Bastion Config

AWS MARKETPLACE · 30-DAY FREE TRIAL

Release 0.2.521 | Self-managed PostgreSQL 18 on EC2

Certificate-based access. Bounded DBA diagnostics.

Bastion runs in your AWS account. Supported application integrations connect with client certificates instead of database passwords. Begin with the documented EC2 reference deployment and verify your application integration before production use.

SECURE PRODUCTION DIAGNOSIS - INVESTIGATE PRODUCTION WITHOUT GRANTING CONTROL

A DBA receives an approved diagnostic window under a configured policy. Bastion connects as a read-only database role; this workflow does not give the DBA a standing credential.

1 Define the policy
A security admin selects tables, columns, panels, export and duration. Bastion checks the read-only role first; the policy card says ready or blocked.

2 Separate approval
A domain admin approves with a security key. The DBA opens its own approved session; a waiting request shows who can approve it. Expiry has a bounded running-query grace.

3 Check each statement
Only policy-permitted SELECT and EXPLAIN run, not EXPLAIN ANALYZE. Panels and CSV export need permission. The DBA gets no database credential.

REVIEWABLE ACTIONS AND APPROVALS

+ Administrative and JIT activity is recorded in your account's audit trail.
+ Signed checkpoints in S3 Object Lock are optional and require configuration.
+ Selected sensitive operations can require separate approval when the relevant policy is enabled.
+ Separate roles back up Bastion (Bastion backup admin) and a domain's PostgreSQL (Database backup admin).
+ Admins are warned about selected access to PostgreSQL hosts or their data that bypassed Bastion; AWS calls are seen only while a CloudTrail trail logs.
+ Evidence supports a security review; it is not regulatory certification or a compliance guarantee.

APPLICATION CERTIFICATES AND AGENT TRUST

+ A new client certificate defaults to 30 days and renews automatically with a supported integration. Existing certificates keep their lifetime.
+ Before issuing one, the console warns when no application using that database user has shown it renews; the key admin may then choose up to one year.
+ Revocation blocks new connections after the change reaches PostgreSQL. Existing sessions are separate.
+ Key admins can find a certificate by its serial.
+ New server certificates default to 90 days. Bastion presents the PostgreSQL agent a TLS leaf issued under its root; the agent renews its own bounded registration certificate.

CHECK YOUR DEPLOYMENT FIT

+ Current scope: self-managed PostgreSQL 18 on Linux/EC2. Bastion does not run on, attach to or manage RDS, Aurora or other managed PostgreSQL services. Bastion can import the data of one PostgreSQL 15 to 18 primary into a new deployment it builds.
+ Confirm your runtime and driver; no universal driver compatibility or uninterrupted-operation guarantee is implied. Marketplace includes one DBA diagnostics admin.
+ The reference deployment supports WAL archiving, scheduled base backups and PITR using your S3 storage.
+ Backup and recovery availability varies by deployment. Prove recovery in a drill; no RTO/RPO is guaranteed.
+ Works with Microsoft Entra ID: a company sign-in alone opens nothing, the security key is still required; a person disabled in Entra is refused by Microsoft at their next sign-in.

SETUP, UPDATES AND OPERATIONS

+ Unlock: two different security keys (FIDO2/PRF), no passphrase. Tested with a hardware key on macOS: Chromium and current Firefox.
+ Admins change a temporary password at first sign-in. After "Register a security key", an admin signs in with the key and its PIN alone, with no login name or password, unless company sign-in is on.
+ From 0.2.506: back up, upgrade the PostgreSQL agents (may restart PostgreSQL), then the stack; restart, unlock.
+ Email support: English, Mon-Thu, US Pacific. First-response target: 5 business days; no SLA or 24/7 coverage.
+ You own operations, alerts, retention and recovery decisions. AWS infrastructure costs are separate.

Check fit. Evaluate on AWS Marketplace.

Start with one non-production application: prove a connection, withdraw access and verify a new connection is refused after propagation. The 30-day software trial excludes AWS infrastructure charges.

Questions: bastion-config@fromkos.com
Accessibility statement: fromkos.com/docs/accessibility

AWS Marketplace