aws pentensting workshop

```
┌──(mahathi㉿SriGanesha)-[~]
└─$  aws configure --profile iam
AWS Access Key ID [****************HVM2]: AKIAX6IOGWSMRGMHHVM2
AWS Secret Access Key [****************C5Mo]: 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
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws sts get-caller-identity --profile iam
{
"UserId": "AIDAX6IOGWSM5UA7LJ2U5",
"Account": "546027517081",
"Arn": "arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Joel"
}
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$  aws iam list-users --profile iam
{
"Users": [
{
"Path": "/",
"UserName": "introduction-to-aws-iam-enumeration-1760675857628-Chris",
"UserId": "AIDAX6IOGWSMUCKLHHORA",
"Arn": "arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Chris",
"CreateDate": "2025-10-17T04:37:44+00:00"
},
{
"Path": "/",
"UserName": "introduction-to-aws-iam-enumeration-1760675857628-Joel",
"UserId": "AIDAX6IOGWSM5UA7LJ2U5",
"Arn": "arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Joel",
"CreateDate": "2025-10-17T04:37:42+00:00"
},
{
"Path": "/",
"UserName": "introduction-to-aws-iam-enumeration-1760675857628-Mary",
"UserId": "AIDAX6IOGWSMSWETHD524",
"Arn": "arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Mary",
"CreateDate": "2025-10-17T04:37:44+00:00"
},
{
"Path": "/",
"UserName": "introduction-to-aws-iam-enumeration-1760675857628-Mike",
"UserId": "AIDAX6IOGWSMXYEFT7UGQ",
"Arn": "arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Mike",
"CreateDate": "2025-10-17T04:37:42+00:00"
}
]
}
```

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam list-attached-user-policies --user-name introduction-to-aws-iam-enumeration-1760675857628-Chris --
```

profile iam
{
"AttachedPolicies": []
}

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam list-user-policies --user-name  introduction-to-aws-iam-enumeration-1760675857628-Chris --profile iam
{
"PolicyNames": []
}

┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam list-user-policies --user-name introduction-to-aws-iam-enumeration-1760675857628-Joel --profile iam
{
"PolicyNames": [
"AllowEnumerateRoles"
]
}

┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam get-user-policy --user-name introduction-to-aws-iam-enumeration-1760675857628-Joel --policy-name
AllowEnumerateRoles --profile iam
{
"UserName": "introduction-to-aws-iam-enumeration-1760675857628-Joel",
"PolicyName": "AllowEnumerateRoles",
"PolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"iam:GetRole",
"iam:GetRolePolicy",
"iam:ListRoles",
"iam:ListRolePolicies"
],
"Resource": "*",
"Effect": "Allow"
}
]
}
}

┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam list-roles --profile iam
{
"Roles": [
{
"Path": "/aws-reserved/sso.amazonaws.com/",
"RoleName": "AWSReservedSSO_LabAdministrationAccess_054e9fc29832c558",
"RoleId": "AROAX6IOGWSMSPPDRHUUV",
"Arn": "arn:aws:iam::546027517081:role/aws-
reserved/sso.amazonaws.com/AWSReservedSSO_LabAdministrationAccess_054e9fc29832c558",
"CreateDate": "2024-07-31T17:47:46+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Federated": "arn:aws:iam::546027517081:saml-provider/AWSSSO_073d9cef9904420c_DO_NOT_DELETE"
```

},
"Action": [
"sts:AssumeRoleWithSAML",
"sts:TagSession"
],
"Condition": {
"StringEquals": {
"SAML:aud": "https://signin.aws.amazon.com/saml"
}
}
}
]
},
"Description": "Administrator access for lab accounts",
"MaxSessionDuration": 43200
},
{
"Path": "/aws-reserved/sso.amazonaws.com/",
"RoleName": "AWSReservedSSO_LabReadOnlyAccess_421aabcfcc983c0a",
"RoleId": "AROAX6IOGWSM55QI3PQFO",
"Arn": "arn:aws:iam::546027517081:role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_LabReadOnlyAccess_421aabcfcc983c0a",
"CreateDate": "2024-07-31T17:47:46+00:00",
"AssumeRolePolicyDocument": {
{
"Roles": [
{
"Path": "/aws-reserved/sso.amazonaws.com/",
"RoleName": "AWSReservedSSO_LabAdministrationAccess_054e9fc29832c558",
"RoleId": "AROAX6IOGWSMSPPDRHUUV",
"Arn": "arn:aws:iam::546027517081:role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_LabAdministrationAccess_054e9fc29832c558",
"CreateDate": "2024-07-31T17:47:46+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Federated": "arn:aws:iam::546027517081:saml-provider/AWSSSO_073d9cef9904420c_DO_NOT_DELETE"
},
"Action": [
"sts:AssumeRoleWithSAML",
"sts:TagSession"
],
"Condition": {
"StringEquals": {
"SAML:aud": "https://signin.aws.amazon.com/saml"
}
}
}
]
},
"Description": "Administrator access for lab accounts",
"MaxSessionDuration": 43200
},
{
"Path": "/aws-reserved/sso.amazonaws.com/",

