AWS Config - Hands-on Exercise

er

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

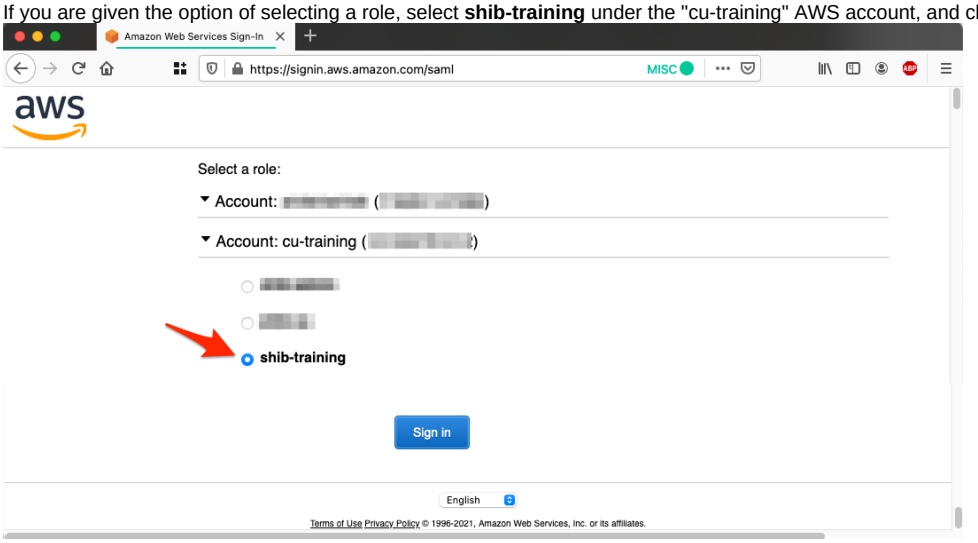
Goal

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.

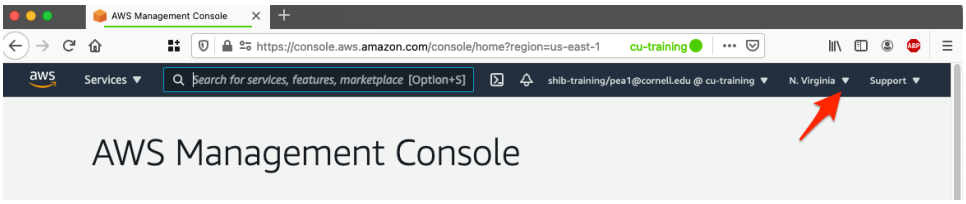
For this exercise, an IAM user was previously created in cu-training for each training participant. In this exercise, you will find "your" IAM user there and whitelist it for the **251-MED-no-iam-users-except-whitelist** Config rule.

Part 1A - Login and get to Config

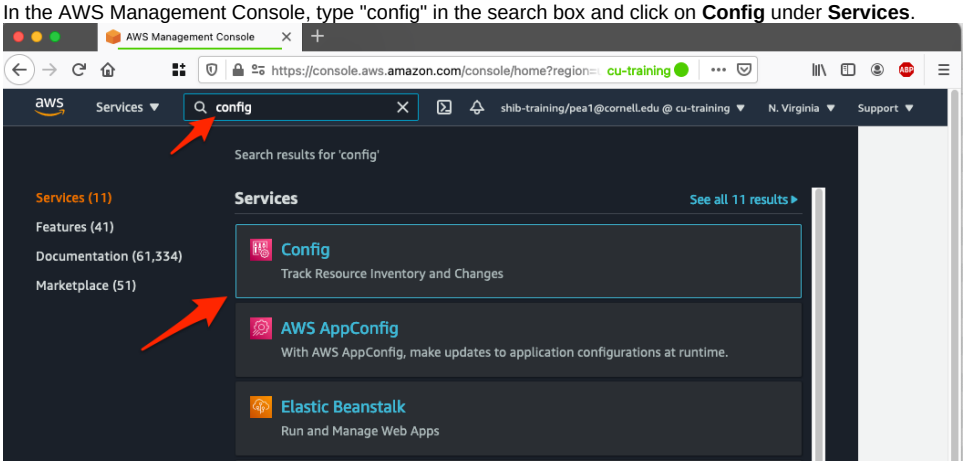
1. Login to the cu-training AWS account using traditional Shibboleth login.
   a. Use this link to initiate login: https://signin.aws.cucloud.net/
      - This will start the usual process for Cornell Two-Step Login process. Complete your two-step login.
      - Once you have finished with DUO, you will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



