Index Management

Wazuh pflegt seine Daten auf dem Server unter unter /var/ossec/logs

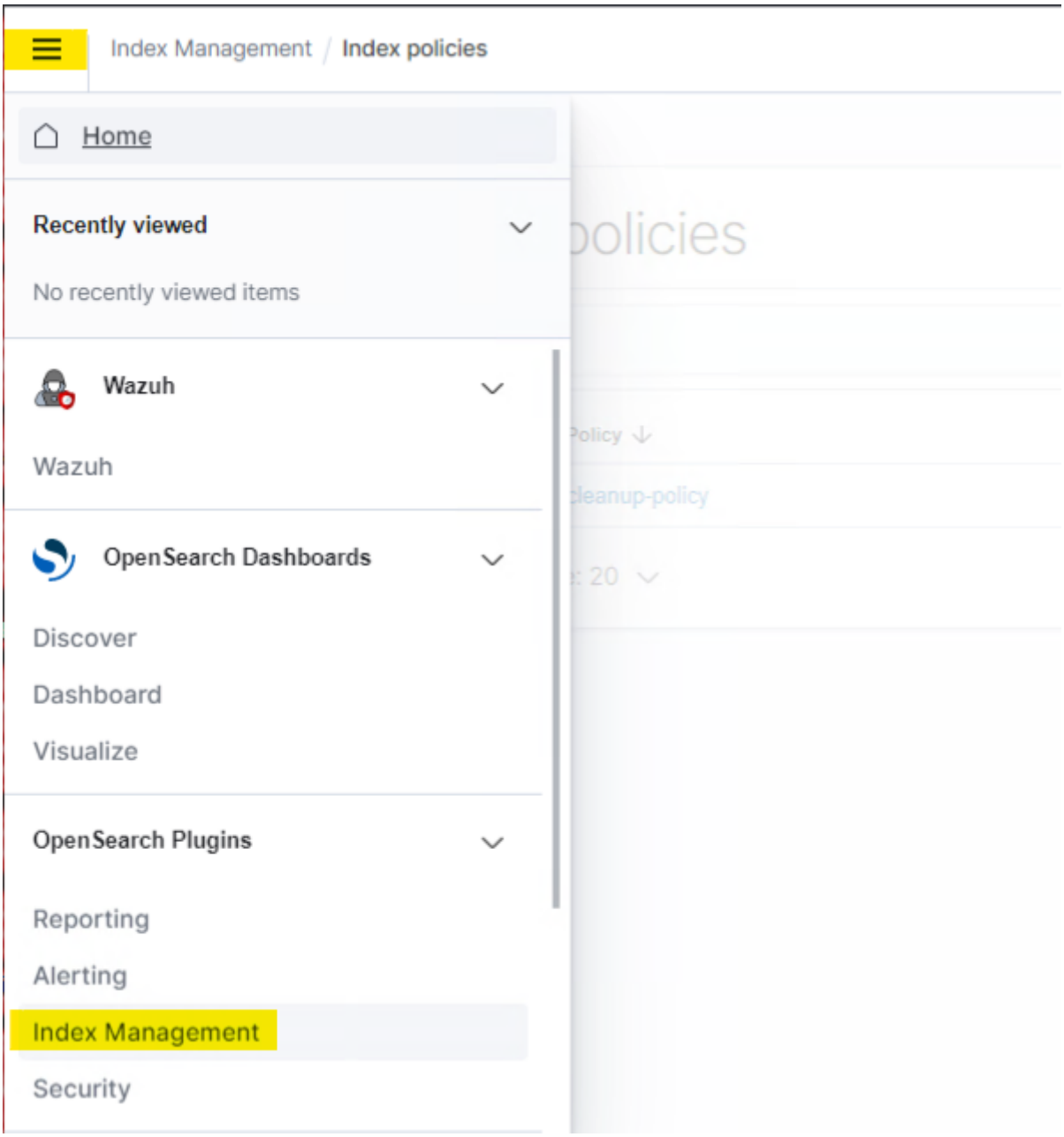
Die wichtigsten sind:

- /var/ossec/logs/alerts
- /var/ossec/logs/archives

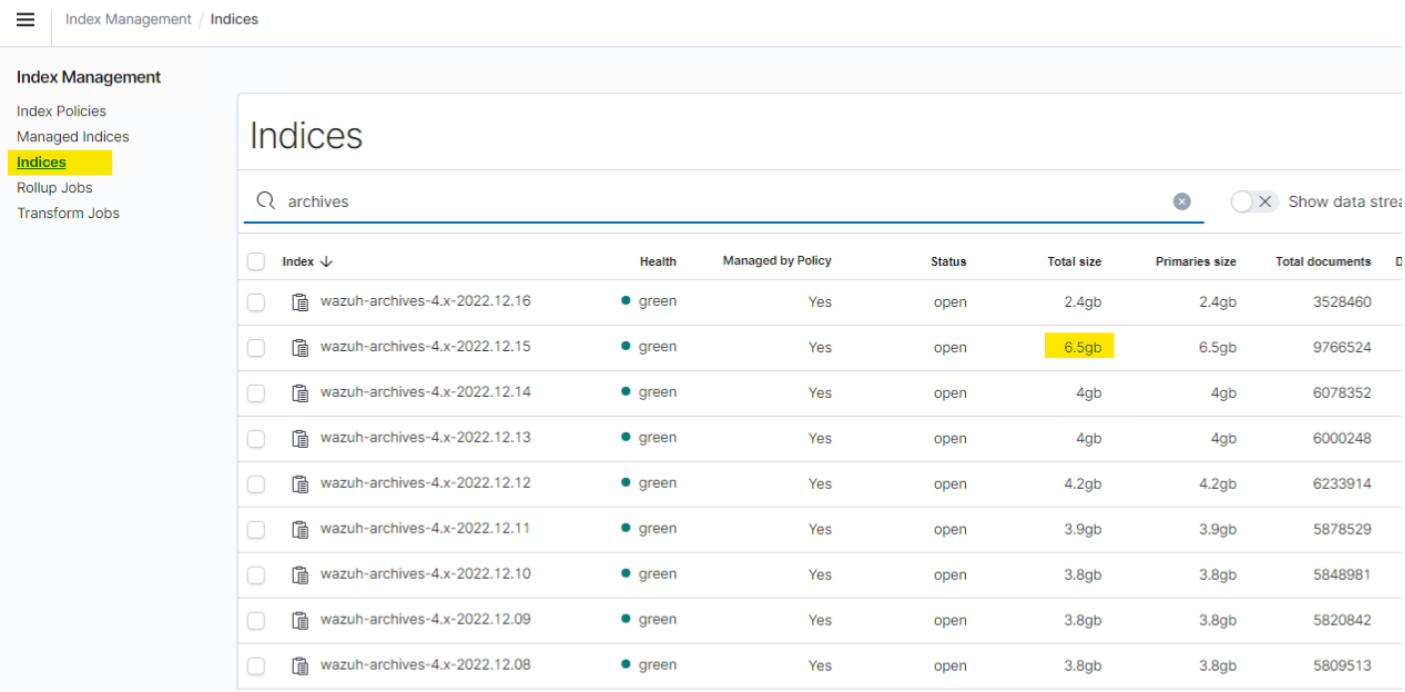
> Letzteren finden Sie, erst wenn die Sysog aktiviert haben und auch Gerät welche keine Agents nutzen können unterstützen wollen (z.B. VMWare, Switche, Firewalls, Gateway, VPNs usw.).

Die Indizies (Logs) finden Sie wie folgt:

- Loggen Sie sich im Wazuh Dashboard ein
- Gehen Sie oben Links auf die drei Balken
- Wählen Sie unten Index Management



- Dann unter Indicies finden sie die Indizies - besonders die unter wazuh-archives-* (für Syslogs) können sehr groß werden.



Damit nun die Festplatte nicht voll läuft, sollten das Index Management eingerichtet werden.

