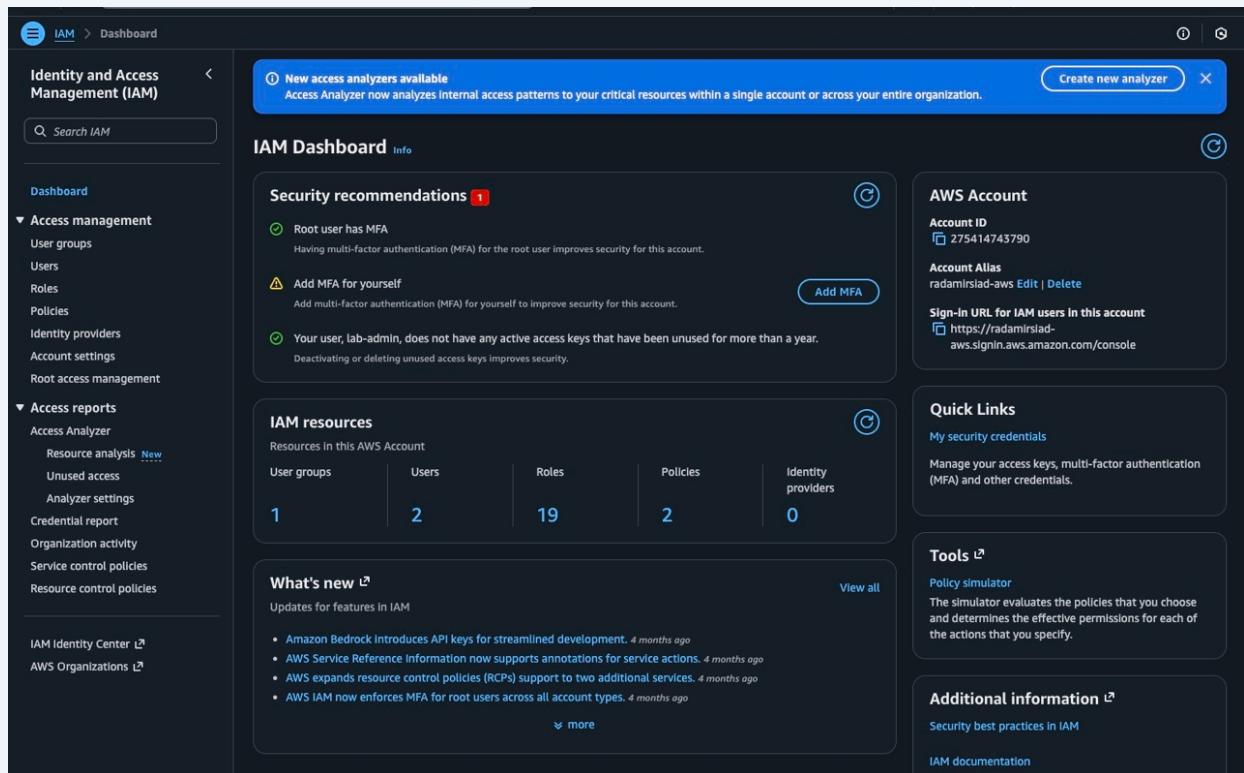


Provisioning/Deprovisioning AWS user groups using PowerShell scripts

Scribe 

1

Navigate to <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/home>



The screenshot shows the AWS IAM Dashboard. On the left, a sidebar navigation includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), 'Access reports' (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies, Resource control policies), 'IAM Identity Center', and 'AWS Organizations'. The main content area has a blue header bar with a message about new access analyzers available. Below it, the 'IAM Dashboard' section displays 'Security recommendations' (Root user has MFA, Add MFA for yourself, Your user, lab-admin, does not have any active access keys that have been unused for more than a year), 'AWS Account' (Account ID: 275414743790, Account Alias: radamirsad-aws, Sign-in URL: https://radamirsad-aws.signin.aws.amazon.com/console), 'IAM resources' (User groups: 1, Users: 2, Roles: 19, Policies: 2, Identity providers: 0), 'What's new' (Amazon Bedrock introduces API keys for streamlined development, AWS Service Reference Information now supports annotations for service actions, AWS expands resource control policies (RCPs) support to two additional services, AWS IAM now enforces MFA for root users across all account types), 'Quick Links' (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials), 'Tools' (Policy simulator, The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify), and 'Additional information' (Security best practices in IAM, IAM documentation).

2 Click "Policies"

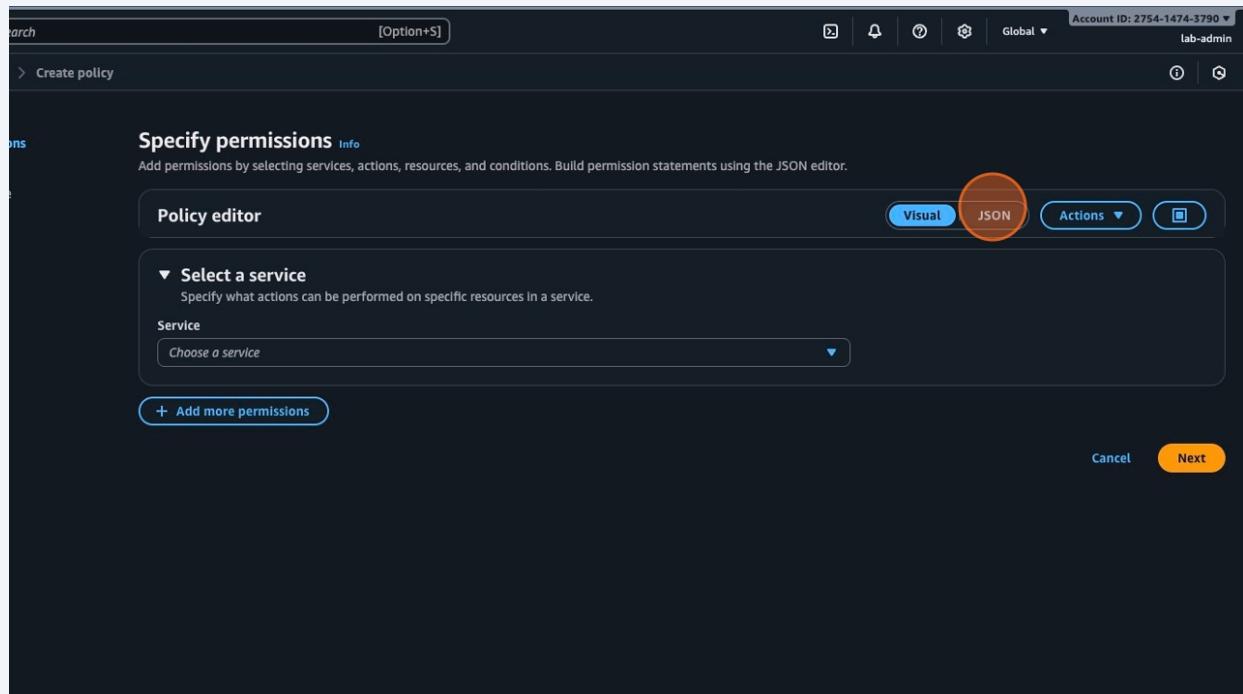
The screenshot shows the AWS IAM Dashboard. On the left sidebar, under the 'Access management' section, the 'Policies' option is highlighted with a red circle. The main content area displays security recommendations, IAM resources (with counts for User groups: 3, Users: 4, Roles: 19, Policies: 2, Identity providers: 0), and a 'What's new' section. On the right side, there are sections for the AWS Account (Account ID: 275414743790, Account Alias: radamirslad-aws) and Quick Links.