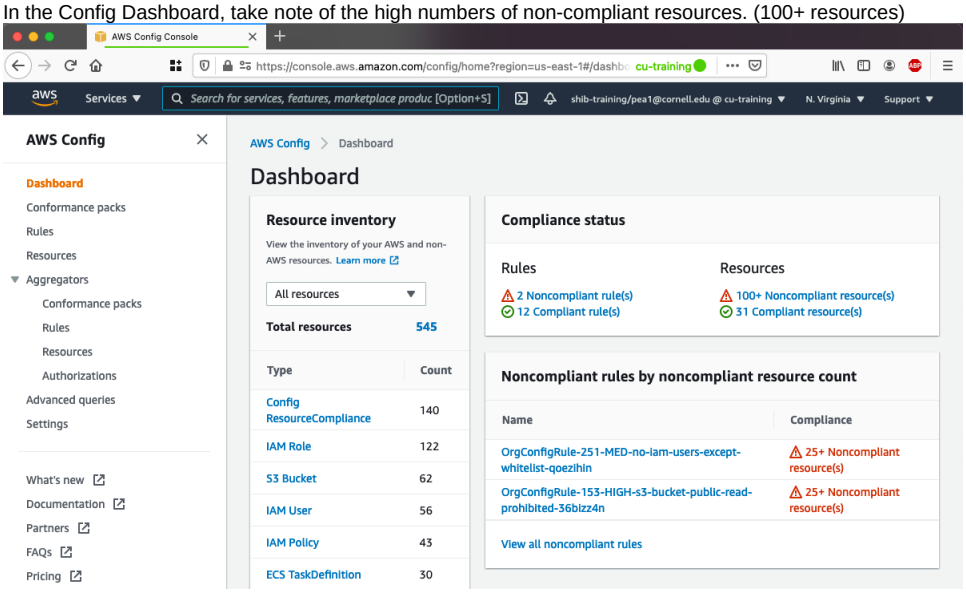
1. Once in the AWS Management Console, check which AWS region your console is pointed at. You want "N. Virginia". If your console is in any other region, change it to "US East (N. Virigina) us-east-1".



