Prashant Lakhera
Feb 19, 2019 · 3 min read · Listen

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

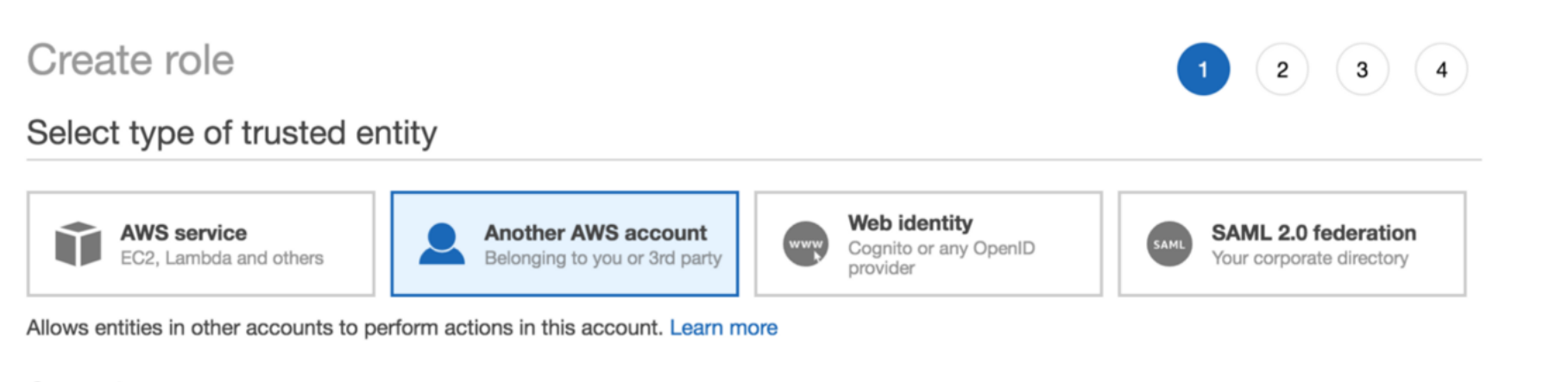
- *We don't need to set up individual IAM user in each account*
- *The user doesn't need to sign out of one account and sign into another account to access resources.*

Pre-requisites

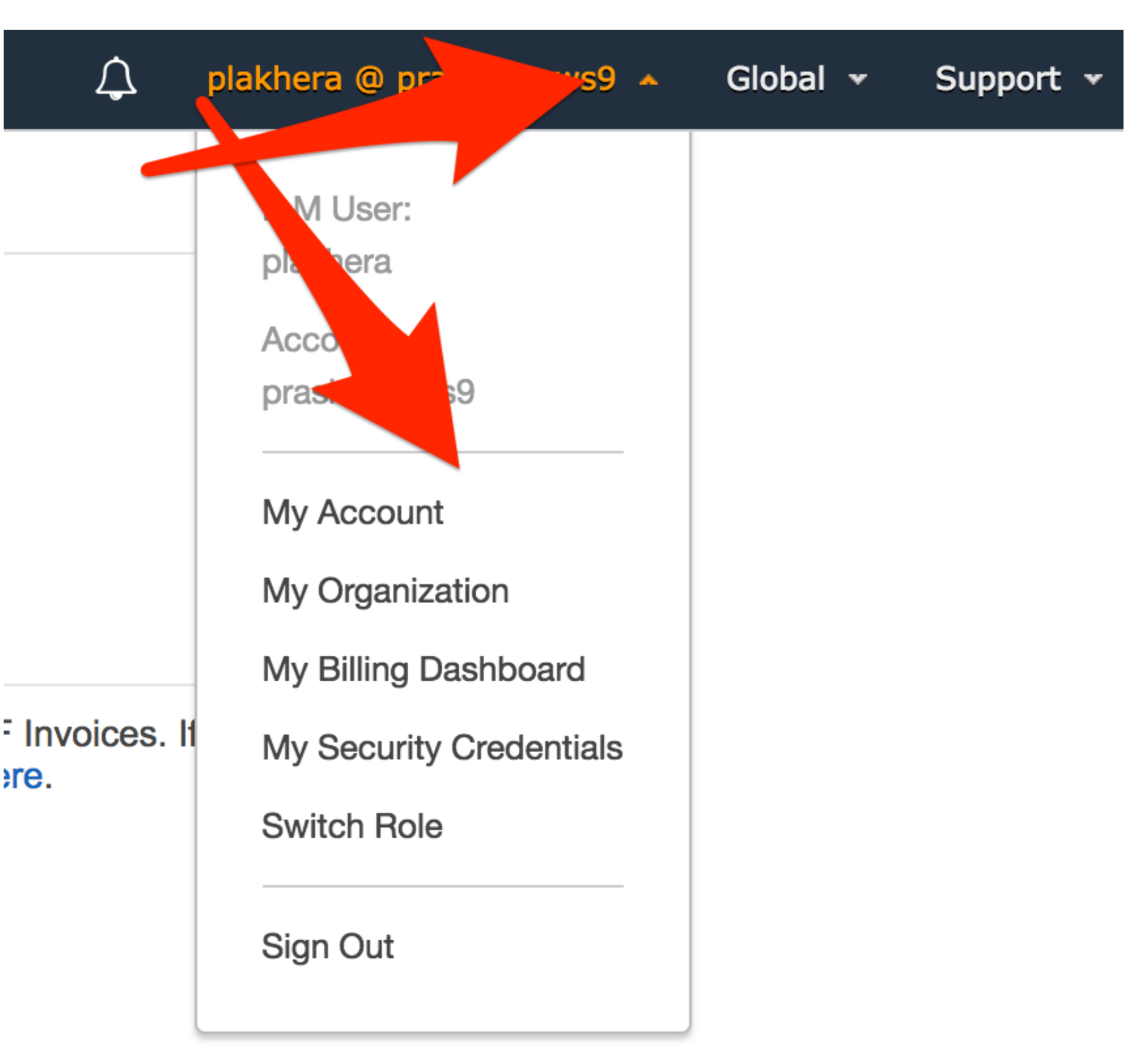
- *You need two AWS accounts(Account A(PROD)) and Account B(Developer))*
- *An AWS S3 bucket created in Production Account A.*

