

AWS Services ▾ Resource Groups ▾ devops ▾ Ohio ▾ Support ▾

History

Console Home

IAM

Glacier

Storage Gateway

Database

Relational Database Service

DynamoDB

ElastiCache

Amazon Redshift

Migration

AWS Migration Hub

Application Discovery Service

Database Migration Service

Server Migration Service

Snowball

Networking & Content Delivery

VPC

CloudFront

Route 53

API Gateway

Direct Connect

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Group A-Z

Analytics

Athena

EMR

CloudSearch

Elasticsearch Service

Kinesis

QuickSight ↗

Data Pipeline

AWS Glue

Customer Engagement

Amazon Connect

Pinpoint

Simple Email Service

Business Productivity

Alexa for Business

Amazon Chime ↗

WorkDocs

WorkMail

Security, Identity & Compliance

IAM

Cognito

GuardDuty

Inspector

Amazon Macie ↗

AWS Single Sign-On

Certificate Manager

CloudHSM

Directory Service

WAF & Shield

Artifact

Desktop & App Streaming

WorkSpaces

AppStream 2.0

Internet Of Things

IoT Core

IoT Device Management

IoT Analytics

Greengrass

Amazon FreeRTOS

Mobile Services

Mobile Hub

AWS AppSync

Game Development

Amazon GameLift

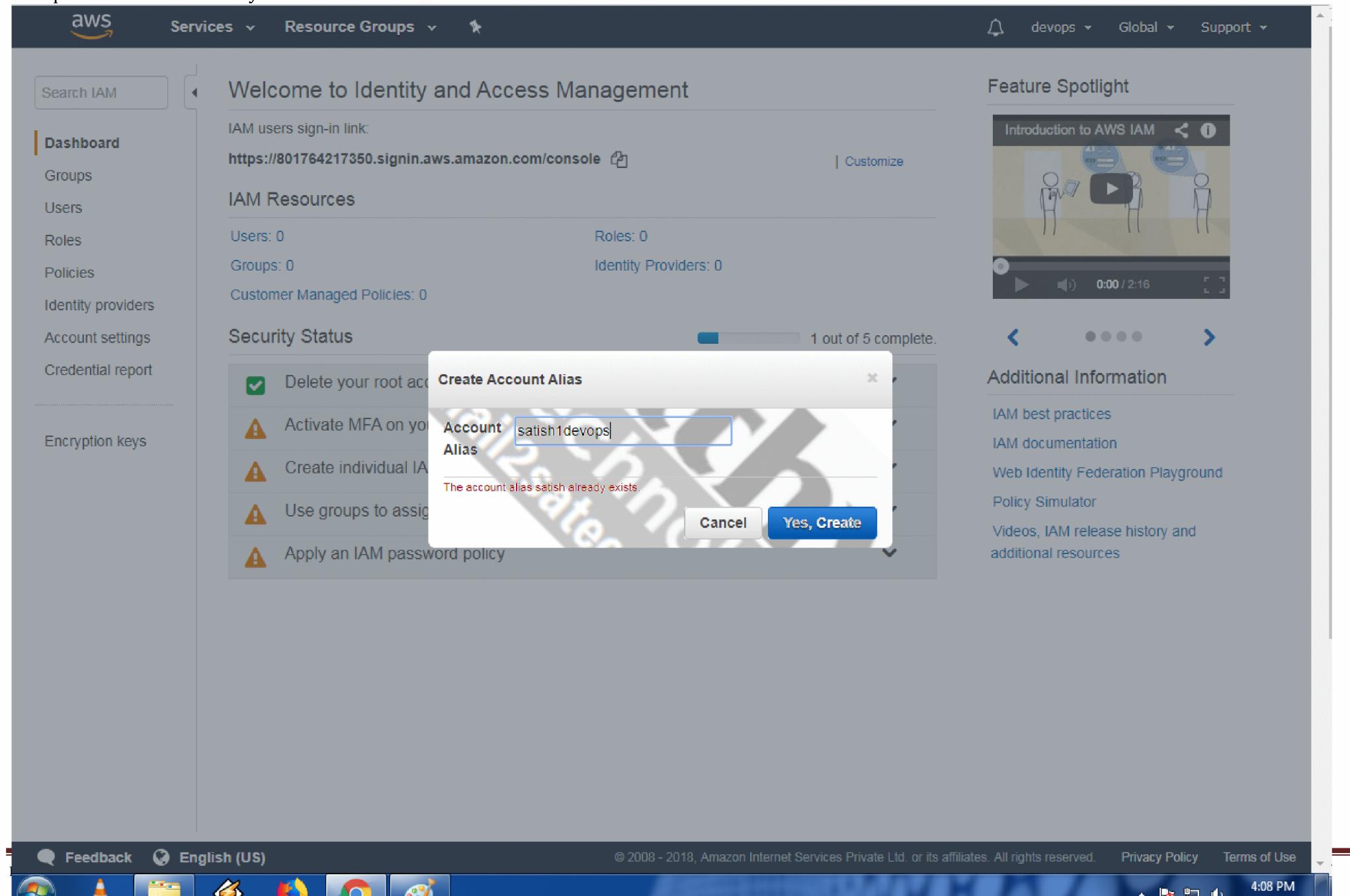
close

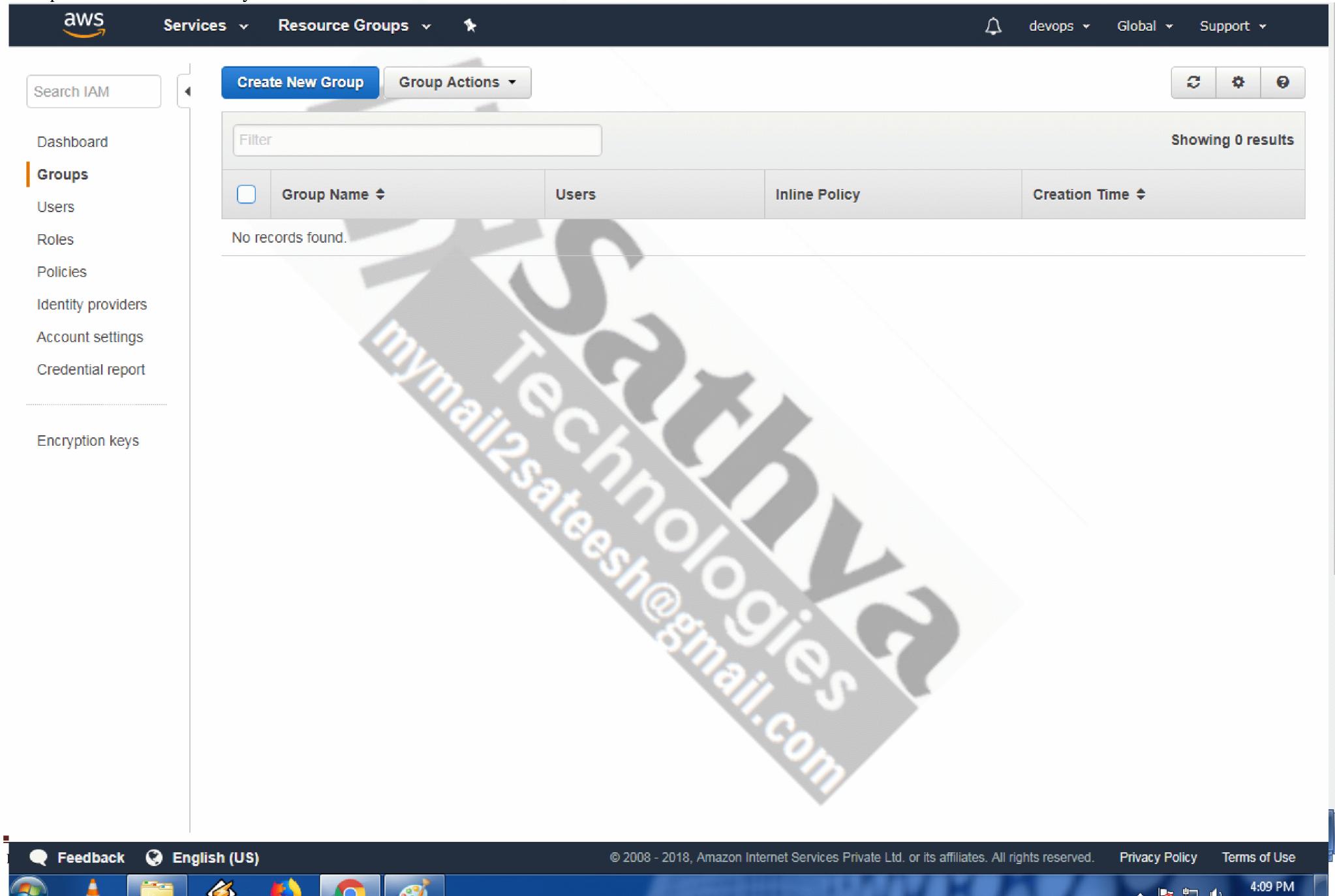
<https://console.aws.amazon.com/iam/home?region=us-east-2>

