**What is X-Pack (xpack)?**

xpack stands for **Elastic X-Pack** — a **set of features** for:

* **Security**
* **Monitoring**
* **Alerting**
* **Machine Learning**
* **Graph analytics**
* **Reporting**
* **Index lifecycle management**
* And more…

As of Elasticsearch 7.x and later, **X-Pack is bundled** by default — you don’t install it separately anymore.

**📦 Common Use Cases of X-Pack**

**1. 🔐 Security (Authentication, Authorization, TLS)**

* Enable **user authentication** (e.g., LDAP, Active Directory, native users).
* **Role-based access control (RBAC)** to restrict who can do what.
* **HTTPS/TLS** encryption between nodes and between clients and nodes.
* **Audit logging** to track user activity.

➡️ *Use case*: Lock down access to sensitive logs, restrict access to production indices, encrypt traffic.

**2. 📊 Monitoring**

* Monitor **cluster health**, node performance, JVM stats, index metrics.
* Integrated with **Kibana Monitoring UI**.
* Monitor **Filebeat, Logstash, Metricbeat**, etc.

➡️ *Use case*: Visualize and troubleshoot performance issues.

**3. 🛎️ Alerting (Watcher)**

* Create alerts on data or cluster conditions.
* Send alerts to **Slack, Email, Webhooks**, etc.
* Example: Alert when error rate > 5%, or node disk usage > 80%.

➡️ *Use case*: Notify ops teams of critical conditions automatically.

**4. 🧠 Machine Learning (Anomaly Detection)**

* Automatically detect **anomalies** in time-series data.
* No need to predefine thresholds.

➡️ *Use case*: Spot sudden spikes in traffic, CPU usage, or fraud patterns.

**5. 📈 Index Lifecycle Management (ILM)**

* Automate moving data across **hot-warm-cold-delete** phases.
* Control index size, age, or performance tiers.

➡️ *Use case*: Keep hot data on fast SSDs, archive cold data on slower disks, delete after 90 days.

**6. 📤 Reporting**

* Export Kibana dashboards and visualizations as **PDF, CSV, PNG**.
* Automate reports on schedule.

➡️ *Use case*: Email daily metrics report to management.

**7. 🔍 Graph Analytics**

* Explore relationships between data — like how users relate to products.

➡️ *Use case*: Recommendation engines, fraud detection, social network analysis.

**🏷️ Licensing Tiers**

* **Basic (Free)**: Includes security (for basic auth), monitoring, ILM, and more.
* **Gold / Platinum / Enterprise**: Required for advanced security (e.g., LDAP), alerting, ML, etc.

You can check your current license via:

bash

CopyEdit

GET /\_license