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*



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

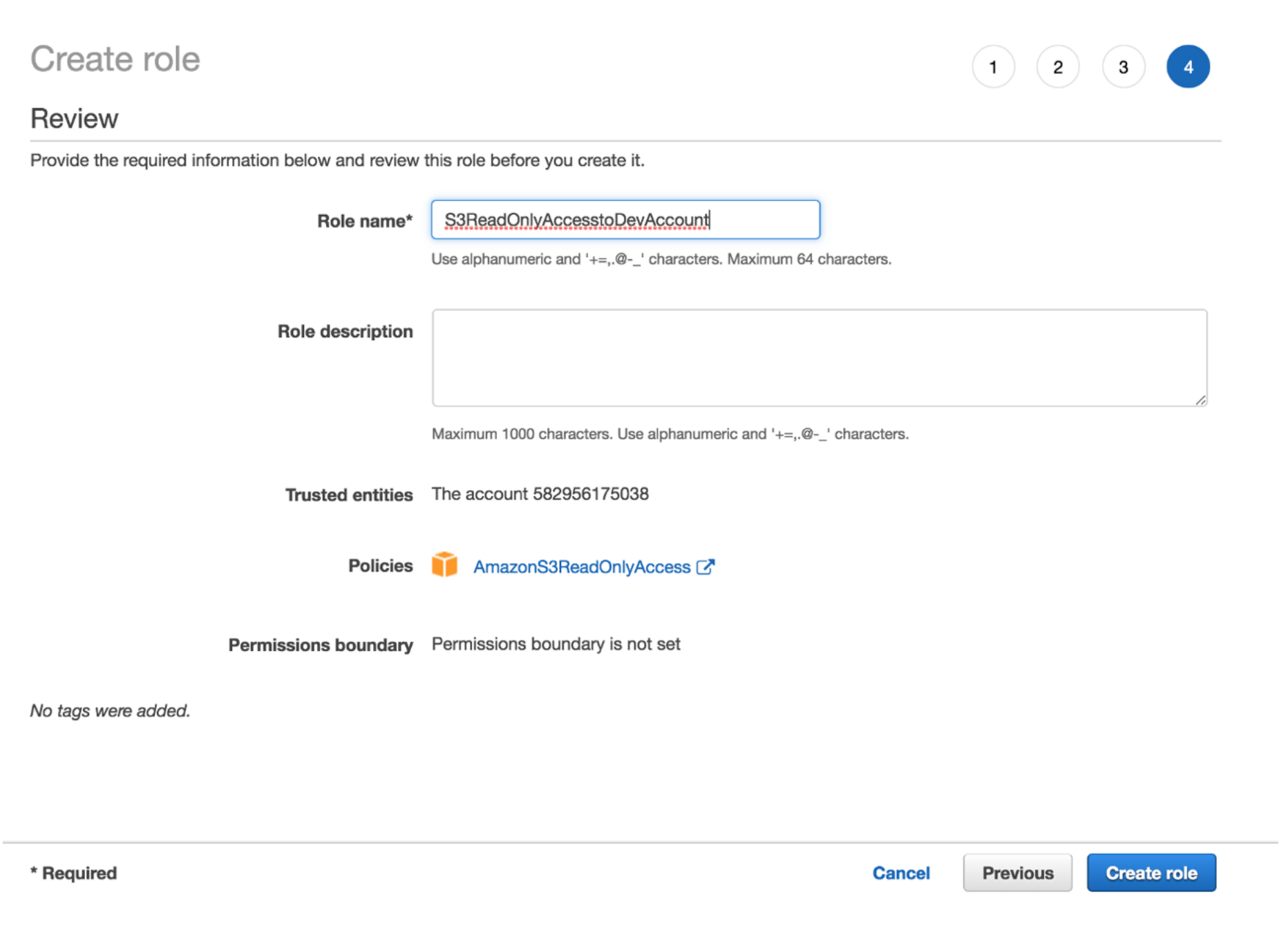


- *In next screen click on Create Policy and paste the below mentioned(Change the bucket name with the name of the bucket you want to share with Development Account) OR Choose S3ReadOnlyPolicy*

