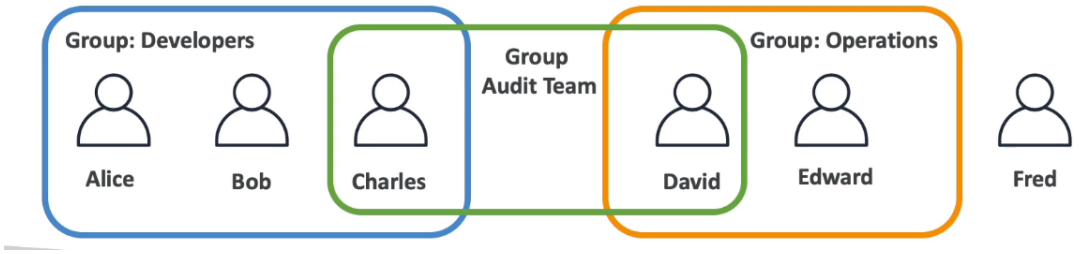
IAM - Identity Access Management

Introduction

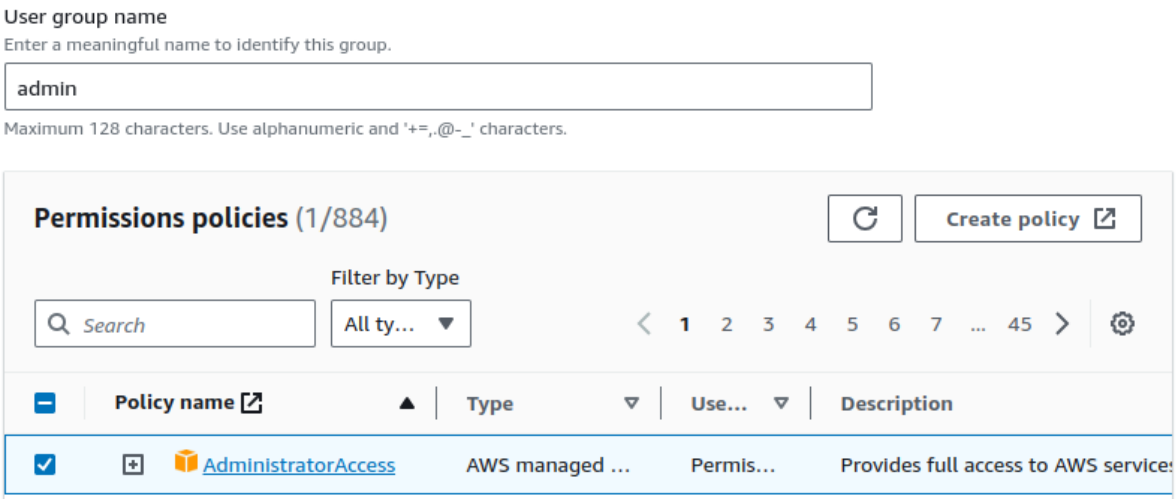
- A global service.
- A service that allows you to create and manage user identities. By doing so, you can control their access to AWS resources.
- These users can be grouped. A group cannot have any sub-groups, only users.
  A single user can be a part of multiple groups or no group (a group can be thought of as a team in your organization).



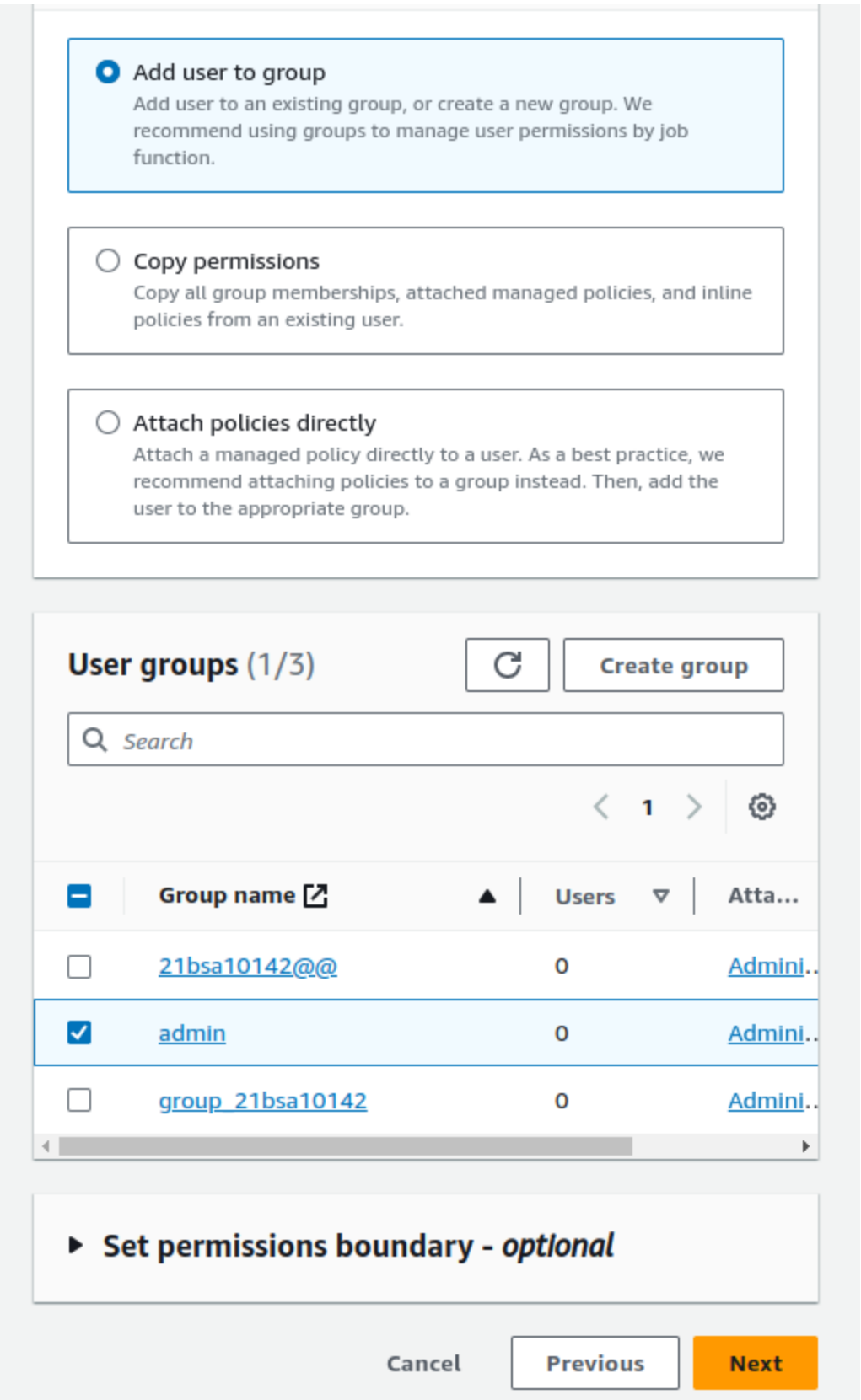
- We create IAM users and groups to allow them access to the organization's AWS account, so they can do their jobs. We do this by allowing a set of permissions to a particular user or a group of users.

Basic IAM hands-on

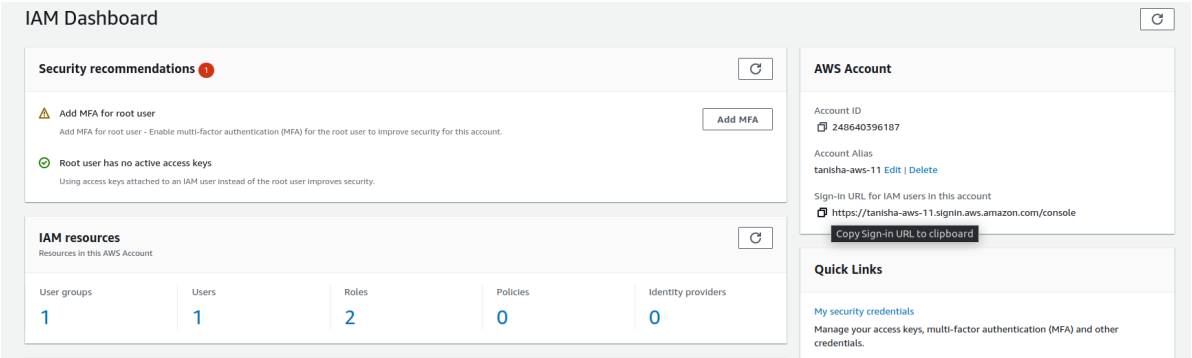
- Created a user
- Created a group and gave access to admin permissions



