Support Forge

Hosting Resilience & Disaster Recovery Plan

Version 1.0 | January 27, 2026

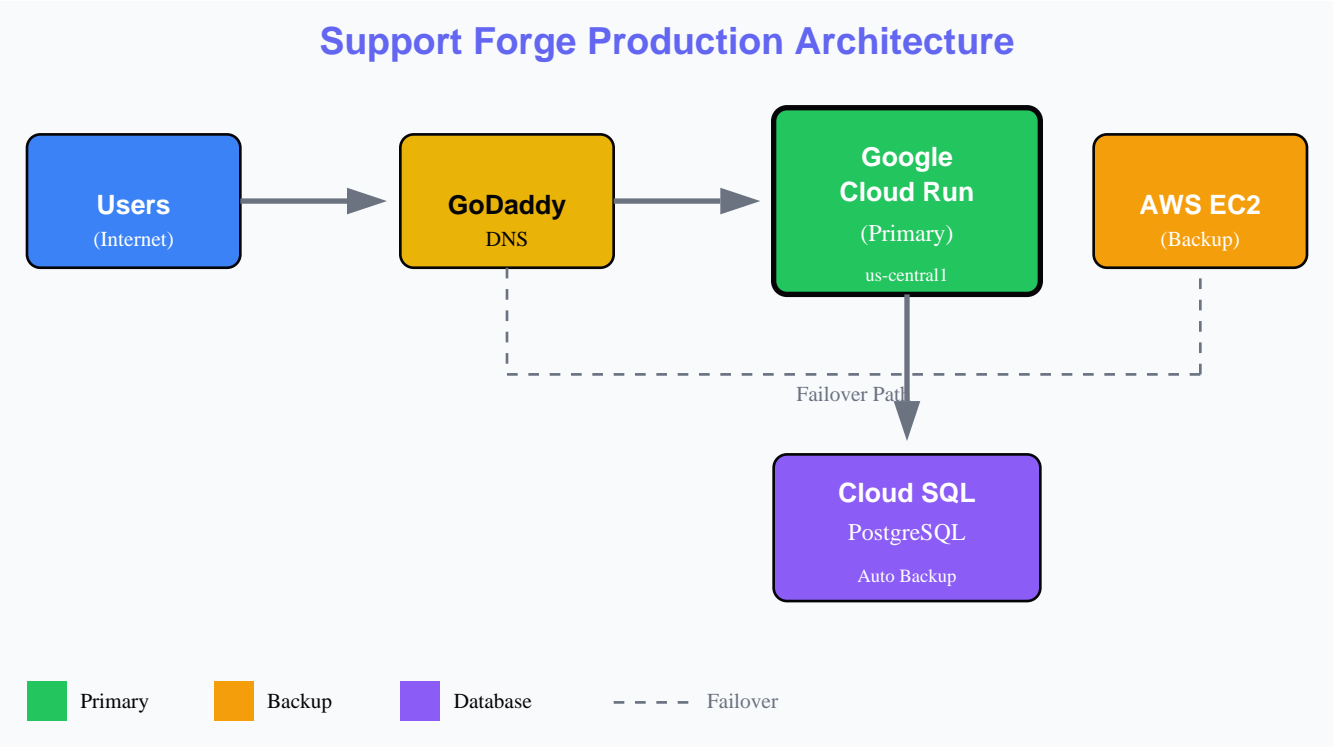support-forge.com

Table of Contents

1. Current Architecture Overview

Support Forge runs on Google Cloud Platform with an AWS EC2 backup instance available for failover. The architecture prioritizes availability, automatic scaling, and data protection.

Support Forge Production Architecture

```
Users                GoDaddy              Google              AWS EC2
(Internet)    →      DNS          →      Cloud Run           (Backup)
                                         (Primary)
                                         us-central1
                                              |
                                              | Failover Path
                                              ↓
                                         Cloud SQL
                                         PostgreSQL
                                         Auto Backup
```

■ Primary   ■ Backup   ■ Database   - - - - Failover

Primary Stack Components

Component	Service	Details
Web Application	Google Cloud Run	us-central1, Auto-scaling 0-20 instances
Database	Cloud SQL PostgreSQL	db-f1-micro, Daily backups at 04:00 UTC
DNS	GoDaddy	A records → Cloud Run IPs
SSL/TLS	Google-managed	Auto-provisioned, auto-renewed
Backup Host	AWS EC2	44.197.15.102 (Elastic IP)

2. Failure Scenario: Cloud Run Service Failure

What Triggers It

- Deployment errors (bad Docker image, missing env vars)
- Resource limits exceeded (memory, CPU)
- Application crashes or unhandled exceptions
- Container startup failures

Automatic Recovery

Cloud Run automatically restarts failed containers and routes traffic only to healthy instances. If all instances fail, Cloud Run will continuously attempt to start new ones.