3 Click "Create policy"

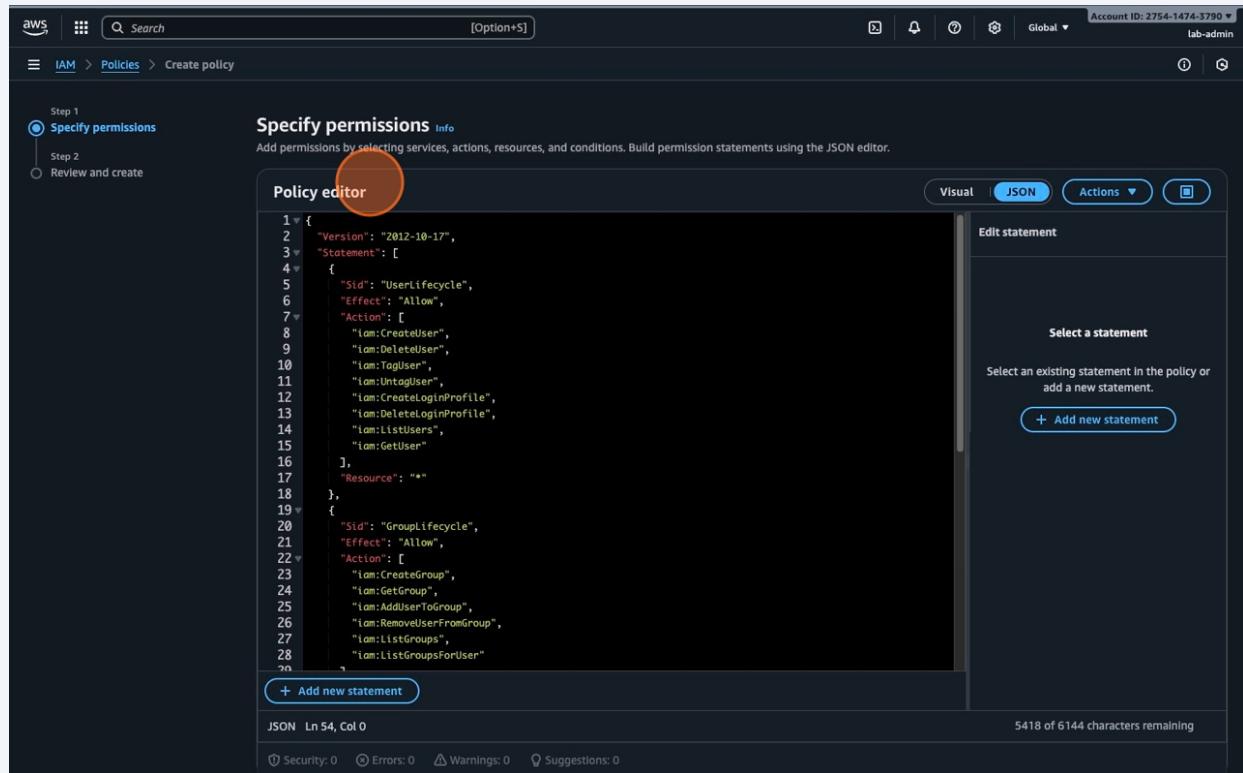
The screenshot shows the 'Policies' list page with 1406 policies. The 'Create policy' button is highlighted with a red circle at the top right of the actions bar. The table lists policies by name, type, used as, and description.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRole...	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permiss...
AdministratorAccess-AWSE...	AWS managed	None	Grants account administrative permiss...
AIOpsAssistantIncidentRep...	AWS managed	None	Provides permissions required by the A...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayE...	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifesizeDe...	AWS managed	None	Provide access to Lifesize AVS devices

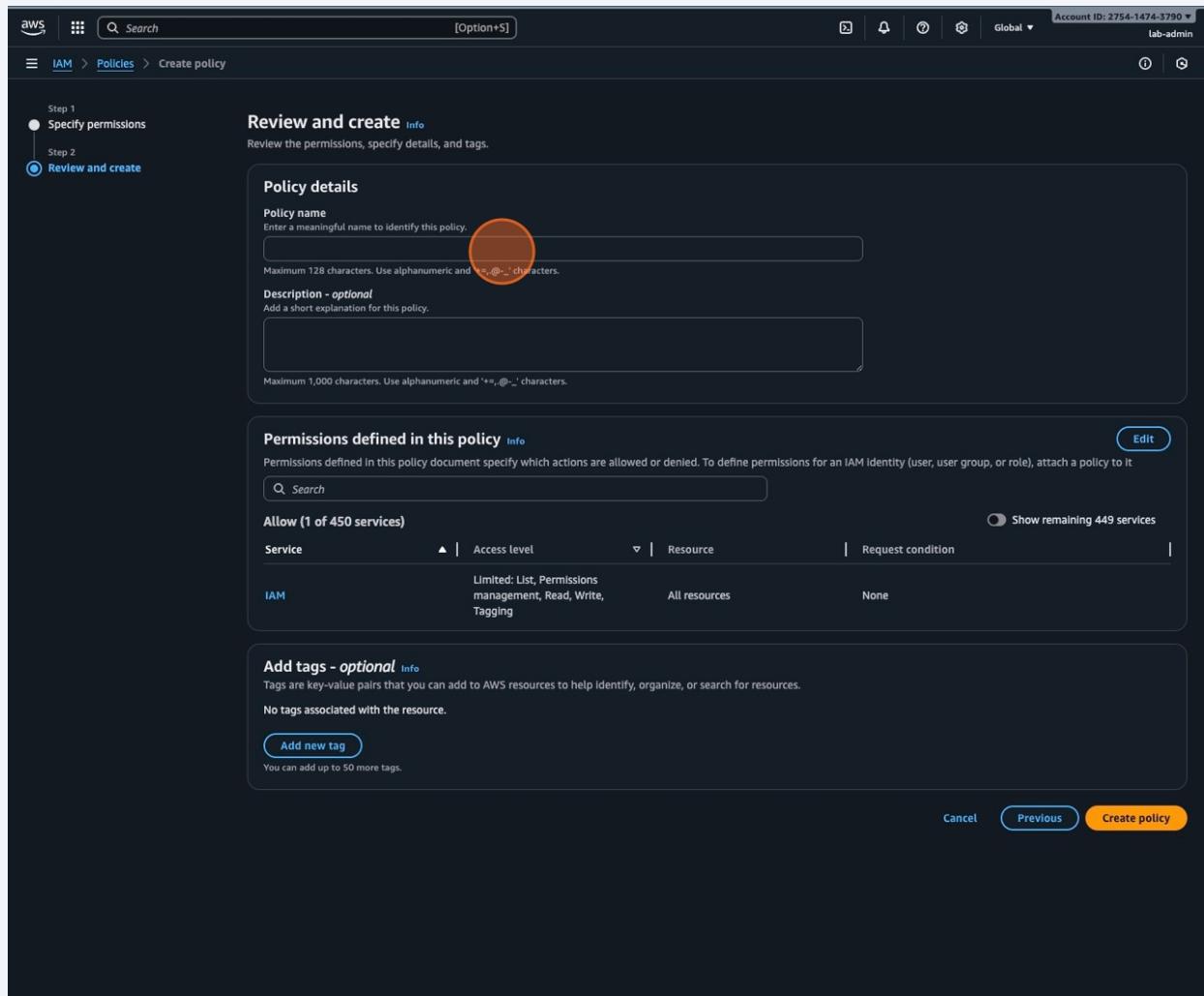
4 Click "JSON"