Discover, procure, and deploy popular software products

4:02 PM

The screenshot shows the AWS Identity and Access Management (IAM) console home page. The top navigation bar includes links for Services, Resource Groups, Global (which is highlighted with a red box), devops, Support, and a bell icon. A search bar labeled "Search IAM" is on the left. The main content area has a heading "Welcome to Identity and Access Management". It features a "Customize" button with a blue arrow pointing up to it. A red box highlights the "IAM users sign-in link" and its URL: <https://801764217350signin.aws.amazon.com/console>. Below this, there's a section for "IAM Resources" showing 0 Users, 0 Groups, 0 Roles, and 0 Identity Providers. A "Security Status" section indicates "1 out of 5 complete" and lists five items: "Delete your root access keys" (checked), "Activate MFA on your root account", "Create individual IAM users", "Use groups to assign permissions", and "Apply an IAM password policy". To the right, a sidebar lists regions: US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon), Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Canada (Central), EU (Frankfurt), EU (Ireland), EU (London), EU (Paris), and South America (São Paulo). A large watermark for "Cloud Academy" and "Cloud Academy @gmail.com" is visible across the page.





A screenshot of the AWS IAM Groups page. The left sidebar shows navigation links: Dashboard, Groups (which is selected and highlighted in orange), Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has tabs for 'Create New Group' and 'Group Actions'. A search bar labeled 'Search IAM' is at the top. Below it is a table header with columns: Group Name, Users, Inline Policy, and Creation Time. A filter input field and a message saying 'Showing 0 results' are also present. A large, semi-transparent watermark with the text 'Sathya Technologies' and an email address 'mymail2sateesh@gmail.com' is overlaid across the center of the page.

aws Services Resource Groups ⚡

Search IAM

Create New Group Group Actions

Filter Showing 0 results

No records found.

Groups

Dashboard

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Feedback English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4:09 PM

Secure | https://console.aws.amazon.com/iam/home?region=us-east-2#/groups

Bookmarks Google Translate ABN Telugu - YouTube Compute Engine - My Blog - Quality Thought Andhra Jyothy Telugu Amazon.com Sign In Hyderabad Movie Tickets

aws Services Resource Groups

Search IAM Create New Group Group Actions

Dashboard Groups Users Roles Policies Identity providers Account settings Credential report

Encryption keys

No records found.

Showing 0 results

Filter Group Name ▾ Users Inline Policy Creation Time ▾

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use 4:09 PM

A screenshot of the AWS IAM Groups page. The 'Groups' option in the left sidebar is highlighted with a red box. A red arrow points from the text 'Create New Group' at the top of the main content area to the 'Create New Group' button itself, which is also highlighted with a red box. The main content area shows a table with columns for Group Name, Users, Inline Policy, and Creation Time. A large watermark for 'Sathya Technologies' and the email 'mymail2sateesh@gmail.com' is overlaid diagonally across the page.

