Ganana Compute Management Platform

Technical User Guide

Version: 1.0.0 **Last Updated:** March 2026

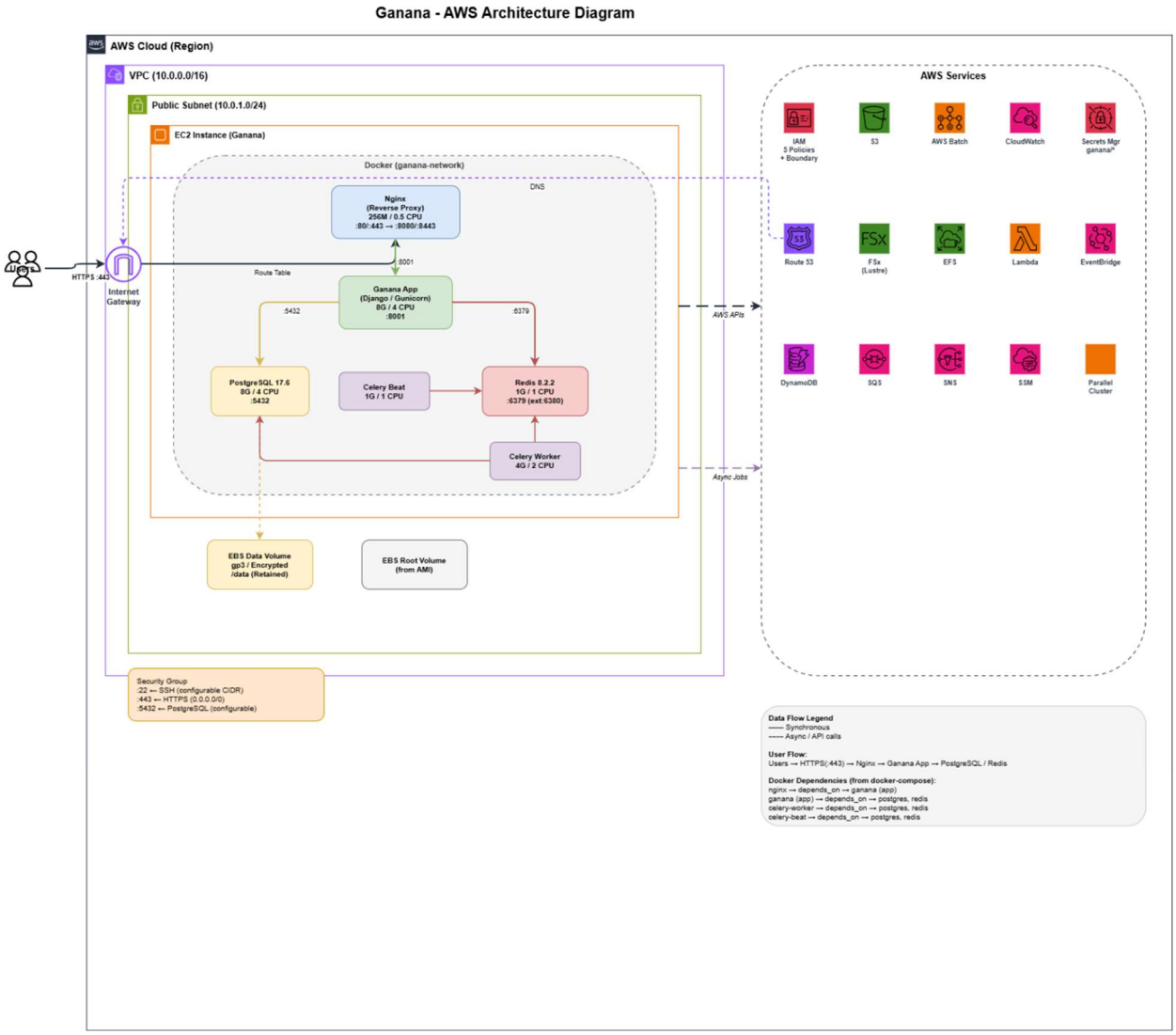
Contents

1. Overview

Ganana HPC Suite provides a web-based platform to simplify the deployment and management of HPC clusters on AWS. This CloudFormation template enables quick setup using a pre-configured AMI, allowing users to launch, manage, and monitor SLURM-based workloads through an intuitive interface. It accelerates HPC adoption by reducing manual configuration and eliminating command-line complexity. The platform is deployed as a single EC2 instance running a containerized application stack via Docker Compose, provisioned through an AWS CloudFormation template available on AWS Marketplace.