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
       ],
      "Resource": "arn:aws:s3:::bucket name"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::bucket name/*"
    }
  ]
}
```

gistfile1.txt hosted with ❤ by GitHub view raw

- *Click Next and give your Role name*



- *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*

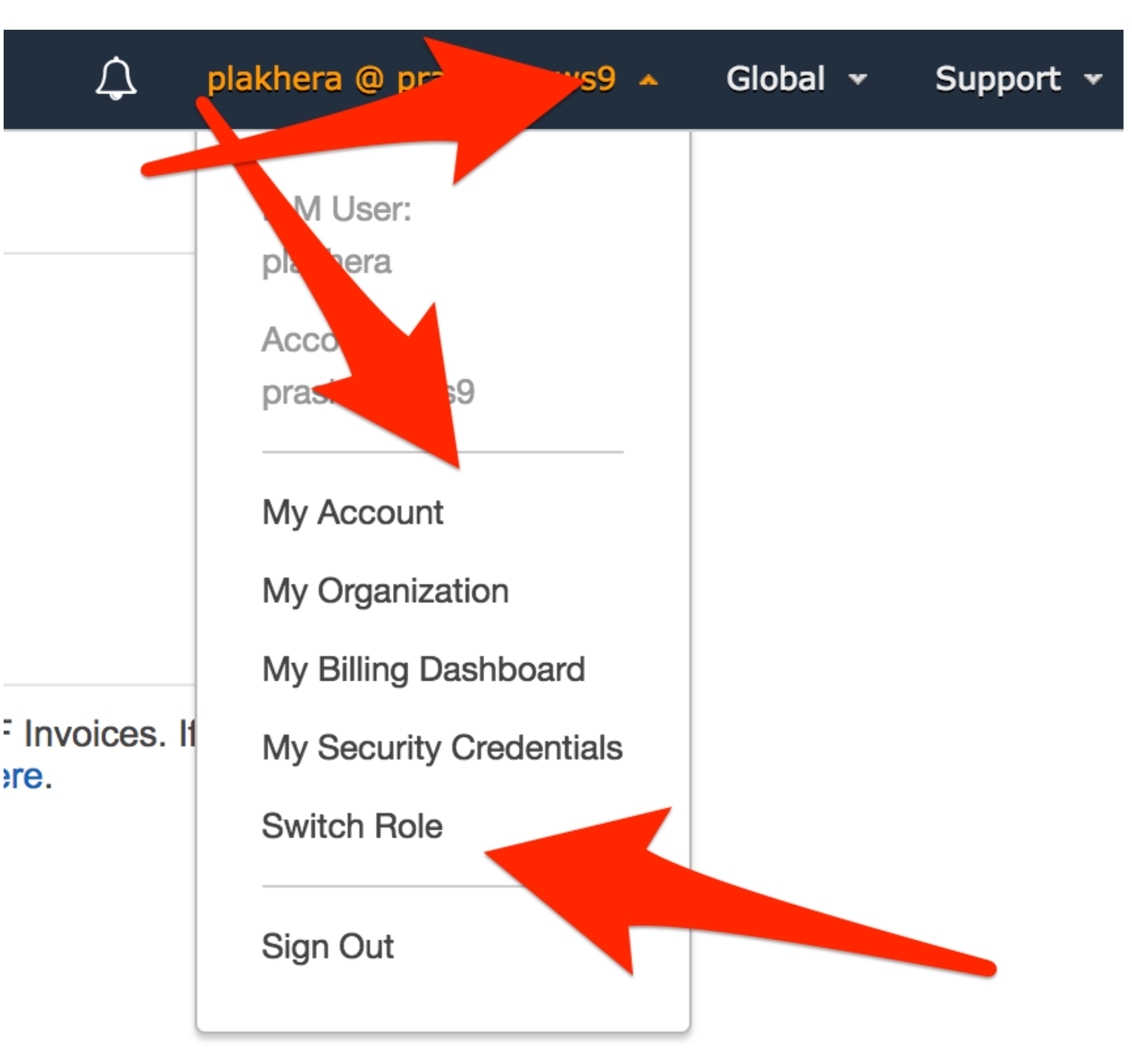
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::XXXXX:root" <----
