

【錯誤處理】watermark 設定太小導致 index 變成唯讀

Log 出現:

```
filebeat-7.17.7-app-integrity-ap-prod-2025.11.09] blocked by:
[TOO_MANY_REQUESTS/12/disk usage exceeded flood-stage watermark, index has
read-only-allow-delete block];
```

以下是 **Elasticsearch** 出現 **flood-stage watermark** (磁碟使用率過高) 導致 index 變成 **read-only-allow-delete** 的完整處理方式 (你目前的錯誤訊息就是這個觸發的)。

❑ 錯誤原因

你的 Filebeat / Logstash 嘗試寫入索引
filebeat-7.7-app-integrity-ap-prod-2025.11.09

但 Elasticsearch 回覆：

```
blocked by: [TOO_MANY_REQUESTS/12/disk usage exceeded flood-stage watermark, index has read-only-allow-delete block]
```

這代表：

1. 磁碟使用量超過 **ES flood-stage watermark** (預設 95%)
2. ES 自己把 index 設成 **唯讀 (read-only-allow-delete)**
3. 所有寫入都會 429 / 403

ES 為了保護資料，所以禁止寫入。

❑ 解決方式

Step 1：檢查磁碟使用率

```
df -h
```

如果你看到 `/var/lib/elasticsearch` 所在的分區超過 95%，你要先：

- 清舊 index
- 增加磁碟空間
- 或移動 data path

Step 2：刪除舊 index (最常見處理方式)

例如刪除 90 天前的索引：

```
curl -X DELETE "http://localhost:9200/filebeat-*-2025.08.*"
```

或手動刪除：

```
curl -X DELETE "http://localhost:9200/filebeat-7.7-momo-app-integrity-ap-prod-2025.11.09"
```

☐你可以先查看所有索引大小：

```
curl -X GET "http://localhost:9200/_cat/indices?v&h=index,store.size"
```

Step 3：解除 ES 的 read-only 保護

即使磁碟清乾淨了，ES 還是會記住 read-only block
要自己取消

對所有 index：

```
curl -X PUT "http://localhost:9200/_all/_settings" -H 'Content-Type: application/json' -d'
{
  "index.blocks.read_only_allow_delete": null
}
'
```

或指定某個 index：

```
curl -X PUT "http://localhost:9200/filebeat-7.7-momo-app-integrity-ap-prod-2025.11.09/_settings" \
-H 'Content-Type: application/json' -d'
{
  "index.blocks.read_only_allow_delete": null
}
'
```

Step 4（建議）：調整 ES Watermark 避免一直被鎖

例如：

```
curl -X PUT "http://localhost:9200/_cluster/settings" \
-H 'Content-Type: application/json' -d'
{
  "persistent": {
    "cluster.routing.allocation.disk.watermark.low": "80%",
    "cluster.routing.allocation.disk.watermark.high": "90%",
    "cluster.routing.allocation.disk.watermark.flood_stage": "95%",
    "cluster.info.update.interval": "1m"
  }
}
'
```

Step 5（可選）：手動清理 translog

如果 ES 卡住很久，也可以清理 translog：

```
curl -X POST "localhost:9200/filebeat-*/_flush"
```

☐ 最快解法（給你直接用）

1. 刪舊 index
2. 解除 read-only

```
curl -X PUT "http://localhost:9200/_all/_settings" \  
-H 'Content-Type: application/json' -d \  
{ \  
  "index.blocks.read_only_allow_delete": null \  
} \  
,
```

3. 恢復 Filebeat 寫入

☐ 什麼是 Watermark ?

Elasticsearch 預設會監控 data 目錄所在磁碟使用率：

Name	意義	預設值	行為
low watermark	開始重新 routing shard	85%	輕警告
high watermark	停止將新 shard 分配到該節點	90%	停止新增 shard
flood-stage watermark	把 index 改成唯讀	95%	造成 read-only-allow-delete

你的錯誤訊息就是因為 flood-stage 達標。

☐ 修改 Watermark (官方標準方式)

☐ 調整 Watermark 百分比

以下 API 會直接套用在整個 cluster：

```
curl -X PUT "http://localhost:9200/_cluster/settings" \  
-H 'Content-Type: application/json' -d \  
{ \  
  "persistent": { \  
    "cluster.routing.allocation.disk.watermark.low": "80%", \  
    "cluster.routing.allocation.disk.watermark.high": "90%", \  
    "cluster.routing.allocation.disk.watermark.flood_stage": "95%", \  
    "cluster.info.update.interval": "1m" \  
  } \  
} \  
,
```

三個參數的用途：

- "low": "80%"
80% 才開始觸發 routing
- "high": "90%"
90% 以上 ES 不會在該 node 分配新的 shard
- "flood_stage": "95%"
超過 95% ES 會鎖 index → read-only

☐ 調整成更寬鬆 (如果磁碟常滿) 建議這組：

你可以把 `flood_stage` 往上調，比如 98% 或 99%：

```
curl -X PUT "http://localhost:9200/_cluster/settings" \  
-H 'Content-Type: application/json' -d '  
{  
  "persistent": {  
    "cluster.routing.allocation.disk.watermark.low": "85%",  
    "cluster.routing.allocation.disk.watermark.high": "92%",  
    "cluster.routing.allocation.disk.watermark.flood_stage": "98%",  
    "cluster.info.update.interval": "30s"  
  }  
}'
```

□ 若是單機環境（非 cluster），98% 是最常見的設定。

⚠ 另一種方式：改用「磁碟剩餘容量 (free bytes)」而不是百分比

例如磁碟剩下 10GB 才鎖 index：

```
curl -X PUT "http://localhost:9200/_cluster/settings" \  
-H 'Content-Type: application/json' -d '  
{  
  "persistent": {  
    "cluster.routing.allocation.disk.watermark.low": "10gb",  
    "cluster.routing.allocation.disk.watermark.high": "5gb",  
    "cluster.routing.allocation.disk.watermark.flood_stage": "2gb"  
  }  
}'
```

這種方式比較直覺、不怕磁碟變大或變小。

□ 注意：調整 Watermark 不會解除 index 的 read-only

如果某些 index 已經被鎖，需要再解除：

```
curl -X PUT "http://localhost:9200/_all/_settings" \  
-H 'Content-Type: application/json' -d '  
{  
  "index.blocks.read_only_allow_delete": null  
}'
```

或指定某個 index：

```
curl -X PUT "http://localhost:9200/filebeat-*/_settings" \  
-H 'Content-Type: application/json' -d '  
{  
  "index.blocks.read_only_allow_delete": null  
}'
```

查看所有 index 大小：

```
curl -X GET "http://localhost:9200/_cat/indices?v&h=index,store.size"
```

🔄 修訂版本 #4

★ 由 treeman 建立於 11 🍌🍌@🍌🍌 2025 14:40:44

✍ 由 treeman 更新於 11 🍌🍌@🍌🍌 2025 15:28:55