2. In the AWS Management Console, type "config" in the search box and click on **Config** under **Services**.

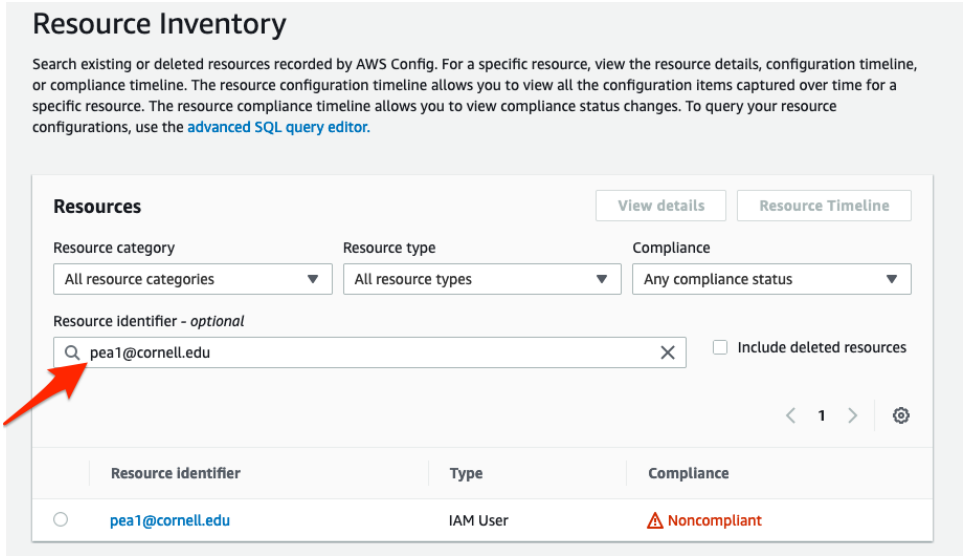


3. In the Config Dashboard, take note of the high numbers of non-compliant resources. (100+ resources)

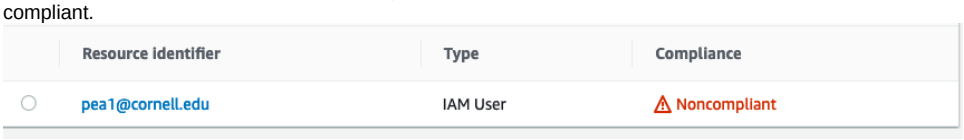


Part 1B – Find "your" IAM user

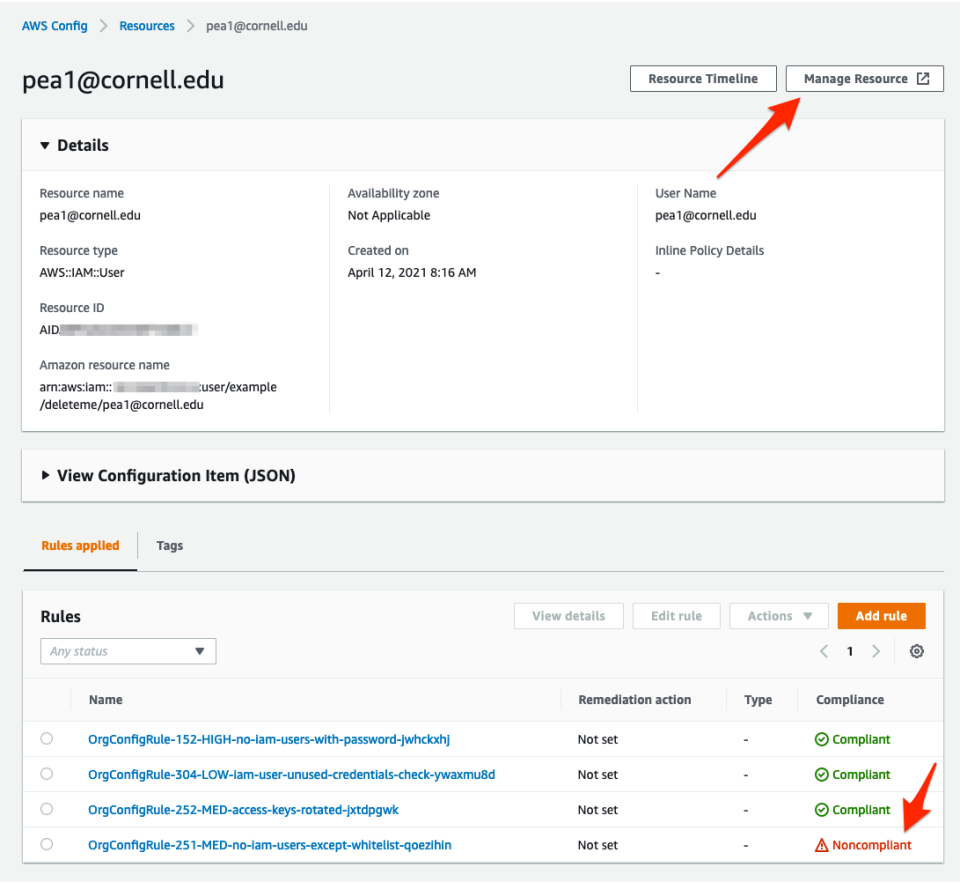
1. Click on **Resources** from the left-hand navigation panel in the Config console.
2. Enter the "netid" form of your Cornell email address (e.g., netid@cornell.edu) in the **Resource identifier** search field and hit "enter" on your keyboard. This will start the search for "your" IAM user.



