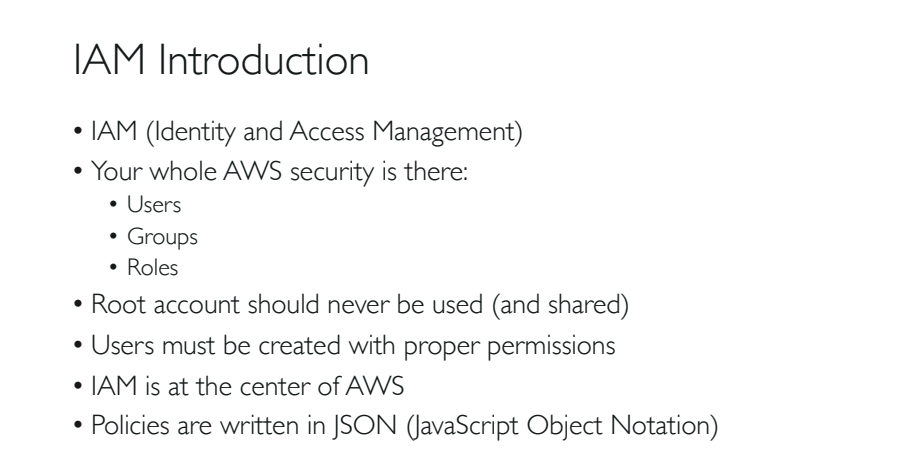
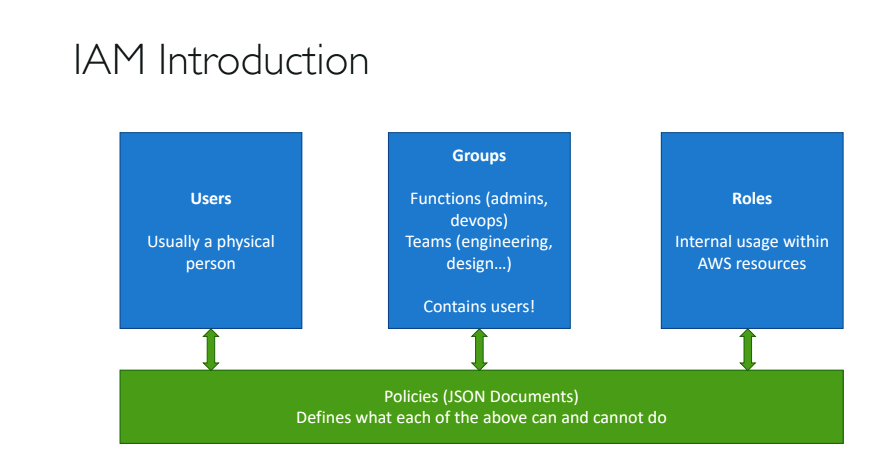
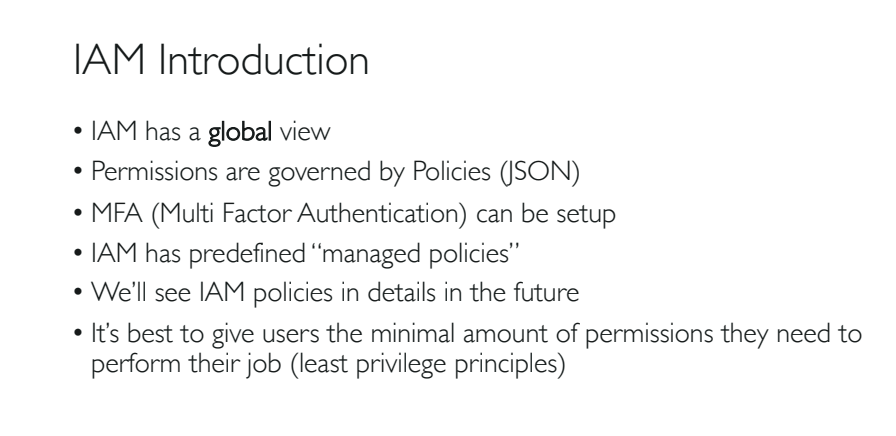
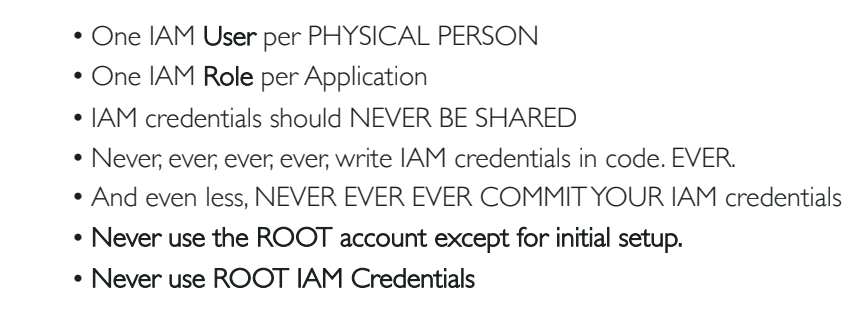
IAM (Identity and Access Management)