The screenshot shows the 'Set Group Name' step of the AWS Resource Groups 'Create New Group Wizard'. The 'Group Name' field is highlighted with a red box and contains the text 'devops'. A red arrow points upwards from the bottom right towards this field. Below the field, a placeholder text says 'Example: Developers or ProjectAlpha'. At the bottom right, there are 'Cancel' and 'Next Step' buttons, with 'Next Step' being highlighted by a red box and a red arrow pointing downwards from the top right towards it.

aws Services Resource Groups

devops Global Support

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: devops

Example: Developers or ProjectAlpha

Maximum 128 characters

Cancel Next Step



Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

set of permissions / instructions

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

	Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/>	AdministratorAccess	0	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+0530
<input type="checkbox"/>	AlexaForBusinessDeviceSet...	0	2017-11-30 22:17 UTC+0530	2017-11-30 22:17 UTC+0530
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	2017-11-30 22:17 UTC+0530	2017-11-30 22:17 UTC+0530
<input type="checkbox"/>	AlexaForBusinessGatewayE...	0	2017-11-30 22:17 UTC+0530	2017-11-30 22:17 UTC+0530
<input type="checkbox"/>	AlexaForBusinessReadOnly...	0	2017-11-30 22:17 UTC+0530	2017-11-30 22:17 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayAdmini...	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayInvoke...	0	2015-07-09 23:06 UTC+0530	2015-07-09 23:06 UTC+0530
<input type="checkbox"/>	AmazonAPIGatewayPushTo...	0	2015-11-12 05:11 UTC+0530	2015-11-12 05:11 UTC+0530
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	2015-02-07 00:10 UTC+0530	2017-09-08 05:26 UTC+0530
<input type="checkbox"/>	AmazonAppStreamReadOnl...	0	2015-02-07 00:10 UTC+0530	2016-12-08 02:30 UTC+0530
<input type="checkbox"/>	AmazonAppStreamServiceA...	0	2016-11-19 09:47 UTC+0530	2017-05-24 04:30 UTC+0530
<input type="checkbox"/>	AmazonAthenaFullAccess	0	2016-11-30 22:16 UTC+0530	2017-09-13 05:43 UTC+0530
<input type="checkbox"/>	AmazonChimeFullAccess	0	2017-11-02 03:45 UTC+0530	2017-11-02 03:45 UTC+0530
<input type="checkbox"/>	AmazonChimeReadOnly	0	2017-11-02 03:34 UTC+0530	2018-01-16 22:48 UTC+0530

Cancel

Previous

Next Step



4:16 PM

AWS Services Resource Groups ★

devops Global Support

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Review

Review the following information, then click **Create Group** to proceed.

Group Name	devops	Edit Group Name
Policies	arn:aws:iam::aws:policy/AdministratorAccess	Edit Policies

Create Group

Cancel Previous Create Group

SATISH TECHNOLOGIES
mymail2sateesh@gmail.com

AWS Services Resource Groups Create New Group Group Actions Search IAM Dashboard Groups Users Roles Policies Identity providers Account settings Credential report Encryption keys

Create New Group Group Actions Filter Showing 1 results

<input checked="" type="checkbox"/> Group Name	Users	Inline Policy	Creation Time
<input checked="" type="checkbox"/> devops	0		2018-03-25 16:19 UTC+0530

select this group

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use 4:20 PM

SATISH

aws Services Resource Groups

devops Global Support

Search IAM

Dashboard Groups Users Roles Policies Identity providers Account settings Credential report Encryption keys

IAM > Groups > devops

Summary

Group ARN: arn:aws:iam::801764217350:group/devops

Users (in this group): 0

Path: /

Creation Time: 2018-03-25 16:19 UTC+0530

Users Permissions Access Advisor

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
AdministratorAccess	Show Policy Detach Policy Simulate Policy

Inline Policies

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use 4:23 PM

A red box highlights the "Actions" column in the Managed Policies table, and a red arrow points to the "Show Policy" link for the "AdministratorAccess" policy.