Hierzu bietet Wazuh einen Blogartikel an: https://wazuh.com/blog/wazuh-index-management/

> Dieser Artikel beruht auf einer älteren Version und sieht ein wenig anders aus - das ist jedoch nicht schlimm, wir benötigen nur den unteren Textteil.

Richten wir nun eine *Index Management Policy* ein:

- Gehen Sie links auf dem Punkt Index Policies
- Wählen Sie oben rechts Create Policy
- Wählen sie bei *Configuration Method* den *JSON Editor* aus
- Vergeben sie nun eine Policy ID wie z.B. *cleanup-policy*
- Ersetzen Sie den Inhalt durch den unten und wählen Sie *Create*

```
{
    "id": "cleanup-policy",
    "seqNo": 3244,
    "primaryTerm": 1,
    "policy": {
        "policy_id": "cleanup-policy",
        "description": "Cleanup Indicies Rule. Set after 15 Days to cold (Read Only) and delte
it after 60 Days.",
```

```
"last_updated_time": 1669980175085,
"schema_version": 12,
"error_notification": null,
"default_state": "hot",
"states": [
    {
        "name": "hot",
        "actions": [
            {
                "replica_count": {
                    "number_of_replicas": 0
                }
            }
        ],
        "transitions": [
            {
                "state_name": "cold",
                "conditions": {
                    "min_index_age": "15d"
                }
            }
        ]
    },
    {
        "name": "cold",
        "actions": [
            {
                "read_only": {}
            }
        ],
        "transitions": [
            {
                "state_name": "delete",
                "conditions": {
                    "min_index_age": "60d"
                }
            }
        ]
    },
    {
```

```
                "name": "delete",
                "actions": [
                    {
                        "delete": {}
                    }
                ],
                "transitions": []
            }
        ],
        "ism_template": [
            {
                "index_patterns": [
                    "wazuh-*"
                ],
                "priority": 100,
                "last_updated_time": 1669967389155
            }
        ]
    }
}
```

> Sollten Sie mehrere Wazuhserver bzw. Knoten haben - dann können Sie auch mehrere Replicas wählen - maximal die Anzahl der Knoten, die sie haben.

> Die Indizies, die aktuell genutzt werden sind *Hot*. *Cold* hingegen sind nur noch zum lesen vorhanden und belegen so weniger Systemressourcen (Ram und CPU, nicht Festplattenplatz). *Delete* gibt hingegen an, ab wann die Indizies (also die Dateien!) gelöscht werden. Diese sind danach nicht mehr zu nutzen, sofern sie diese nicht ausgelagert oder gesichert haben.

Ab nun an, werden die Indicies auf die Zukunft gepflegt. Sollten Sie diese Regel zu Anfang einrichten - sind sie nun fertig.

> Sollten Sie jedoch schon Indizies haben und möchten diese bereinigen (sehen Sie bitte davon ab, diese einfach von der Festplatte zu löschen - da sonst Wazuh nicht mitbekommt, das diese entfernt wurden), gehen sie einfach links auf Indicies und geben bei Search *wazuh-alerts* ein - wählen sie alle aus und klicken sie oben auf Apply Policy und wählen die eben erstellte Policy aus.

>

> Sollte die Festplatte schon vollgelaufen sein und sie virtualisieren - dann können Sie in der Virtualisierung die Festplatte vergrößern und mit Tools wie Gparted booten und damit die virtuelle Festplatte vergrößern. Sollten sie ein physiches System benutzen könnten Sie eine weitere Platte einsetzen, diese formatieren und temporär mounten - die Dienste beenden, danach die Dateien rüberkopieren und anschließend den alten Ordner löschen. Nachdem sie die fstab angepasst haben und neugestartet haben, sollten wieder alles in Ordnung sein. **Sie sollten jedoch unbedingt vorher Sicherungen erstellen!**

Revision #9
Created 2022-12-16 13:41:21 UTC by Peter Leibling
Updated 2022-12-22 22:57:11 UTC by Peter Leibling