2. Architecture

High-Level Architecture



Deployed Resources

Resource	Type	Description
VPC	AWS::EC2::VPC	10.0.0.0/16 CIDR (created if not provided)
Public Subnet	AWS::EC2::Subnet	10.0.1.0/24 with auto-assign public IP (created if not provided)
Internet Gateway	AWS::EC2::InternetGateway	For outbound internet access (created with VPC)
Route Table	AWS::EC2::RouteTable	Default route to IGW (created with VPC)
Security	AWS::EC2::SecurityGroup	Ports 22 (SSH), 443 (HTTPS), 5432

Resource	Type	Description
Group		(PostgreSQL)
EC2 Instance	AWS::EC2::Instance	Ganana application host
EBS Volume	AWS::EC2::Volume	gp3, encrypted, mounted at /data
IAM Role	AWS::IAM::Role	Instance role with permissions boundary
Instance Profile	AWS::IAM::InstanceProfile	Attached to EC2 instance
IAM Policies (8)	AWS::IAM::ManagedPolicy	Scoped policies for compute, storage, orchestration

3. Prerequisites

Before deploying Ganana, ensure the following:

- **AWS Account** with permissions to create CloudFormation stacks, EC2 instances, IAM roles, and VPC resources
- **EC2 Key Pair** in the target deployment region (create one in the EC2 Console → Key Pairs if needed)
- **Service Quotas** — Sufficient limits for:
  - VPCs (if creating new networking)
  - EC2 instances of the selected type
  - EBS volumes
  - IAM managed policies (template creates 9 policies)
- **Existing VPC/Subnet (optional)** — If using existing networking:
  - VPC must have DNS hostnames and DNS support enabled
  - Subnet must be public (MapPublicIpOnLaunch enabled)
  - Resources should be tagged with `Application=Ganana` for auto-discovery

Minimum Instance Requirements

Resource	Minimum
vCPUs	8
Memory	32 GB RAM
Storage	50 GB EBS (data volume)

4. Deployment Parameters

Ganana Instance Configuration

Parameter	Required	Default	Description
Instance Type	Yes	t3.2xlarge	EC2 instance type. See table below for options.

Parameter	Required	Default	Description
SSH Key Pair	Yes	—	Existing EC2 key pair for SSH access
Data Volume Size (GB)	Yes	100	EBS data volume size (50–1000 GB)

Supported Instance Types

Type	vCPUs	Memory	Use Case
t3.2xlarge	8	32 GB	Burstable, evaluation/dev
m5.2xlarge	8	32 GB	General purpose
m5.4xlarge	16	64 GB	**Recommended for production**
c5.4xlarge	16	32 GB	Compute-heavy workloads
r5.2xlarge	8	64 GB	Memory-heavy workloads
m5.8xlarge	32	128 GB	Large-scale deployments

Network Settings

Parameter	Required	Default	Description
VPC ID	No	*(empty — creates new)*	Existing VPC ID (vpc-xxxxxxxx)
Subnet ID	No	*(empty — creates new)*	Existing public subnet ID (subnet-xxxxxxxx)

Security & Access Control

Parameter	Required	Default	Description
SSH Access CIDR	Yes	N/A	CIDR for SSH access. **Strongly recommended:** use YOUR_IP/32
Database Access CIDR	Yes	10.0.0.0/16	CIDR for PostgreSQL access (default: VPC internal only)

> **Security Warning:** Avoid using 0.0.0.0/0 for SSH access in production. Restrict to your specific IP address using YOUR_IP/32 format.

