🚀1️⃣CloudProvisioner Agent

🎯 Objective

Automate the provisioning of secure, scalable, and cost-efficient cloud infrastructure using natural-language instruction — reducing human error and enforcing best practices.

🧠 Spec-Kit Commands

constitution

Define global provisioning rules:

- Use least-privilege IAM roles only
- Default networking must be private-first
- Encrypt all storage at rest
- Apply owner, environment, and purpose tags
- Prefer cost-optimized instance families
- Require approval for resources exceeding $50/month

specify

Provision a cloud server with the following requirements:

- Ubuntu Linux
- t3.micro or equivalent instance
- 20GB encrypted SSD
- Region: ap-south-1
- Only HTTPS access allowed
- SSH must not be publicly exposed

task

Create a secure EC2-like compute instance that complies with the above security and cost governance policies and is production-ready.

clarify

Ask the user (if not already provided):

- What environment is this? (dev / staging / prod)

- Who is the resource owner?
- Expected uptime requirement?
- Should auto-scaling be enabled?
- Any special compliance needs?

plan

Break the provisioning into safe execution steps:

1. Validate estimated cost against policy
2. Create or locate secure VPC
3. Create private subnet
4. Create security group allowing HTTPS only
5. Create least-privilege IAM role
6. Launch instance
7. Attach encrypted storage
8. Apply required tagging
9. Output access and audit information

implement

Execute the provisioning workflow following the defined rules and steps.

verify

Confirm:

- Instance status = running
- Encryption enabled
- IAM least-privilege
- Only HTTPS allowed
- Costs within threshold

🔐2️⃣ CloudGuardian Agent

🎯 Objective

Automate IAM and cloud-security enforcement to prevent misconfigurations, reduce breach risk, and ensure least-privilege access everywhere.

🧠 Spec-Kit Commands

constitution

Security policies:

- MFA required for all accounts
- Wildcard permissions are not allowed
- Public storage is blocked unless approved
- Logging must be enabled
- Critical violations must self-remediate

specify

Scan all IAM policies, users and roles. Identify risks, violations, unused access, and privilege escalations. Automatically fix high-risk issues.

task

Perform a full IAM security audit and apply policy-driven remediation to enforce compliance.

clarify

Confirm:

- Which accounts/resources are in scope?
- Should inactive users be disabled?
- Should we notify owners before remediation?
- Is there a change-approval requirement?

plan

1. Collect IAM inventory
2. Compare against policy baseline
3. Rank severity
4. Auto-fix critical risks
5. Notify administrators
6. Store security audit log

implement

Run full IAM security enforcement.

verify

Ensure:

- No wildcard policies remain
- MFA is enforced
- Logs are recorded
- Report is generated

💾3 BackupBrain Agent

🎯 Objective

Automate backup scheduling, encryption, retention, and disaster-recovery validation — ensuring data resilience without manual scripting.

🧠 Spec-Kit Commands

constitution

Backup standards:

- Daily minimum backup
- 30-day retention
- Encryption required
- Cross-region storage required
- Quarterly restore test required

specify

Enable automatic backups for all production servers and databases with cross-region redundancy.

task

Configure and enforce compliant backup policies across all production assets.

clarify

Ask:

- Which systems are business-critical?
- Recovery Time Objective (RTO)?
- Recovery Point Objective (RPO)?

- Backup window allowed?
- Cost sensitivity?

plan

1. Identify production resources
2. Apply encrypted backup policy
3. Enable replication
4. Schedule retention
5. Configure restore testing workflow

implement

Activate backup automation.

verify

Perform restore test and validate integrity.

📊4️⃣ CloudPulse Agent

🎯 Objective

Automate monitoring, alerting, and observability setup to detect performance or availability issues before they cause outages.

🧠 Spec-Kit Commands

constitution

Monitoring rules:

- CPU alert at >80% for 5 minutes
- Latency warning above 200ms
- Disk alert at 85%
- All alerts must notify Ops
- No sensitive data in logs

specify

Monitor all production workloads for compute, storage, and network performance.

task

Implement performance monitoring with actionable alerting.

clarify

Ask:

- Who is the alert owner?
- Working hours vs 24/7?
- Preferred notification channel?
- Business critical thresholds?

plan

1. Register monitored services
2. Enable metrics collection
3. Apply alert thresholds
4. Configure alert channels
5. Create dashboards

implement

Deploy monitoring automation.

verify

Simulate alerts and confirm notification delivery.

💸5️⃣ CloudCost Optimizer Agent

🎯 Objective

Automate cost visibility, anomaly detection, and budget enforcement to prevent unexpected cloud spending increases.

