|  |
| --- |
| Section 8) AWS CLI,SDK,IAM Roles and Policies    Machine generated alternative text: Section Introduction  • So far, we've interacts with services manually and they exposed standard  information for clients:  • EC2 exposes a standard Linux machine we can use any way we want  • RDS exposes a standard databas  • ElastiCache exposes a cache U  • ASG / ELB are automated and e  • Route53 was setup manual  connect to using a URL  n nnect to using a URL  to program against them  • Developing against AWS has two components:  • How to perform interactions with AWS without using the Online Console?  • How to interact with AWS Proprietary services? (S3, DynamoDB, etc... )  This is where cli come in picture  Machine generated alternative text: Section Introduction  • Developing and performing AWS tasks against AWS can be done in  several ways  • Using the AWS CLI on our local computer  • Using the AWS CLI on our EC2 machines  • Using the AWS SDK on our local computer  • Using the AWS SDK on our EC2 machines  • Using the AWS Instance Metadata Service for EC2  • In this section, we'll learn:  • How to do all of those  • In the right & most secure way, adhering to best practices    **AWS CLI( command line interface)**    **Aws cli configuration**    Machine generated alternative text: AWS CLI Configuration  • Let's learn how to properly configure the CLI  AWS NETWORK  AWS Account  CLI access over www  Computer  (checks credentials and  permissions)  • We'll learn how to get our access credentials and protect them  • Do not share your AWS Access Key and Secret key with anyone! |
| Don’t share it  Machine generated alternative text: awS configure  AWS Access Key ID (None): AKIA3U3ESLUCOWGA34A  AWS secret Access Key (None) : vuøjYLacKc4zpwyqHGb9WINassøZXIN-mupt  Default region name (None):  Default Output format (None) :  configure  AWS A c s Key ID :  AWS Secret Access Key :  Default region name :  Default Output format (None) :  config  credentials  cat -4 .aws/config  Idefault)  cat  (default)  aws secret access_key      AWS CLI on EC2    Machine generated alternative text: AWS CLI ON EC2... THE BADWAY  • We could run configure' on EC2 just like we did (and it'll work)  • But... it's SUPER INSECURE  • NEVER EVER EVER PUT YOUR PERSONAL CREDENTIALS ON AN EC2  • Your PERSONAL credentials are PERSONAL and only belong on your  PERSONAL computer  • If the EC2 is compromised, so is your personal account  • If the EC2 is shared, other people may perform AWS actions while  impersonating you  • For EC2, there's a better way... it's called AWS IAM Roles    Machine generated alternative text: AWS CLI ON EC2... THE RIGHT WAY  • IAM Roles can be attached to EC2 instances  • IAM Roles can come with a policy authorizing exactly what the EC2 instance  should be able to do  EC2 Instance  IAM ROLE  AWS NETWORK  AWS Account  CLI  (checks credentials and  permissions of the ROLE)  • EC2 Instances can then use these profiles automatically without any additional  configurations  • This is the best practice on AWS and you should 100% do this.    **NOTE: always use IAM roles never put credential on EC2 machine**    **Note this instance don’t have any IAM role attached**    Machine generated alternative text: Launch Instance  Connect  Actions  Availability Zone  eu-west-3c  Status Checks  0 2/2 checks  1 to 1 of 1  Q Filter by tags and attributes or search by keyword  Alarm Status  None  Name  Instance ID  i-Oe3862d740eOb89...  Instance Wpe  t2.micro  Instance State  running  Public DNS (IP  15— 188— 14— •  Private DNS  Private IPS  Secondary private IPS  VPC ID  Platform  Platform details  Usage operation  Source/dest. check  T2/T3 Unlimited  EBS-optimized  eu-west-3c  launch-wizard-I. view inbound rules.  view outbound rules  No scheduled events  amzn2-ami-hvm-2.O.20200917.O-  x86 64-gp2 (ami-Ode12f76efe134f2f)  subnet-d61e6a9b  eth0  Ec2 Tutorial  398678778168  October 5, 2020 at PM  ip-172-31-40-237.eu-west-  3.compute.internal  172.31.40.237  vpc-c14dafa9  Amazon Linux  Linux/UNlX  Runlnstances  True  Disabled  False  Availability zone  Security groups  Scheduled events  AMI ID  Subnet ID  Network interfaces  ro  Key pair name  Owner  Launch time |