---

5. Deployment Guide

Step 1: Launch from AWS Marketplace

1. Navigate to the Ganana Compute Management Platform listing on AWS Marketplace
2. Click **Continue to Subscribe** → **Accept Terms**
3. Click **Continue to Configuration**
4. Select your preferred **AWS Region**
5. Click **Continue to Launch**

6. Under **Choose Action**, select **Launch CloudFormation**
7. Click **Launch**

Step 2: Configure Stack Parameters

1. Enter a **Stack Name** (e.g., ganana-platform)
2. Fill in the parameters as described in Section 4
3. Review and acknowledge IAM resource creation capabilities:
   - CAPABILITY_IAM
   - CAPABILITY_NAMED_IAM

Step 3: Monitor Deployment

1. Navigate to **CloudFormation → Stacks → your stack**
2. Monitor the **Events** tab for progress
3. The stack uses a WaitCondition with a **15-minute timeout** to confirm successful application startup
4. Stack status will show CREATE_COMPLETE when deployment is successful

Step 4: Retrieve Connection Details

Once the stack is complete, go to the **Outputs** tab:

Output	Description
InstanceId	EC2 Instance ID
PublicIP	Public IP address (only when subnet is auto-created)
PrivateIP	Private IP address

---

6. Infrastructure Details

Networking

When no VPC/Subnet is provided, the template creates: - **VPC:** 10.0.0.0/16 CIDR with DNS hostnames and support enabled - **Public Subnet:** 10.0.1.0/24 in the first available AZ, with auto-assign public IP - **Internet Gateway:** Attached to the VPC with a default route (0.0.0.0/0) - **Route Table:** Associated with the public subnet

All created resources are tagged with Application=Ganana for identification.

Storage

- **Root Volume:** Included with the AMI (OS and application binaries)
- **Data Volume (EBS):**
  - Type: gp3 (3000 IOPS baseline)
  - Encrypted: Yes (AWS-managed key)
  - Mount Point: /data
  - Filesystem: ext4

- **DeletionPolicy: Retain** — The data volume is NOT deleted when the stack is deleted. You must manually delete it to avoid ongoing charges.
- Persisted across reboots via /etc/fstab

Security Group Rules

Port	Protocol	Source	Purpose
22	TCP	SSHAccessCIDR parameter	SSH access
443	TCP	0.0.0.0/0	HTTPS (Ganana web UI)
5432	TCP	DatabaseAccessCIDR parameter	PostgreSQL (default: VPC internal)

7. Application Services

Ganana runs as a multi-container Docker Compose application managed by a systemd service. The application stack consists of 5 services:

Service Architecture

Service	Container	Image	Port	Resource Limits
Nginx	ganana-nginx	nginx:alpine	80→8080, 443→8443	256 MB / 0.5 CPU
Ganana App	ganana-app	ganana-app:latest	8001 (internal)	8 GB / 4 CPU
PostgreSQL	ganana-postgres	postgres:17.6	5432	8 GB / 4 CPU
Redis	ganana-redis	redis:8.2.2	6380→6379	1 GB / 1 CPU
Celery Worker	celery-worker	ganana-app:latest	—	4 GB / 2 CPU
Celery Beat	celery-beat	ganana-app:latest	—	1 GB / 1 CPU

Total Resource Reservations: ~11 GB RAM / 6.25 CPUs (minimum) **Total Resource Limits:** ~22.25 GB RAM / 12.5 CPUs (maximum)

Service Descriptions

- **Nginx** — Reverse proxy handling TLS termination (Self signed SSL certificates are created and placed at /etc/ssl/ganana/). Routes HTTPS traffic to the Ganana application.
- **Ganana App** — Main Python web application (Gunicorn on port 8001). Provides the management UI and API.
- **PostgreSQL 17.6** — Primary database for application state, cluster configurations, and metadata.