Servic... Resource Groups ...

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

IAM > Groups > devops

Summary

Group ARN: arn:aws:iam::801764217350:group/devops

Users (in this group): 0

Path: /

Creation Time: 2018-03-25 16:19 UTC+0530

Show Policy

Permissions

Users

Access Advisor

Managed Policies

The following managed policies are attached to this group.

Attach Policy

Policy Name

AdministratorAccess

Inline Policies

Cancel

Simulate Policy

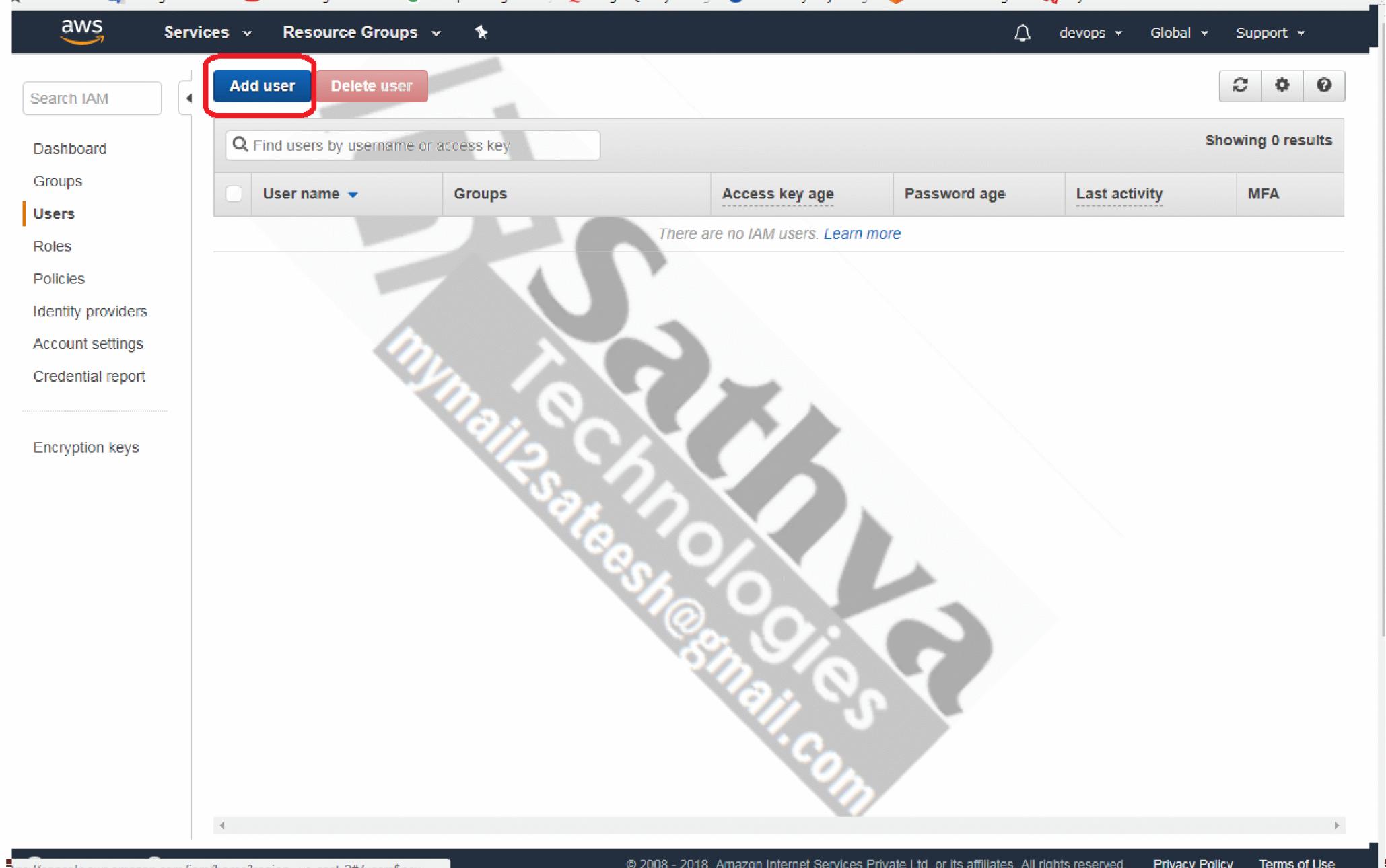
json fromat

Feedback English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4:23 PM

Sathya Technologies
mymail2sateesh@gmail.com



The screenshot shows the AWS IAM User Management console. The top navigation bar includes the AWS logo, Services (dropdown), Resource Groups (dropdown), a bell icon, devops (dropdown), Global (dropdown), and Support (dropdown). On the left, a sidebar menu lists: Dashboard, Groups, Users (selected), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has a search bar ('Search IAM') and two buttons: 'Add user' (highlighted with a red box) and 'Delete user'. A search field ('Find users by username or access key') and a status message ('Showing 0 results') are also present. A table header with columns 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA' follows. Below the table, a message states 'There are no IAM users. Learn more'.

Add user

1

2

3

4

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

satish_admin

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

 Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

 AWS Management Console access

Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

 Autogenerated password Custom password

.....

 Show password

Require password reset

 User must create a new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.



Add user

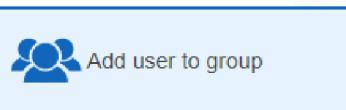
1

2

3

4

Set permissions for satish_admin



Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

[Create group](#)[Refresh](#) Search

Showing 1 result

Group ▾	Attached policies
<input checked="" type="checkbox"/> devops	AdministratorAccess

Add user

1

2

3

4

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	satish_admin
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	devops
Managed policy	IAMUserChangePassword

[Cancel](#)[Previous](#)[Create user](#)

Add user

1 2 3 4

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name satish_admin

AWS access type Programmatic access and AWS Management Console access

Console password type Custom

Require password reset Yes

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	devops
Managed policy	IAMUserChangePassword

Cancel

Previous

Create user



AWS Services Resource Groups 1 2 3 4

Add user

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://satish1devops.signin.aws.amazon.com/console>

[Download .csv](#)

	User	Access key ID	Secret access key	Email login instructions
▶	satish_admin	AKIAINPTY4II6ILVQM7A	***** Show	Send email

