

100 Days of DevOps — Day 9-Delegate Access Across AWS Accounts Using IAM Roles

Check the updated 101 Days of DevOps Course

Course Registration link: <https://www.101daysofdevops.com/register/>

Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/>

YouTube link: <https://www.youtube.com/user/laprashant/videos>

Welcome to Day 9 of 100 Days of DevOps, On Day 8 I explained about the really critical topic STS <https://medium.com/@devopslearning/100-days-of-devops-day-8-introduction-to-aws-security-token-service-sts-b0f164e5d6a3> on Day 9 let's continue this journey in talking about Delegate Access Across AWS Accounts Using IAM Roles(Basically doing things via AWS Console)

Problem: How to share resources in different AWS accounts i.e User in Account B(Developer) should have Read-Only Access to S3 Bucket in Account A(Production).

Solution: By setting up cross-account access using IAM roles.

Advantage

- We don't need to set up individual IAM user in each account
- The user doesn't need to sign out of one account and sign into another account to access resources.

Pre-requisites


- You need two AWS accounts(Account A(PROD)) and Account B(Developer)
- An AWS S3 bucket created in Production Account A.


Step1: Create an IAM Role in Account A(This is to establish the trust between the two accounts)


- Go to IAM console <https://console.aws.amazon.com/iam/home?region=us-west-2#/home>
- Click on Roles, Create role
- This time, select Another AWS account and enter Account ID of Account B


Create role

Select type of trusted entity

 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 entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

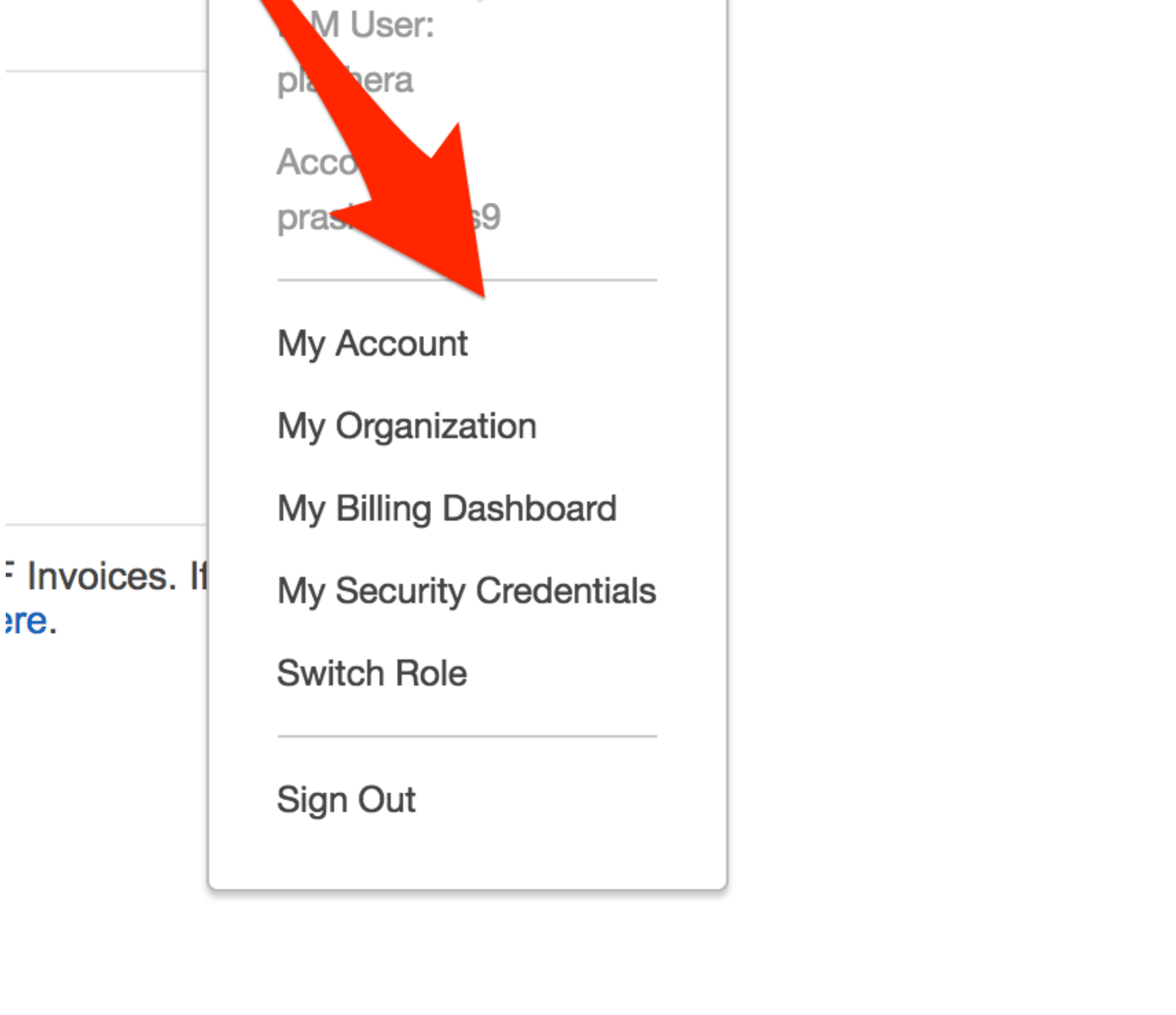
Account ID*

Options

☐ Require external ID (Best practice when a third party will assume this role)


