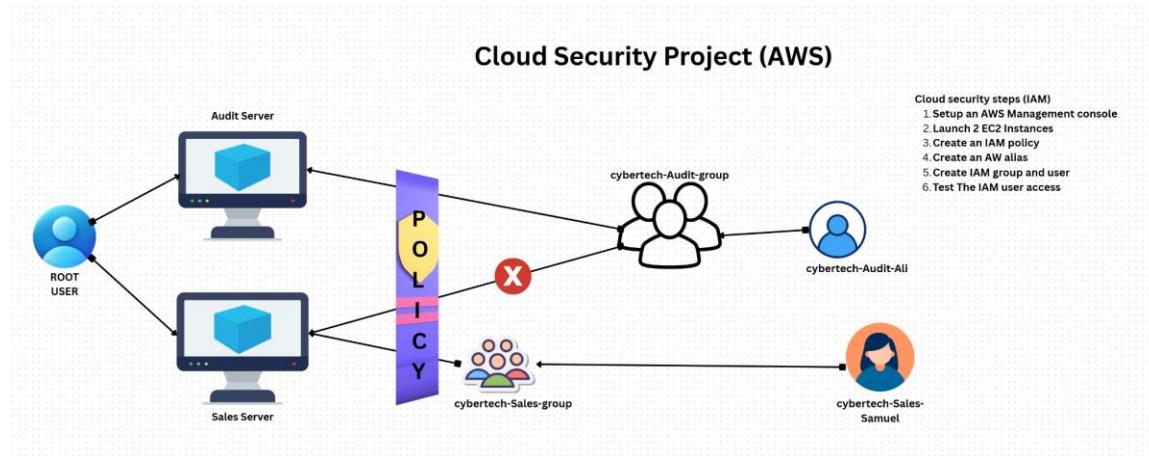


AWS IAM Cloud Security Project

1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least-privilege policy, attach it to a user group, and verify that the policy correctly restricts actions on two Amazon EC2 instances (audit and sales).



2. Tools & Concepts

- AWS IAM – users, groups, policies, account alias
- Amazon EC2 – instance tagging and lifecycle actions
- JSON policy syntax – Effect, Action, Resource
- Principle of least privilege and policy testing

3. Tagging Strategy

I applied a descriptive tag to each EC2 instance:	Instance Tag Key Tag Value	Tag Value
Instance Tag Key	audit Environment	Audit
sales Environment Sales		

4. Creating the IAM Policy

I authored the following JSON policy to block instance stop/start actions on the audit server but allow those actions on the sales server:

