ZABBIX

Resolvendo desafios de monitoramento de logs no SEB Bank

Estudo de caso

SEB

Cliente

SETOR
FINANCEIRO

NÚMERO DE FUNCIONÁRIOS
APROXIMADAMENTE 17.500 FUNCIONÁRIOS (2023)

LOCALIZAÇÃO
ESTOCOLMO, SUÉCIA

RECEITA
80,19 BILHÕES DE COROAS SUECAS (2023)

O SEB Bank é um grande grupo de serviços financeiros com sede em Estocolmo, na Suécia. Ele atende o norte da Europa, especialmente as regiões nórdicas e bálticas.

Conhecido por sua inovação digital e compromisso com a sustentabilidade, o SEB oferece serviços bancários, de investimento e consultoria financeira para pessoas físicas, empresas e instituições, com foco em relacionamentos de longo prazo e estabilidade financeira.

Desafio

Entre 2016 e 2020, a Divisão Báltica do SEB Group lançou uma plataforma de TI unificada para todos os três países bálticos. Diferentes países tinham diferentes ferramentas e atitudes em relação à maneira como o monitoramento deveria operar. Após inúmeras discussões e ponderação dos prós e contras de contar com múltiplas ferramentas de monitoramento, o SEB concluiu que a maneira mais eficaz de atingir a unificação seria (re)implementar tudo o que fosse necessário com o Zabbix.

Descobriu-se que uma grande quantidade de dados valiosos para monitoramento reside nos logs. Os logs variavam em frequência de atualização e estrutura, assim como os requisitos para extração de dados. Alguns itens de monitoramento eram padrões regex simples para contar entidades correspondentes ou capturar erros, enquanto outros tinham uma lógica mais complexa, como unir várias linhas para avaliação ou detectar dinamicamente padrões específicos a serem observados.

No início da jornada do SEB com o Zabbix, eles estavam usando a versão 3.0, que vinha com algumas limitações há muito esquecidas:

- Nenhum item `log.count` ainda
- Nenhuma expressão regular PCRE - apenas ERE estava disponível
- Recursos limitados de painel e visualização

Solução

Para abordar todos os desafios relacionados a logs, o SEB escolheu aproveitar os recursos "UserParameter" do Zabbix. Este recurso é inestimável para estender a funcionalidade do Zabbix.

- **log.discovery**

  Essa abordagem personalizada depende da capacidade de converter efetivamente grupos de captura de regex em objetos LLD (Descoberta de Baixo Nível). Quando novos elementos que precisam de monitoramento aparecem nos logs, os objetos de monitoramento correspondentes podem ser criados automaticamente no Zabbix.

  Certas combinações significativas são aprimoradas com gatilhos, gerenciados de forma eficiente usando a seção "Substituir" (“Override”) na configuração do LLD para garantir que sejam criados apenas para casos específicos. Com essa abordagem, problemas como lentidão inesperada podem ser detectados mais facilmente.

- **log.reader**

  Para cenários complexos de coleta de dados, havia a necessidade de implementar uma solução que permitisse extrair dados de logs com limitações mínimas. A abordagem foi

criar um mecanismo de leitura de log que, além disso, pudesse suportar qualquer lógica de extração de dados necessária.

- **Zabbix Agent2**
  Além das técnicas de processamento de log personalizadas mencionadas, o SEB tinha um bom motivo para usar o Zabbix Agent2. Tanto log quanto log.count são do tipo de item "Ativo". Esses itens não são processados em paralelo pelo agente Zabbix. Em locais com muitos itens baseados em log, o Agent2 foi usado, porque ele suporta o processamento simultâneo de verificações ativas.

Resultados

A capacidade de usar LLD em logs foi uma mudança radical para o SEB. Imagine centenas de itens diferentes descobertos a partir de uma única regra, juntamente com a exigência de monitorar qualquer nova entidade que corresponda a um padrão específico assim que ela aparecer.

Sem o LLD, atender a tal requisito teria sido simplesmente impossível. Essa abordagem abrange muitas áreas diferentes, incluindo métricas de missão crítica, como contagens de várias solicitações e durações de processamento.

Ser capaz de fatiar os próprios logs e, além disso, criar qualquer lógica necessária torna possível quase qualquer requisito de monitoramento personalizado. Com isso, a ferramenta oferece a capacidade de analisar dados de maneiras que nunca seriam possíveis de outra forma (por exemplo, monitoramento de duração média para grandes conjuntos de dados).

Conclusão

O SEB Bank nos países bálticos depende muito da coleta de dados de logs. O Zabbix é flexível o suficiente para atender à maioria das necessidades quando se trata de monitoramento. Além disso, permite implementações personalizadas quando necessário.

Essa flexibilidade é muito apreciada, pois remove muitas barreiras ao monitorar os vários componentes do ecossistema de TI e funções comerciais do SEB.