- **Redis 8.2.2** — Message broker and cache for Celery task queue and application caching.
- **Celery Worker** — Asynchronous task processor for long-running operations (cluster provisioning, monitoring, etc.).
- **Celery Beat** — Periodic task scheduler for recurring operations (health checks, metric collection, etc.).

Docker Volumes

Volume	Purpose
postgres_data	PostgreSQL database files
redis_data	Redis persistence
app_data	Application data

Systemd Service

The application is managed by a systemd template unit ganana@.service:

- **Service Name:** ganana@prod.service
- **Working Directory:** /opt/ganana
- **Environment File:** /opt/ganana/ganana/.env.prod
- **Compose File:** docker-compose.prod.yaml
- **Start Timeout:** 300 seconds
- **Stop Timeout:** 120 seconds
- **Runs as:** root (required for Docker socket access)
- **Auto-start:** Enabled on boot via WantedBy=multi-user.target

---

8. Security Model

IAM Permissions Boundary

All IAM roles created by Ganana (including for ParallelCluster) are constrained by a permissions boundary that:

- **Denies** privilege escalation (creating IAM users, groups, login profiles, access keys)
- **Denies** modification of the permissions boundary itself
- **Allows** scoped access to AWS services required for compute/storage/orchestration
- **Restricts** IAM mutable actions to resources prefixed with ganana-* or parallelcluster-*

IAM Policies Summary

Policy	Scope	Purpose

Policy	Scope	Purpose
ganana-boundary-*	Permissions Boundary	Ceiling for all Ganana-created roles
ganana-compute-readonly-*	EC2, AutoScaling, ECS	Describe/List compute resources
ganana-compute-mutable-*	EC2, AutoScaling, ECS	Create/modify/delete compute resources (tag-gated)
ganana-storage-read-*	S3, FSx, EFS, CloudWatch, Route53, DynamoDB, SQS, SNS	Read storage/network/monitoring resources
ganana-storage-mutable-*	S3, FSx, EFS, Route53, CloudWatch, DynamoDB, SQS, SNS	Mutate storage/network resources (tag-gated)
ganana-orchestrate-mutable-*	IAM, CloudFormation, Batch, Lambda, Events, SSM	Create/manage orchestration resources (tag-gated)
ganana-orchestrate-read-*	IAM, CloudFormation, Batch, Lambda, Events, SSM	Read orchestration resources
ganana-s3-*	S3	Read-only access to vendor scripts bucket
ganana-secrets-*	Secrets Manager	Access to ganana/* secrets

Tag-Based Access Control

Most mutable operations are gated by the tag `Application=Ganana`. Ganana can only create, modify, or delete AWS resources that carry this tag. This prevents the platform from affecting resources outside its scope.

Network Security

- HTTPS enforced via Nginx with TLS (certificates at `/etc/ssl/ganana/`)
- SSH access restricted by user-defined CIDR
- PostgreSQL access restricted by user-defined CIDR (default: VPC internal only)
- Docker socket mounted read-only for container management

---

9. Post-Deployment Access

Accessing the Web UI

1. Retrieve the instance's **Public IP** from CloudFormation Outputs or the EC2 Console
2. Open your browser and navigate to: `https://<PUBLIC_IP>`

3. Accept the self-signed certificate warning (if applicable)
4. Log in with the default credentials (provided separately)

SSH Access

```
ssh -i /path/to/your-key.pem ec2-user@<PUBLIC_IP>
```

---

10. Operations & Management

Service Management Commands

SSH into the instance and use the following commands:

```
# Check service status
sudo systemctl status ganana@prod.service

# Stop the application
sudo systemctl stop ganana@prod.service

# Start the application
sudo systemctl start ganana@prod.service

# Restart the application (full down + up)
sudo systemctl reload ganana@prod.service

# View service logs
sudo journalctl -u ganana@prod.service -f
```

Docker Container Management

```
cd /opt/ganana

# View running containers
docker compose -p ganana -f docker-compose.prod.yaml ps

# View container logs
docker compose -p ganana -f docker-compose.prod.yaml logs -f
docker compose -p ganana -f docker-compose.prod.yaml logs -f ganana    # specific service
docker compose -p ganana -f docker-compose.prod.yaml logs -f postgres  # database logs

# Restart a specific service
docker compose -p ganana -f docker-compose.prod.yaml restart ganana
```

