Implementing Governance with AWS SecurityViz or Control Tower

Lab Title:

Implementing Cloud Governance Framework with AWS SecurityViz or AWS Control Tower

---

Use Case Scenario:

Your organization, **TechGuard Innovations**, is transitioning to the cloud and requires a governance framework to ensure security, compliance, and visibility across its cloud resources. The leadership has provided two options:

1. Use **AWS SecurityViz** to visualize and analyze security configurations.
2. Use **AWS Control Tower** to implement a multi-account governance structure.

Your task is to choose **one approach** and implement it to secure and govern cloud operations.

Objective:

By the end of this lab, students will:

1. Understand and apply governance principles in AWS.
2. Use either AWS SecurityViz or AWS Control Tower to establish security and governance.
3. Analyze compliance and security effectiveness.

Lab Requirements:

- An AWS account with administrative access.
- Basic understanding of AWS IAM, S3, and networking concepts.

Instructions:

Option 1: Using AWS SecurityViz

1. **Set Up AWS SecurityViz:**
    - Log in to your AWS account and install AWS SecurityViz
    - Ensure you have **AWS CLI** installed and configured on your machine.
2. **Generate Security Configuration Visualizations:**

- Use SecurityViz to create visualizations of IAM policies and roles in your AWS environment.
- Run the following command (replace placeholders with your AWS account details):

```
bash
Copy code
security-viz visualize --account <your-account-id>
```

- Generate diagrams that show relationships between AWS services, IAM policies, and roles.

3. **Analyze Security and Governance:**
   - Review the visualizations to identify:
     - Overly permissive IAM roles or policies.
     - Unused or orphaned resources that pose security risks.
   - Document any changes you would make to improve governance.
4. **Optional Challenge:**
   - Modify an IAM policy to align with least privilege principles and generate an updated visualization.

Option 2: Using AWS Control Tower

1. **Set Up AWS Control Tower:**
   - Log in to the AWS Management Console and navigate to **Control Tower**.
   - Set up Control Tower by following the guided setup process. This will create a multi-account environment with centralized logging and monitoring.
2. **Create Organizational Units (OUs):**
   - Create two OUs: **Development** for non-critical resources and **Production** for critical workloads.
   - Assign governance policies (guardrails) to these OUs.
3. **Apply Guardrails:**
   - Enable key guardrails such as:
     - **Mandatory Encryption** for S3 buckets.
     - **IAM Governance** to prevent root account access.
   - Use the Control Tower dashboard to monitor compliance.
4. **Verify Compliance:**
   - Access the **Compliance Dashboard** to ensure all accounts adhere to applied guardrails.
5. **Optional Challenge:**
   - Use AWS Security Hub to cross-check security findings for the accounts managed by Control Tower.

Submission Requirements:

1. **If using AWS SecurityViz:**
   - Submit a screenshot of the generated security visualizations.

- Write a short report (1-2 paragraphs) summarizing identified security issues and proposed governance improvements.

2. **If using AWS Control Tower:**
   - Submit a screenshot of the Control Tower dashboard showing OUs, accounts, and guardrails.
   - Write a short report (1-2 paragraphs) explaining the governance strategy applied and the compliance status.