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

root_trust_policy hosted with ❤ by GitHub view raw

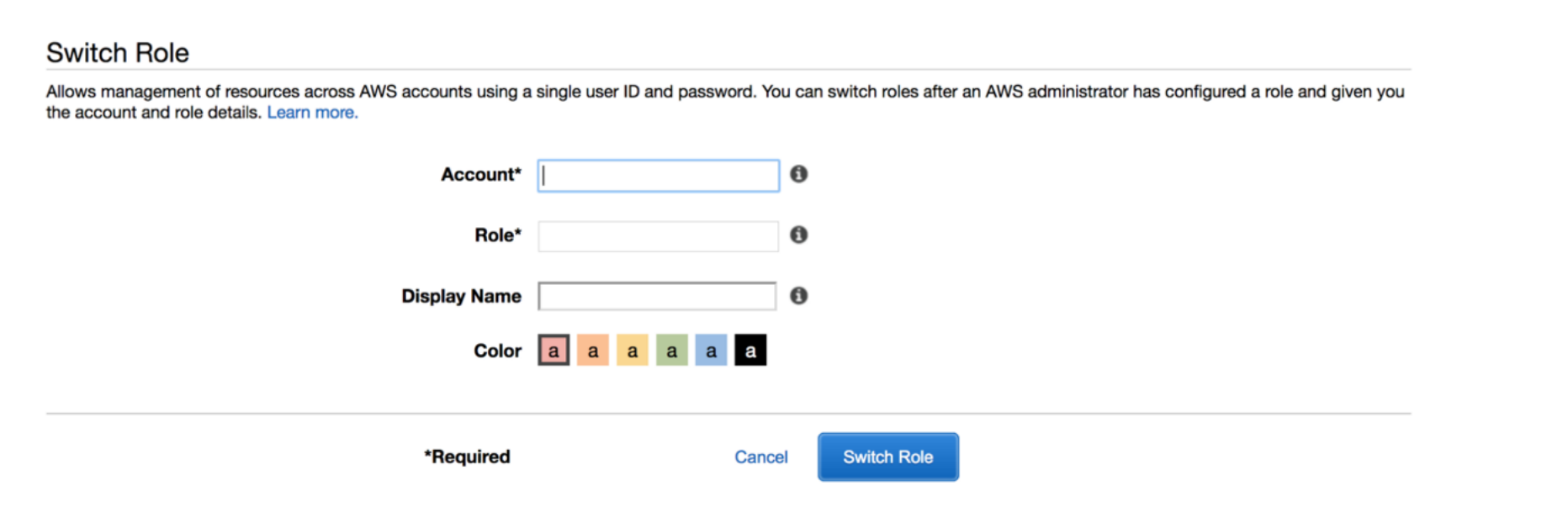
- *As you can see only root user has access to AssumeRole, change it with the arn of the user you want to assume this role*

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*



** 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