5 Add the JSON policy

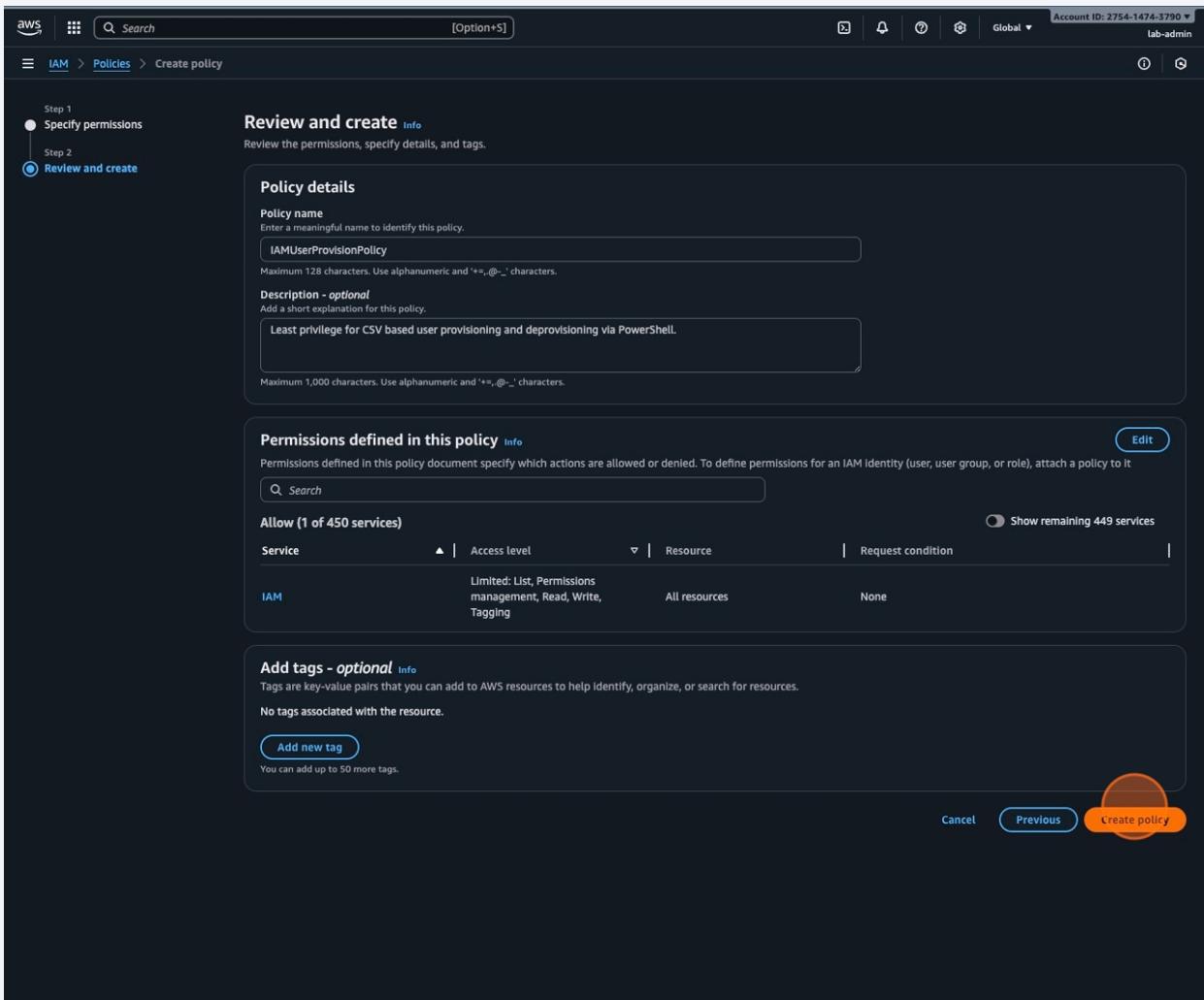


6 Click the "Policy name" field. Name the policy



7

Click "Create policy"



8

Click "Users"

The screenshot shows the AWS Identity and Access Management (IAM) Policies page. On the left, a sidebar menu is visible with several sections: Dashboard, Access management (User groups, Users, Roles, Policies), Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies), and IAM Identity Center and AWS Organizations. The 'Users' link under 'Access management' is highlighted with a red circle. The main content area displays a table titled 'Policies (1407)' with a green banner at the top stating 'Policy IAMUserProvisionPolicy created.' The table has columns for Policy name, Type, Used as, and Description. The 'Used as' column shows 'None' for all listed policies.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRole...	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
AdministratorAccess-AWSE...	AWS managed	None	Grants account administrative permis...
AIOpsAssistantIncidentRep...	AWS managed	None	Provides permissions required by the A...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayE...	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifesizeDe...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNetworkP...	AWS managed	None	This policy enables Alexa for Business ...
AlexaForBusinessPolyDeleg...	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessReadOnly...	AWS managed	None	Provide read only access to AlexaForB...
AmazonAPIGatewayAdmini...	AWS managed	None	Provides full access to create/edit/delete...
AmazonAPIGatewayInvoke...	AWS managed	None	Provides full access to invoke APIs in A...
AmazonAPIGatewayPushT...	AWS managed	None	Allows API Gateway to push logs to us...
AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlo...

9 Click "Create user"

The screenshot shows the AWS IAM 'Users' page. A green notification bar at the top says 'Policy IAMUserProvisionPolicy created.' with a 'View policy' link. Below it, a message encourages using Identity Center for managing workforce users. The main table lists four IAM users: alice.johnson, bob.miller, lab-admin, and Radimir. The 'Create user' button in the top right corner is highlighted with a red circle.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access summary
alice.johnson	/	1	-	-	-	-	-
bob.miller	/	1	-	-	-	-	-
lab-admin	/	1	14 minutes ago	-	21 hours	4 hours ago	Action history
Radimir	/	1	693 days ago	-	783 days	693 days ago	Action history