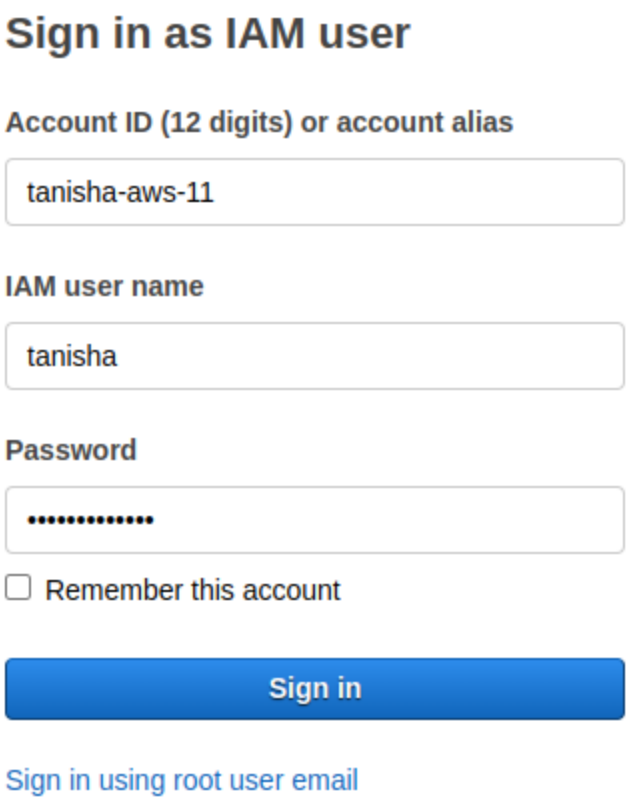
- Added user to the admin group


Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
User groups (1/3)
Create group
Search
1
Group name
Users
Atta...
21bsa10142@@
0
Admini..
admin
0
Admini..
group_21bsa10142
0
Admini..
Set permissions boundary - optional
Cancel
Previous
Next

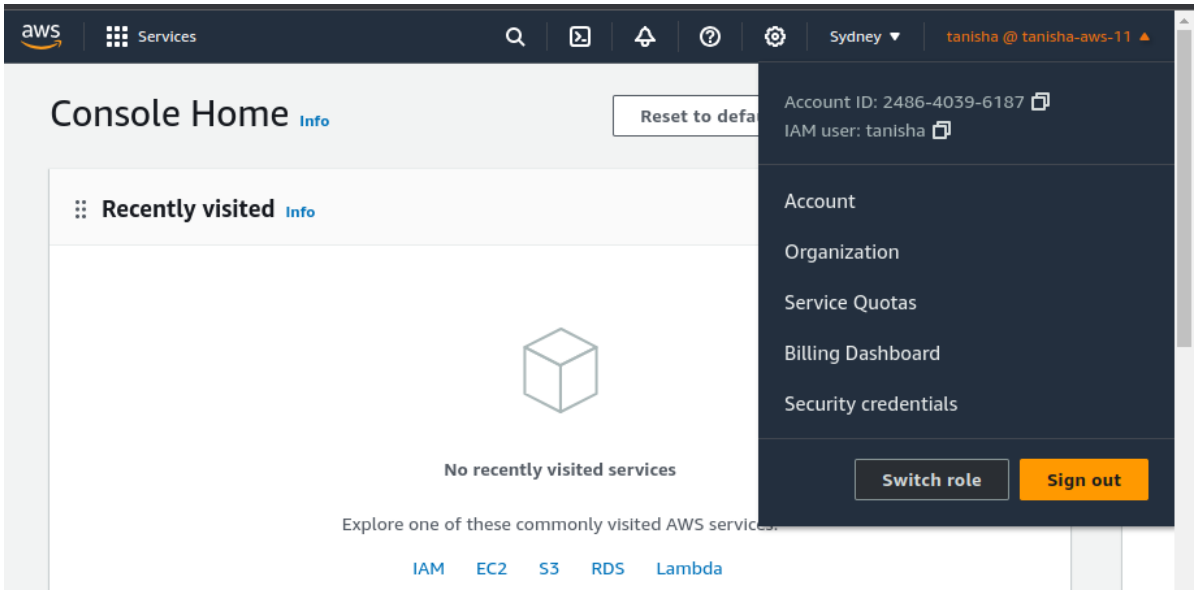
- User created, we can now either email them the signing instructions or download a csv file with username and password.
- **To log in with the user created tanisha:**
  - Copy the sign in URL from the IAM Dashboard.



  - Open this link in either incognito or a different browser. This will take you to the sign in page as an IAM user.



- You are now signed in as an IAM user. Indication is “tanisha @ tanisha-aws-11” which implies tanisha (the IAM user) is using the root account with the alias tanisha-aws-11.



IAM POLICIES

- Policies are in the form of a JSON document which define permissions for the users or groups.
- The **least privilege principle** in AWS allows to keep security intact.

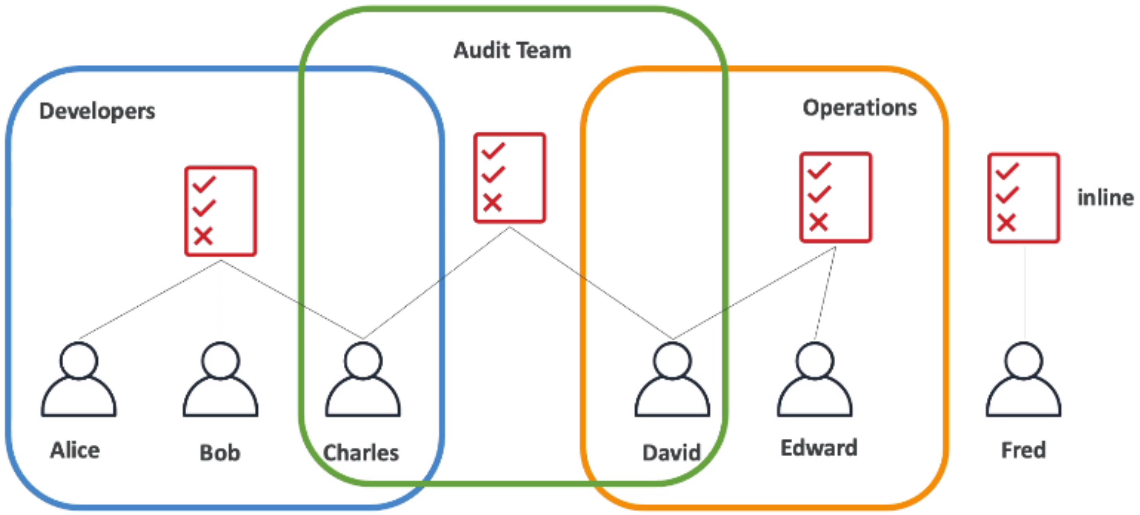
IAM: Permissions

- **Users or Groups** can be assigned JSON documents called policies
- These policies define the **permissions** of the users
- In AWS you apply the **least privilege principle**: don't give more permissions than a user needs

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

- **Inline Policies** are policies that apply to a particular user. That user may or may not be in a group.

IAM Policies inheritance



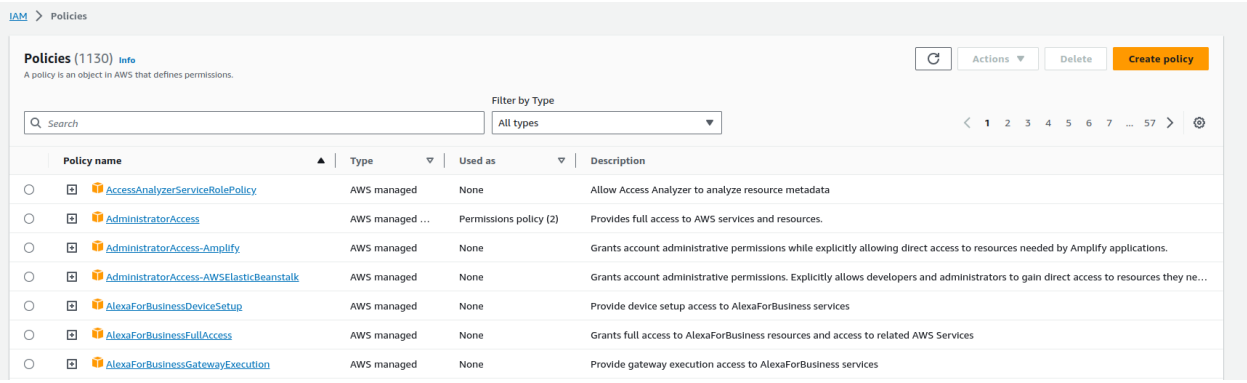
- **Structure of an IAM Policy (the JSON doc):**

- Consists of
  - Version: policy language version, always include "2012-10-17"
  - Id: an identifier for the policy (optional)
  - Statement: one or more individual statements (required)
- Statements consists of
  - Sid: an identifier for the statement (optional)
  - Effect: whether the statement allows or denies access (Allow, Deny)
  - Principal: account/user/role to which this policy applied to
  - Action: list of actions this policy allows or denies
  - Resource: list of resources to which the actions applied to
  - Condition: conditions for when this policy is in effect (optional)