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



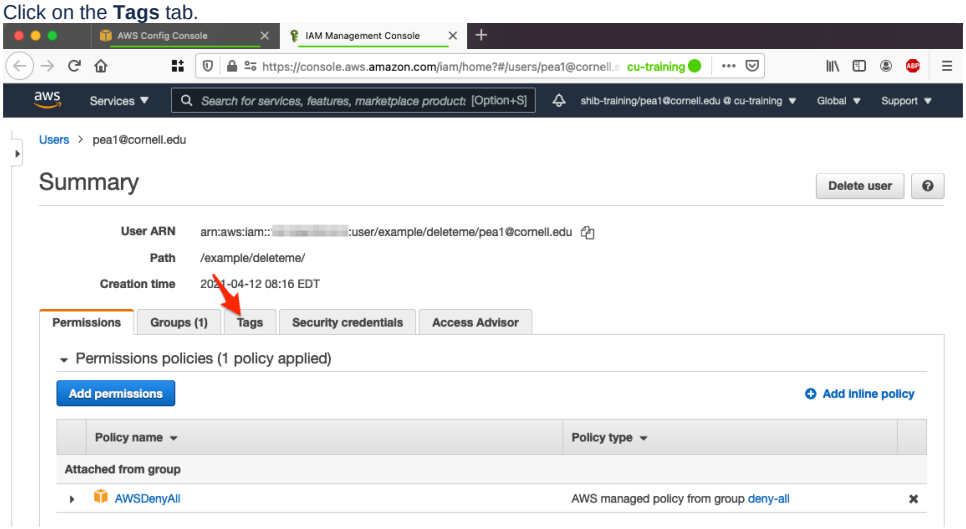
4. Click on the IAM user name (i.e., netid@cornell.edu) to drill into that resource.
5. Review the **Rules** at the bottom to confirm that "your" IAM user is indeed non-compliant with respect to the **251-MED-no-iam-users-except-whitelist** rule.



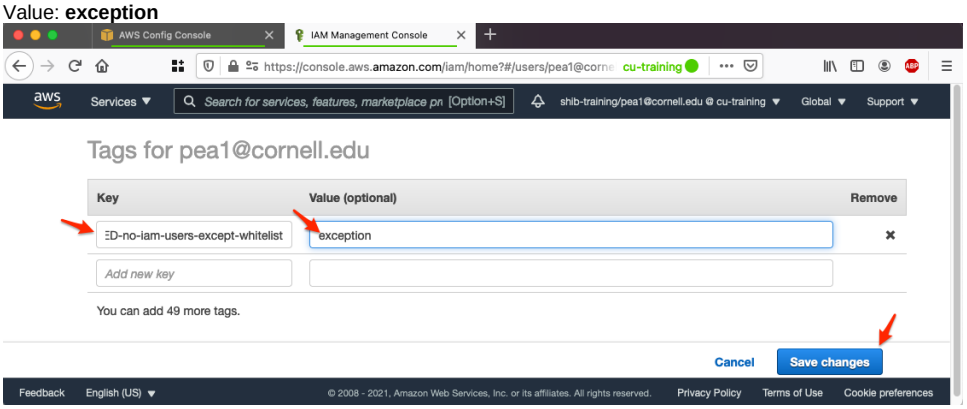
6. In the top right of that page, click on **Manage Resource**.

