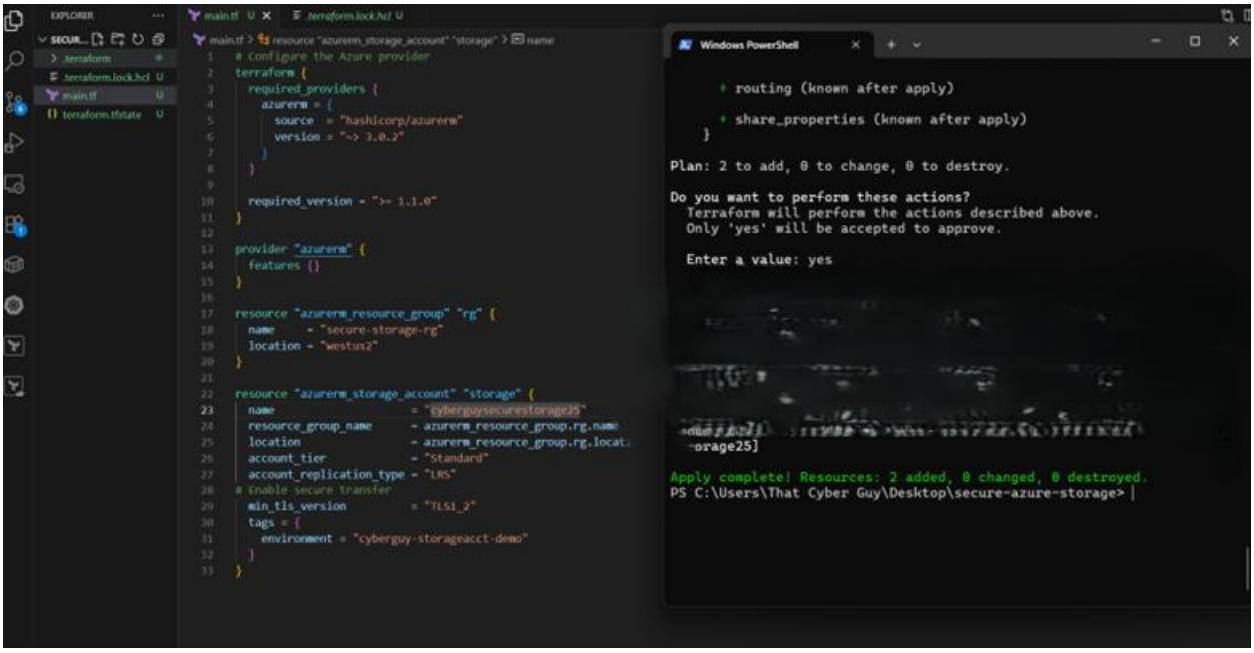
Use **Terraform** to create an **Azure Storage Account**, enforce a custom **Azure Policy** (Block Public Network Access), enable **diagnostic logging**, and manage everything through **GitHub pull requests**.

Workflow Overview:

1. Write Terraform configuration to define Azure resources.
2. Push code to GitHub and open a pull request.
3. GitHub Actions runs Terraform plan to preview changes.
4. Merge pull request to finalize changes.
5. Azure Portal confirms successful deployment.