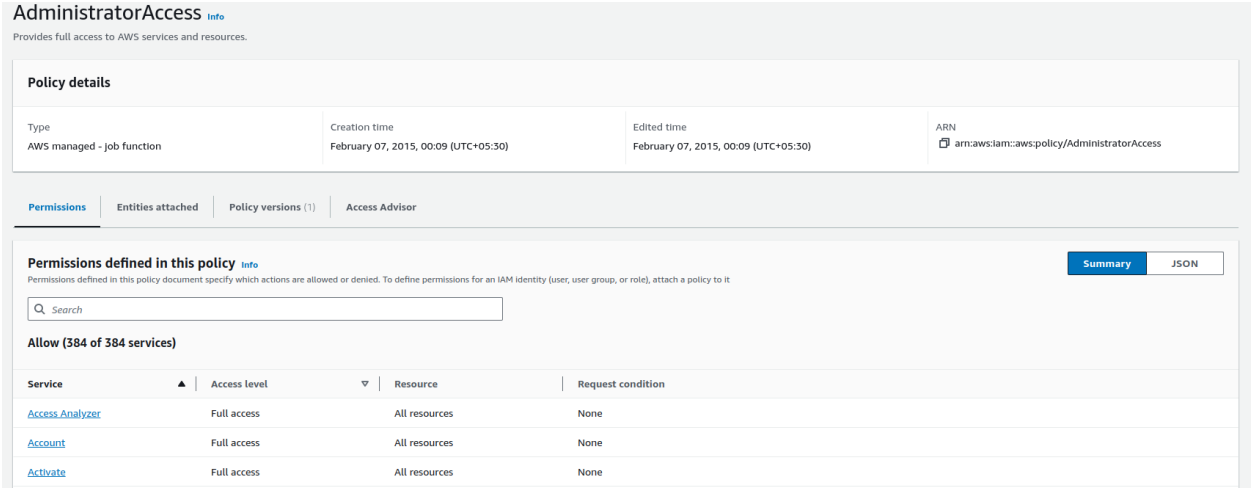
```
{
    "Version": "2012-10-17",
    "Id": "S3-Account-Permissions",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": ["arn:aws:iam::123456789012:root"]
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": ["arn:aws:s3:::mybucket/*"]
        }
    ]
}
```

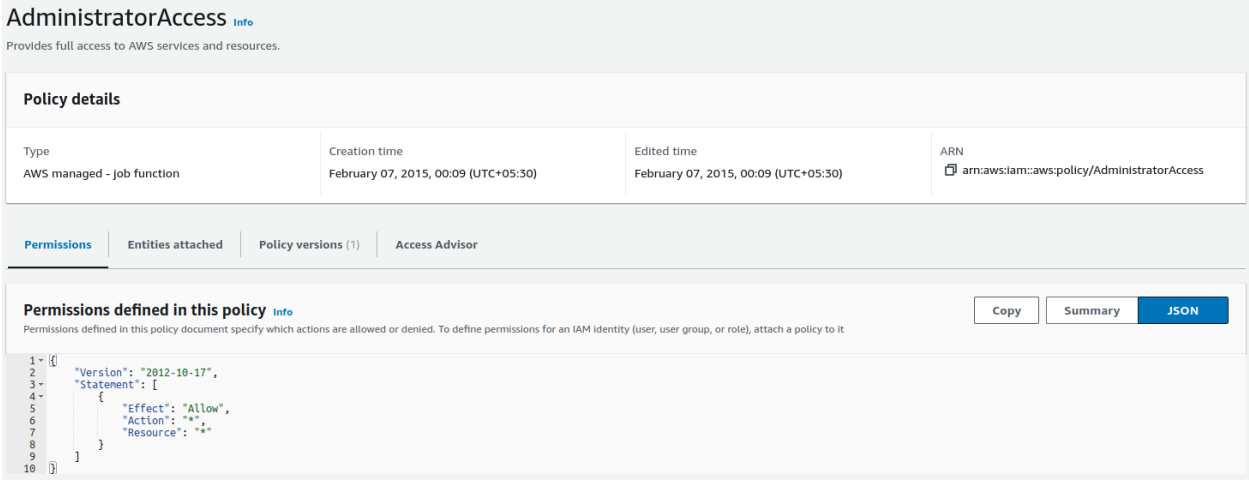
IAM hands-on

- You can create users and groups and assign or revoke permissions of users or remove users from particular groups. This has so much power, I am amazed.
- AWS has a bunch of policies, each with different set of permissions and access to resources.

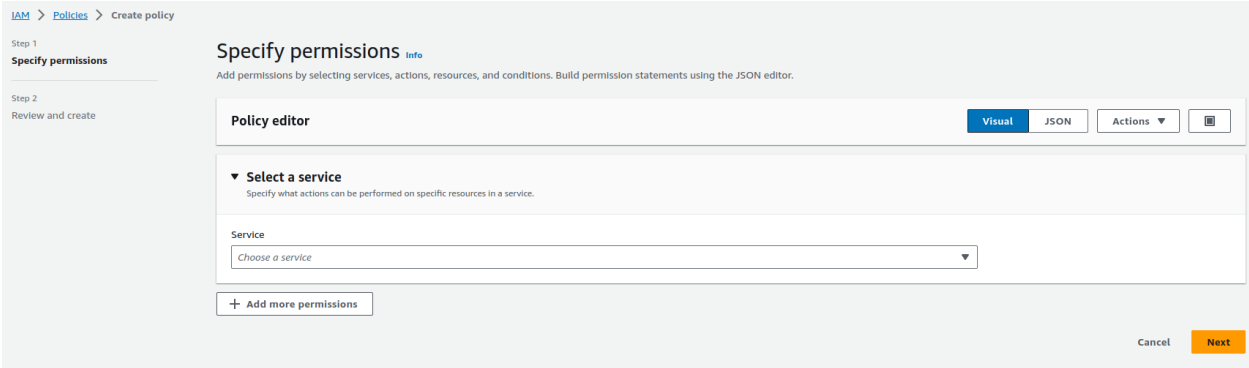


- You can view the set of permissions for any policy either in **summary form or in JSON form.**





- **You can also create your own policy.**



EC2

Set permissions for EC2

Specify what actions can be performed on specific resources in EC2.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

Allow Deny

Manual actions | Add actions

All EC2 actions (ec2:*)

Access level

Expand all | Collapse all

- List (168)
- Read (31)
- Write (406)
- Permissions management (5)
- Tagging (2)

Resources

Specify resource ARNs for these actions.

Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

Cancel Next

Manual actions | Add actions

All EC2 actions (ec2:*)

Access level

Expand all | Collapse all

- List (168)
- Read (Selected 31/31)

All read actions

- ExportClientVpnClientCertificateRevocationList Info
- GetAssociatedIpv6PoolCidrs Info
- GetCoipPoolUsage Info
- GetDefaultCreditSpecification Info
- GetFlowLogsIntegrationTemplate Info
- GetIpamAddressHistory Info
- GetIpamPoolCidrs Info
- GetManagedPrefixListAssociations Info
- GetNetworkInsightsAccessScopeContent Info
- GetResourcePolicy Info
- GetSubnetCidrReservations Info
- ExportClientVpnClientConfiguration Info
- GetAwsNetworkPerformanceData Info
- GetConsoleOutput Info
- GetEbsDefaultKmsKeyId Info
- GetHostReservationPurchasePreview Info
- GetIpamDiscoveredAccounts Info
- GetIpamResourceCidrs Info
- GetManagedPrefixListEntries Info
- GetPasswordData Info
- GetSerialConsoleAccessStatus Info
- GetAssociatedEnclaveCertificateIamRoles Info
- GetCapacityReservationUsage Info
- GetConsoleScreenshot Info
- GetEbsEncryptionByDefault Info
- GetInstanceUefiData Info
- GetIpamDiscoveredResourceCidrs Info
- GetLaunchTemplateData Info
- GetNetworkInsightsAccessScopeAnalysisFindings Info
- GetReservedInstancesExchangeQuote Info
- GetSpotPlacementScores Info

- Write (406)
- Permissions management (5)
- Tagging (2)

Resources

Specify resource ARNs for these actions.

All

▼ Resources

Specify resource ARNs for these actions.

○ All

◉ Specific

capacity-reservation Info	⚠ Specified capacity-reservation resource ARN for the **CancelCapacityReservation** and 8 more actions. Add ARNs to restrict access.	☐ Any in this account
certificate Info	⚠ Specified certificate resource ARN for the **AssociateEnclaveCertificateIamRole** and 2 more actions. Add ARNs to restrict access.	☐ Any in this account
client-vpn-endpoint Info	⚠ Specified client-vpn-endpoint resource ARN for the **ApplySecurityGroupsToClientVpnTargetNetwork** and 20 more actions. Add ARNs to restrict access.	☐ Any in this account
coip-pool Info	⚠ Specified coip-pool resource ARN for the **CreateCoipCidr** and 8 more actions. Add ARNs to restrict access.	☐ Any in this account
instance Info	⚠ Specified instance resource ARN for the **AssociateAddress** and 44 more actions. Add ARNs to restrict access.	☐ Any in this account
ipam-pool Info	⚠ Specified ipam-pool resource ARN for the **AllocateIpamPoolCidr** and 19 more actions. Add ARNs to restrict access.	☐ Any in this account
ipam-resource-discovery Info	⚠ Specified ipam-resource-discovery resource ARN for the **AssociateIpamResourceDiscovery** and 7 more actions. Add ARNs to restrict access.	☐ Any in this account
ipam-scope Info	⚠ Specified ipam-scope resource ARN for the **CreateIpamPool** and 8 more actions. Add ARNs to restrict access.	☐ Any in this account

▼ Resources

Specify resource ARNs for these actions.