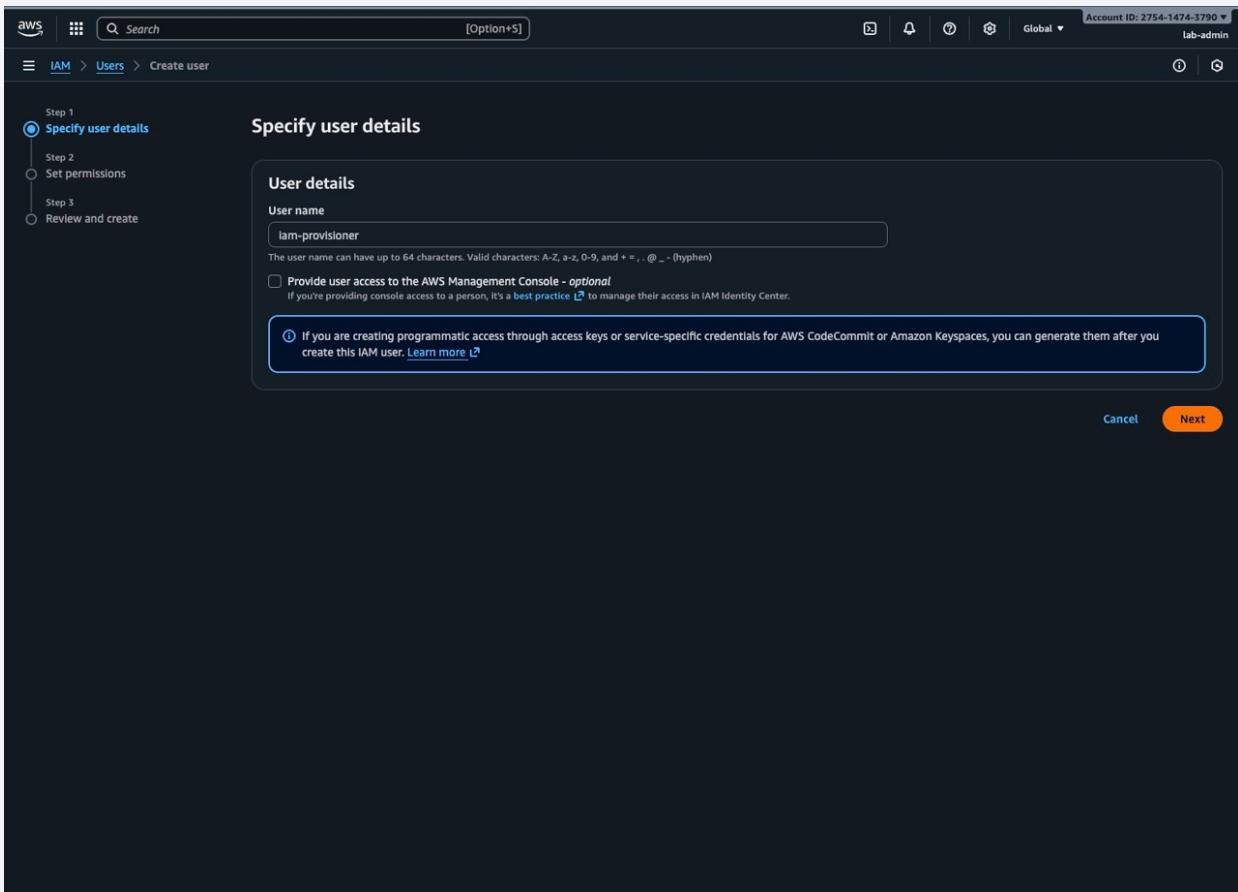
10 Click the "User name" field.

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. The 'User name' input field is highlighted with a red circle. Below it, a note specifies character restrictions: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + - _ @ (hyphen)'. There's also an optional checkbox for 'Provide user access to the AWS Management Console'.

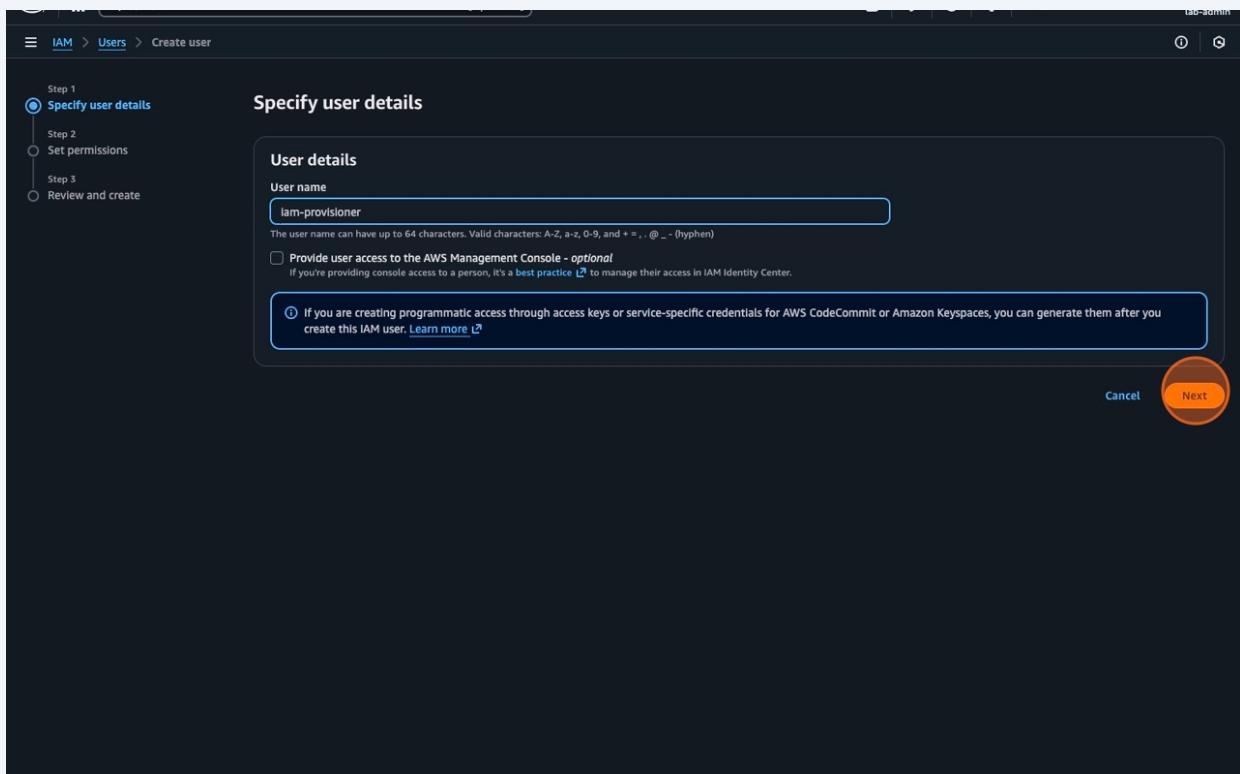
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

