

Multi-node cluster setup

Set up and verify GAJWAF on more than one node

One secret. Every node.

The single most important thing to get right when GAJWAF runs on more than one node. Get it wrong and users see **endless re-challenges, lost sessions and bans that don't stick** — all tracing back to one setting.

1 setting

That matters most

5 steps

Topology → secret → sync → HA
→ verify

1 record

Of every node in the cluster

GajShield Infotech Private Limited
Mumbai, India

Version 1.0 · October 2026
For GAJWAF administrators

LEGAL NOTICE

© 2026 GajShield Infotech Private Limited All rights reserved. This document is provided for the use of GAJWAF 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 GAJWAF 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 GAJWAF is not a substitute for network-layer (L3/L4) DDoS protection.

GAJWAF 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

Why one setting matters

GOLDEN RULE

Every node must share the same **cluster secret**. The browser-check signing key and session passes are derived from it.

If node B has a different secret, it treats node A's passes as invalid — and the user is challenged again on every request that lands on the "wrong" node.

✓ **Clustered**

Shared cluster secret

Node A

key K

— pass —→

Node B

key K

Valid — no re-challenge

- Every node derives the **same signing key**
- A pass issued on node A is accepted on node B
- Sessions and bans follow the user

✗ **Not clustered**

No shared secret

Node A

key K1

— pass —→

Node B

key K2

Rejected — challenged again

- Each node uses **its own key**
- Fine for one node — **broken** behind a load balancer
- Users re-challenged whenever they land on the "wrong" node

TIP

Users behind an HA pair or load balancer report *"challenged over and over, it never sticks"*? This is the **first** — and usually the **only** — thing to check.

✗ **DON'T**

- **Don't** run multiple nodes behind one load balancer with different (or default per-node) secrets — that is the re-challenge bug.
- **Don't** expect the on-prem floating VIP to work on cloud networking — use the cloud load balancer.
- **Don't** leave a site enabled on some nodes and not others.
- **Don't** lose the cluster secret — store it with your other node secrets.

CONTENTS

1	Confirm the topology.....	3
2	Set the same cluster secret on every node	3
3	Keep site configuration in sync.....	4
4	Use the right high-availability model	4
5	Verify the nodes agree.....	5
✓	Cluster record.....	6

STEP 1 OF 5

1 Confirm the topology

PHASE **SET UP** WHO Admin ON Your network design

Your deployment	Is it a cluster?	What to do
One GAJWAF node	No	Nothing in this playbook is required.
Two or more nodes behind a load balancer	Yes	Configure it as a cluster — Steps 2–5.
An HA pair (active / standby)	Yes	Configure it as a cluster — Steps 2–5.

✓ MOVE ON WHEN

You know how many nodes you run and how traffic reaches them.

STEP 2 OF 5

2 Set the same cluster secret on every node

PHASE **SET UP** WHO Admin ON Every node**WHERE** Settings → High-availability clustering — on each node

Setting	Config key	Value
Cluster secret	<code>cluster.secret</code>	A long random string, kept secret — identical on every node .
Node name	<code>cluster.node</code>	A distinct name for each node (e.g. <code>waf-a</code> , <code>waf-b</code>).

IMPORTANT

- Store the cluster secret in your **secret store** the moment you create it — see the *Backup & recovery* playbook.
- Lose it, and you can't add or rebuild a node that shares state with the others.

✓ MOVE ON WHEN

Every node has the same cluster secret and its own node name.

STEP 3 OF 5

3 Keep site configuration in sync

PHASE **SET UP** WHO Admin ON Every node

A site must exist and be **enabled** on **every** node. Use the console's **Export / Import**, or your own automation, to copy the configuration from one node to the others — and repeat it after every change.

IMPORTANT

A site present on one node but missing or disabled on another causes **421 errors and intermittent failures**, depending on which node the load balancer picks.

✓ **MOVE ON WHEN**

Every node carries the same sites, all enabled, from the same configuration export.

STEP 4 OF 5

4 Use the right high-availability model

PHASE **SET UP** WHO Admin + network / cloud team ON Your platform

Where you run	Use for HA	Cluster secret
On-premises, on a Layer-2 network	GAJWAF's built-in floating VIP clustering	Required — same on every node
AWS / Azure	The cloud load balancer	Required — same on every node

IMPORTANT

The floating VIP is for on-premises Layer-2 networks **only** — it won't work on cloud networking. On AWS and Azure, use the cloud load balancer.

✓ **MOVE ON WHEN**

HA uses the model that matches your platform.

STEP 5 OF 5

5 Verify the nodes agree

PHASE **VERIFY** WHO Admin ON A fresh browser

1. From a **fresh browser** (or a private window), visit the site and **solve the browser check once**.
2. **Reload several times** so the load balancer routes you to different nodes. You should **not** be challenged again.
3. **Ban a test IP on one node**, and confirm the ban applies wherever the load balancer sends that client.

NOTE

Still re-challenged, but can't tell why? Turn on **Bot check** → "**Debug logging**" on each node, reproduce the problem, note the time and your IP, and send them to **GajShield Support** — the logs show whether the nodes agree on their signing key.

✓ MOVE ON WHEN

- A browser that passed the check on one node is **never** re-challenged on another.
- Bans apply across every node.

KEEP THIS UP TO DATE

✓ Cluster record

One row per node. **Never write the cluster secret here** — only confirm it is set and where it is stored.

Node name	Address	Secret set	Sites in sync	Passes shared
		☐	☐	☐
		☐	☐	☐
		☐	☐	☐
		☐	☐	☐

HA model	☐ Cloud load balancer (AWS / Azure) ☐ On-prem floating VIP
Cluster secret stored in	
Last config export synced	
Re-challenge test passed	☐ Yes
Ban test passed	☐ Yes
Verified by / date	

Related documents

Document	Use it for
Backup & recovery (playbook)	Storing the cluster secret, and rebuilding a node that rejoins the cluster.
Tuning the bot challenge (playbook)	Getting the browser check right for your users.
GAJWAF Troubleshooting & Support Manual	Chapter H.1 — "Multi-node / HA — the one setting that matters"; chapter D — repeated challenges.
GAJWAF Features & Configuration Guide	High-availability clustering (13.11).