◉ All

○ Specific

⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▼ Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

☐ User is MFA Authenticated

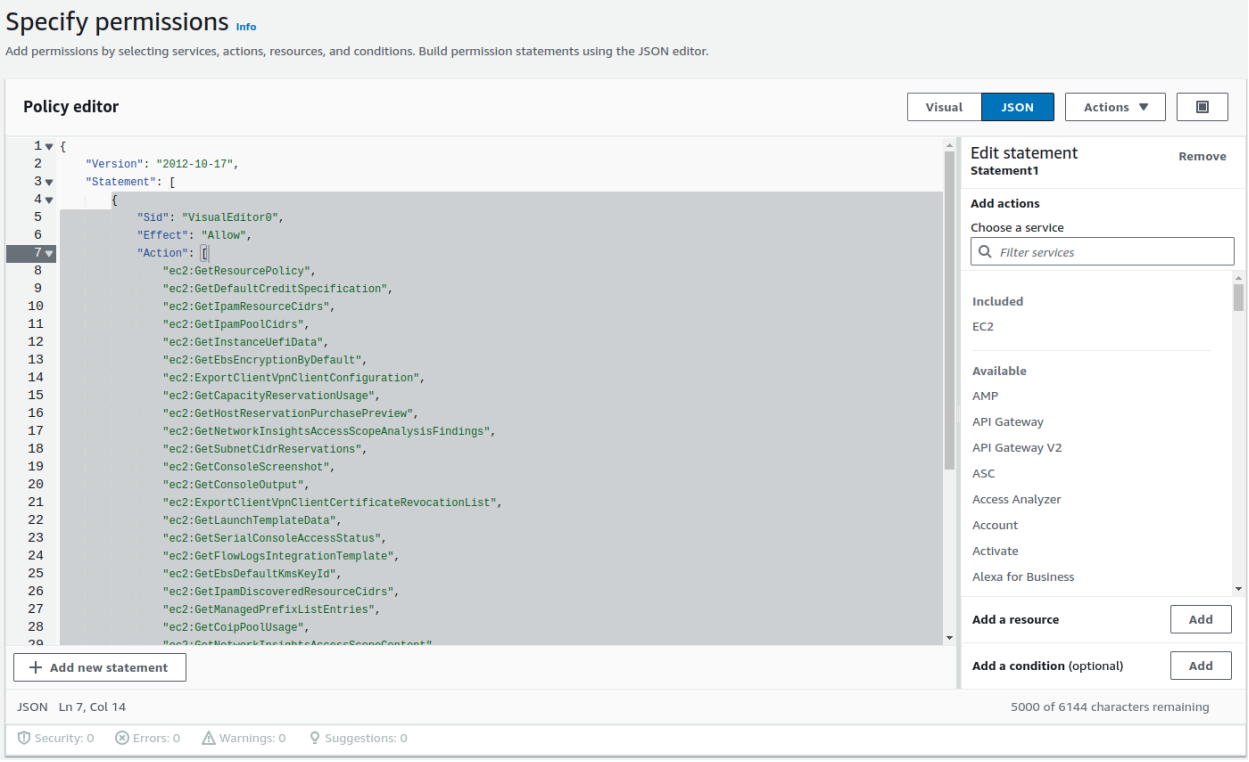
Filters access if MFA was used to validate the temporary security credentials that made the request

☐ Requested from IP

Filters access by the requester's IP address

+ Add another condition

As you keep making changes to the Visual console, the JSON keeps getting updated.



IAM MFA (Multiple Factor Authentication)

Now that we have created users and groups, it is time for us to protect these users and groups from being compromised. So for this we can have two defense mechanisms.

1. **Define a Password Policy**:

IAM – Password Policy

- Strong passwords = higher security for your account
- In AWS, you can setup a password policy:
  - Set a minimum password length
  - Require specific character types:
    - including uppercase letters
    - lowercase letters
    - numbers
    - non-alphanumeric characters
  - Allow all IAM users to change their own passwords
  - Require users to change their password after some time (password expiration)
  - Prevent password re-use

2. **MFA (Multiple Factor Authentication)**
   - With IAM, users have access to your account and they can possibly change configurations or delete resources or simply mess up, especially the ones with admin access.
   - So, it is advised to protect your root account and all IAM user accounts with MFA.

- MFA = password *you know* + security device *you own*

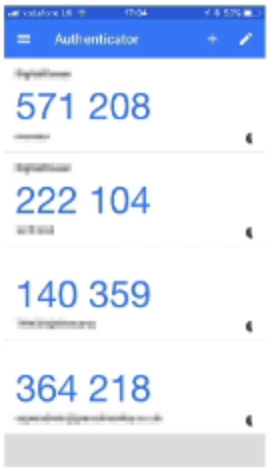
- Main benefit of MFA:
  <u>if a password is stolen or hacked, the account is not compromised</u>

- **MFA DEVICE OPTIONS YOU HAVE:**
  1. **Virtual MFA Device**:

Supports multiple tokens on a single device. You can have as many users and accounts as you want on your MFA device which make it super handy. This is basically an app or a web app on your device. Commonly used are:

i. **Google Authenticator (only on phone)**

ii. **AWS Authy (on multiple devices)**



Google Authenticator
(phone only)

Authy
(multi-device)

2. **U2F (Universal 2 Factor) Security Key**

   It is a physical device that you can just plug in and access your accounts. For example, a **YubiKey** by Yubico (3rd party). This YubiKey supports multiple root and IAM users so you don't need as many keys as the users (thankfully).

YubiKey by Yubico (3rd party)

3. Other devices are:

Hardware Key Fob MFA Device

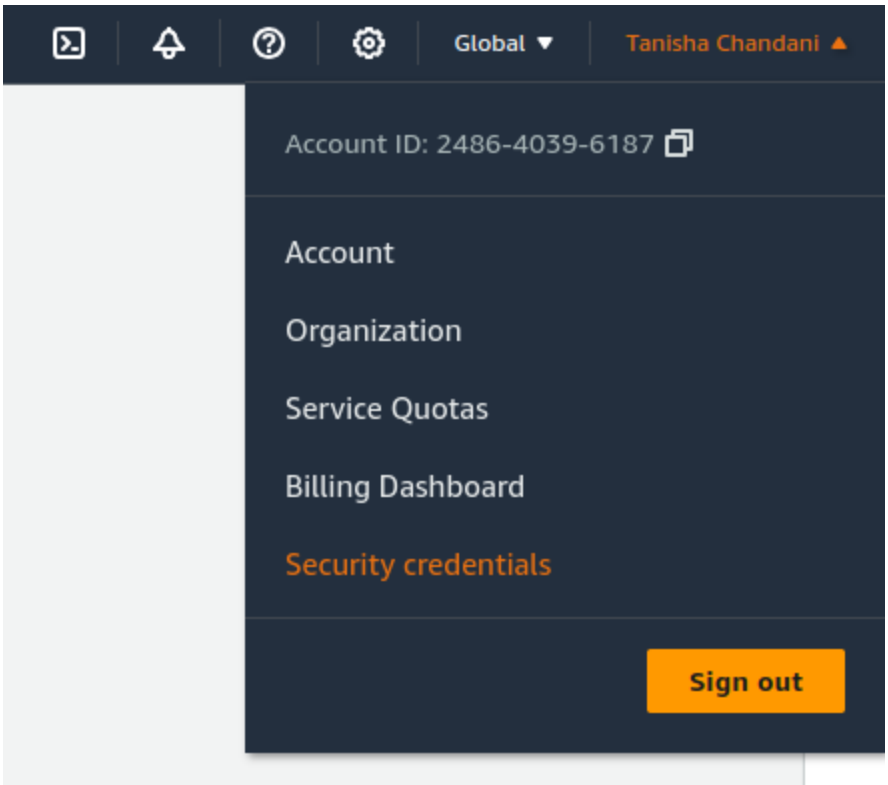
Provided by Gemalto (3rd party)

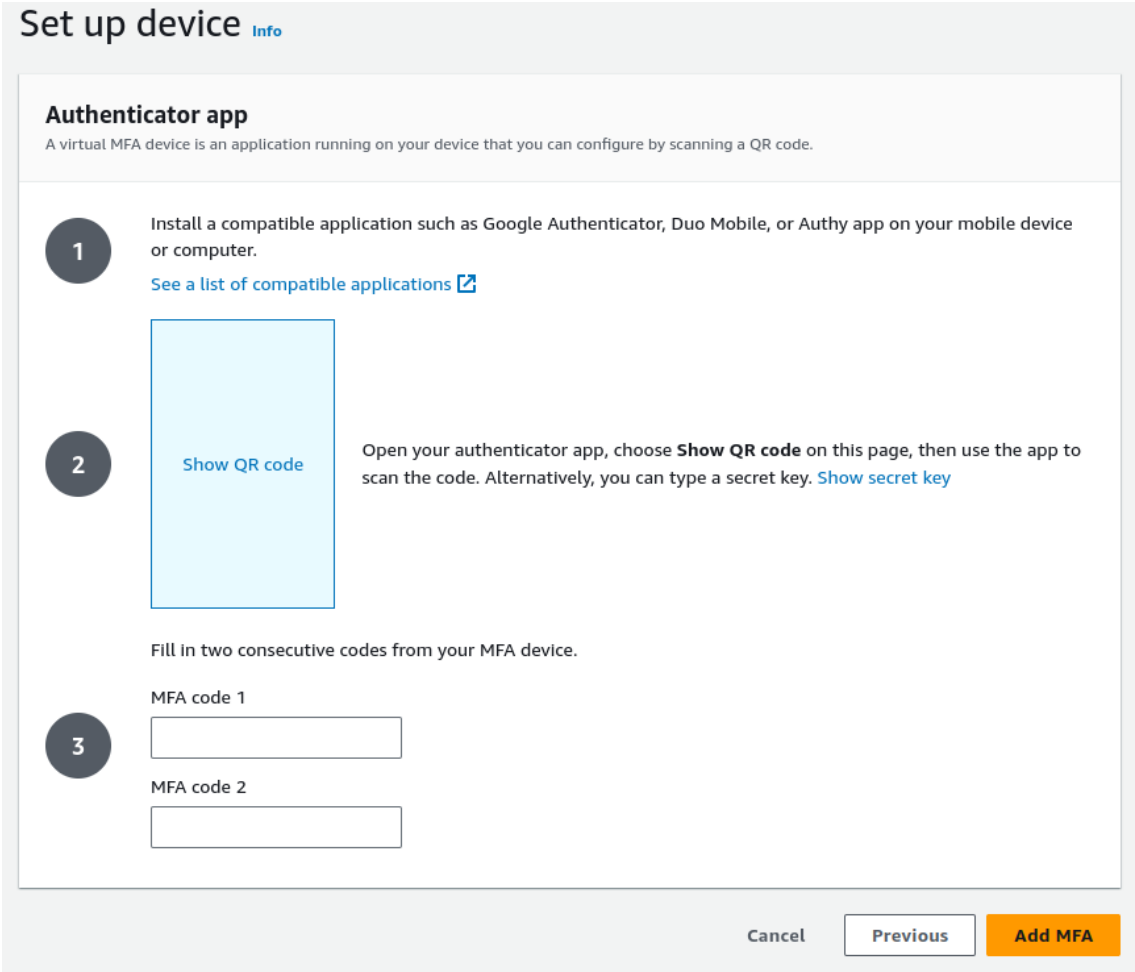
Hardware Key Fob MFA Device for AWS GovCloud (US)