Manual Recovery Steps

Step	Action	Command / Notes
1	Check service status	`gcloud run services describe support-forge --region=us-central1`
2	View logs for errors	`gcloud run services logs read support-forge --region=us-central1 --limit=50`
3	List revisions	`gcloud run revisions list --service=support-forge --region=us-central1`
4	Rollback to previous	`gcloud run services update-traffic support-forge --to-revisions=REVISION=100`

3. Failure Scenario: Google Cloud Account Suspension

CRITICAL: This is the most severe scenario requiring immediate failover to AWS.

Warning Signs

- Email notifications about billing issues
- Terms of Service violation notices
- Unusual activity alerts from Google
- Unable to access GCP Console

Immediate Impacts

All GCP resources become inaccessible: Cloud Run stops serving traffic, Cloud SQL database is unreachable, and the custom domain mapping fails. Users will see connection errors.

Failover Procedure to AWS EC2

Step	Action	Details
1	Verify AWS backup is current	SSH to 44.197.15.102 and check deployment
2	Update GoDaddy DNS	Change A record from Cloud Run IPs to 44.197.15.102
3	Update database connection	Point to backup DB or restore from Cloud SQL backup
4	Verify SSL certificate	AWS should have valid cert or use Let's Encrypt
5	Monitor propagation	nslookup support-forge.com (may take 5-60 min)
6	Test site functionality	Full QA of critical paths

GoDaddy DNS Update Commands

Login to GoDaddy → My Products → DNS → Manage → Edit A Records:

Record Type	Current Value (Cloud Run)	Change To (AWS)
A	`216.239.32.21`	`44.197.15.102`
A	`216.239.34.21`	`(delete)`
A	`216.239.36.21`	`(delete)`
A	`216.239.38.21`	`(delete)`
CNAME (www)	`ghs.googlehosted.com`	`support-forge.com`

4. Failure Scenario: Cloud SQL Database Failure

Backup Configuration

Setting	Value
Backup Window	Daily at 04:00 UTC
Retention	7 backups retained
Point-in-Time Recovery	Enabled
Binary Logging	Enabled for PITR

Point-in-Time Recovery (PITR)

PITR allows restoration to any point within the retention window. Use this when you need to recover from data corruption or accidental deletion to a specific moment before the incident.

```
gcloud sql instances clone support-forge-db support-forge-db-recovery \
  --point-in-time 2026-01-27T10:30:00.000Z
```

Manual Backup Restoration

Step	Command
1. List backups	`gcloud sql backups list --instance=support-forge-db`
2. Get backup ID	`Note the ID from the list (e.g., 1706345600000)`
3. Restore backup	`gcloud sql backups restore BACKUP_ID --restore-instance=support-forge-db`
4. Verify data	`Connect and run validation queries`

5. Failure Scenario: DNS/Domain Issues

GoDaddy Outage

If GoDaddy DNS is experiencing issues, DNS resolution will fail even if the hosting is healthy. Users may see 'DNS_PROBE_FINISHED_NXDOMAIN' or similar errors.

Immediate Workarounds

- **Direct IP Access:** Share direct Cloud Run URL with critical users: https://support-forge-301352865144.us-central1.run.app
- **Check GoDaddy Status:** https://status.godaddy.com/
- **Alternative DNS:** If prolonged, consider migrating DNS to Cloudflare or Route53

