Webinar: How to Secure Elasticsearch in Production A Practical Implementation Guide

Anja Glauch · 2026-05-11

ON-Demand webinar · One quick registration. Watch now or whenever you're ready.

Elasticsearch out of the box is fast, flexible — and not production-secure. Default configurations leave authentication open, access controls flat, and audit trails missing. For teams running Elasticsearch in regulated industries or any environment touching sensitive data, the gap between "it works" and "it's safe to ship" is wider than most engineers realize.

In this 60-minute session, Marc walks through the security patterns that production-grade Elasticsearch deployments actually require. You'll see how to wire up enterprise authentication (LDAP, SAML, OIDC), design role-based access control that scales beyond a handful of users, set up multi-tenant isolation that holds up under audit, and capture the audit logs your compliance team will eventually ask for.

We'll close with the five most common Elasticsearch security misconfigurations Marc sees in real customer environments — and exactly how to fix each one. If you take one thing away from this session, it'll be that list.

Webinar – US Time Zone (PST)
(On-Demand, available for 2 month)

This link is no longer valid. Please cont

What you'll learn

- **Authentication that scales** — How to integrate Elasticsearch with LDAP, SAML, and OIDC, with a live walkthrough of an OIDC + Keycloak setup
- **Role-based access control done right** — Patterns for designing roles that survive contact with real users, real teams, and real data
- **Multi-tenancy without the leakage** — How to isolate workloads, indices, and dashboards so one tenant's data never reaches another
- **Audit logging your compliance team will accept** — What to capture, where to ship it, and how to make audits boring
- **The 5 misconfigurations to fix this week** — Marc's most-seen mistakes from real Search Guard deployments, with the exact remediation for each

Who should attend

Platform and DevOps engineers running Elasticsearch or OpenSearch clusters, security engineers evaluating search infrastructure, engineering leaders making build-vs-buy decisions, and compliance-adjacent engineers preparing for ISO, PCI, SOC 2, or GDPR reviews.

You don't need to be a Search Guard customer, most of the patterns apply to any Elasticsearch security stack.

Format

60 minutes total: 45 minutes of content and live demo, plus a 15-minute Q&A with Marc. Recording sent to all registrants within 24 hours.

This article was published on the Search Guard blog: https://search-guard.com/blog/webinar-how-to-secure-elasticsearch-in-production-a-practical-implementation-guide/