

Analyze the challenge

Plan of action

-
- The diagram illustrates three methods for accessing AWS services:
- AWS managed policy:** A user icon points to an AWS managed policy icon (blue square with a shield and checkmarks). An arrow labeled "Access service" points to the Amazon GuardDuty icon (blue square with a shield and gear).
 - Customer managed policy:** A user icon points to a customer managed policy icon (blue square with a shield and checkmarks). An arrow labeled "View policies (Assume role)" points to the BackendDev role and attached policy icon (blue square with a person and checkmarks). An arrow labeled "Access service" points to the Secrets Manager secret icon (blue square with a padlock and checkmarks).
 - Inline policy:** A user icon points to an inline policy icon (blue square with a shield and checkmarks). An arrow labeled "Access service" points to the Amazon S3 bucket icon (green square with a bucket).

Perform the steps to enumerate the AWS IAM permissions and retrieve the flag.

1 / 3

```
aws sts get-caller-identity

# Expected Output (Account and Arn will vary):
# {
#   "UserId": "AIDA...",
#   "Account": "xxxxxxx7501",
#   "Arn": "arn:aws:iam::xxxxxxx57501:user/dev01"
# }

# 3. Enumerate User Policies
aws iam list-attached-user-policies --user-name dev01
# Expected Output:
# {
#   "AttachedPolicies": [
#     {
#       "PolicyName": "AmazonGuardDutyReadOnlyAccess",
#       "PolicyArn":
# "arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess"
#     },
#     {
#       "PolicyName": "dev01",
#       "PolicyArn": "arn:aws:iam::xxxxxxx57501:policy/dev01"
#     }
#   ]
# }

aws iam list-user-policies --user-name dev01
# Expected Output:
# {
#   "PolicyNames": [
#     "S3_Access"
#   ]
# }

# 4. Examine S3 Permissions
aws iam get-user-policy --user-name dev01 --policy-name S3_Access
# Expected Output:
# {
#   "UserName": "dev01",
#   "PolicyName": "S3_Access",
#   "PolicyDocument": {
#     "Version": "2012-10-17",
#     "Statement": [
#       {
#         "Effect": "Allow",
#         "Action": [
#           "s3:ListBucket",
#           "s3:GetObject"
#         ],
#         "Resource": [
#           "arn:aws:s3:::hl-dev-artifacts",
#           "arn:aws:s3:::hl-dev-artifacts/*"
#         ]
#       }
#     ]
#   }
# }
```

```
# ]
# }
# }

# 5. Access S3 Bucket
aws s3 ls s3://hl-dev-artifacts
# Expected Output:
# 2023-11-21 17:47:46          40 flag.txt

# 6. Retrieve Flag
aws s3 cp s3://hl-dev-artifacts/flag.txt .

# 7. Extract Flag
cat flag.txt
# Expected Output:
# xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx7514
```