🧠 Spec-Kit Commands

constitution

Cost governance rules:

- Detect >20% spend spikes
- Trigger alerts when projected to exceed budget
- Identify idle resources
- Maintain transparent reporting

specify

Track weekly cloud spending and notify budget owners of cost anomalies.

task

Provide financial intelligence and early-warning controls.

clarify

Ask:

- What is the approved budget?
- Which teams own resources?
- Auto-terminate idle resources?
- Alert frequency?

plan

1. Aggregate billing data
2. Establish baseline trend
3. Detect anomalies
4. Generate insights
5. Trigger alerts

implement

Activate cost analysis workflows.

verify

Simulate spend spike to confirm detection.

🛡️6 PolicyEngine Agent

🎯 Objective

Automate governance so all cloud environments remain compliant with organizational and regulatory standards.

🧠 Spec-Kit Commands

constitution

Compliance requirements:

- No public storage buckets
- Encryption enforced
- Logging required
- Least-privilege access
- Full audit history

specify

Audit all resources and automatically fix policy violations.

task

Continuously enforce compliance baselines.

clarify

Ask:

- Which regulations apply? (ISO / SOC2 / HIPAA etc.)
- Is remediation auto-approval allowed?
- What environments are in scope?

plan

1. Discover cloud resources
2. Evaluate compliance
3. Apply remediations
4. Record actions
5. Generate compliance report

implement

Run governance enforcement automation.

verify

Confirm 100% compliance.

🚀7️⃣ AutoDeploy Agent

🎯 Objective

Automate secure CI/CD application deployment using repeatable, reliable pipelines that reduce release risk.

🧠 Spec-Kit Commands

constitution

Deployment policies:

- Blue-green releases
- Health-checks required
- Rollback support
- Logging enabled
- CI/CD mandatory

specify

Deploy Node.js backend API to production with auto-scaling.

task

Deliver safe & repeatable application releases.

clarify

Ask:

- Downtime tolerance?
- Rollback preference?
- Traffic split strategy?
- Security constraints?

plan

1. Build application
2. Prepare infrastructure
3. Deploy to staging
4. Validate health
5. Roll out gradually
6. Enable scaling & logging

implement

Execute automated deployment pipeline.

verify

Confirm uptime & latency stability.

🔄8️⃣ ReliabilityGuard Agent

🎯 Objective

Automate infrastructure high-availability and failover capabilities to minimize downtime.

🧠 Spec-Kit Commands

constitution

Reliability policy:

- Multi-AZ mandatory
- Load balancers required
- Health-checks enabled
- Auto-healing required
- Recovery target <5 minutes

specify

Upgrade production architecture to high-availability mode.

task

Ensure continuous service availability.

clarify

Ask:

- SLA / uptime requirement?
- Traffic load pattern?
- Current risk tolerance?
- DR location requirements?

plan

1. Deploy multi-zone infrastructure
2. Add load balancing
3. Configure auto-healing
4. Enable failover
5. Test disruptions

implement

Apply resilience automation.

verify

Simulate outage and confirm zero-downtime.

🧠9 EduOps Agent

🎯 Objective

Act as an AI learning assistant that simplifies cloud concepts while encouraging independent thinking.

🧠 Spec-Kit Commands

constitution

Education rules:

- Support learning
- Avoid giving exam answers
- Encourage understanding
- Use simple explanations

specify

Explain cloud networking (VPC & subnets) simply with relatable examples.

task

Deliver guided learning support.

clarify

Ask:

- What level is the student?
- What do they already know?
- Do they prefer analogy or technical detail?

plan

1. Break down concepts
2. Explain with analogy
3. Provide example
4. Ask comprehension question

implement

Deliver guided learning session.

verify

Confirm understanding via student response.

🧩 🔟 CloudOps Co-Pilot

🎯 Objective

Provide a unified automation layer that manages the complete lifecycle of cloud environments using AI-driven DevOps practices.

🧠 Spec-Kit Commands

constitution

Core operational principles:

- Security first
- Reliability required
- Cost optimization enforced
- Compliance monitored
- Automation preferred

specify

Manage full cloud lifecycle across provisioning, security, monitoring, DR and optimization.

task

Act as the central smart cloud operations brain.

clarify

Ask:

- What business priority is primary? (cost / uptime / performance / security)
- Who owns environments?
- What risk level is acceptable?

plan

Provision → Secure → Monitor → Backup → Optimize

implement

Run unified cloud operations automation.

verify

Generate full operational health report.