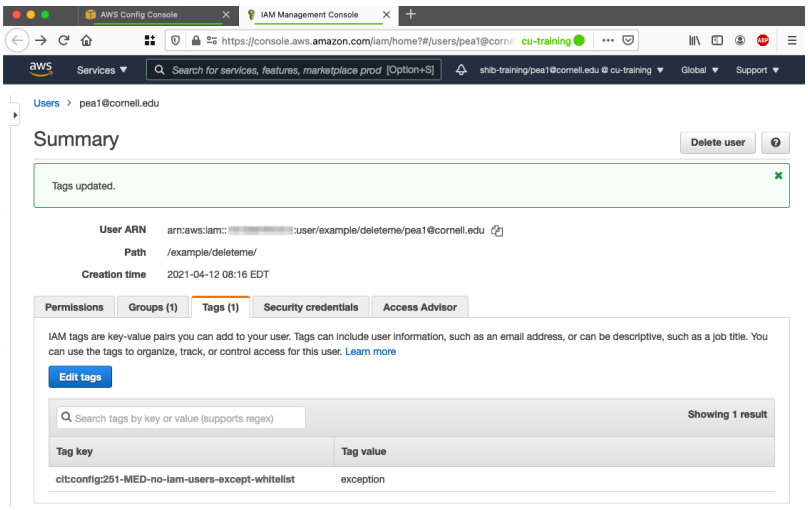
Part 1C – Whitelist "your" IAM user

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



3. Click on **Add tags**.
4. Add a tag with the following settings, and click **Save changes**:
    a. Key: **cit:config:251-MED-no-iam-users-except-whitelist**
    b. Value: **exception**





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).

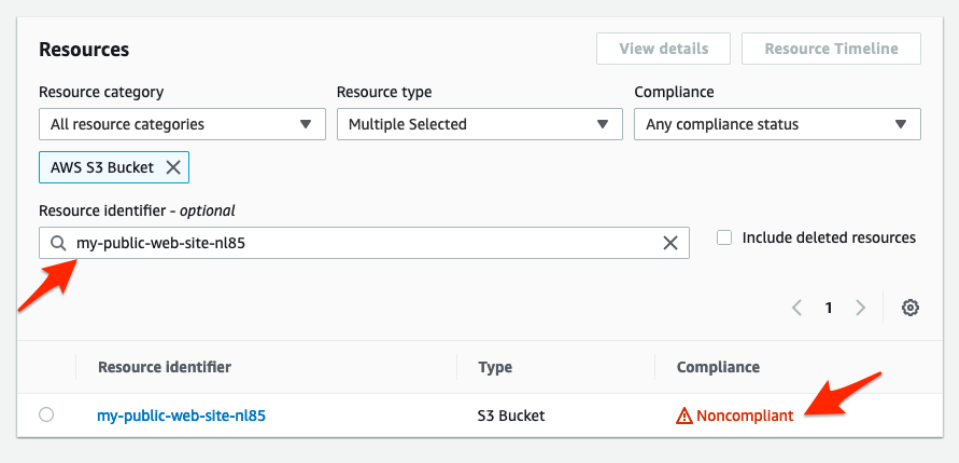
For this exercise, an S3 bucket was previously created in cu-training for each training participant. In this exercise, you will find "your" S3 web site bucket and whitelist it for the **153-HIGH-s3-bucket-public-read-prohibited** Config rule.

Part 2A - Login and go to Config

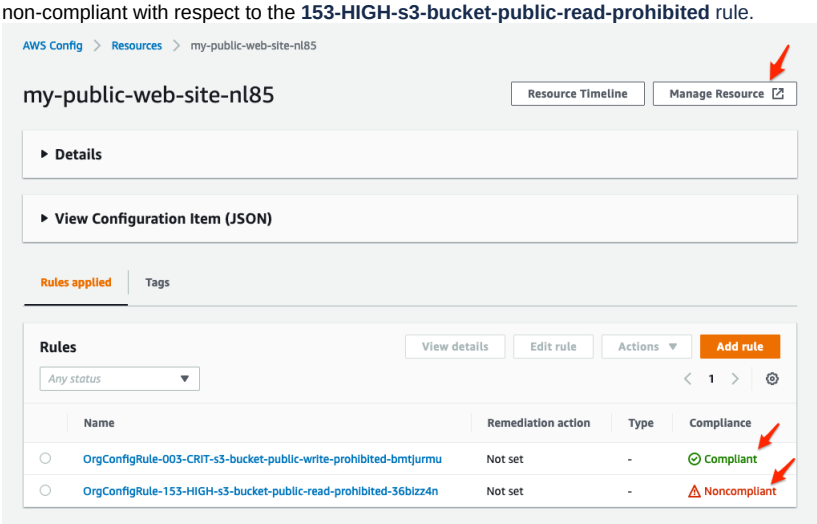
1. If you aren't logged in to the cu-training account with role **shib-training**, follow the instructions in **Part 1A** above to login and navigate to the Config console.