☐ Require MFA

- To get the account id(Click on the IAM user on the top of the console and click on My Account)



- In next screen click on Create Policy and paste the below mentioned(Change the bucket name with the name of the bucket you want to share with Development Account) OR Choose S3ReadOnlyPolicy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "s3:ListAllMyBuckets",
7       "Resource": "*"
8     },
9     {
10      "Effect": "Allow",
11      "Action": [
12        "s3:ListBucket",
13        "s3:GetBucketLocation"
14      ],
15      "Resource": "arn:aws:s3:::bucket name"
16    },
17    {
18      "Effect": "Allow",
19      "Action": [
20        "s3:GetObject",
21        "s3:PutObject",
22        "s3:DeleteObject"
23      ],
24      "Resource": "arn:aws:s3:::bucket name/*"
25    }
26  ]
27 }
```

gistfile1.txt hosted with  by GitHub [view raw](#)

- Click Next and give your Role name


Create role


Review

Provide the required information below and review this role before you create it.

Role name*
Use alphanumeric and +,=,_,@,., characters. Maximum 64 characters.

Role description
Maximum 1000 characters. Use alphanumeric and +,=,_,@,., characters.

Trusted entities  The account 582956175038

Policies  AmazonS3ReadOnlyAccess [?](#)

Permissions boundary Permissions boundary is not set

No tags were added.


* Required [Cancel](#) [Previous](#) [Create role](#)

- Note down the Role ARN, we need it later

Step2: Grant Access to the role(This will allow users in Account B permissions to allow switching to the role)

- Go to the Role we have just created
- Click on Trust relationships → Edit trust relationships

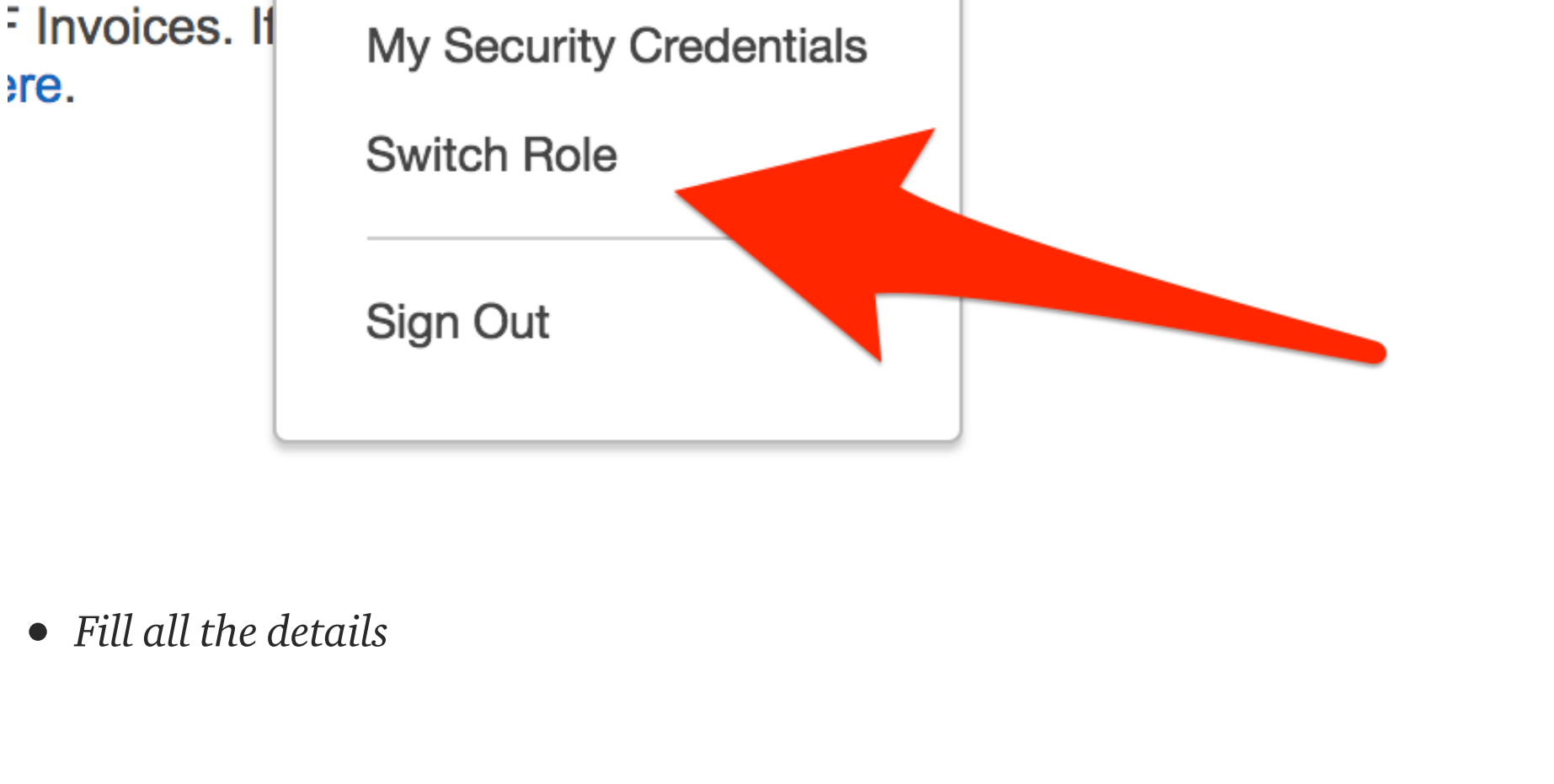
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::XXXXX:root" <-----
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {}
11    }
12  ]
13 }
```