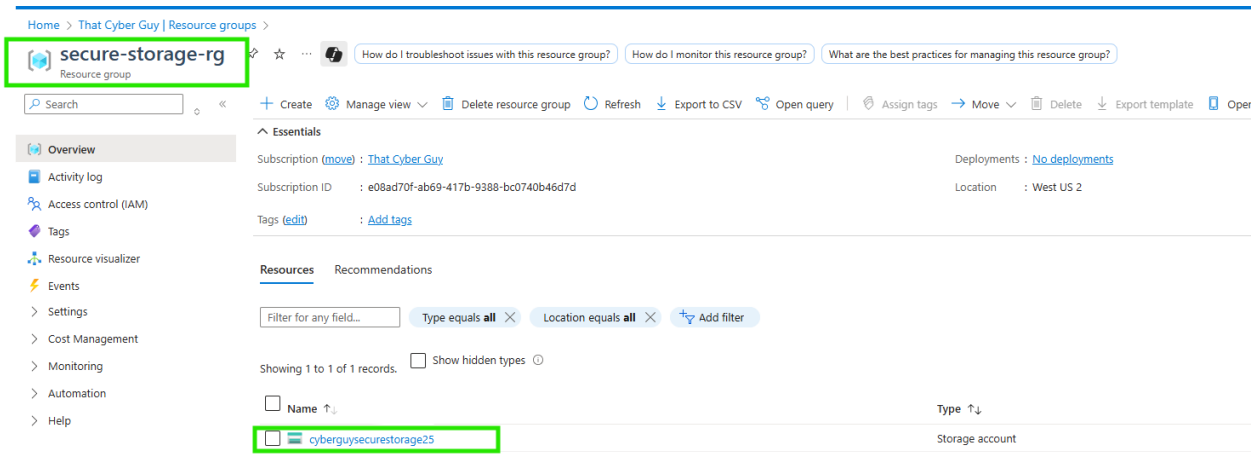


Figure 1.0. Creating the resource group and naming the resource using Terraform.

Public network access is enabled from all networks, which poses a high risk of data exposure or unauthorized access.

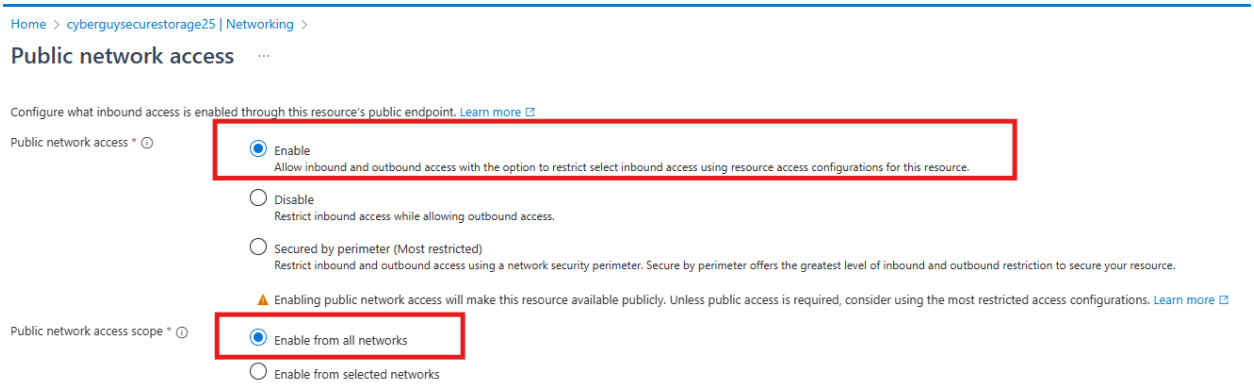


Figure 2.0. Public network access enabled from all networks.

To address this issue, I used Azure Policy to create a custom policy that enforces the 'Storage accounts should restrict network access' rule. This ensures that only trusted networks can access our storage resources, reducing exposure to public internet threats and aligning with the principle of least privilege.

Home > Policy | Definitions > Deny public network access on Storage Accounts >

Assign policy

Basics | Parameters | Remediation | Non-compliance messages | Review + create

Scope

Scope * That Cyber Guy/secure-storage-rg

Learn more about setting the scope

Exclusions *Optionally select resources to exclude from the policy assignment.*

Resource selectors (Expand) Using resource selectors, you can further refine this assignment's applicability by targeting specific subsets of resources. Expand to learn more.

Basics

Policy definition * Deny public network access on Storage Accounts

Overrides (Expand) Using overrides, you can change the effects or referenced versions of definitions for all or a subset of resources evaluated by this assignment. Expand to learn more.

Assignment name * Deny public network access on Storage Accounts

Description This policy denies storage accounts that have public network access enabled.

Policy enforcement Enabled

Previous | Next | Review + create

Figure 3.0. Policy definition.