Application Logs

Log Location	Description
/var/log/userdata.log	CloudFormation UserData bootstrap log
/var/log/ganana/	Ganana application logs

Log Location	Description
/var/log/nginx/	Nginx access and error logs

Health Checks

The application includes built-in health checks:

Service	Check	Interval	Timeout	Retries
PostgreSQL	pg_isready	10s	10s	5
Redis	redis-cli ping	10s	5s	3
Ganana App	HTTP GET http://localhost:8001/	30s	10s	3

Monitoring the Data Volume

```
# Check volume mount and usage
df -h /data

# Verify fstab entry for persistence
cat /etc/fstab | grep /data
```

---

11. Activation of Custom SSL Certificate

Purchased custom SSL certificates and rename Certificate and Private key file, server.cert and server.key, respectively and place them in /etc/ssl/ganana/custom/ directory and restart the service by using below command. Application will configure custom SSL certificates and application can be accessed by using domain name.

```
sudo systemctl restart ganana@prod.service
```

12. Troubleshooting

Stack Creation Failed

1. Check **CloudFormation** → **Events** tab for the specific failure reason
2. Common causes:
   - **WaitCondition timeout (15 min):** Application failed to start. SSH into the instance and check /var/log/userdata.log
   - **Volume attachment timeout:** EBS volume didn't attach within 5 minutes. Check AZ alignment between subnet and volume.
   - **Key pair not found:** Ensure the key pair exists in the deployment region
   - **Insufficient capacity:** Try a different instance type or AZ

Application Not Starting

```
# Check bootstrap log
cat /var/log/userdata.log

# Check systemd service
sudo systemctl status ganana@prod.service
sudo journalctl -u ganana@prod.service --no-pager -n 50

# Check Docker
sudo systemctl status docker
docker ps -a

# Check container logs for errors
cd /opt/ganana
docker compose -f docker-compose.prod.yaml logs --tail=100
```

Cannot Access Web UI

1. Verify the instance has a public IP: curl http://169.254.169.254/latest/meta-data/public-ipv4
2. Check security group allows port 443 from your IP
3. Verify Nginx is running: docker ps | grep nginx
4. Check Nginx logs: docker logs ganana-nginx
5. Verify the Ganana app is healthy: docker ps | grep ganana-app

Database Connection Issues

1. Check PostgreSQL container: docker ps | grep postgres
2. Check PostgreSQL logs: docker logs ganana-postgres
3. Verify security group allows port 5432 from your CIDR
4. Test connectivity: docker exec ganana-postgres pg_isready

Volume Not Mounted

```
# Check if volume is attached
lsblk

# Check mount
mount | grep /data

# Try manual mount
sudo mount /dev/sdf /data  # or /dev/nvme1n1 for NVMe instances
```

---

12. Stack Deletion & Cleanup

Deleting the Stack

1. Navigate to **CloudFormation → Stacks**

2. Select the Ganana stack
3. Click **Delete**
4. Confirm deletion

Important: Retained Resources

The following resources are **NOT deleted** with the stack and must be cleaned up manually:

Resource	Reason	Cleanup Action
EBS Data Volume	DeletionPolicy: Retain (data protection)	EC2 Console → Volumes → Delete

> **Warning:** Retained EBS volumes incur ongoing storage charges. Delete them manually after confirming you no longer need the data.

Post-Deletion Checklist

- ☐ Delete retained EBS data volume (if data is no longer needed)
- ☐ Remove any manually created resources tagged with Application=Ganana
- ☐ Delete the EC2 key pair if it was created specifically for Ganana
- ☐ Review and clean up any ParallelCluster stacks created through Ganana

---

13. Support

For technical support and assistance:

- **Support Portal:** https://www.locuz.com/contact-us/
- **Architecture Diagram:** View on S3