root_trust_policy hosted with  by GitHub [view raw](#)

- As you can see only root user has access to AssumeRole, change it with the arn of the user you want to assume this role

Step3: Test access by Switching the role

- Again go back to the Account Tab but this time click on Switch Role



- Fill all the details


Switch Role

Allows management of resources across AWS accounts using a single user ID and password. You can switch roles after an AWS administrator has configured a role and given you the account and role details. [Learn more](#)

Account*

Role*

Display Name

Color 

* Required [Cancel](#) [Switch Role](#)

* Account: This is Prod/Account A ID

* Role: Role we created in Step1: S3ReadOnlyAccessToDevAccount(Dont give full arn here just the Role name)

* Display Name: Any display name

* Switch Role

- You will see something like this

NOTE: You cannot switch to a role when you are signed in as the AWS account root user.

- Now go to S3 console and try to access S3 bucket which is present in Account A.

Looking forward from you guys to join this journey and spend a minimum an hour every day for the next 100 days on DevOps work and post your progress using any of the below medium.



- Twitter: [@100daysofdevops](#) OR [@lakhera2015](#)
- Facebook: <https://www.facebook.com/groups/795382630808645/>
- Medium: <https://medium.com/@devopslearning>
- Slack: <https://devops-myworld.slack.com/messages/CF41EFG49/>
- GitHub Link:<https://github.com/100daysofdevops>



Reference

100 Days of DevOps — Day 0


D-day is just one day away and finally, this is a continuation of the post(I posted a month earlier)

medium.com

 6 

Get an email whenever Prashant Lakhera publishes.

 Subscribe

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.

More from Prashant Lakhera


AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHCDs, RHCE, Docker Certified, 4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP

Published in FAUN Publication · Feb 18, 2019

100 Days of DevOps — Day 8-Introduction to AWS Security Token Service(STS)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 4 min read



Share your ideas with millions of readers. [Write on Medium](#)

100 Days of DevOps — Day 7(AWS S3 Event)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/>...


AWS 3 min read



100 Days of DevOps — Day 6-CloudWatch Logs(Metric Filters)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 3 min read



100 Days of DevOps — Day 5-(CloudWatch to Slack Notification)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 6 min read



100 Days of DevOps — Day 4(CloudWatch log agent Installation — Centos7)

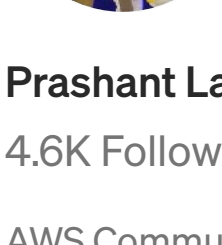
Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 8 min read

Love podcasts or audiobooks? Learn on the go with our new app. [Try Knowable](#)

[Get started](#) [Sign in](#)

 Search




Prashant Lakhera
4.6K Followers

AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHCDs, RHCE, Docker Certified, 4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP

[Follow](#) 


More from Medium

 Ama... in DevOp...
4.6K Followers

Auto Scaling in AWS

 Neelam Jyoti
4.6K Followers

Challenges with DevOps

 Neal Davis
4.6K Followers

What does AWS mean by Cost Optimization?

 Slav... in Nextdo...
4.6K Followers

Learn DevOps by Doing

Help Status Writers Blog Careers
Privacy Terms About Knowable