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": "ec2:*",
7        "Resource": "*",
8        "Condition": {
9          "StringEquals": {
10            "ec2:ResourceTag/Env": "Audit"
11          }
12        }
13      },
14      {
15        "Effect": "Allow",
16        "Action": "ec2:Describe*",
17        "Resource": "*"
18      },
19      {
20        "Effect": "Deny",
21        "Action": [
22          "ec2:DeleteTags",
23          "ec2:CreateTags"
24        ],
25        "Resource": "*"
26      }
27    ]
28  }

```

[Copy](#) [Edit](#) [Summary](#) | [JSON](#)

The screenshot shows the AWS IAM Policies page. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main area displays a table titled 'Policies (1401)'. A search bar at the top has 'gid' entered. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. One row is highlighted, showing 'GideontechAuditEnvPolicy' under 'Policy name', 'Customer managed' under 'Type', 'None' under 'Used as', and 'IAM policy for users in the Audit Environ...' under 'Description'.

5. Account Alias

I set a memorable account alias to replace the default numeric URL, making sign-in easier for team members.

The screenshot shows the 'AWS Account' page. Under 'Account ID', it shows '630493077427'. Under 'Account Alias', it shows 'gideontechusers' with 'Edit | Delete' links. Under 'Sign-in URL for IAM users in this account', it shows 'https://gideontechusers.signin.aws.amazon.com/console'.

The screenshot shows the 'AWS Account' page with two additional sections. The 'Quick Links' section contains 'My security credentials' and a link to manage access keys, MFA, and other credentials. The 'Tools' section contains a link to tools.

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Access reports', and 'Access Analyzer'. The main area has a green banner at the top stating 'Alias gideonTechUsers created for this account.' Below it, the 'IAM Dashboard' section includes 'Security recommendations' (with one item: 'Add MFA for root user') and 'IAM resources' (listing 0 User groups, 0 Users, 3 Roles, 1 Policies, and 0 Identity providers). To the right, there are three boxes: 'AWS Account' (Account ID: 6304-9307-7427, Alias: gideonTechUsers), 'Quick Links' (My security credentials), and 'Sign-in URL for IAM users in this account' (https://gideonTechUsers.signin.aws.amazon.com/console).

6. IAM Users & Groups

1. I Created an IAM user group called gideonTech-Audit-group.
2. Attached is the **gideonTechAuditEnvPolicy** policy to the group.
3. I have added individual IAM users who require controlled EC2 access.

The screenshot shows the 'User groups' page in the AWS IAM console. The sidebar includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (selected), 'User groups' (which is the current view), and 'Access reports'. The main area displays a green banner 'gideonTech-Audit-group user group created.' Below it, a table lists 'User groups (1)'. The table has columns for 'Group name' (gideonTech-Audit-group), 'Users' (0), 'Permissions' (Defined), and 'Creation time' (Now). There are buttons for 'View group' and 'Create group'.

7. Logging in as an IAM User

IAM users can sign in through:

- AWS Management Console (using <https://gideonTechUsers.signin.aws.amazon.com/console>)
- AWS CLI via programmatic keys

The screenshot shows the AWS Console Home page. In the top right, there's a search bar and a 'Region' dropdown set to 'United States (Ohio)'. Below the search bar, there are sections for 'Recently visited' services (EC2, S3, Aurora and RDS, Lambda), 'Applications' (0), 'Welcome to AWS', and 'AWS Health'. The 'Applications' section has a red box highlighting an error message: 'Access denied to servicelogicatalog:ListApplications'. At the bottom, there are links for 'View all services', 'Go to myApplications', and navigation icons.

8. Testing the Policy

Test	Action	Expected	Result	Actual	Result
Stop	audit instance	Denied	Access denied	error	displayed
Stop	sales instance	Allowed	Instance stopped	stopped	successfully
Start	audit instance	Denied	Access denied	error	displayed
Start sales instance Allowed Instance started successfully					