| Note**: we can attach role to lot of different services** |
| **Roles: any services have own set of permission**    **Step: to create role and attached it**    **Do ssh from poweshell**  Don’t configure aws access key and secret key here use role for that     1. **Select role in IAM /create role/select EC2 next**   Machine generated alternative text: Create role  Select type of trusted entity  AWS service  EC2, Lambda and others  2  3  4  Another AWS account  Belonging to you or 3rd party  Web identity  Cognito or any OpenlD  provider  KMS  SAML 2.0 federation  SAML  Your corporate directory  Rekognition  Allows AWS services to perform actions on your behalf. Learn more  Choose a use case  Common use cases  EC2  Allows EC2 instances to call AWS services on your behalf.  Lambda  Allows Lambda functions to call AWS services on your behalf.  Or select a service to view its use cases  EMR  API Gateway  * Required  CodeBuild  Cancel  Next: Permissions      **Attach policy to role**    Machine generated alternative text: Create role  Attach permissions policies  Choose one or more policies to attach to your new role.  Create policy  Filter policies v  Policy name  AmazonDMSRedshiftS3Role  AmazonS3FullAccess  AmazonS30utpostsFullAccess  AmazonS30utpostsReadOnlyAccess  AmazonS3ReadOnlyAccess  QuickSightAccessForS3StorageManagementAnalyticsReadOnly  * Required  Used as  None  None  None  None  None  None  Cancel  3  4  Showing 6 results  Previous  Next: Tags    **Step 3)**  Machine generated alternative text: Create role  Review  Provide the required information below and review this role before you create it.  00  Create role  Role name*  Role description  Trusted entities  Policies  Permissions boundary  * Required  MyFirstEc2R01e  Use alphanumeric and characters. Maximum 64 characters.  Allows EC2 instances to make read only call to amazon s3  Maximum 1000 characters. Use alphanumeric and characters.  AWS service: ec2.amazonaws.com  AmazonS3ReadOnlyAccess  Permissions boundary is not set  Cancel  Previous      **STEP 4) go to ec2 machine ( right click - instance setting /attach replace IAM role )**    Machine generated alternative text: Instances Attach/Replace IAM Role  Attach/Replace IAM Role  Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console.  If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.  Apply  Create new IAM role  Cancel  Instance ID i-Oe3862d740eOb899d O  IAM role* No Roe  Q Filter by attributes  * Required  Profile Name  No Role  MyFirstEc2Role    **Now see IAM role is attached**    Machine generated alternative text: Launch Instance  Connect  Actions  Availability Zone  eu-west-3c  Instance State  running  Status Checks  0 2/2 checks  1 to 1 of 1  Q Filter by tags and attributes or search by keyword  Alarm Status  None  Name  Instance ID  i-Oe3862d740eOb89...  Instance Wpe  t2.micro  Public DNS (IP  15— 188— 14— •  Private IPS  Secondary private IPS  VPC ID  Platform  Platform details  Usage operation  Source/dest. check  T2/T3 Unlimited  EBS-optimized  3.compute.internal  172.31.40.237  vpc-c14dafa9  Amazon Linux  Linux/UNlX  Runlnstances  True  Disabled  False  Security groups  Scheduled events  AMI ID  Subnet ID  Network interfaces  IAM role  Key pair name  Owner  Launch time  launch-wizard-I. view inbound rules.  