1. User account is a physical independent account.
2. One or more users can be grouped together are called Groups. Usually in groups there can be members by their functions(admins, devops engineers etc) or teams(engineering, design etc). Admin can give permission to groups and users(members) of groups will inherit these permissions.
3. Roles are internal usage within AWS resources. Roles are given to machines.
4. All the above IAM users, roles and users are given with permissions using ‘JSON documents.
5. In JSON documents we can give permission or cancel a permission using policies.





Hands on with IAM:

* IAM dosent require any region selection.
* Search and select the service IAM and select ‘Users’ in the left side of the ‘IAM Dash Board’.
* Select ‘Add Users’.
* Provide ‘user name’ , check ‘Password’ option and then select ‘ Custom password’. Finally click ‘Next’.
* In ‘Set Permissions’ window, select ‘Add user to group’ , if there is no group then select ‘create a group’.
* Provide group name like ‘admin’
* NOTE: any user placed in the admin group will inherit the permissions associated with that group.
* In ‘Filter policies’ option select ‘AdministratorAccess’ policy. Finally select ‘Create Group’.
* Click ‘Next:Tags’ button.
* Providing tags is optional. Next click on ‘Review’ button.
* Go through the user details and then finally click ‘Create user’ . This will create you the user account.

NOTE: You will get a button ‘Download.csv’. by click it will download your users account credentials to a .csv file.

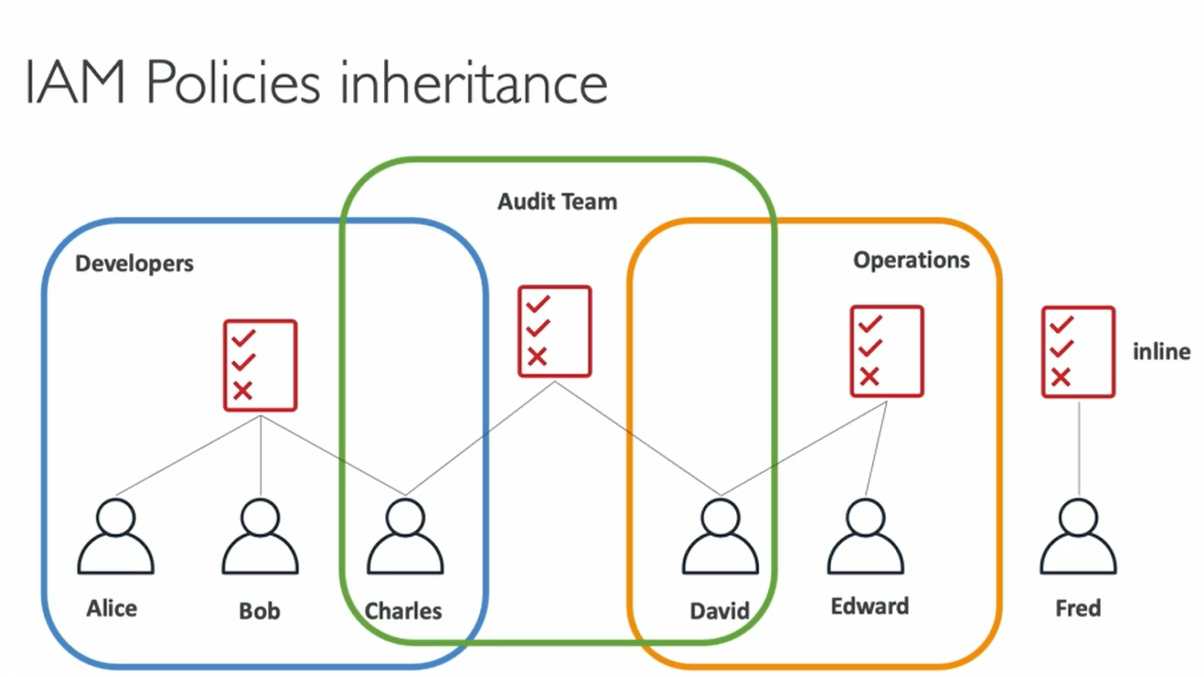
Or you can even have a link to email your IAM login instructions for some one else.