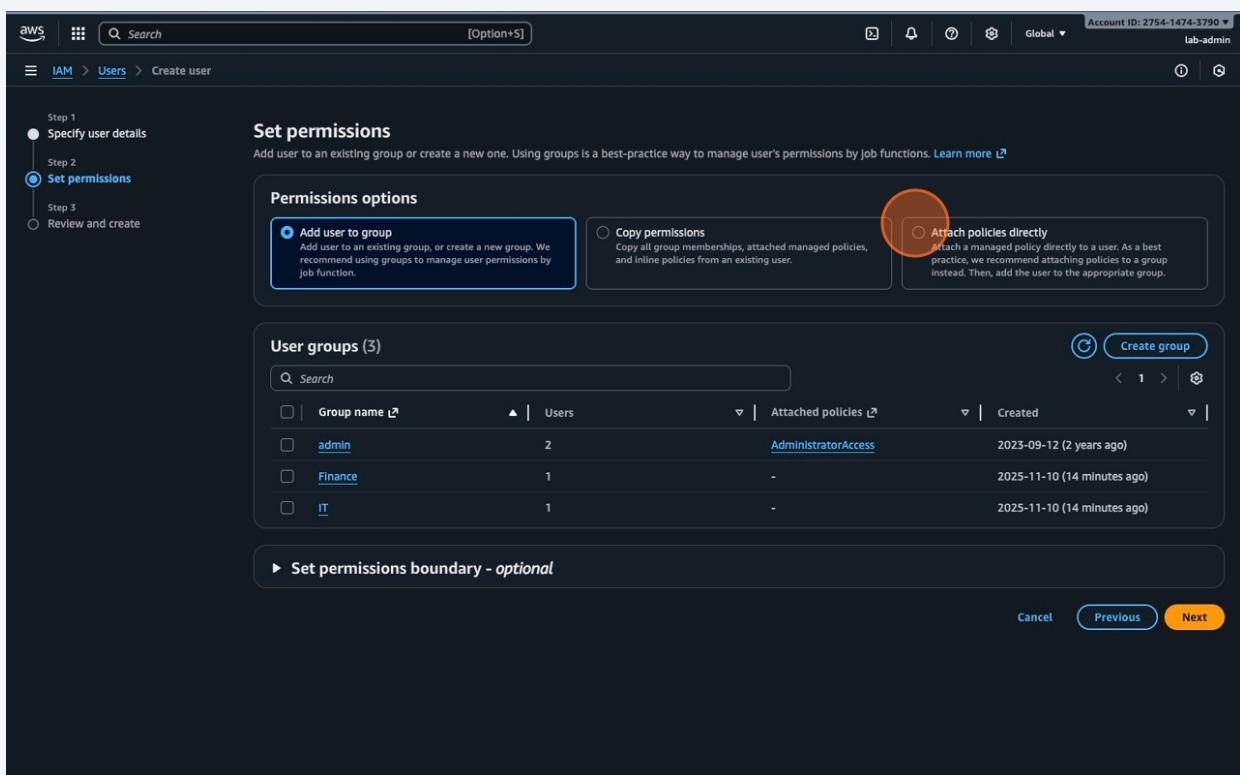
11 Type "iam-provisioner"



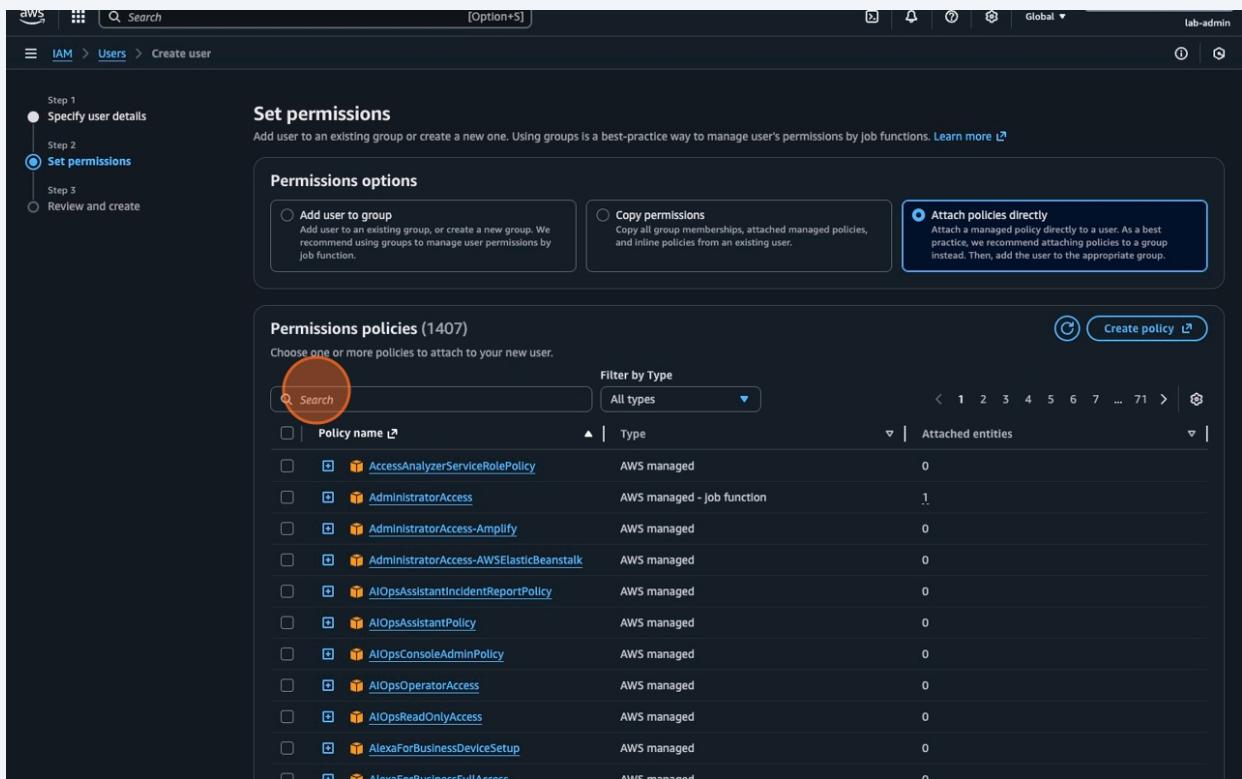
12 Click "Next"



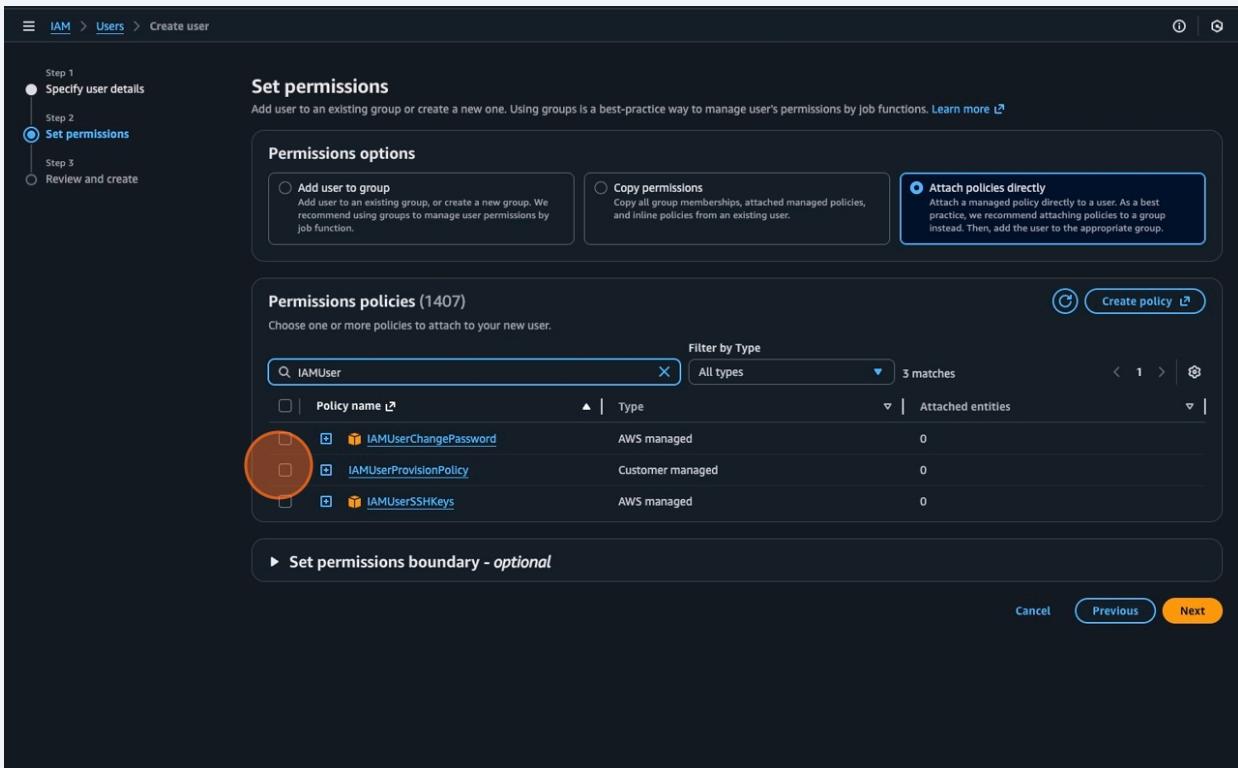
13 Click this radio button.