"RoleName": "AWSReservedSSO_LabReadOnlyAccess_421aabcfcc983c0a",
"RoleId": "AROAX6IOGWSM55QI3PQFO",
"Arn": "arn:aws:iam::546027517081:role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_LabReadOnlyAccess_421aabcfcc983c0a",
"CreateDate": "2024-07-31T17:47:46+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Federated": "arn:aws:iam::546027517081:saml-provider/AWSSSO_073d9cef9904420c_DO_NOT_DELETE"
},
"Action": [
"sts:AssumeRoleWithSAML",
"sts:TagSession"
],
"Condition": {
"StringEquals": {
"SAML:aud": "https://signin.aws.amazon.com/saml"
}
}
}
]
},
"Description": "Read only access for lab accounts",
"MaxSessionDuration": 43200
},
{
"Path": "/aws-service-role/member.org.stacksets.cloudformation.amazonaws.com/",
"RoleName": "AWSServiceRoleForCloudFormationStackSetsOrgMember",
"RoleId": "AROAX6IOGWSM4QX2TN63Z",
"Arn": "arn:aws:iam::546027517081:role/aws-service-role/member.org.stacksets.cloudformation.amazonaws.com/AWSServiceRoleForCloudFormationStackSetsOrgMember",
"CreateDate": "2024-05-15T17:04:12+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "member.org.stacksets.cloudformation.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"Description": "Service linked role for CloudFormation StackSets (Organization Member)",
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/cloudtrail.amazonaws.com/",
"RoleName": "AWSServiceRoleForCloudTrail",
"RoleId": "AROAX6IOGWSM3KIUALQY5",
"Arn": "arn:aws:iam::546027517081:role/aws-service-role/cloudtrail.amazonaws.com/AWSServiceRoleForCloudTrail",
"CreateDate": "2024-03-09T03:08:53+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",

```
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "cloudtrail.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/remediation.config.amazonaws.com/",
"RoleName": "AWSServiceRoleForConfigRemediation",
"RoleId": "AROAX6IOGWSMY3HYMJBXA",
"Arn": "arn:aws:iam::546027517081:role/aws-service-
role/remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
"CreateDate": "2024-07-16T14:27:34+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "remediation.config.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/elasticloadbalancing.amazonaws.com/",
"RoleName": "AWSServiceRoleForElasticLoadBalancing",
"RoleId": "AROAX6IOGWSMY5UPO7WPS",
"Arn": "arn:aws:iam::546027517081:role/aws-service-
role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
"CreateDate": "2024-07-13T10:07:11+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "elasticloadbalancing.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"Description": "Allows ELB to call AWS services on your behalf.",
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/fms.amazonaws.com/",
"RoleName": "AWSServiceRoleForFMS",
```

"RoleId": "AROAX6IOGWSMX7VV7ZEL4",
"Arn": "arn:aws:iam::546027517081:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS",
"CreateDate": "2025-01-16T20:44:08+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "fms.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/organizations.amazonaws.com/",
"RoleName": "AWSServiceRoleForOrganizations",
"RoleId": "AROAX6IOGWSM5CBLFWWPG",
"Arn": "arn:aws:iam::546027517081:role/aws-service-role/organizations.amazonaws.com/AWSServiceRoleForOrganizations",
"CreateDate": "2023-08-22T16:49:37+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "organizations.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"Description": "Service-linked role used by AWS Organizations to enable integration of other AWS services with Organizations.",
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/sso.amazonaws.com/",
"RoleName": "AWSServiceRoleForSSO",
"RoleId": "AROAX6IOGWSMU6HWRSMYH",
"Arn": "arn:aws:iam::546027517081:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO",
"CreateDate": "2023-08-22T16:49:46+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "sso.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},

"Description": "Service-linked role used by AWS SSO to manage AWS resources, including IAM roles, policies and SAML IdP on your behalf.",
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/support.amazonaws.com/",
"RoleName": "AWSServiceRoleForSupport",
"RoleId": "AROAX6IOGWSM5VYPVQGDU",
"Arn": "arn:aws:iam::546027517081:role/aws-service-role/support.amazonaws.com/AWSServiceRoleForSupport",
"CreateDate": "2023-08-22T16:49:36+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "support.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"Description": "Enables resource access for AWS to provide billing, administrative and support services",
"MaxSessionDuration": 3600
},
{
"Path": "/aws-service-role/trustedadvisor.amazonaws.com/",
"RoleName": "AWSServiceRoleForTrustedAdvisor",
"RoleId": "AROAX6IOGWSM5GFEXXZQF",
"Arn": "arn:aws:iam::546027517081:role/aws-service-role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor",
"CreateDate": "2023-08-22T16:49:36+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "trustedadvisor.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"Description": "Access for the AWS Trusted Advisor Service to help reduce cost, increase performance, and improve security of your AWS environment.",
"MaxSessionDuration": 3600
},
{
"Path": "/",
"RoleName": "lab",
"RoleId": "AROAX6IOGWSMU6A74NXSC",
"Arn": "arn:aws:iam::546027517081:role/lab",
"CreateDate": "2023-08-22T16:49:36+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{