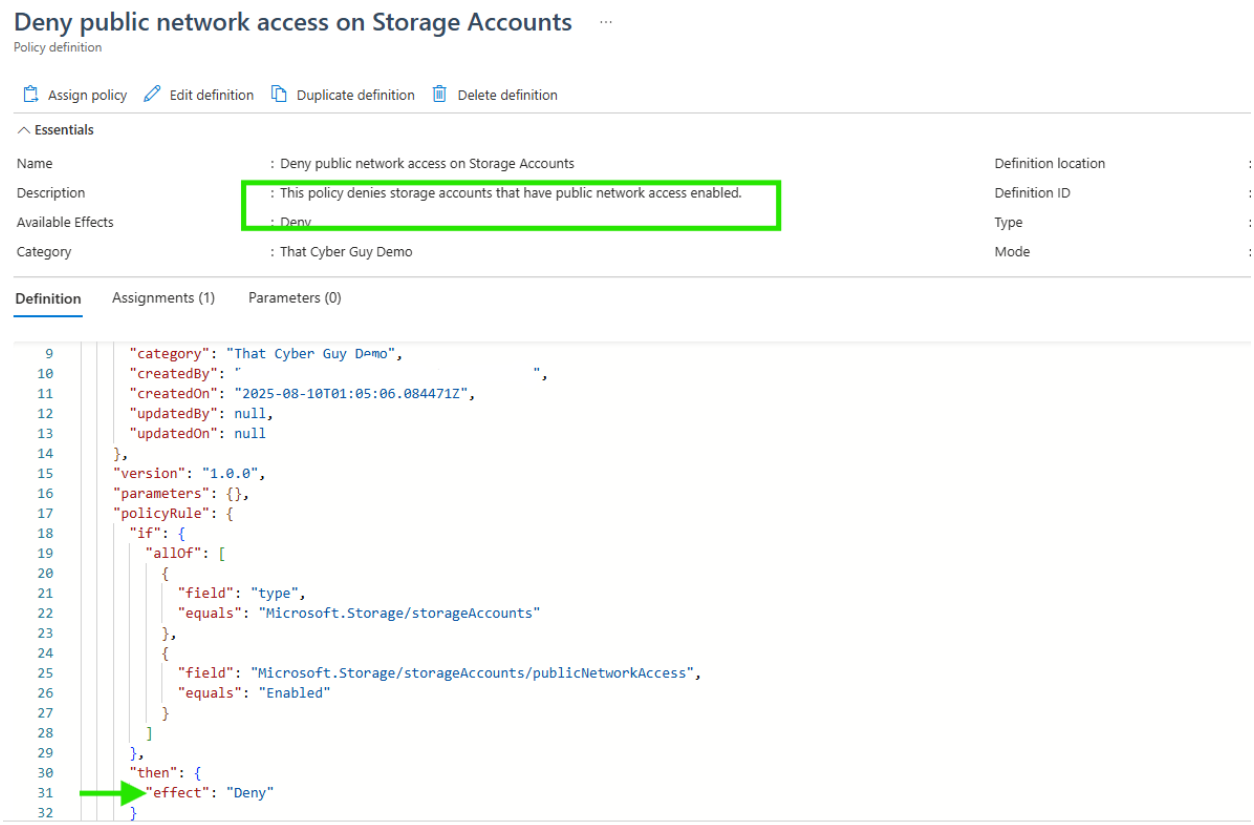


Figure 3.1. Custom policy definition that denies public access to the storage account.

After the custom policy shown in Figures 3 and 3.1 is applied, users **cannot** enable public network access for any storage accounts.