Domain Expiration Prevention

Ensure domain auto-renewal is enabled and payment method is current. Set calendar reminders for 90, 30, and 7 days before expiration.
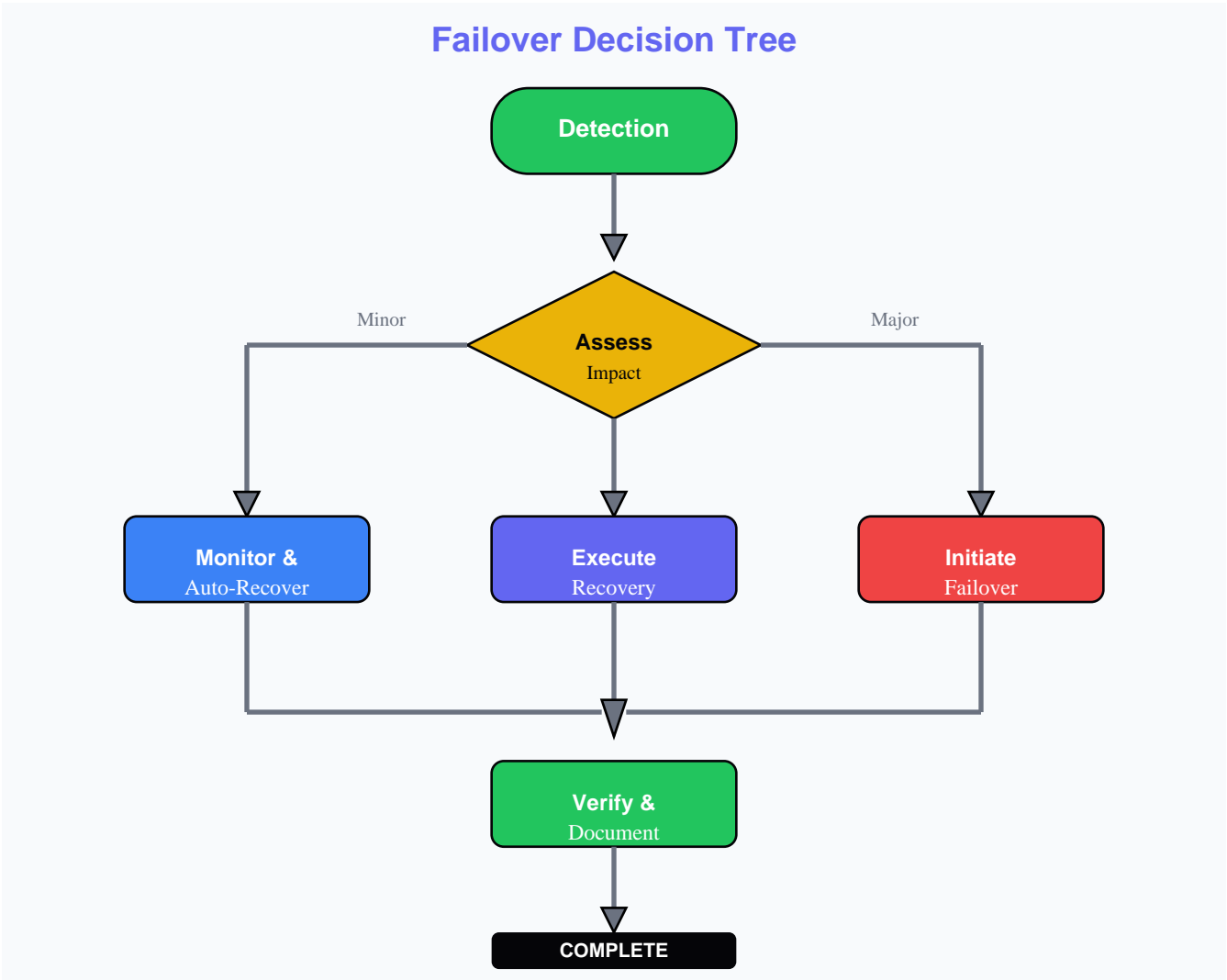
SSL Certificate Issues

Google Cloud Run manages SSL certificates automatically. If certificate provisioning fails:

Issue	Solution
Certificate stuck 'Pending'	Delete and recreate domain mapping (forces retry)
CAA record blocking	Add: 0 issue "pki.goog" to DNS
Propagation delay	Wait up to 24 hours, or use Google DNS (8.8.8.8) to verify

6. Failover Decision Tree

Use this flowchart to determine the appropriate response to any hosting failure.

Failover Decision Tree

```
                    Detection
                       │
                       ▼
        Minor      ╱ Assess ╲      Major
      ┌──────────◄  Impact   ►──────────┐
      │            ╲        ╱           │
      │                 │               │
      ▼                 ▼               ▼
  Monitor &         Execute         Initiate
  Auto-Recover      Recovery        Failover
      │                 │               │
      └─────────────────┼───────────────┘
                        ▼
                    Verify &
                    Document
                        │
                        ▼
                    COMPLETE
```

Decision Criteria

Severity	Indicators	Response
Minor	Single instance failure, <5 min downtime, auto-recovering	Monitor, no action needed
Moderate	Multiple failures, 5-30 min downtime, partial functionality	Manual restart/rollback
Major	Complete service outage, data at risk, >30 min impact	Initiate failover to AWS
Critical	Account suspension, security breach, data loss	Emergency failover + incident response

7. Emergency Contacts & Access

Console Access

Service	URL	Notes
GCP Console	console.cloud.google.com	Project: gen-lang-client-0978337543
GoDaddy	godaddy.com/en/accounts/products	DNS management
AWS Console	console.aws.amazon.com	Profile: support-forge

SSH Access

AWS EC2 Backup Server:

```
ssh -i ~/.ssh/support-forge-key.pem ubuntu@44.197.15.102
```

Quick Recovery Commands

Action	Command
Check Cloud Run status	`gcloud run services describe support-forge --region=us-central1`
View recent logs	`gcloud run services logs read support-forge --limit=50`
List Cloud Run revisions	`gcloud run revisions list --service=support-forge`
Check Cloud SQL	`gcloud sql instances describe support-forge-db`
DNS lookup	`nslookup support-forge.com`
Test SSL	`curl -Iv https://support-forge.com 2>&1	head -20`
Restart AWS Docker	`cd /home/ubuntu/support-forge-app && docker-compose restart`

Document maintained by: Support Forge Team
Last updated: January 27, 2026 at 17:34