سوال:

آیا امکان استفاده از **Zabbix Agent**  به جای **Filebeat**  وجود دارد؟ در زیر مقایسه دقیق این دو ابزار و سناریوهای مناسب برای جایگزینی آورده شده است:

**مقایسه Zabbix Agent vs. Filebeat**

| **ویژگی** | **Zabbix Agent** | **Filebeat** |
| --- | --- | --- |
| **هدف اصلی** | جمع‌آوری **متریک‌ها** (CPU, Memory, Network) و مانیتورینگ سلامت سیستم | جمع‌آوری و انتقال **لاگ‌ها** به مقصد (مانند Elasticsearch, Logstash) |
| **پروتکل** | طراحی شده برای Zabbix Server | طراحی شده برای Elastic Stack (Beats) |
| **انعطاف‌پذیری** | پشتیبانی از **اسکریپت‌های سفارشی** (UserParameters) | تمرکز روی **لاگ‌های از پیش تعریف‌شده** با پشتیبانی از ماژول‌ها (مانند Nginx, Apache) |
| **پردازش داده** | پردازش محدود (معمولاً داده خام به Zabbix ارسال می‌شود) | قابلیت **پارسرسازی** و **فیلتر کردن** داده قبل از ارسال |
| **یکپارچه‌سازی** | یکپارچه با Zabbix Server/Dashboard | یکپارچه با Elasticsearch, Logstash, Kibana |
| **مصرف منابع** | متوسط (وابسته به تعداد متریک‌ها) | بسیار سبک (بهینه‌شده برای انتقال لاگ) |
| **استفاده متداول** | **مانیتورینگ سیستم** و **هشداردهی** | **لاگ جمع‌کنی** و **ارسال به مرکز تحلیل** |

**سناریوهایی که می‌توان Zabbix Agent را جایگزین Filebeat کرد**

۱. **جمع‌آوری لاگ‌های ساده**

* اگر نیاز به جمع‌آوری **لاگ‌های محدود** (مثلاً یک فایل خاص) دارید، می‌توانید از قابلیت **UserParameters** در Zabbix Agent استفاده کنید.

۲. **تمرکز روی یک ابزار واحد**

* اگر از **Zabbix**  برای مانیتورینگ سیستم استفاده می‌کنید و می‌خواهید همه داده‌ها (متریک + لاگ) در یک پلتفرم متمرکز شوند، Zabbix Agent گزینه مناسب‌تری است.

۳. **هشداردهی یکپارچه**

* Zabbix Agent امکان **هشداردهی بلادرنگ** بر اساس لاگ‌ها را فراهم می‌کند (با استفاده از Triggers). این در حالی است که Filebeat نیاز به ابزارهای جانبی مانند ElastAlert یا Logstash دارد.

**سناریوهایی که جایگزینی توصیه نمی‌شود**

۱. **پردازش لاگ‌های پیچیده**

* اگر نیاز به **پارسرسازی پیشرفته** (مثلاً استخراج فیلدهای خاص از لاگ) دارید، Filebeat با ماژول‌های از پیش ساخته‌شده (مثل module: nginx) بسیار کارآمدتر است.

۲. **انتقال داده به Elastic Stack**

* اگر هدف نهایی شما **ایندکس کردن لاگ‌ها در Elasticsearch** و استفاده از **Kibana** است، Filebeat به دلیل یکپارچگی ذاتی با Elastic Stack انتخاب بهتری است.

۳. **حجم بالای لاگ‌ها**

* Zabbix Agent برای مدیریت **لاگ‌های حجیم** (مثلاً ترابایت داده) بهینه نیست، در حالی که Filebeat قابلیت **فشرده‌سازی** و **تقسیم داده (Batching)** دارد.

**راه‌حل ترکیبی (استفاده همزمان از هر دو)**

در بسیاری از سیستم‌ها، از هر دو ابزار به صورت همزمان استفاده می‌شود:

* **Zabbix Agent**: برای مانیتورینگ متریک‌ها و سلامت سیستم.
* **Filebeat**: برای ارسال لاگ‌ها به Elasticsearch جهت تحلیل پیشرفته.

**نتیجه‌گیری**

* **بله**، می‌توان از Zabbix Agent به جای Filebeat استفاده کرد، اما **فقط برای نیازهای محدود و ساده**.
* **خیر**، اگر نیاز به **پردازش لاگ در مقیاس بزرگ** یا **یکپارچه‌سازی با Elastic Stack** دارید، Filebeat گزینه بهتری است.

برای تصمیم‌گیری نهایی، پاسخ به این سوالات کلیدی است:

1. **هدف شما از جمع‌آوری لاگ چیست؟** (هشداردهی ساده vs. تحلیل پیشرفته)
2. **داده‌ها به کجا ارسال می‌شوند؟** (Zabbix Server vs. Elasticsearch)
3. **مقیاس سیستم شما چقدر است؟** (سرورهای محدود vs. خوشه‌های بزرگ)