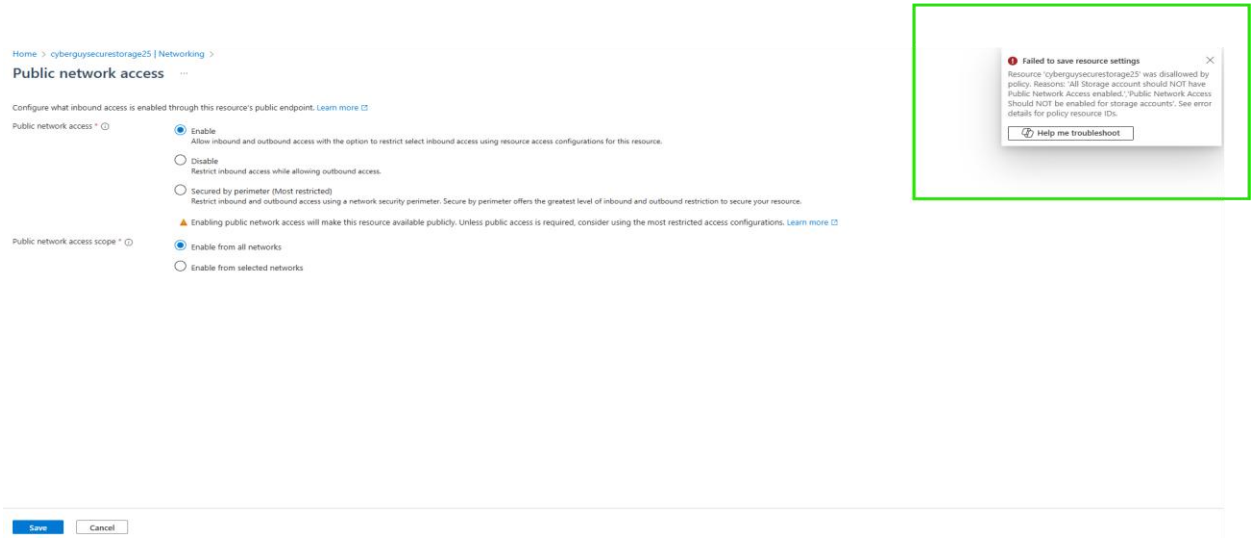


Figure 3.2. Policy enforcement.

Created a new ***logging.tf*** file to provision a Log Analytics resource that will serve as the destination for storage account logs.