Provided by SurePassID (3rd party)

IAM MFA hands-on

- You need to download an external app on your phone to set it up.
- You can set up MFA on your phone if you are a root user. It adds an extra layer of protection. It is recommended to set it up on multiple devices so you don't get locked out of your aws account if you lose your device.
- The steps are pretty simple.


Global
Tanisha Chandani
Account ID: 2486-4039-6187
Account
Organization
Service Quotas
Billing Dashboard
Security credentials
Sign out



Different ways users can access AWS

You got 3 ways:

1. **AWS Console** - the simplest way, more time taking as compared to the rest, protected by a password and MFA.
2. **AWS CLI (Command Line Interface)** - access aws using your terminal, protected by access keys.
3. **AWS SDK (Software Development Kit)** - is used whenever you want to call APIs from AWS from within your application code, protected by access keys.

- **Access keys** can be generated through the AWS console. An access key can be thought of as your password, so, don't share it.

Example (Fake) Access Keys

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. Learn more

Create access key

Access key ID	Created	Last used	Status	
AKIASK4E37PV4TU3RD6C	2020-05-25 15:13 UTC+0100	N/A	Active | Make inactive	✖

- **AWS CLI:**

  - A tool that enables you to interact with AWS services using commands in your command-line shell
  - Direct access to the public APIs of AWS services
  - You can develop scripts to manage your resources
  - It's open-source https://github.com/aws/aws-cli
  - Alternative to using AWS Management Console

```
➜  ~ aws s3 cp myfile.txt s3://ccp-mybucket/myfile.txt
upload: ./myfile.txt to s3://ccp-mybucket/myfile.txt
➜  ~ aws s3 ls s3://ccp-mybucket
2021-05-14 03:22:52          0 myfile.txt
➜  ~
```

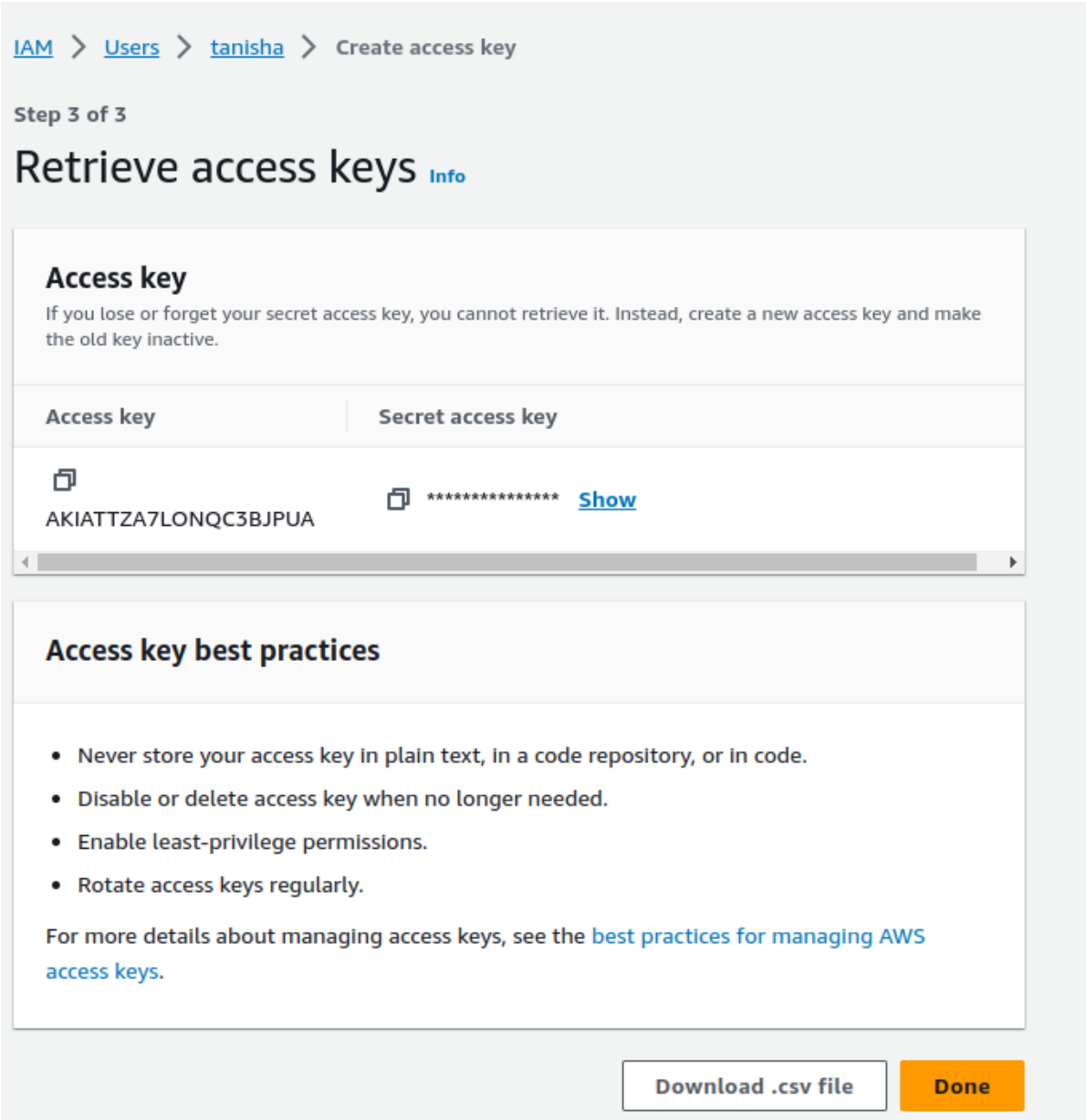
- **AWS SDK:**

  - AWS SDKs are language specific APIs that enable you to manage and access aws services programmatically. **You can embed the SDK within your application's code.**

- Supports
  - SDKs (JavaScript, Python, PHP, .NET, Ruby, Java, Go, Node.js, C++)
  - Mobile SDKs (Android, iOS, …)
  - IoT Device SDKs (Embedded C, Arduino, …)

AWS CLI Hands-on

1. Create an access key for a user.



2. Go to your terminal / CLI, follow commands below to configure your access key.

```
meowmeow@tanishas-penguin:~$ aws configure
AWS Access Key ID [None]: AKIATTZA7LONQC3BJPUA
AWS Secret Access Key [None]: s2479P3eZbgNjD9vs3vFDTKtESXYOrnPYWDiQmIw
Default region name [None]: ap-south-1
Default output format [None]:
```

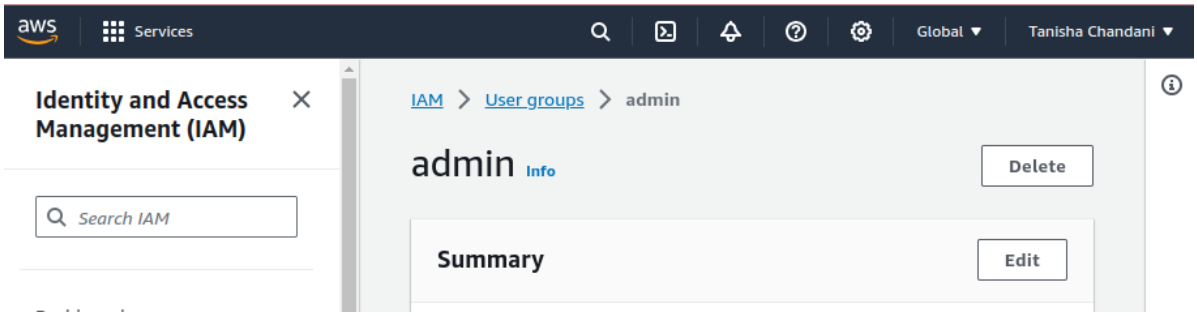
3. It is now configured. You can use your CLI for the user. For example, let's fetch the list of users.