1. On left hand side go to ‘User Groups’ , find the user group ‘admin’ and click on it.
2. There you can find one user with the given while creating the user.
3. Go to ‘permissions’ you can find the policy name attached to the group.
4. If you click on the username, you can see the user permissions.

Creating Account Alias:

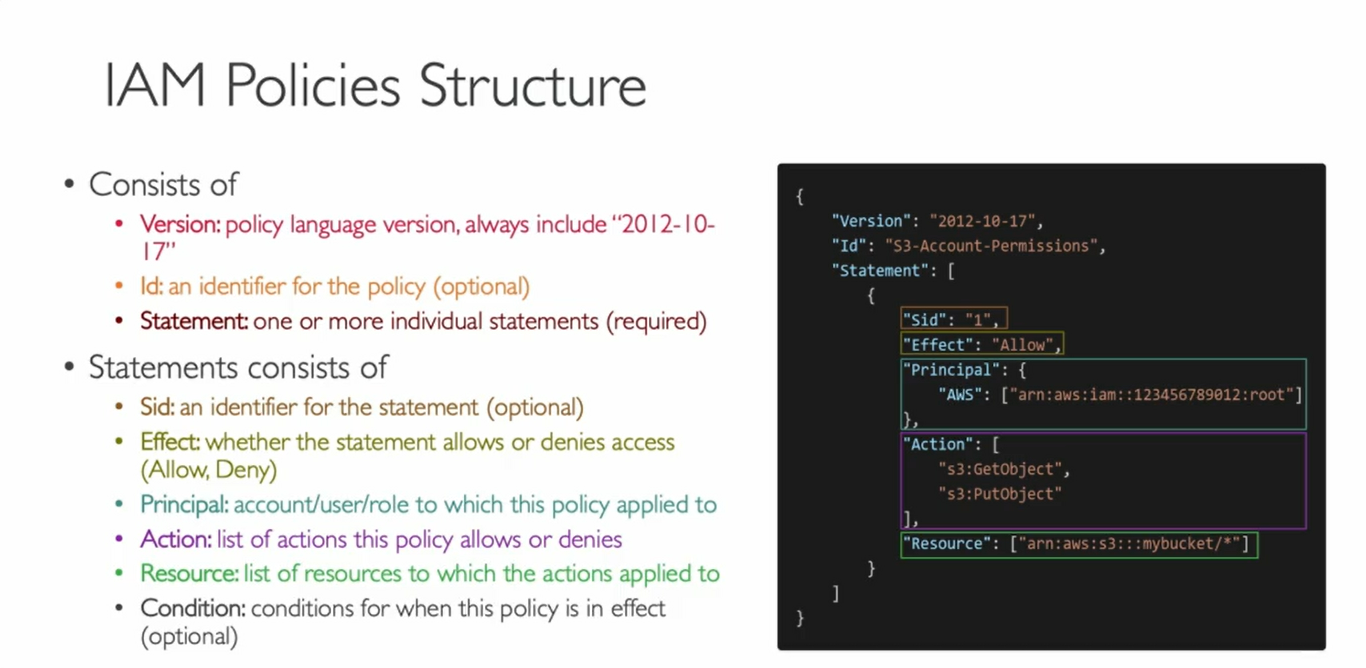
1. Go back to the ‘Dashboard’ on left side.
2. Under ‘AWS account’ on right side, you can find your account ID
3. Under ‘Account Alias’, next to your user id you have a link named ‘Create’.
4. Click that link to create account alias. Provide a name without spaces and click ‘Save Changes’.
5. Now you have your account alias created.
6. Back to the ‘AWS account’, on right side, you can also find sign-in URL that is customised for your alias account.
7. Copy that URL, open an incognito tab or a new browser, paste the URL and press enter.
8. Now you can directly login to your login page of the IAM account.