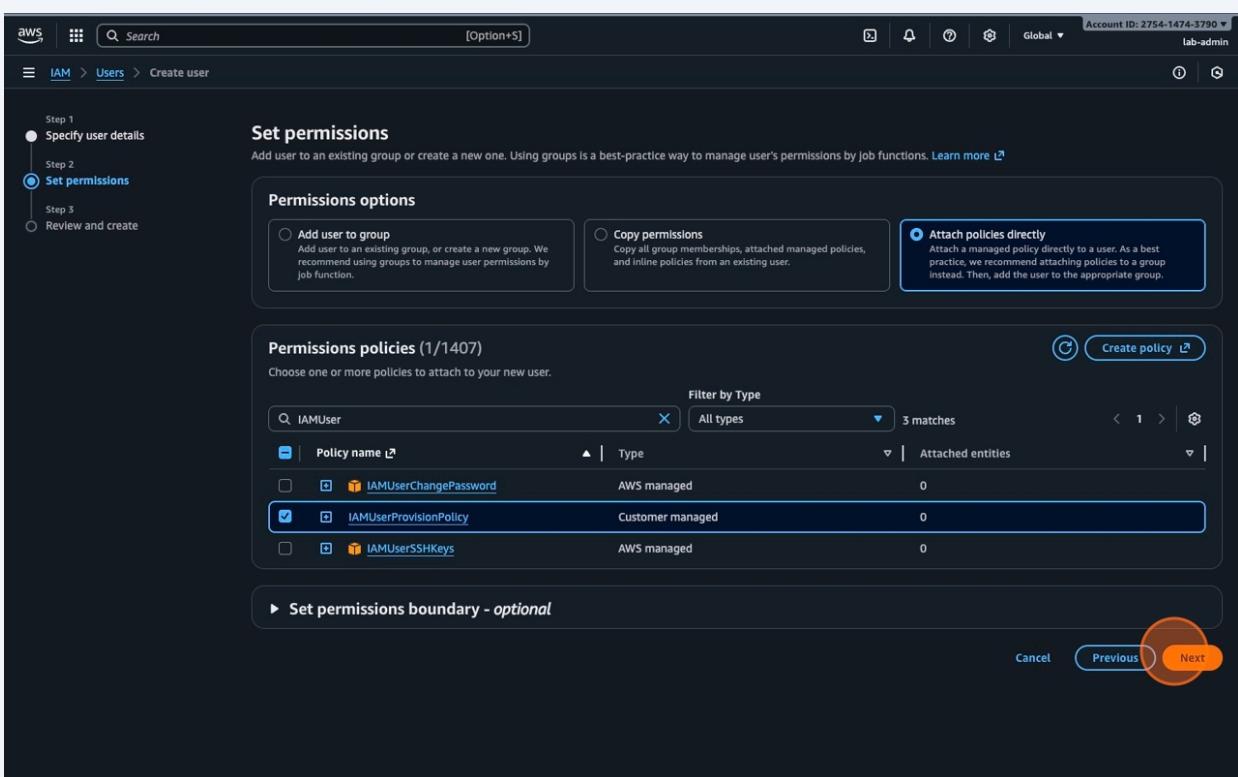
14 Click the "Search" field.



15 Click this checkbox.

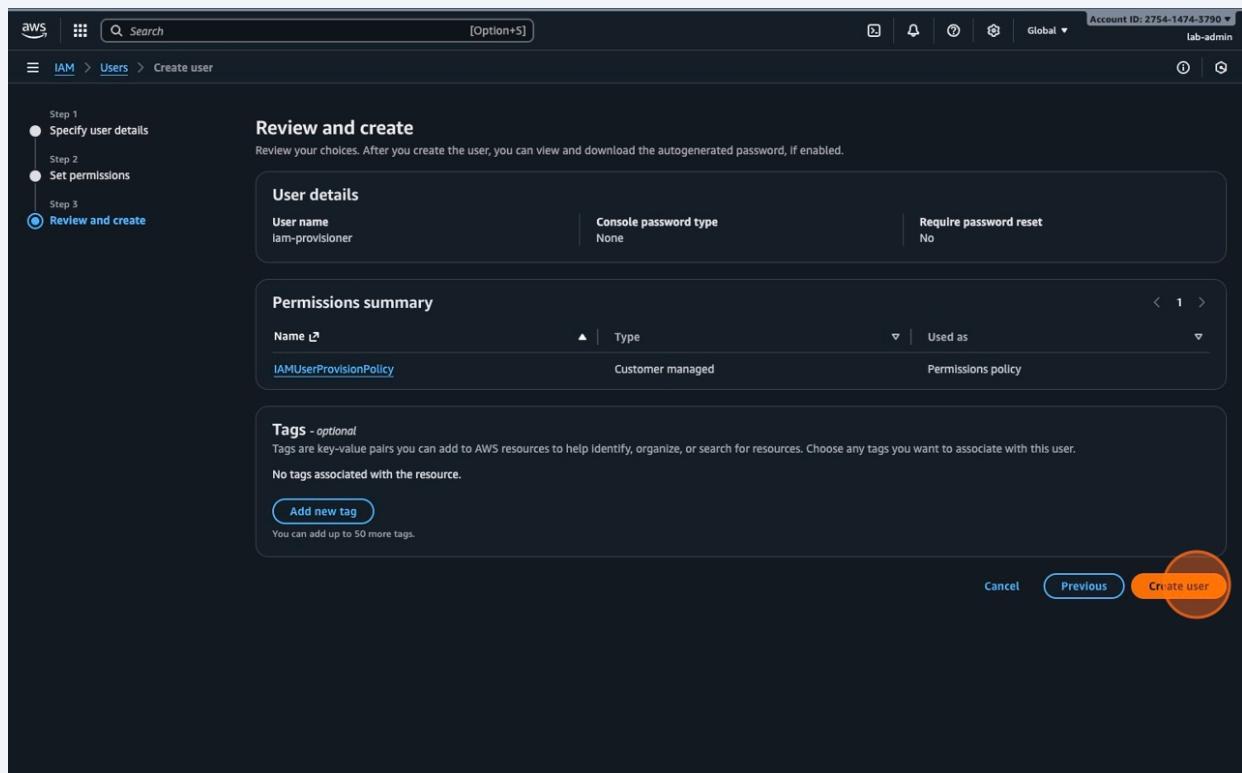


16 Click "Next"



17

Click "Create user"