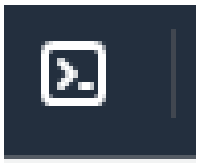
```
meowmeow@tanishas-penguin:~$ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "tanisha",
            "UserId": "AIDATTZA7LONUEYGIGVBB",
            "Arn": "arn:aws:iam::248640396187:user/tanisha",
            "CreateDate": "2023-10-18T08:12:23+00:00",
            "PasswordLastUsed": "2023-11-02T13:13:47+00:00"
        }
    ]
}
```

4. Conclusion: this is how you can use AWS using your CLI, with some commands. Once you configure your CLI (with your access key and secret access key), you can then simply access your whole aws account using the CLI.

AWS CloudShell Hands-on

- An alternative to using the CLI.

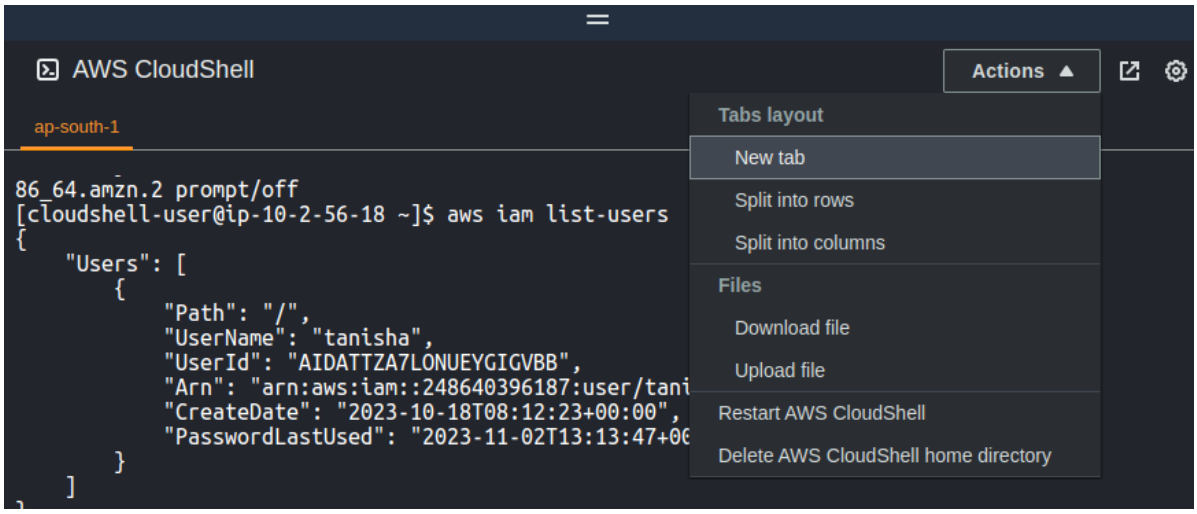




this icon is for cloudshell

- Cloudshell is not a global service. It is only available in some regions.

- You can explore cloudshell and its commands to access the console through it. Its pretty dope and convenient.

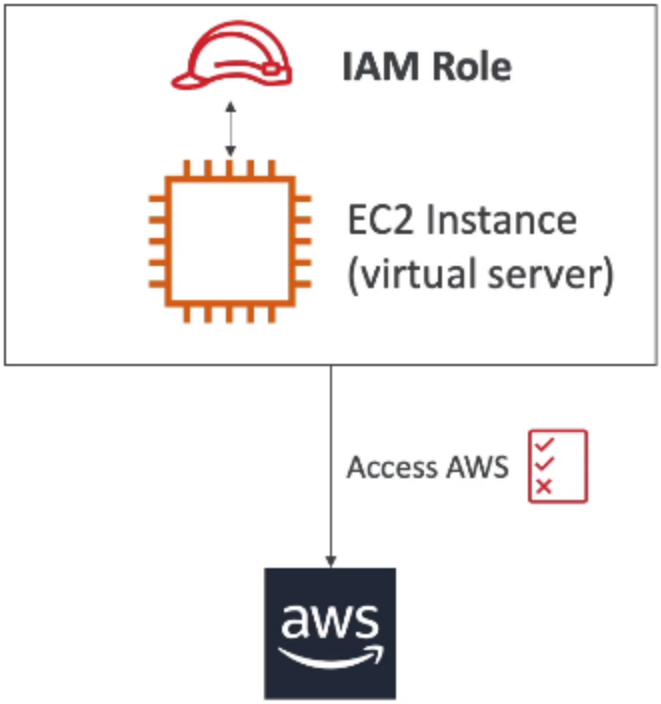


IAM Roles

- Sometimes, some AWS services will need to perform actions on your behalf, using your account. For which, we assign IAM roles to these services.
- It is similar to assigning permissions to users but this is for AWS services and not actual people.

- Common roles:
  - EC2 Instance Roles
  - Lambda Function Roles
  - Roles for CloudFormation

- For example, an EC2 server might need some permissions to access info or data. So, we will assign IAM Role to that EC2 server allowing it to do so, and when it does try to access AWS can check the permissions in IAM role and proceed to give access only if it's allowed.



IAM Roles Hands-on

- For exam, you need to know how to create an IAM role for a particular AWS service.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

- (●) **AWS service**
  Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ( ) **AWS account**
  Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ( ) **Web identity**
  Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ( ) **SAML 2.0 federation**
  Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ( ) **Custom trust policy**
  Create a custom trust policy to enable others to perform actions in this account.

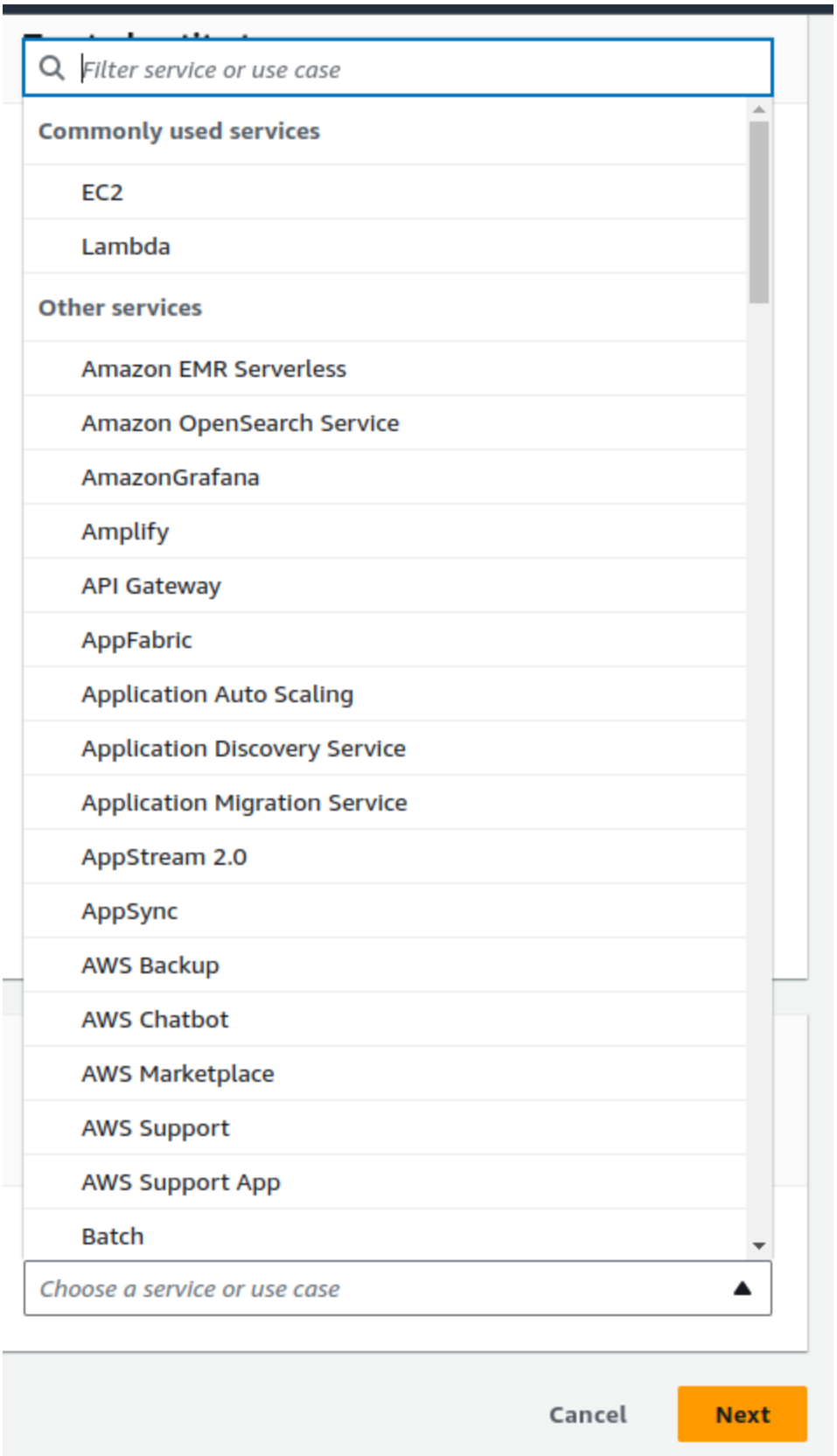
Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