view outbound rules  No scheduled events  amzn2-ami-hvm-2.O.20200917.O-  x86 64-gp2 (ami-Ode12f76efe134f2f)  subnet-d61e6a9b  eth0  MyFirstEc2R01e  Ec2 Tutorial  398678778168  October 5, 2020 at PM  UTC+5:30 (less than one hour)    **NOTE:**    **Now the command is succeeded**    Machine generated alternative text: make  bucket failed:  Lec2-user@ip-172-31  Lec2-user@ip-172-  2323-13-35 07:56.  Lec2-user@ip-172-  2020-10-05  2323-13-35 37  2323-13-35 37  2020-10-05 37  Lec2-user@ip-172-  •46  31  31  31-40-237 aws Is  thebucketofsaurabh2Ø2Ø  Access  -43-237 M$ aws s3 Is s3://thebucketofsaurabh2Ø2Ø  5581 beach. jpg  66882 coffee. jpg  23 error. html  172 index. html  -43-237 M$ aws s3 mb s3://newbucketdemo  s3://newbucketdemo An error occurred (AccessDenied) when calling the CreateBucket operation:  -43-237 M$    **NOTE :**    **That means ec2 role is not enough permission to make bucket**    **Note: we can also attach policy to role later**    **NOTE**: iam policy can take little bit of time to be effective    **Remove bucket**  Machine generated alternative text: Lec2-user@ip-172-31-aa-237 M$ aws s3 rb s3://newbucketdemohe110e  remove bucket: newbucketdemohelloe  Lec2-user@ip-172-31-aa-237 M$      **NOTE:**  **IAM role can be attached to many ec2 instance but ec2 instance can be attach to only one IAM role at a time**    **Iam role use to give permission to EC2 instance so that they can make call**    **AWS cli practice with s3**    **In google we can search aws s3 cli : and the check examples**      **We can play with s3**    <https://docs.aws.amazon.com/cli/latest/reference/s3/>  Machine generated alternative text: Lec2-user@ip-172-31-aa-237 M$ aws s3 cp s3://thebucketofsaurabh2Ø2Ø/coffee.jpg coffee. jpg  download: s3://thebucketofsaurabh2Ø2Ø/coffee.jpg to ./coffee.jpg  Lec2-user@ip-  172-31-43-237 M$ 11  total 68  coffee . jpg  ec2-user ec2-user 66882 oct 5 ø7:43  -rw-rw-r-- 1  Lec2-user@ip-  172-31-aø-237 M$      **IAM Roles and Policies hands on**    **NOTE :** Attached policies are managed or we can create our own    **We can also attach inline policy**  **Ec2 role /select created policy /inline policy**    Machine generated alternative text: Identity and Access  Management (IAM)  Dashboard  Access management  Groups  Users  Roles  Policies  Identity providers  Account settings  Access reports  Access analyzer  Archive rules  Analyzers  Roles MyFirstEc2R01e  Summary  Role ARN  Role description  Instance Profile ARNs  Path  Creation time  Last activity  Maximum session duration  Allows EC2 instances to make read only call to amazon s3 1 Edit  arn:aws:iam::398678778168:instance-profile/MyFirstEc2Role  2020-10-05 17:26 UTC+0530  2020-10-05 17:41 UTC+0530 (Today)  1 hour Edit  Delete role  O Add inline policy  Access Advisor  Permissions  Tags  Trust relationships  Revoke sessions  Permissions policies (2 policies applied)  Attach policies      **This policy is added just for that role not for other role ( but don’t use it)**    Machine generated alternative text: tec2—user@ip—172—31—3—136 M$ aws ec2 run—instances help  tec2—user@ip—172—31—3—136 aws ec2 run—instances —dryrun —image—id ami—Ø634Øc8c12baa6aØ9 —instance—type t2.micro  An error occurred (UnauthorizedOperation) when calling the Runlnstances operation: You are not authorized to perform this operation. Enc  Oded authorization failure message:  QOtmv5tdUY5Ve IEAhc5090C8h4fYR1egBxflNrGSCq  K8F91YqgdbW_XVXYBi2 BE12P-8gFz4LmBkba1UdEy1h-WUS95X1nC301J8i3wzz-xKExGwu1HwoqS9QAq1qrn6jmrwwbTK  