitelist "your" bucket

1. In the S3 console, with "your" bucket selected, click on the Properties tab and scroll down to Tags.

Objects Properties Permiss	ions Metrics Management Access	Points
Bucket overview		
AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN)	Creation date April 12, 2021, 08:27:29 (UTC-04:00)
Bucket Versioning Versioning is a means of keeping multiple varia object stored in your Amazon S3 bucket. With the Edit	ints of an object in the same bucket. You can use versioning to versioning, you can easily recover from both unintended user a	preserve, retrieve, and restore every version of every ctions and application failures. Learn more 🔀
Bucket Versioning		
Multi-factor authentication (MFA) delete An additional layer of security that requires mu modify MFA delete settings, use the AWS CLI, # DIsabled	l Iti-factor authentication for changing Bucket Versioning setti WS SDK, or the Amazon S3 REST API. <b>Learn more </b>	ngs and permanently deleting object versions. To
Tags (0) Track storage cost or other criteria by tagging y	your bucket. Learn more	Edit
Кеу	Value	
	No tags associated with this resource.	
Edit in the tags section.		
Edit in the tags section. on Add tag. hazon S3 > my-public-web-site-	nl85 > Edit bucket tagging	
Edit in the tags section. on Add tag. azon S3 > my-public-web-site- dit bucket tagging	nl85 > Edit bucket tagging	
Edit in the tags section. on Add tag. hazon S3 > my-public-web-site- dit bucket tagging Tags Track storage cost or other criteria by ta	nl85 > Edit bucket tagging g	

Add a tag with the following details, and click on Save changes:
 a. Key: cit:config:153-HIGH-s3-bucket-public-read-prohibited

2. 3.

Value: exception	
Amazon S3 > my-public-web-site-nl85 > Edit bucket tagging	
Edit bucket tagging	
Tags Track storage cost or other criteria by tagging your bucket. Learn more	
tey Value - optional	Bomovo
Add tag	Remove
	Cancel Save changes

5. On resulting bucket Properties page confirm that your new tag is shown as one of the bucket tags.

linh	Augertes Pour	istens Metrics Management Access	Points
Bucket av	waiwa		
vala organi Jano Japana	in observed 1	литеон кака такала (жа). Д алтама и текрология (жа).	creater data Auto 17, 2021, 55 2723 part 14005
Bucket Ve Index top 1 a Index - mentle Index	e <b>sioning</b> man offensies, as deares generation: Whatei We	n de vier de set de ser nécessé Yonan en contents hans als gans a readjourness frantation donn dess	e vraen na ma ma en anter serg es sen yéner ye na le sona agi se les tel est basean en 🛃
Bucket Ver national in a adm adm backet Seester Stations	esioning na chinang as isara parasawa Siladai Mi	e vikolar uljanak iko se eskanaj Vanes viranskog kver sel gipe – voolgren verkensk ingelijken stree faar	a onan na na mano adore carpo cha of ser y a ferena a pi o far fall exclusionerae ど
Bucket Ver autoristication additional State of Version State of Version State of Version State of Version State of Version State of Version State of Version	estioning man of brokey and wave part of and the first part of and the first set of an exception of the work an exception of the set of an exception of the	e offolder offolder in the set to only formal of equations in the set of a given is nondependent the list of the dependent of the set of the set of the set of the se	automiterate analos bergio estas de la constante dela constante

## Part 3 – Wait for Config Rule re-evaluation

#### Goal

b.

In a typical Config workflow you would whitelist, reconfigure, or delete resources that Config has flagged and then tell Config to re-evaluate the relevant Rules. However, there are complicating factors.

## Part 3A - Find "your" resources in Config again

- 1. Use the Config console to open two browser windows one with Config details for "your" IAM user, and one with the Config details for "your" S3 bucket.
  - Each of those resources started out as non-compliant to one Config rule.
- 2. Wait until the exercise leader says that re-evaluation has been triggered and completed.
- 3. Once you get the go-ahead, refresh each of the resource Config details pages.

## Part 3B - Be prepared for delayed gratification

- In all likelihood one, if not both, of "your" resources remain flagged as non-compliant.
- One reason for this is that Config evaluations operate on snapshots of resource configurations, not from an instantaneous reading of the resource details.
- Another factor that seems to come into play is that Config evaluation results themselves are cached and sometimes you may be looking at results from the previous evaluation.
- The secret for maintaining your sanity with Config is to check back with Config for new results on the <u>day after</u> you make resource configuration changes. What you see after 24 hours is typically a meaningful set of results.

This rule has been created by control of the service-linked AWS Control of the service of the se	onfig-multlaccountsetup.ar fig rule (SLR) and it's a uniqu 'S services that these rules a	nazonaws.com Ie type of managed config rule tha re linked to. Read more about Ser	at supports other AWS services to create A vice-Linked AWS Config Rules. [2]	WS Config rules in your account. You canno	t edit or delete these
rgConfigRule-153-F	HGH-s3-bucke	et-public-read-pro	ohibited-36bizz4n	_	Actions 🔺
					Manage remediation
<ul> <li>Rule details</li> </ul>					Re-evaluate Delete results
Description [CIT custom rule] Ensure that S3 buckel readable, except those explicitly whiteli Config rule ARN am:aws:config-us-east-1: rule/config-multiaccountsetup.amazon. L2dtyn	is are not publicly sted. 	Trigger type Periodic: 24 hours Scope of changes Resources		Last successful evaluation	Detete Thre
<ul> <li>Resources in scope</li> </ul>				View details	Remediate
Noncompliant 🔻				<	1 2 > ③
ID	Туре	Status	Annotation		Compliance
	S3 Bucket	-	Trusted Advisor marks this bucket wit	h status "Yellow" and it is not whitelisted.	A Noncompliant
my-public-web-site-					
my-public-web-site- my-public-web-site-	S3 Bucket	-	Trusted Advisor marks this bucket wit	h status "Yellow" and it is not whitelisted.	A Noncompliant