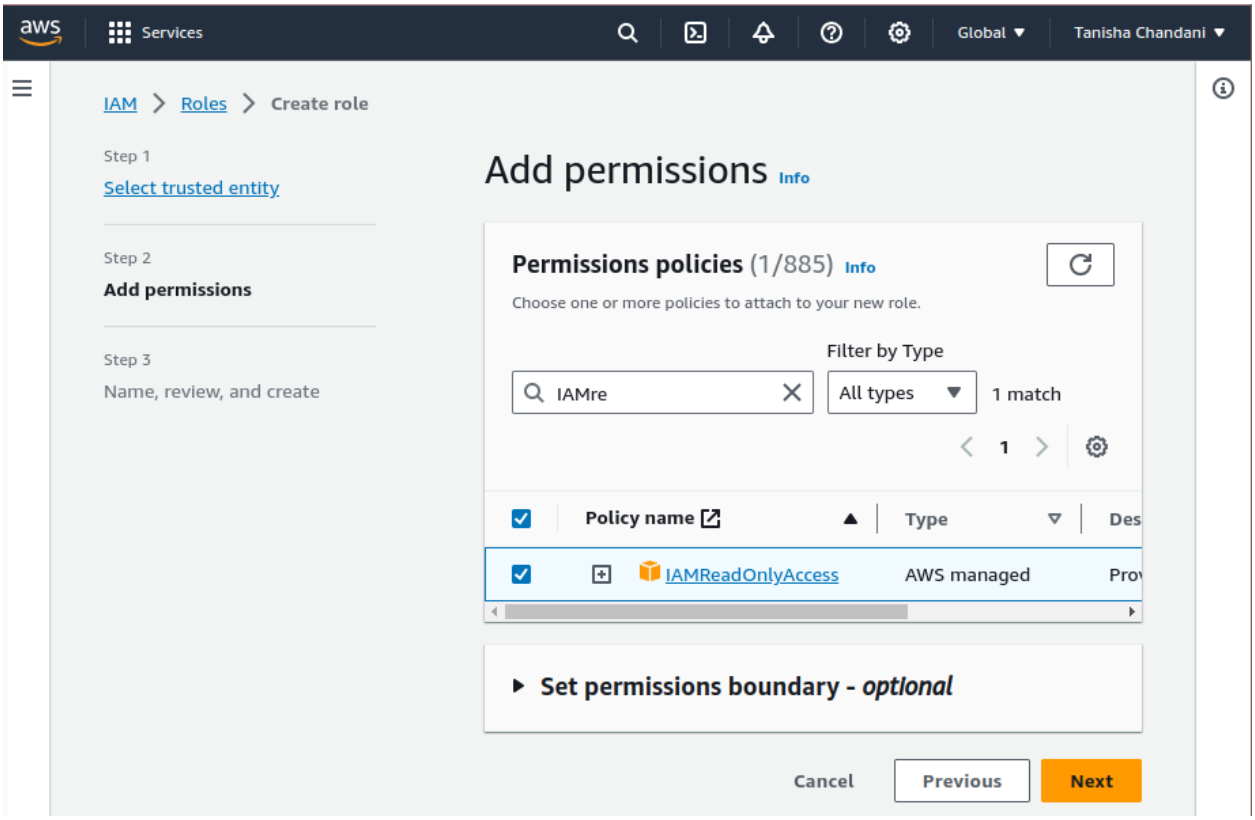
Service or use case

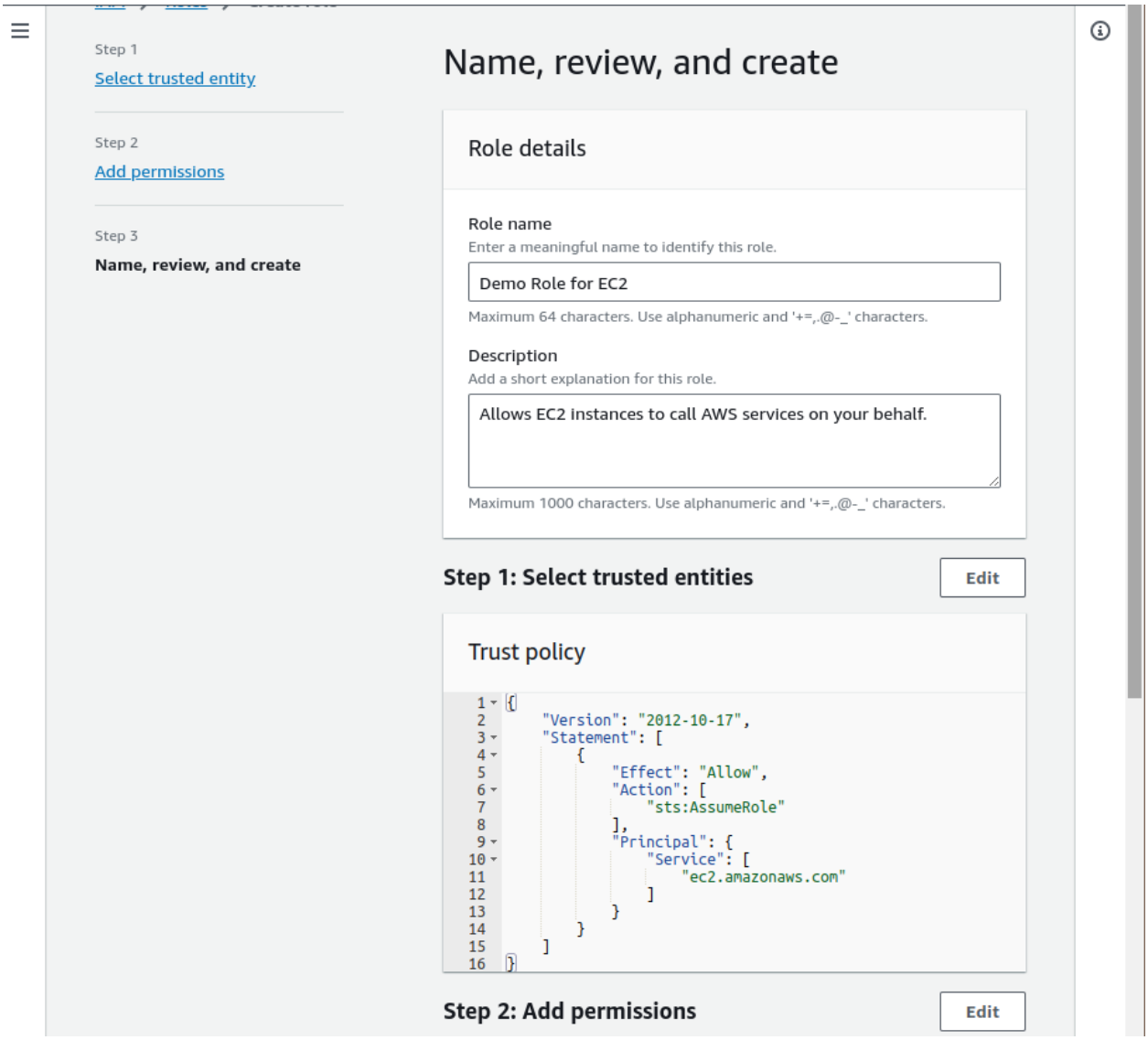
Choose a service or use case ▼

Cancel **Next**


Filter service or use case
Commonly used services
EC2
Lambda
Other services
Amazon EMR Serverless
Amazon OpenSearch Service
AmazonGrafana
Amplify
API Gateway
AppFabric
Application Auto Scaling
Application Discovery Service
Application Migration Service
AppStream 2.0
AppSync
AWS Backup
AWS Chatbot
AWS Marketplace
AWS Support
AWS Support App
Batch
Choose a service or use case
Cancel
Next

- Now that we have selected EC2, we are going to add permissions. For now, we have selected IAMReadOnlyAccess permission to enable the instance to read whatever is in IAM.