18 Click "iam-provisioner"

The screenshot shows the AWS IAM 'Users' page. On the left, there's a sidebar with navigation links like 'Dashboard', 'Access management', 'Access reports', and 'IAM Identity Center'. The main area displays a table of users with columns for 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', and 'Access key'. There are five users listed: 'alice.johnson', 'bob.miller', 'iam-provisioner', 'lab-admin', and 'Radamir'. The 'iam-provisioner' row is circled in red.

19 Click "Security credentials"

The screenshot shows the AWS IAM 'User Details' page for 'iam-provisioner'. The left sidebar is identical to the previous screenshot. The main area has a 'Summary' section with details like ARN, Console access status, and creation date. Below it is a 'Permissions' tab, which is currently active and highlighted with a red circle. Other tabs include 'Groups', 'Tags', 'Security credentials', and 'Last Accessed'. Under the 'Permissions' tab, there's a 'Permissions policies' section listing a single policy: 'IAMUserProvisionPolicy'. At the bottom, there are sections for 'Permissions boundary' and 'Generate policy based on CloudTrail events'.

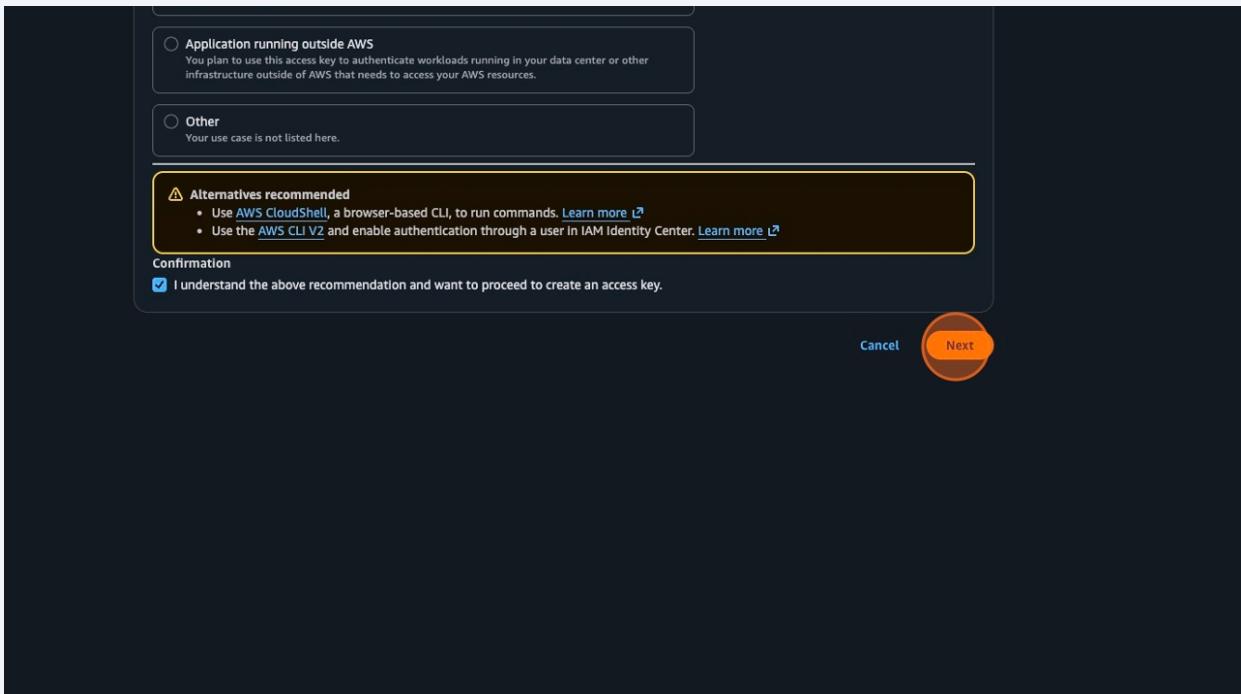
20 Click "Create access key"

The screenshot shows the AWS IAM Access Keys page. At the top, there's a section for Multi-factor authentication (MFA) with a 'Create access key' button. Below it is the 'Access keys' section, which also has a 'Create access key' button. This second 'Create access key' button is circled in orange. Further down is the 'API keys for Amazon Bedrock' section, and at the bottom is the 'SSH public keys for AWS CodeCommit' section.

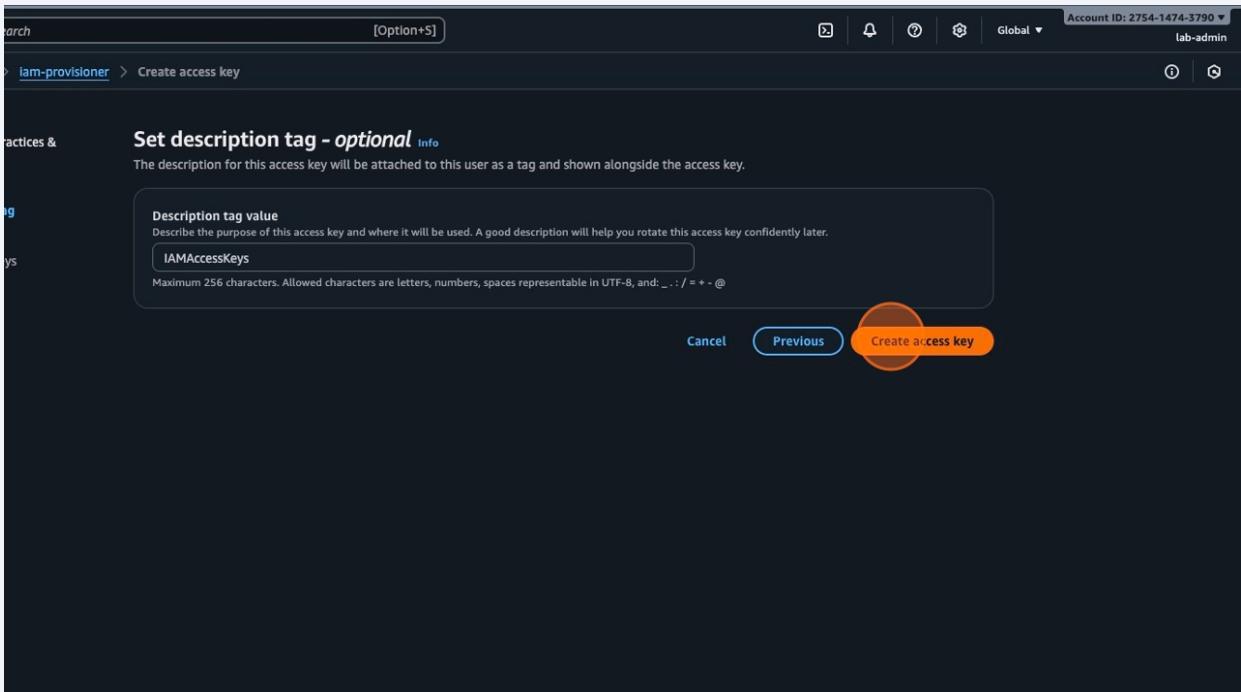
21 Click this radio button.

