

GAJWAF · OPERATIONS PLAYBOOK

Backup & recovery

Rebuild a node from scratch without losing a thing

Back up what you can't regenerate.

Be able to rebuild a GAIWAF node from scratch without losing its configuration, its place in the cluster, or its license. This playbook lists what to keep, how to keep it, and how to restore — then proves the restore works.

4 essentials

That cannot be regenerated

7 steps

To rebuild a node

1 register

To track every backup

GajShield Infotech Private Limited
Mumbai, India

Version 1.0 · October 2026
For GAIWAF administrators

LEGAL NOTICE

© 2026 GajShield Infotech Private Limited All rights reserved. This document is provided for the use of GAIWAF customers and partners. No part of it may be reproduced, distributed or transmitted in any form or by any means without the prior written permission of GajShield Infotech Private Limited

The information in this document is provided "as is", without warranty of any kind, express or implied, and is subject to change without notice. Features, menu labels and default values may differ between GAIWAF releases. While every effort has been made to ensure its accuracy, GajShield Infotech Private Limited accepts no liability for any loss, damage or service disruption arising from the use of, or reliance on, this document. This playbook is general operational guidance. It does not replace your organisation's own incident-response or change-control procedures, and GAIWAF is not a substitute for network-layer (L3/L4) DDoS protection.

GAIWAF and GajShield are trademarks of GajShield Infotech Private Limited Amazon Web Services, AWS and AWS Shield are trademarks of Amazon.com, Inc. or its affiliates. Microsoft and Azure are trademarks of the Microsoft group of companies. All other product and company names mentioned in this document are trademarks of their respective owners; they are used for identification purposes only, and their mention does not imply endorsement.

AT A GLANCE

What you can't regenerate

GOLDEN RULE

The things you cannot regenerate are the **site configuration**, the **license**, the **TLS certificates** and the **cluster secret**. Back those up.

Lose the cluster secret and your nodes can no longer share passes and bans.

1 Site configuration Sites, rules, exclusions → Console Export	2 Cluster secret Shared signing key for all nodes → Secret store	3 License Your licensed tier → Config / secret store	4 TLS certs & keys HTTPS for each site → Secure store
--	--	--	---

THE PLAYBOOK

BACK UP 1 Know what to back up	BACK UP 2 Make it routine	RECOVER 3 Rebuild a node	VERIFY 4 Prove it works
---	--	---	--

✗ DON'T

- **Don't** store the cluster secret, license or TLS keys in a code repository or in plain files — they're secrets.
- **Don't** assume a disk snapshot alone is a backup — without the config export, license and secret you can't cleanly rebuild.
- **Don't** let a rebuilt node rejoin with a *different* secret — it won't share state.

WHO Admin.

CONTENTS

1	Know what to back up	3
2	Make backups routine	3
3	Rebuild a node	4
4	Prove you can restore	5
✓	Backup register.....	6

STEP 1 OF 4

1 Know what to back up

PHASE **BACK UP** WHO Admin WHEN Once, when you deploy — then keep it current

Five things make up a GAJWAF node. The first four **cannot be regenerated** — lose them and you cannot rebuild cleanly.

Item	Why it matters	How to back it up	Keep it in
Site configuration	The whole policy — sites, rules, exclusions.	Console Export .	Off the node — your document or config store.
Cluster secret (<code>cluster.secret</code>)	Nodes derive their shared signing key from it.	Record it when you set it (Settings → clustering).	Your secret store .
License	Restores the licensed tier on a rebuilt node.	Keep the license file you received.	With the config, or in your secret store.
TLS certificates & keys	HTTPS for each site.	Keep the full-chain certificate and private key you installed.	A secure store — treat keys as secrets.
Node state (<i>optional</i>)	Bans, learned traffic baselines and other runtime state.	Snapshot the instance's disk in your cloud console (AWS EBS snapshot / Azure disk snapshot).	Your cloud account's snapshot storage.

IMPORTANT

Lose the **cluster secret** and your nodes can no longer share browser-check passes, device cookies, login sessions and bans.

✓ MOVE ON WHEN

You know where each of the five items lives today — and who can get to it.

STEP 2 OF 4

2 Make backups routine

PHASE **BACK UP** WHO Admin WHEN Regularly — and after every significant change

When	Do this
Regularly , and after any significant change (new site, new exclusions, rule changes)	Export the site configuration from the console and store the file off the node .
When you set or rotate a secret, renew a certificate or receive a new license	Put the new cluster secret , certificate key or license into your normal secrets management.
Before maintenance, or on your normal VM backup schedule	Snapshot the instance's disk if you want to keep bans and learned baselines across a rebuild.

✗ DON'T

- **Don't** keep the cluster secret, license or TLS keys in a code repository, a shared drive or any plain, readable file — they are secrets.

✓ MOVE ON WHEN

The latest config export is off the node, and every secret is in your secret store.

STEP 3 OF 4

3 Rebuild a node

PHASE **RECOVER** WHO Admin WHEN When a node is lost or replaced

1. **Launch a fresh GAJWAF instance** from the AWS or Azure Marketplace — the **same or a newer version**. (First sign-in: *GAJWAF Quick Setup Guide*.)
2. **Restore the license** — Settings → License.
3. **Restore the certificates** — for each site, **HTTPS certificate** → **Validate & install**.
4. **Import the site configuration** from your latest export.
5. **Set the cluster secret** — the **same value** as the other nodes — and this node's `cluster.node` name.
6. **Confirm it has joined the cluster**: a browser that passed the check on another node is **not** re-challenged here.
7. **Verify sites serve and Events flow**, then return the node to the load balancer.

IMPORTANT

Never let a rebuilt node rejoin with a **different** cluster secret — it will not share state, and clients moving between nodes will be re-challenged and lose sessions.

✓ MOVE ON WHEN

- The node is licensed, serves every site over HTTPS, and shares passes with the cluster.
- It is back in the load balancer.

STEP 4 OF 4

4 Prove you can restore

PHASE **VERIFY** WHO Admin WHEN Periodically — on a scratch node

A backup you have never restored is a hope, not a backup. Test it:

- **Test restore**: run Step 3 on a **scratch node**. It should come up working, **correctly licensed**, and **sharing passes** with the cluster.

- **Check the export:** the config export **opens and matches production**.

NOTE

A disk snapshot on its own is **not** a backup — without the config export, license and cluster secret you can't cleanly rebuild.

✓ MOVE ON WHEN

The last test restore succeeded, and its date is in the backup register.

KEEP THIS UP TO DATE

✓ Backup register

One row per item. Never write the secret itself here — only **where** it is kept.

Item	Last backed up	Stored where	Owner	Verified
Site configuration export				☐
Cluster secret				☐
License				☐
TLS certificates & keys				☐
Node disk snapshot				☐
Last test restore				☐

RECOVERY SIGN-OFF

NODE REBUILT / TESTED

COMPLETED BY

DATE

Related documents

Document	Use it for
Multi-node cluster setup & verification (playbook)	Setting up and checking the cluster a rebuilt node rejoins.
Upgrade & rollback (playbook)	Moving nodes between versions safely.
GAJWAF Features & Configuration Guide	Licensing (13.12) and high-availability clustering (13.11).
GAJWAF Quick Setup Guide — AWS & Azure	Launching and signing in to a fresh instance.