Close

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

credentials.csv Show all

4:46 PM

DevOps with AWS & LINUX by Mr. SATISH

Universal Document Converter

Home Insert Page Layout Formulas Data Review View

Cut Copy Format Painter Paste

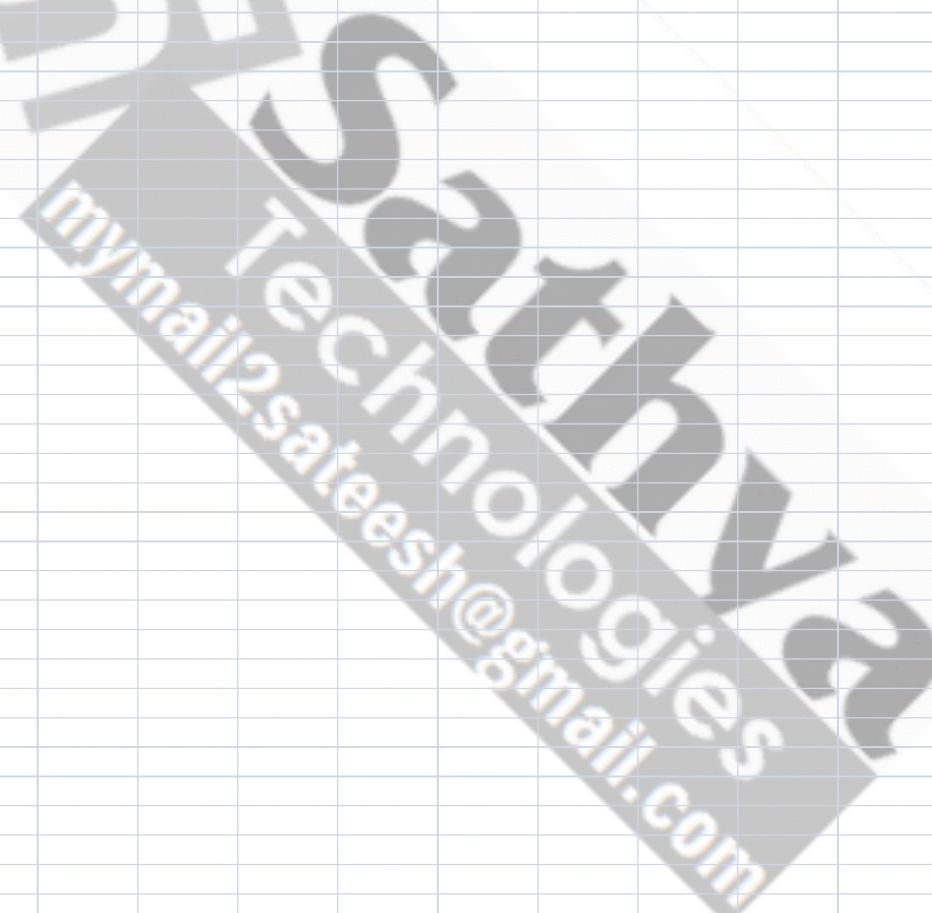
Font Alignment Number Styles Cells Editing

User name

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	User name	Password	Access key ID	Secret acc	Console login	link												
2	satish_admin		AKIAINPTY4II6ILVQM7.5IGik46RD	https://satish1devops.signin.aws.amazon.com/console														
3																		
4																		
5																		
6																		
7																		
8																		
9																		
10																		
11																		
12																		
13																		
14																		
15																		
16																		
17																		
18																		
19																		
20																		
21																		
22																		
23																		
24																		
25																		
26																		
27																		
28																		
29																		
30																		
31																		
32																		
33																		
34																		
35																		

credentials

Ready 100% 4:51 PM



The screenshot shows the AWS IAM Roles page. On the left, a sidebar menu is open with the 'Roles' option selected. A red box highlights the 'Create role' button at the top of the main content area. The main content area contains information about IAM roles, a list of examples, and a section for additional resources. Below this is a table showing one existing role named 'myrole_s3'. The table has columns for Role name, Description, and Trusted entities.

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

Role name	Description	Trusted entities
<input type="checkbox"/> myrole_s3	Allows EC2 instances to call AWS services on your behalf.	AWS service: ec2

AWS Services Resource Groups ⚙️ 🔍

devops Global Support

Create role

Select type of trusted entity

1 2 3

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2 (highlighted with a red box)
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	DMS	Elastic Transcoder	Machine Learning	SageMaker
Application Auto Scaling	Data Pipeline	Elastic Load Balancing	MediaConvert	Service Catalog
Auto Scaling	DeepLens	Glue	OpsWorks	Step Functions
Batch	Directory Service	Greengrass	RDS	Storage Gateway
CloudFormation	DynamoDB	GuardDuty	Redshift	
CloudHSM	EC2	Inspector	Rekognition	
CloudWatch Events	EMR	IoT	S3	
CodeBuild	ElastiCache	Kinesis	SMS	
CodeDeploy	Elastic Beanstalk	Lambda	SNS	
Config	Elastic Container Service	Lex	SWF	

* Required

Cancel Next: Permissions (highlighted with a red box)

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

My Dashboard Google Chrome 6:03 AM 2023



1

2

3

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

[Create policy](#) [Refresh](#)