IAM Policies:



1. Alice, Bob and Charles are three group of developers, and we attach a policy at the group level.
2. In such case all the three members get access and inherit this policy.
3. There is another second group of Operations with different policy with David and Edward as members.
4. If Fred is a user, and he doesn’t belong to a group and he has an ‘inline’ policy which is only attached to the Fred(user).
5. A user could or couldn’t belong to a group can get ‘inline’ policies.
6. If Charles and David both belong to ‘Audit Team’ which has a different policy, then Charles and David will also inherit policies from ‘Audit Team’.
7. So, in such case Charles has a policy from Developers and Audit Team, whereas David has a policy from Operations and Audit Team.

IAM Policies Structure:



IAM Policies Lab:

1. Go to IAM Dashboard in IAM root account.
2. Select ‘User Groups’ , click group name for ex: admin
3. You can see the no of users in that group.
4. If you login as a user account and repeat the above three steps then you can also see the users.
5. If you select ‘your user’ and click ‘Remove User’ button from root account.
6. You will see the user will be gone in root account, and you will get an error message saying ‘You need permissions’ in user account.
7. To fix the above error, go to User in your root account, click the user link, you will find a button to ‘Add permissions’ to the user.
8. Select ‘Add permissions’ or click ‘Add inline policy’ link.
9. If you select ‘Add permissions’ then select ‘Attach existing policies directly’ option.
10. In ‘Filter Policies’ search for ‘IAM’ and select ‘IAMReadOnlyAccess’ check box.
11. ‘Review’ and ‘Add Permissions’.
12. Now your user account has only readonly permissions. Check in the user account.
13. Means if user tries to create a new group from ‘User Groups’, ‘Create Group’ than , that user will not have any permissions to create one.

Resetting you IAM policies back to normal:

1. From root account go to IAM dashboard.
2. Select ‘User Groups’.
3. Select the available group link. Ex: admin
4. Click ‘Add Users’ button.
5. Select the user and click ‘Add Users’ button.
6. Also create a new group called ‘developers’ for example , and add the user, add any policy for the user and than to the ‘developer’ group.
7. Now you will have two groups. Ex admin and developer
8. User will be in both the groups.
9. Click on the user link and you can see the polices available for the user.

How Policies Work:

1. On IAM Dashboard, go to ‘Policies’.
2. You can see all the policies available within AWS.
3. Click on ‘Administrator Access’ policy.
4. You can see the JSON code.
5. Also check ‘IAMReadOnlyPolicy’ . Check the JSON document.

NOTE: Any time you can create your own policy.

How to create User-Defined Pollicy:

1. On IAM Dashboard, go to ‘Policies’.
2. Click on ‘Create Policy’.
3. Either you can use ‘Visual Editor’ or plain JSON document to create the policy.
4. In Visual Editor, search service like IAM, in action type ‘ListUser’ select, and also select ‘GetUser’ and so on you can select.
5. And in ‘Resources’ option you can select ‘Specific’ or ‘All Resources’.
6. Now go to JSON document and you can see the updated policy.
7. If you want you can cancel the Policy creation any time.

Setting your IAM account clean and back to normal:

1. Go to ‘User Groups’ and delete developer group, cause we don’t need to.
2. Go to ‘Users’ , click the link user , and press the cross(x) button to remove the policy.
3. Now your user account has full administrator accesses, because it is inherited from the admin group.
4. Check in you IAM console.