Part 2B – Find "your" S3 bucket

1. Click on **Resources** from the left-hand navigation panel in the Config console.
2. 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.



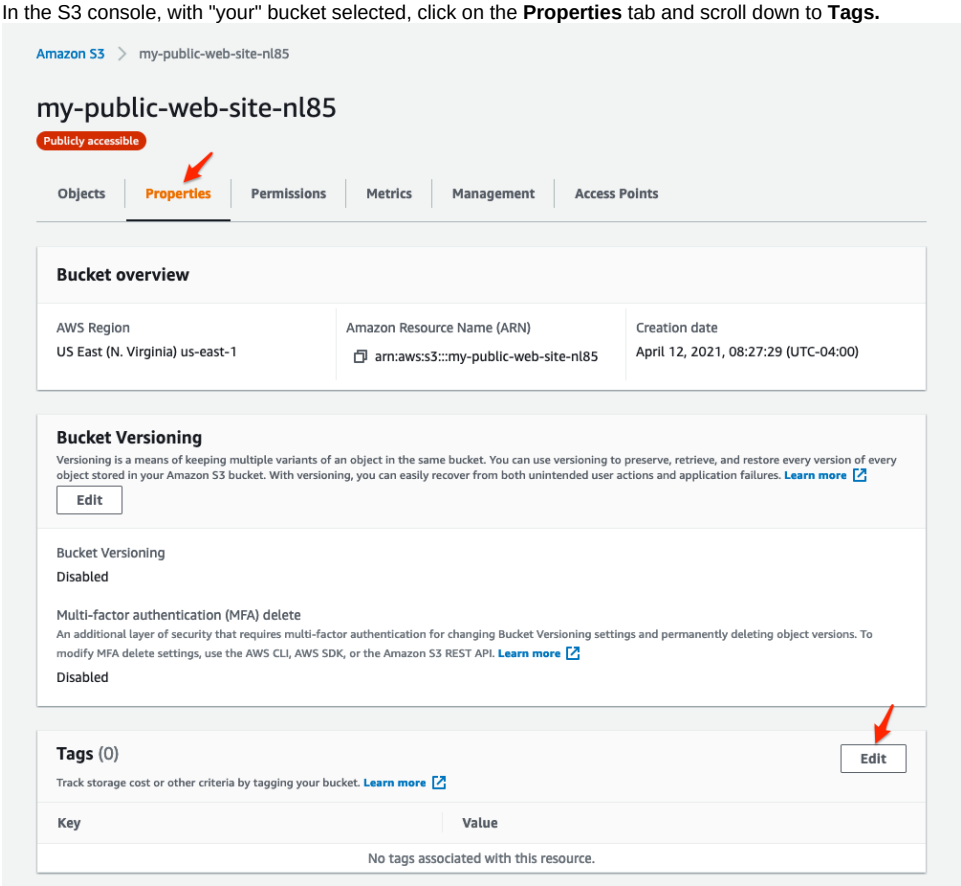
3. Config should show one search result, listing an S3 bucket user named like **my-public-web-site-NETID**. That bucket will be labelled as non-compliant.
4. Click on the bucket name to drill into the Config details for that resource.
5. Review the **Rules** at the bottom of the page. They will show 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.