Filter: Policy type ▾			Showing 4 results
	Policy name ▾	Attachments ▾	Description
<input type="checkbox"/>	▶ AmazonDMSRedshiftS3Role	0	Provides access to manage S3 settings for Redshift endpoint...
<input checked="" type="checkbox"/>	▶ AmazonS3FullAccess	0	Provides full access to all buckets via the AWS Management ...
<input type="checkbox"/>	▶ AmazonS3ReadOnlyAccess	0	Provides read only access to all buckets via the AWS Manag...
<input type="checkbox"/>	▶ QuickSightAccessForS3StorageManagementA...	0	Policy used by QuickSight team to access customer data pro...

* Required

[Cancel](#)[Previous](#)[Next: Review](#)

Feedback



English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#)[Terms of Use](#)

6:04 AM

The screenshot shows the 'Create role' process in the AWS IAM Management Console. The 'Review' step is displayed, showing the configuration details for a new role:

- Role name:** EC2_S3_fullAccess (highlighted with a red box)
- Role description:** Allows EC2 instances to call AWS services on your behalf.
- Trusted entities:** AWS service: ec2.amazonaws.com
- Policies:** AmazonS3FullAccess (selected)

At the bottom of the screen, there are three numbered steps (1, 2, 3) indicating the review process. Step 3 is highlighted with a blue circle. A large watermark for 'Dynamite Technologies Sateesh@gmail.com' is visible across the page. A red arrow points downwards to the 'Create role' button, which is also highlighted with a red box.

AWS Services Resource Groups ⌂

devops Global Support

Search IAM

Dashboard Groups Users Roles Policies Identity providers Account settings Credential report Encryption keys

Policies > AmazonS3ReadOnlyAccess

Summary

One entity was attached to the **AmazonS3ReadOnlyAccess** policy.

Policy ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

Description: Provides read only access to all buckets via the AWS Management Console.

Attached entities (2)

Permissions Policy summary { } JSON

Filter

Service	Access level	Resource	Request condition
Allow (1 of 134 services) Show remaining 133	S3 Full: Read Limited: List	All resources	None

Feedback English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

6:15 AM

Servic... Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Policies > AmazonS3ReadOnlyAccess

Summary

One entity was attached to the **AmazonS3ReadOnlyAccess** policy.

Policy ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

Description: Provides read only access to all buckets via the AWS Management Console.

Permissions Attached entities (2) Policy versions Access Advisor

Attach Detach

Filter: Filter Search Showing 2 results

	Name	Type
<input type="checkbox"/>	prod	Group
<input checked="" type="checkbox"/>	myrole_s3	Role

Feedback English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

6:16 AM

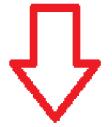
A screenshot of the AWS IAM Policies page. The left sidebar shows navigation links like Dashboard, Groups, Users, Roles, and Policies. The Policies link is selected and highlighted with an orange bar. The main content area shows the 'AmazonS3ReadOnlyAccess' policy summary. It includes the Policy ARN, a description, and tabs for Permissions, Attached entities (2), Policy versions, and Access Advisor. The Attached entities tab is active, showing two entities: 'prod' (Group) and 'myrole_s3' (Role). The 'myrole_s3' entry has a checkmark next to it. A red box highlights the 'Attach' button, and a large red arrow points upwards towards the 'Attached entities' section.



Attach Policy

Attach the policy to users, groups, or roles in your account.

Filter: Filter <input type="button" value="Search"/>		Showing 7 results
<input type="checkbox"/> Name	Type	
<input type="checkbox"/> bob_dev	User	
<input type="checkbox"/> ravi_prod	User	
<input type="checkbox"/> sam_dev	User	
<input checked="" type="checkbox"/> satish_admin	User	
<input type="checkbox"/> EC2_S3_fullAccess	Role	
<input type="checkbox"/> dev	Group	
<input type="checkbox"/> devops	Group	



Cancel

Attach policy