The screenshot shows the 'Access key best practices & alternatives' step in the IAM Access Key creation wizard. It lists several use cases with radio buttons. The first option, 'Command Line Interface (CLI)', is circled in orange. Other options include 'Local code', 'Application running on an AWS compute service', 'Third-party service', 'Application running outside AWS', and 'Other'.

22 Click "Next"



23 Click "Create access key"



Step 24 – Developed .CSV file PowerShell script. Ran the following command in the terminal ->

```
Last login: Mon Nov 10 14:33:45 on ttys000
[radamirsiad@Radamirs-MacBook-Pro ~ % brew install awscli
Warning: awscli 2.31.32 is already installed and up-to-date.
To reinstall 2.31.32, run:
  brew reinstall awscli
[radamirsiad@Radamirs-MacBook-Pro ~ % aws configure --profile provisioner
AWS Access Key ID [*****YT7L]: AKIAUAH77PLXJ7SJYT7L
AWS Secret Access Key [*****d56r]: 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
Default region name [us-east-2]: us-east-2
Default output format [json]: json
[radamirsiad@Radamirs-MacBook-Pro ~ % pwsh
PowerShell 7.5.4
PS /Users/radamirsiad> Install-Module AWS.Tools.Common -Scope CurrentUser -Force
PS /Users/radamirsiad> Install-Module AWS.Tools.IdentityManagement -Scope CurrentUser -Force
PS /Users/radamirsiad>
PS /Users/radamirsiad> Initialize-AWSDefaultConfiguration -ProfileName provisioner
PS /Users/radamirsiad> cd ~/Downloads
[PS /Users/radamirsiad/Downloads> ./provisioning.ps1
Transcript started, output file is /Users/radamirsiad/Downloads/provisioning_log.txt
Loaded 3 user entries from CSV.

Processing user: alice.johnson (Create)
User already exists: alice.johnson
Added alice.johnson to group Finance
Processing user: bob.miller (Create)
User already exists: bob.miller
Added bob.miller to group IT
Processing user: eve.smith (Delete)
Delete failed for eve.smith: The user with name eve.smith cannot be found.

Provisioning run complete. Check AWS Console and provisioning_log.txt for results.
Transcript stopped, output file is /Users/radamirsiad/Downloads/provisioning_log.txt
```

25 Click "alice.johnson"

The screenshot shows the AWS IAM 'Users' page. On the left, there's a sidebar with navigation links like 'Dashboard', 'Access management', 'Access reports', etc. The main area displays a table titled 'Users (5)'. The table has columns for 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last'. The user 'alice.johnson' is highlighted with a red circle. Other users listed are 'bob.miller', 'iam-provisioner', 'lab-admin', and 'Radimir'. A modal at the top right says 'Ready to streamline human access to AWS and cloud apps?'.

26 Click "Groups"

The screenshot shows the AWS IAM 'User Details' page for 'alice.johnson'. The left sidebar is identical to the previous screenshot. The main area shows the 'Summary' section with ARN, creation date, and access keys. Below it is a 'Permissions' section with tabs for 'Permissions', 'Groups (1)', 'Tags', 'Security credentials', and 'Last Accessed'. The 'Groups (1)' tab is highlighted with a red circle. It shows a table with one item: 'Group Name: lab-admin'. At the bottom, there's a 'Generate policy based on CloudTrail events' section with a 'Generate policy' button.

27 Alice Johnson is in the Finance group

The screenshot shows the AWS IAM User Details page for 'alice.johnson'. The 'Groups' tab is selected, displaying the 'User groups membership' section. The 'Finance' group is listed, highlighted with a red circle. Other tabs include 'Permissions', 'Tags', 'Security credentials', and 'Last Accessed'.

28 Now select the second user created

The screenshot shows the AWS IAM User Details page for 'bob.miller'. The 'Permissions' tab is selected, displaying the 'Permissions policies (0)' section. This section indicates that no policies are attached to the user directly or through groups. Other tabs include 'Groups', 'Tags', 'Security credentials', and 'Last Accessed'.

29

Click "Groups"

The screenshot shows the AWS IAM User Details page for a user named bob.miller. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and other services like IAM Identity Center and AWS Organizations. The main content area displays the user's summary, including ARN, console access status, creation date, and access keys. Below the summary is a tab navigation bar with 'Permissions', 'Groups (1)', 'Tags', 'Security credentials', and 'Last Accessed'. The 'Groups (1)' tab is currently selected and highlighted with a red circle. Under this tab, there is a section titled 'Permissions policies (0)' which states 'No resources to display'. There is also a 'Generate policy based on CloudTrail events' section with a 'Generate policy' button.

30 Bob Miller is a member of the IT group

The screenshot shows the AWS IAM User Details page for the user 'bob.miller'. The left sidebar shows navigation options like Dashboard, Access management, and Access reports. The main content area displays the user's ARN (arn:aws:iam::275414743790:user/bob.miller), creation date (November 10, 2025, 12:48 (UTC-05:00)), and access information (Console access Disabled, Last console sign-in -). The 'Groups' tab is selected, showing one group: 'IT'. A circled orange box highlights the 'IT' entry in the 'User groups membership' table.

Step 31 -> Made edits to the .CSV file to include “Delete” function to Bob Millers profile.

Ran the following PowerShell command

```
[PS /Users/radimirsiad/Downloads> ./provisioning.ps1
Transcript started, output file is /Users/radimirsiad/Downloads/provisioning_log.txt
Loaded 3 user entries from CSV.

Processing user: alice.johnson (Create)
User already exists: alice.johnson
Added alice.johnson to group Finance
Processing user: bob.miller (Delete)
Deleted user: bob.miller
Processing user: eve.smith (Delete)
eve.smith does not exist - skipping delete.

Provisioning run complete. Check AWS Console and provisioning_log.txt for results.
Transcript stopped, output file is /Users/radimirsiad/Downloads/provisioning_log.txt
```

Step 32 – Going back to the AWS Console the user Bob Miller was deprovisioned

The screenshot shows the AWS IAM Users page. A green banner at the top indicates that the policy 'IAMUserProvisionPolicy' has been updated. Below the banner, a message encourages users to streamline access to AWS and cloud apps via Identity Center. The main table lists four users:

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key status
alice.johnson	/	1	-	-	-	-	-	-	-
iam-provisioner	/	0	7 minutes ago	-	-	-	Active - AKIAUAH77PL...	1 hour	OK
lab-admin	/	1	1 hour ago	-	22 hours	5 hours ago	Active - AKIAUAH77PL...	4 hours	OK
Radimir	/	1	693 days ago	-	783 days	693 days ago	Active - AKIAUAH77PL...	789 days	OK