"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::174005215664:root"
},
"Action": "sts:AssumeRole"
},
{
"Effect": "Allow",
"Principal": {
"Service": "codebuild.amazonaws.com"
},
"Action": "sts:AssumeRole"
},
{
"Effect": "Allow",
"Principal": {
"Service": "lambda.amazonaws.com"
},
"Action": "sts:AssumeRole"
},
{
"Effect": "Allow",
"Principal": {
"Service": "cloudformation.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
},
"MaxSessionDuration": 3600
},
{
"Path": "/",
"RoleName": "stacksets-exec-27c01f4bbd8bccd1670ea1389052cd5b",
"RoleId": "AROAX6IOGWSMZAV5YYILO",
"Arn": "arn:aws:iam::546027517081:role/stacksets-exec-27c01f4bbd8bccd1670ea1389052cd5b",
"CreateDate": "2024-05-15T17:04:20+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Id": "stacksets-exec-27c01f4bbd8bccd1670ea1389052cd5b-assume-role-policy",
"Statement": [
{
"Sid": "1",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::174005215664:role/aws-service-
role/stacksets.cloudformation.amazonaws.com/AWSServiceRoleForCloudFormationStackSetsOrgAdmin"
},
"Action": "sts:AssumeRole"
}
]
},
"Description": "Role created by AWSCloudFormation StackSets",
"MaxSessionDuration": 3600
},
{
"Path": "/",
"RoleName": "SupportRole",

"RoleId": "AROAX6IOGWSM4OIX6VYW3",
"Arn": "arn:aws:iam::546027517081:role/SupportRole",
"CreateDate": "2025-10-17T04:37:59+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::546027517081:root"
},
"Action": "sts:AssumeRole",
"Condition": {
"ArnEquals": {
"aws:PrincipalArn": "arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Mary"
}
}
}
]
},
"Description": "Assumable role for internal support",
"MaxSessionDuration": 3600
}
]
}

(END)

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam get-role --role-name AWSReservedSSO_LabAdministrationAccess_054e9fc29832c558 --profile iam
```


{
"Role": {
"Path": "/aws-reserved/sso.amazonaws.com/",
"RoleName": "AWSReservedSSO_LabAdministrationAccess_054e9fc29832c558",
"RoleId": "AROAX6IOGWSMSPPDRHUUV",
"Arn": "arn:aws:iam::546027517081:role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_LabAdministrationAccess_054e9fc29832c558",
"CreateDate": "2024-07-31T17:47:46+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Federated": "arn:aws:iam::546027517081:saml-provider/AWSSSO_073d9cef9904420c_DO_NOT_DELETE"
},
"Action": [
"sts:AssumeRoleWithSAML",
"sts:TagSession"
],
"Condition": {
"StringEquals": {
"SAML:aud": "https://signin.aws.amazon.com/saml"
}
}
}
]
},
"Description": "Administrator access for lab accounts",

"MaxSessionDuration": 43200,
"RoleLastUsed": {
"LastUsedDate": "2025-07-23T20:05:48+00:00",
"Region": "us-east-1"
}
}
}


```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam get-role --role-name SupportRole --profile iam
```


{
"Role": {
"Path": "/",
"RoleName": "SupportRole",
"RoleId": "AROAX6IOGWSM4OIX6VYW3",
"Arn": "arn:aws:iam::546027517081:role/SupportRole",
"CreateDate": "2025-10-17T04:37:59+00:00",
"AssumeRolePolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::546027517081:root"
},
"Action": "sts:AssumeRole",
"Condition": {
"ArnEquals": {
"aws:PrincipalArn": "arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Mary"
}
}
}
]
},
"Description": "Assumable role for internal support",
"MaxSessionDuration": 3600,
"PermissionsBoundary": {
"PermissionsBoundaryType": "Policy",
"PermissionsBoundaryArn": "arn:aws:iam::546027517081:policy/RoleBoundaryPolicy"
},
"Tags": [
{
"Key": "RoleType",
"Value": "SupportRole"
},
{
"Key": "cybr-lab",
"Value": "auto-deployed"
}
],


```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam list-attached-role-policies --role-name SupportRole --profile iam
```

An error occurred (AccessDenied) when calling the ListAttachedRolePolicies operation: User: arn:aws:iam::546027517081:user/introduction-to-aws-iam-enumeration-1760675857628-Joel is not authorized to perform: iam:ListAttachedRolePolicies on resource: role SupportRole because no identity-based policy allows the iam:ListAttachedRolePolicies action

```
┌──(mahathi㉿SriGanesha)-[~]
└─$ aws iam list-role-policies --role-name SupportRole --profile iam
{
"PolicyNames": [
"AllowS3FullAccessForRole"
]
}
```

Notes

Transcript