CbGBd t stckPXkesyNS5hLSNLBj j  d4QA9aMh38j TP1_-COPWLsvNq5Nbt  tec2—user@ip—172—31—3—136 aws ec2 run—instances —dryrun —image—id ami—Ø634Øc8c12baa6aØg —instance—type t2.micro  An error occurred (DryRunOperation) when calling the Runlnstances operation: Request would have succeeded, but DryRun flag is set.  1      Machine generated alternative text: AWS CLI STS Decode Errors  • When you run API calls and they fail, you can get a long error message  sing the STS command line:  • This error message can be deco  • Sts decode-authorization-mes  • Let's practice!    **AWS EC2 Instance Metadata**    Machine generated alternative text: AWS EC2 Instance Metadata  • AWS EC2 Instance Metadata is powerful but one of the least known features  to developers  • It allows AWS EC2 instances to "l  IAM Role for that purpose.  ut themselves" without using an  • The URL is http://169.254. 169. 4/1 -••••qrn a-data  • You can retrieve the IAM Role  m le metadata, but you CANNOT  retrieve the IAM Policy.  • Metadata Info about the EC2 instance  • Userdata launch script of the EC2 instance    **Remember this ip**  USING THIS url we will get lot of information about ec2    Machine generated alternative text: "Expiration  tec2-user@ip-172-31-3-136 curl http://16g.254.16g.254/1atest,'meta-data/  arni-id    Machine generated alternative text: tec2-userup-172-31-3-136 -v)$ curt http://169.254.169.254  l.ø  2øø7-ø1-19  2øø7-ø3-ø1  2øø7-ø8-29  2øø7-1ø-1ø  2øø7-12-15  2øø8-ø2-ø1  2øø8-ø9-ø1  2ø11-ø1-ø1  2ø11-ø5-ø1  2ø12-ø1-1É  2ø14-ø2-25  2ø14-11-ø5  2ø15-1ø-2ø  2ø16-ø4-19  2ø16-ø6-3ø  2ø16-øg-ø2  2ø18-ø3-28  1  latest lec2-useQip-172-31-3-136    Machine generated alternative text: tec2-userup-172-31-3-136 -v)$ curt http://169.254.169.254/1atest/  dynamic  meta—data  user-datalec2-userup-172-31-3-136 curl http://169.254.169.254/1atest,1    Machine generated alternative text: tec2-userup-172-31-3-136 -v)$ curt http://169.254.169.254/1atest/  dynamic  meta—data  user—data  ami—id  ami-launch—index  ami—manifest-path  block—device—mapping  1  hostname  iam/  instance—action  instance—id  instance—type  local—hostname  local—ipv4  mac  metrics/  netwo rk/  placement/  profile  pub tic—hostname  pub lic—ipv4  pub tic—keys/  reservation—id  security—g roups  services/ lec2-userUp-172-31-3-136  curl http://169.254.169.254/1atest/meta-data,'      **Anytime / means more to it**    **Will get role name**  Machine generated alternative text: ip—172—31—3—136.eu—west—3.compute. internal --)$ curl http://169.254.16g.254/latest/meta—data/iam/  info  security-credentials/ --1$ curl http://169.254.16g.254/latest/meta—data/iam/security—credentials  M $ curl http://169.254.169.254/Iatest/meta—data/iam/security—credentiaIs/    **Very important**  **Behind the scene when we attached role to ec2 instance it get access key id and secret**    Machine generated alternative text: ip—172—31—3—136.eu—west—3.compute. internal --)$ curl http://169.254.16g.254/latest/meta—data/iam/  info  security-credentials/ M$ curl http://169.254.169.254/latest/meta—data/iam/security—credentials  M $ curl http://169.254.169.254/Iatest/meta—data/iam/security—credentiaIs/  curl http://169.254.169.254/Iatest/neta—data/ian/security—credentials/MyFirstEC2ROIe  Code" : "Success",  "LastlJpdated"  "Type"  "AWS-H.IAC" ,  "AccessKeyId  " : "ASIAVUITFK302PW4H5JF" ,  "SecretAccessKey" : "KqlccsxSseYKiGu+rNCIM65/T9ØLSK7ssyec4/H"  "Token  " : "FQ0GZX1vYXdzEcwaDC7swnGeewy181g6hSKxA1qGPXJHk7esxtLALMtC61i  Y/Y8v1cøkjDKPUxgvøSLg/lPNQDU6fzBSACShyPlH5/KYDPh162NPFføecaB/i Ai4Y/xhvAnsr7CGDJ8R09+uwDYjøk3ymnfGByvP+Zw29TøkGEYP07mvuy5Kaox4DAGF  