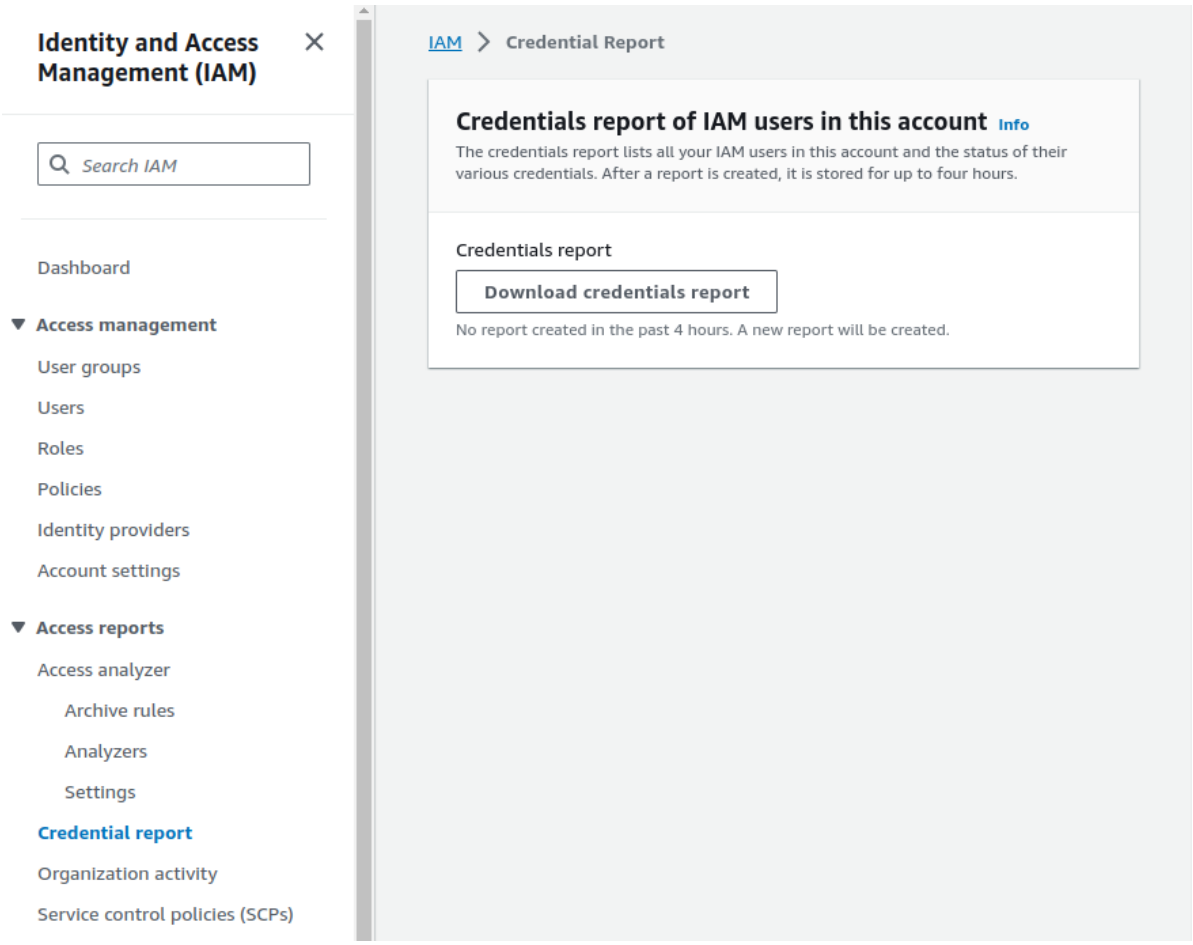
IAM Security Tools

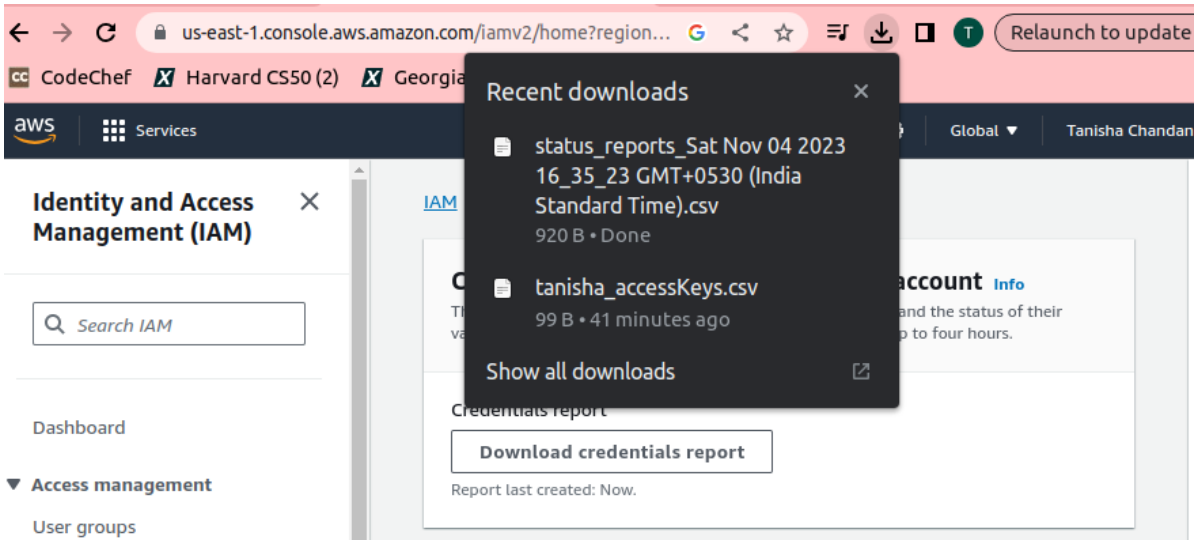
IAM Security Tools

- IAM Credentials Report (account-level)
  - a report that lists all your account's users and the status of their various credentials
- IAM Access Advisor (user-level)
  - Access advisor shows the service permissions granted to a user and when those services were last accessed.
  - You can use this information to revise your policies.

IAM Security Hands-on

1. Credentials Report


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > Credential Report
Credentials report of IAM users in this account Info
The credentials report lists all your IAM users in this account and the status of their various credentials. After a report is created, it is stored for up to four hours.
Credentials report
Download credentials report
No report created in the past 4 hours. A new report will be created.


us-east-1.console.aws.amazon.com/iamv2/home?region...
Relaunch to update
CodeChef
Harvard CS50 (2)
Georgia
Recent downloads
status_reports_Sat Nov 04 2023 16_35_23 GMT+0530 (India Standard Time).csv
920 B • Done
tanisha_accessKeys.csv
99 B • 41 minutes ago
Show all downloads
aws
Services
Global
Tanisha Chandan
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
IAM
Download credentials report
Report last created: Now.

Column type:

	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard
1	user	arn	user_creation_time	password_enabled	password_last_used	password_last_changed	password_next_rotation	mfa_active	access_key_1_ac
2	<root_account>	arn:aws:iam::248640396187:root	2023-06-15T06:56:05+00:00	not_supported	2023-11-04T10:01:01+00:00	not_supported	not_supported	false	false
3	tanisha	arn:aws:iam::248640396187:user/tanisha	2023-10-18T08:12:23+00:00	true	2023-11-02T13:13:47+00:00	2023-10-18T08:12:24+00:00	N/A	false	true

You can use this report to monitor all the user activities. It contains information of all the users (from transcript of the lecture: This report provides comprehensive insights into user account details, including the user's creation date, password status (enabled or disabled), the last usage and change of the password, and the anticipated next password rotation if enabled. It also checks for the activation of Multi-Factor Authentication (MFA) and the status of access keys, whether they have been generated and their last rotation or usage. Moreover, it allows you to access additional information about other access keys and certificates. This report proves invaluable for identifying users who have not recently updated their passwords or utilized their accounts, aiding in pinpointing potential security concerns that require immediate attention.)

2. Access advisor

IAM > Users > tanisha

tanisha Info

Delete

Summary

ARN
arn:aws:iam::248640396187:user/tanisha

Console access
Enabled without MFA

Access key 1
Create access key

Created
October 18, 2023, 13:42 (UTC+05:30)

Last console sign-in
Yesterday

oups (1) | Tags | Security credentials | Access Advisor

Access Advisor shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn More

Allowed services (366)

IAM reports activity for services and management actions. Learn more about action last accessed information. To see actions, choose the appropriate service name from the list.

Filter by services access history

Search | No Filter

1 2 3 4 5 6 7 ... 37

Service	Policies granting ...	Last accessed
AWS Identity and ...	AdministratorAccess	Today
AWS Health APIs ...	AdministratorAccess	Yesterday
AWS User Notifica...	AdministratorAccess	2 days ago
Amazon EC2	AdministratorAccess	2 days ago
AWS Cost Explore...	AdministratorAccess	2 days ago
AWS Organizations	AdministratorAccess	17 days ago
AWS App2Container	AdministratorAccess	Not accessed in th...
Alexa for Business	AdministratorAccess	Not accessed in th...
AWS IAM Access A...	AdministratorAccess	Not accessed in th...
AWS Account Man...	AdministratorAccess	Not accessed in th...

Access Advisor is going to show me which services were accessed by my user and when.

IAM Best Practices

- Don't use the root account except for AWS account setup
- One physical user = One AWS **user**
- **Assign users to groups** and assign permissions to groups
- Create a **strong password policy**
- Use and enforce the use of **Multi Factor Authentication (MFA)**
- Create and use **Roles** for giving permissions to AWS services
- Use Access Keys for Programmatic Access (CLI / SDK)
- Audit permissions of your account using IAM Credentials Report & IAM Access Advisor
- Never share IAM users & Access Keys

Shared Responsibility Model in AWS

- Imp for exam
- This is for awareness, it make sure you know what you are responsible for and what AWS is responsible for.
- AWS is basically responsible for all the infrastructure and you are responsible for HOW you choose to use that infrastructure.

- Infrastructure (global network security)
- Configuration and vulnerability analysis
- Compliance validation

You

- Users, Groups, Roles, Policies management and monitoring
- Enable MFA on all accounts
- Rotate all your keys often
- Use IAM tools to apply appropriate permissions
- Analyze access patterns & review permissions

Concluding

IAM Section – Summary

- **Users:** mapped to a physical user, has a password for AWS Console
- **Groups:** contains users only
- **Policies:** JSON document that outlines permissions for users or groups
- **Roles:** for EC2 instances or AWS services
- **Security:** MFA + Password Policy
- **AWS CLI:** manage your AWS services using the command-line
- **AWS SDK:** manage your AWS services using a programming language
- **Access Keys:** access AWS using the CLI or SDK
- **Audit:** IAM Credential Reports & IAM Access Advisor