AWS CloudFormation Cheat Sheet

DevOps · Quick Reference

OVERVIEW & INSTALL

AWS CloudFormation DevOps and automation tool

```
# Install
brew install aws-cloudformation
# Or via official installer
curl -L https://... | sh
aws version
```

CORE CONCEPTS

Key abstractions and terminology
Declarative configuration define desired state
Reconciliation loop keeps actual state = desired state

```
# Check current state
aws status
```

Infrastructure as Code: version control your infra

CONFIGURATION

```
# Main config file
aws.yaml / aws.tf / .awsrc
# Set environment
export
AWS_CLOUDFORMATION_HOME=/path/to/config
```

Use environment-specific configs for dev/staging/prod

```
# Validate config
aws validate
```

CORE COMMANDS

```
aws init       # initialize
aws plan       # preview changes
aws apply      # apply changes
aws destroy    # tear down
aws --help     # help
aws version    # check version
```

INTEGRATION & CI/CD

Integrate with GitHub Actions / GitLab CI / Jenkins

```
# GitHub Actions example
- name: Run AWS CloudFormation
uses: aws-actions/github@v1
with:
command: apply
```

Automate validation and deployment in pipelines

SECURITY

Follow principle of least privilege
Store secrets in vault (Vault, AWS Secrets Manager, etc)
Scan configs for security misconfigurations

```
# Example: secret management
secret =
data.vault_secret.db_password.data["password"]
```

Enable audit logging for all changes

MONITORING & OBSERVABILITY

Monitor deployment status and health

```
# Check status
aws status
aws logs
```

Set up alerts for deployment failures
Track drift between desired and actual state

SCALING & PERFORMANCE

Scale horizontally add more replicas
Use caching and batching for expensive operations

```
# Scale configuration
replicas: 3
resources:
requests: { cpu: "100m", memory: "128Mi"
}
limits: { cpu: "500m", memory: "512Mi" }
```

BEST PRACTICES

Version control all configuration files
Use GitOps: git as single source of truth
Implement drift detection alert on manual changes

```
# Lint and validate before applying
aws validate && aws plan
```

Test in dev/staging before production

TROUBLESHOOTING

```
aws status --verbose
aws logs --follow
```

Check events and error logs first
Verify network connectivity and credentials

```
# Debug mode
AWS_LOG=debug aws apply
```

CLI REFERENCE

```
aws --help           # full help
aws version          # show version
aws config           # manage config
aws apply -auto-approve # skip prompt
aws output           # show outputs
```

COMMON GOTCHAS

Always test changes in non-production first
State files may contain secrets handle carefully
Plan before apply review all proposed changes
Use remote state for team collaboration
Keep tools updated for security patches