ICmm8ud7j8rZ610cuP3UnaCISR4bØ1fcYnCCyKBB2UOØCj hFKxau,'gowzAwS  Gj 9D2uVvkYE7LwoRGn6r93psEXidzfRrMicw1umD+e•y7Cwgv1pWpTQ1q liDBsj  +1fPQ07Hmv9bEJL6b&hBqu91D5/1YEtdY41tWWfpmx1vryrq9DwQPRt7Pv  "Expiration"  1  lec2-userup-172-31-3-136  _„.4E98ufEpcDKØ02vCi3QU:" ,      **AWS CLI PROFILES**    **Note : to configure multiple aws account from cli we will use profile**    **Aws configure --profile profile name**    Machine generated alternative text: Default output format  aws configure —profile  AWS Access Key ID (None) : Dkn86Vv9q7JE8hHn  AWS Secret Access Key (None) : hgsJgWwVR7WhRxu7z84rRAFDkPqd6  Default region name (None): us—west—2  Default output format (None): 1    Machine generated alternative text: region —  aWS 53 IS —profile  1    **AWS CLI with MFA** |
| Machine generated alternative text: MFA with CLI  • To use MFA with the CLI, you must create a temporary session  • To do so, you must run the STS GetSessionToken API call  • aws Sts get-session-token --serial-number am-of-the-mfa-device --token-  code code-from-token --duration-seconds 3600  "Credentials":  "SecretAccessKey": "secret—access—key" ,  "SessionToken": "temporary—session—token" ,  " Expiration": ,  "AccessKeyId" :      **Step 1)**    **Enabled mfa in security credential of user iam**    Machine generated alternative text: avvS  Iden tity and Access  Management (IAM)  Identity providers  settings  Access reports  activity  Sewice Control  Resource Groups  Uses  Summary  creation tin.  Sign-in credentials  2018&-191323 uTC*01m  Global  Ena—  password  MFA  Access keys  •use acces to REST HTTP AVG APB_ you *tare wdh AS a  we key rotatm  Create ac•ss k"  Access key ID  2018-11-2614:21 UTC*01cn 2020-os.ca-49  Active  Make inactive    Machine generated alternative text: aws Sts get-session—token help  aws Sts get—session—token —serial—number arn:aws:iam: :387124123361:mfa/stephane —token—code 82846*    **Note : now we will get credential**    Machine generated alternative text: "Credentials" .  "AccessKeY1d": "ASIAVUITFK3Q61NEXA5K" ,  ' 'SecretAccessKey" : "XEucPd1SiCOG50zFFeOGyJzvzCquARxkq2n6jm+T" ,  "SessionToken": "IQoJb3JpZ21uX2VjEFoaCWILXd1c3QtMSJ+1EUCIAN01+VRyYAdQgPd5a6FkodfL46egGauG9EKF6XBhvWOAiEA2T5Yk1TOsGSuPpzKp1nmbbh  y/CQrWZ093nFH17bJcoqsOE1k// // EiDAC1 FfReoRyddoOD6SqFAZITUf1Dwn8/080VOKØHCoFOrB136VZH59ØntGqKn/DIXk1 ITJtRDx  3 nGt+8Kpe4LLZi IGeegxzj j u r7 j æxY4Br334BhX1fpgZRk-w8YDgsQCSbsq6gVR9+pQø8witXG9QlJ63gE  ZG040NR-J j J Les BIG keBiC1uøseLJUV/n+0isRxeGmhSygbrFJPXayC3n9rK19e1vibkB19kvBz51JuXxLpøt9ZseDRQlJykEWQ rm1Ms IWROJMOPLmk+XhL rtgupi 171hLXj zppq8W  do IDØwcZk+dMOJEK3Pzk11YU-" ,  "Expiration  ( END)    Machine generated alternative text: aws Sts get-session—token help  aws Sts get—session—token —serial—number arn:aws:iam: :387124123361:mfa/stephane  aws Sts get—session—token —serial—number  aws configure —profile mfa  AWS Access Key ID (None) : ASIAVUITFK3QIJO'WRTSW1  AWS Secret Access Key (None) : M9dqxXYLIQfdXi+QOOiuX/FPMgNp2RL8mHYudzNB  Default region name (Nonel :  Default output format (None):  —token-code 828463  —token-code 889485      Machine generated alternative text: AVVS SDK Overview  • What if you want to perform actions on AWS directly from your applications  code ? (without using the CLI).  • You can use an SDK (software development kit) !  • Official SDKs are...  • Java  • .NET  Node.js  •  • Python (named bot03 / botocore)  • Ruby    Machine generated alternative text: AVVS SDK Overview  • We have to use the AWS SDK when coding againstAWS Services such  as DynamoDB  • Fun fact... the AWS CLI uses the Python SDK (bot03)  • The exam expects you to know when you should use an SDK  • We'll practice the AWS SDK when we get to the Lambda functions  • Good to know: if you don't specify or configure a default region, then  us-east- I will be chosen by default    Machine generated alternative text: AWS Limits (Quotas)  • API Rate Limits  • Describelnstances API for EC2 has a limit of 100 calls per seconds  • GetObject on S3 has a limit of 5500 GET per second per prefix  • For Intermittent Errors: implem Expo tial Backoff  • For Consistent Errors: request limit increase  • Service Ouotas (Service Limits)  • Running On-Demand Standard Instances: 1 152 vCPU  • You can request a service limit increase by opening a ticket  • You can request a service quota increase by using the Service Quotas API    **Note : if we get throtling exception will use exponential backoff**  **Increase time of double for api call**  Machine generated alternative text: Exponential Backoff (any AWS service)  • If you get ThrottlingException intermittently, use exponential backoff  • Retry mechanism included in SDK API calls  • Must implement yourself if using the API as is or in specific cases    Machine generated alternative text: AWS CLI Credentials Provider Chain  • The CLI will look for credentials in this order  2.  3.  4.  5.  6.  Command line options — —region, --output, and --profile  Environment variables-AWS ACCESS KEY ID,AWS SECRET ACCESS KEY,  and  CLI credentials file —aws configure  —/.aws/credentials on Linux / Mac & C:wsersxuserx.awsxcredentials on Windows  CLI configuration file — aws configure  —/.aws/config on Linux / macOS & C:XUsersXUSERNAMEX.awsXconfig on Windows  Container credentials — for ECS tasks  Instance profile credentials — for EC2 Instance Profiles      Machine generated alternative text: AWS SDK Default Credentials Provider Chain  • The Java SDK (example) will look for credentials in this order  2.  3.  4.  5.  Environment variables —  AVVS ACCESS KEY ID and ANS SECRET ACCESS KEY  Java system properties — aws.accessKeyld and aws.secretKey  The default credential profiles file — ex at: —/.aws/credentials, shared by  many SDK  Amazon ECS container credentials — for ECS containers  Instance profile credentials— used on EC2 instances    Machine generated alternative text: AWS Credentials Scenario  • An application deployed on an EC2 instance is using environment variables  with credentials from an IAM user to call the Amazon S3 API.  • The IAM user has S3FullAccess permissions.  • The application only uses one S3 bucket, so according to best practices:  • An IAM Role & EC2 Instance Profile was created for the EC2 instance  • The Role was assigned the minimum permissions to access that one S3 bucket  • The IAM Instance Profile was assigned to the EC2 instance, but it still had  access to all S3 buckets.VVhy?  the credentials chain is still giving priorities to the environment variables      Machine generated alternative text: AWS Credentials Best Practices  • Overall, NEVER EVER STORE AWS CREDENTIALS IN YOUR CODE  • Best practice is for credentials to be inherited from the credentials chain  • If using working within AWS, use IAM Roles  • EC2 Instances Roles for EC2 Instances  • ECS Roles for ECS tasks  • Lambda Roles for Lambda functions  • If working outside ofAWS, use environment variables / named profiles    Machine generated alternative text: Signing AWS API requests  • When you call the AWS HITP API, you sign the request so that AWS  can identify you, using your AWS credentials (access key & secret key)  • Note: some requests to Amazon S3 don't need to be signed  • If you use the SDK or CLI, the HTV P requests are signed for you  • You should sign an AWS HIT P request using Signature v4 (SigV4)  to |