The screenshot shows the AWS EC2 Instances page. The left sidebar includes 'EC2' (selected), 'Dashboard', 'EC2 Global View', 'Events', 'Instances' (selected), 'Images', 'Elastic Block Store', and 'Capacity Manager'. The main area shows a red error message for instance 'i-0fb8ea2f980160214': 'Failed to stop the instance i-0fb8ea2f980160214'. It details the IAM policy issue: 'User: arn:aws:iam:630493077427:user/gideontech-Audit-gid is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-2:630493077427:instance/i-0fb8ea2f980160214 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: 7IQWeKch0J0R8e7iyQp2C_MWVY7wUgpf2PvNVi2lir_V7CeRMefYtww_ef9ExoULFKEKtvu6MxqrMjqGq1kyqqEJN7tpw0xNXXatn5F5wyNeY oR75C_2DLbqRQ57Lyj2w9idqHpsKLJGcouv4xfu7w2grWjp8DjeY4za4Man3h801uk9lQBROPiDL177McCegZf9t1y4KKFaNdaAnYR4vKDaf-Mas-UZT1-74LJHkm4X8uyueqNnOVModhMaS-nKwRnhz_42JUFLJEHILHUGY9UAYXqACSFd2zJQWgGbNvk_AxJvYp8YPAu5X13rbxSjBUzIm9VX9SETp5-zGrnIcsqbhlgIEJD0IKFHQ_Cmny6zrsouzvTCUeI8895YaqY2SWX-5LFN32MdRWL_Dk85u0R7CpPe7M7u0cOqH1_x9jqM2zpqnKvBGDCVODlCrHfYwdA3SMRn8pL-KIK7MGJxybvXST7KpdksQGwyXqRJWHA8e2Puj6xxr_kok_q_OJNHkU9IMHDHeOQN_970UP01Rw6FcqXpYe15CqTVC-h59bVRJl2xysT7-kcOGuWd34hdNLnN76a42fmoD0lowvKvA6hDnq3zYwmq3LU2jVAQzNzN50pPGgAe3u0J5Jlwbdpnoi2cJKaNuRgt44ajRn0-IThe0gVa-RVTQGj0MimAdRpL3d-UaMNY1VTR6GgggNmOrJf4TGkz-3-VFkvDiCOSVhJ5tq5EE6mt4ArwGgChobqj151OLVmsaZ-K5tr3cKFUzunpmFVD25gXcpEvbqQnH4xYjCslyqwpp0laEfCzP-zfaD92-0IVWui2lxJWOrUqj1t50tkGL35vhKlecbmtkPYOLFUw

The instance details for 'i-0fb8ea2f980160214 (Gideontech-Sales-Gid)' are shown, including 'Details' tab, 'Status and alarms', 'Monitoring', 'Security', 'Networking', 'Storage', and 'Tags'. The 'Details' tab shows the instance ID (i-0fb8ea2f980160214), Public IPv4 address (18.191.48.71), Private IPv4 addresses (172.31.37.35), and Public DNS (ec2-18-191-48-71.us-east-2.compute.amazonaws.com).

IAM Dashboard Info

Security recommendations 0



✖ Access denied

You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::288645738432:user/cybertech-Audit-Ali



Action: iam:GetAccountSummary

Context: no identity-based policy allows the action

[Diagnose with Amazon Q](#)

✖ Access denied

You don't have permission to `iam>ListMFADevices`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::288645738432:user/cybertech-Audit-Ali



Action: iam>ListMFADevices

Context: no identity-based policy allows the action

✖ Failed to stop the instance i-0b9626f2835a5f977

[Diagnose with Amazon Q](#)



You are not authorized to perform this operation. User: arn:aws:iam::288645738432:user/cybertech-Audit-Ali is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:288645738432:instance/i-0b9626f2835a5f977 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: sAVefFO1XITMRJ52x0fhO4bpSGLz7IfQ-T-w1DqTxLoat_lVAT5r87OMhHzrfsSmG4VXfVa2zDWhfQ1uQO0shFk8kUgfZhoC9Tn_lhCnKyVswG-blglkfFw90Lb4-2CT9TP841l8nI9O6Ea5TAt0ztgtsh2t1VXnMzhUuPZeEqMg3Aje6wr21S90c0le6YNjRMmcGw8Gd_xH9dfdp-4ilwiFOH1uwtPAt1QHqrBFw3KJue7UMNuHgZJzgCiA30Q5pqHwW1_AlxzQAuthMpW9i6xdEfRRLOfQG_W-dfTm6Z7YNPth09woBuuiXzLbc13Mz5-ciFyB_0PBgVz8xKMy4kunc1_zDrnTsNfyv0sszpKwvYxm8Du71JN3rStmBylKAIW0cA0nzxFVFWI0Q9kigwtxbT-gocng2gZG1qoW2RxlqW8XBc420EN3lZ-URe-xZC51palfmic1RidvCBzJNWPr4rK_0WgaADMkcFgQjk7mmnNmF12mgHr5Aw46VvHCp-pqURgYZ_Oa8xBng7y6iuL_MxiUb20p2zDhB0SynHoNGRrm0MRzRy1etyCipN14aBfvWB12hSkMoXobUZawc9Rat-Pk_vPsblm-Opv1riuGTCT-YJtIZ6FSYUFFECxnmX6B3iFHqgGTOp6sDaZlXMCX3g2yqEqbTNSf-CLwsZbvA7Ck5m5yf8nt1po_-8fBDM672wyEe21nGxikjEmj_nMMMFQVPqk46tBHdwRYHlxQQA2b-cG58fOMUsv_eHnT1xBHLtxVMB7vxU-_Scg_KyhwQlMrGy4NR4Ho_RumoDyK8aWNLTixh-j1yTKrjk8ctDTtf11QzyfSAKRTQp_-j1QBrzXEA47t8IxAwgRD3vWCNE3PL3YfwcYpRHP

Instances (1/2) Info



Connect

Instance state ▾

Actions ▾

Launch instances ▾

Find Instance by attribute or tag (case-sensitive)

All states ▾

< 1 > ⚙

i-0b9626f2835a5f977 (Cybertech-sales-Ali)

⚙️ | ⌂

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/home

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists navigation options: Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), and Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report). The main content area is titled "IAM Dashboard". It features a "Security recommendations" section with two items: "Access denied to iam>ListMFADevices" and "Access denied to iam>ListAccessKeys". Each item includes a user (arn:aws:iam::630493077427:user/gideontech-Audit-gid), action (iam>ListMFADevices or iam>ListAccessKeys), and context (no identity-based policy allows the action). Below each item is a "Diagnose with Amazon Q" button. To the right is an "AWS Account" section with a single item: "Access denied to iam>ListAccountAliases". It also includes a user, action (iam>ListAccountAliases), context (no identity-based policy allows the action), and a "Diagnose with Amazon Q" button. At the bottom right are links for "My security credentials", "Manage your access keys, multi-factor authentication", and footer links for "© 2025, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".