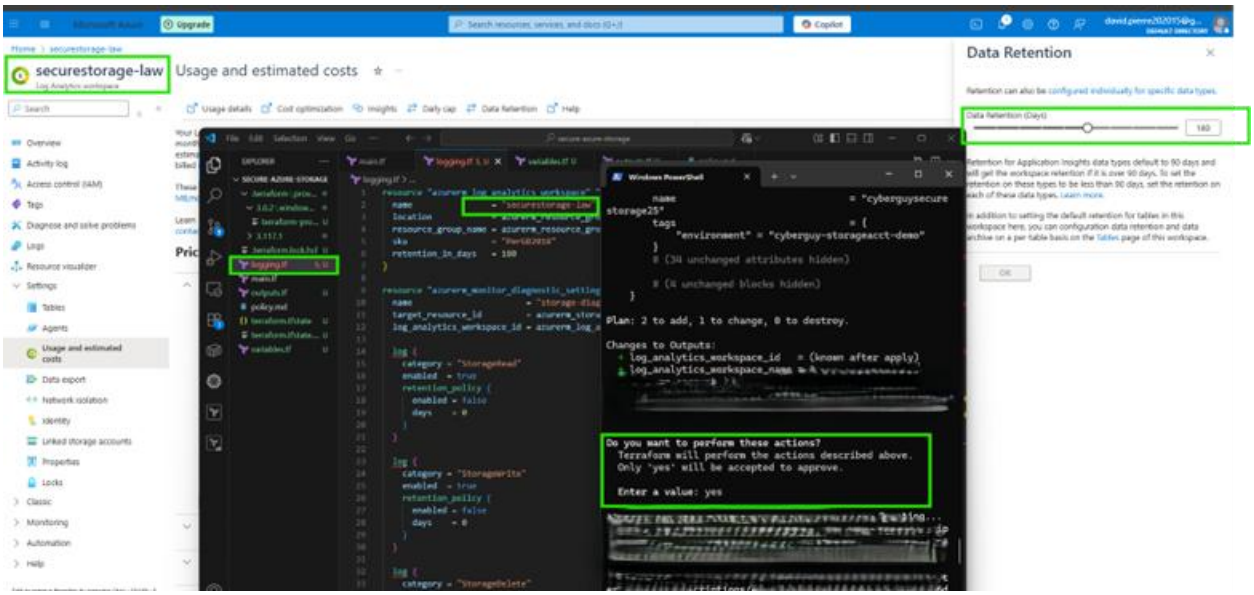


Figure 4.0. Log analytics creation.

L Blob storage logs are now forwarded to Log Analytics, where they are retained for 180 days.

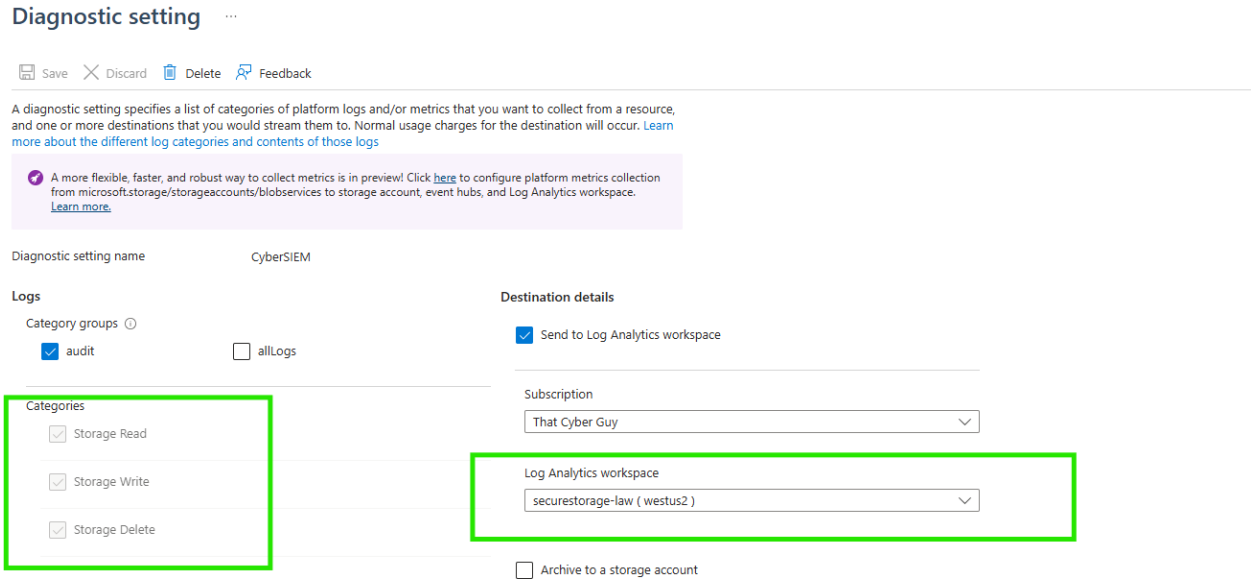


Figure 5.0. Log Analytics workspace configured as the destination for storage account logs.

secure-azure-storage / .github / workflows / terraform.yml

thatcyberguyofficial Update terraform.yml version

Code Blame 22 lines (17 loc) · 379 Bytes

```yaml
name: Terraform Plan

on:
  pull_request:
    branches:
      - main

jobs:
  terraform:
    runs-on: ubuntu-latest
    steps:
      - name: Checkout code
        uses: actions/checkout@v3

      - name: Setup Terraform
        uses: hashicorp/setup-terraform@v2

      - name: Terraform Init
        run: terraform init

      - name: Terraform Plan
        run: terraform plan
```

Figure 6.0. Terraform plan..

This project demonstrates a complete Infrastructure-as-Code (IaC) workflow using **Terraform** to provision resources in **Microsoft Azure**, integrated with **GitHub Actions** for automated CI/CD.