**✅ Non-Disruptive AWS Resources & CLI Commands**

| **#** | **Resource Type** | **Description** | **AWS CLI Command** |
| --- | --- | --- | --- |
| 1 | **CloudWatch Dashboards** | UI views only, no runtime impact | aws cloudwatch list-dashboards |
| 2 | **CloudWatch Alarms (non-critical)** | Alerting logic, not service-breaking | aws cloudwatch describe-alarms |
| 3 | **CloudWatch Log Groups (no logs)** | Can be deleted if not active | aws logs describe-log-groups |
| 4 | **Security Groups (unused)** | No effect unless attached | aws ec2 describe-security-groups --query "SecurityGroups[?length(IpPermissions)==\0` && length(IpPermissionsEgress)==`0`]"` |
| 5 | **NACLs (not in use)** | No impact unless attached | aws ec2 describe-network-acls |
| 6 | **Route 53 Hosted Zones (unused)** | Only affects DNS | aws route53 list-hosted-zones |
| 7 | **VPC Endpoints (not in use)** | No effect unless tied to services | aws ec2 describe-vpc-endpoints |
| 8 | **IAM Roles (unused)** | Safe if not used in policies/instances | aws iam list-roles + aws iam get-role --role-name <RoleName> |
| 9 | **IAM Policies (not attached)** | No effect if not attached | aws iam list-policies --scope Local + aws iam list-entities-for-policy --policy-arn <ARN> |
| 10 | **IAM Users (inactive)** | Safe if not used/accessed | aws iam list-users + aws iam get-user --user-name <username> |
| 11 | **CloudFormation Stacks (test)** | If not provisioning prod resources | aws cloudformation describe-stacks |
| 12 | **Step Functions (idle/test)** | Not active = safe | aws stepfunctions list-state-machines |
| 13 | **EventBridge Rules (disabled)** | Disabled rules are safe | aws events list-rules |
| 14 | **CodeBuild Projects (unused)** | Can be cleaned if not triggered | aws codebuild list-projects |
| 15 | **CodePipeline (disabled/test)** | No builds = non-critical | aws codepipeline list-pipelines |
| 16 | **ELB/ALB (no targets)** | No backend = safe to delete | aws elbv2 describe-load-balancers |
| 17 | **Target Groups (no instances)** | Safe unless attached | aws elbv2 describe-target-groups |
| 18 | **Key Pairs (unused)** | Only for SSH | aws ec2 describe-key-pairs |
| 19 | **Launch Templates (old/test)** | Safe unless referenced | aws ec2 describe-launch-templates |
| 20 | **Placement Groups (empty)** | Safe if no instance assigned | aws ec2 describe-placement-groups |
| 21 | **Snapshots (manual/test)** | If not tied to backups | aws ec2 describe-snapshots --owner-ids self |
| 22 | **CloudTrail (not org-wide)** | Safe if not your primary trail | aws cloudtrail describe-trails |

#!/bin/bash

output\_file="non\_disruptive\_resource\_check\_$(date +%F).log"

echo "AWS Non-Disruptive Resource Check - $(date)" > "$output\_file"

echo "-------------------------------------------" >> "$output\_file"

check() {

echo -e "\n🔍 Checking: $1" >> "$output\_file"

echo "Command: $2" >> "$output\_file"

eval "$2" >> "$output\_file" 2>&1

}

check "CloudWatch Dashboards" "aws cloudwatch list-dashboards"

check "Unused Security Groups" "aws ec2 describe-security-groups --query \"SecurityGroups[?length(IpPermissions)==\`0\` && length(IpPermissionsEgress)==\`0\`]\""

check "IAM Roles" "aws iam list-roles"

check "IAM Policies (Local)" "aws iam list-policies --scope Local"

check "VPC Endpoints" "aws ec2 describe-vpc-endpoints"

check "Step Functions" "aws stepfunctions list-state-machines"

check "Snapshots (owned)" "aws ec2 describe-snapshots --owner-ids self"

check "CodePipelines" "aws codepipeline list-pipelines"

check "EventBridge Rules" "aws events list-rules"

echo "✅ Done! Output saved to $output\_file"