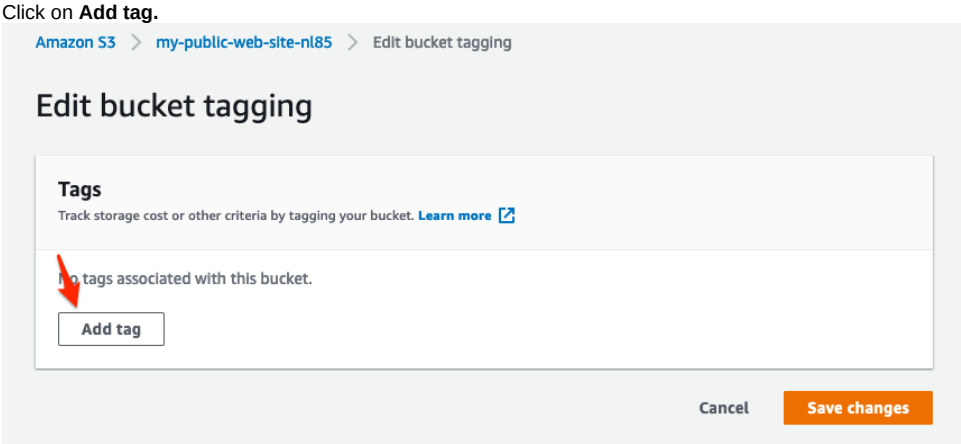
6. In the top right of the details page, click on **Manage Resource**. This will take you to the S3 console for that bucket.

Part 2C – Whitelist "your" bucket

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

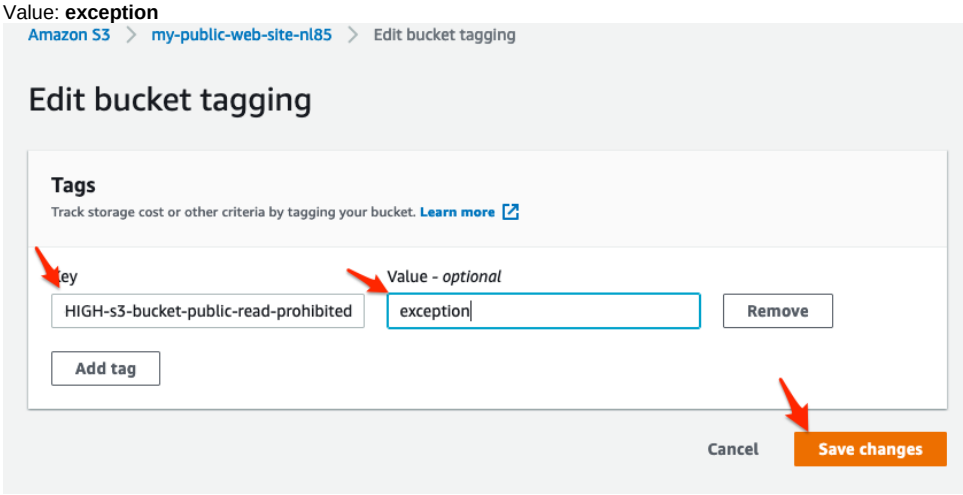


2. Click **Edit** in the tags section.
3. Click on **Add tag.**

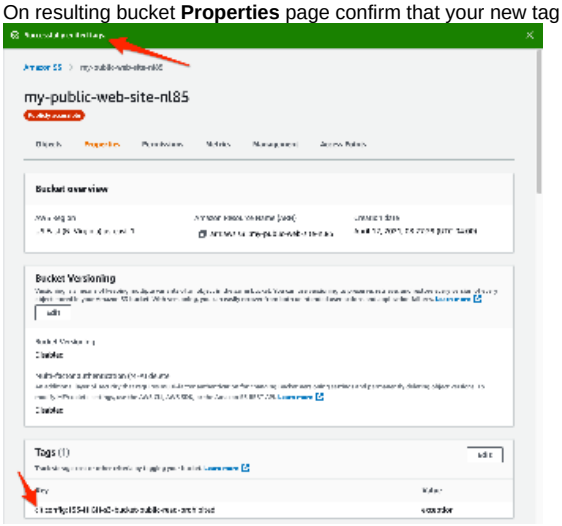


4. Add a tag with the following details, and click on **Save changes**:
    a. Key: **cit:config:153-HIGH-s3-bucket-public-read-prohibited**

b. Value: **exception**



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



Part 3 – Wait for Config Rule re-evaluation

Goal

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 day after you make resource configuration changes. What you see after 24 hours is typically a meaningful set of results.

If you wanted to force Config to evaluate a Rule within your own AWS account, you would use the **Re-evaluate** action, as shown below.