elastic

Search. Observe. Protect.

Migração para o Elastic Stack

Uma estratégia para ter velocidade, escala e relevância

elastic.co/pt

Índice

Introdução 3

Por que a Elastic? 4

Planejamento de uma migração 5

- Avaliação 5
- Prova de conceito (POC) 6
- Planejamento 6

Design e implantação 7

- Práticas recomendadas de design 7
- Otimização para o seu caso de uso 8
- Design pensando na simplicidade operacional 9
- Implantação do Elastic Stack 9
- Automação 10

Testes e preparo para produção 11

Migração 12

- Abordagens de migração 12
- Priorização de fontes de dados 14
- Migração de buscas, dashboards e alertas 15

Produção 16

- Dicas operacionais 16
- Centro de excelência (CoE) 16

Para montar a sua equipe Elastic 17

Referências adicionais 19

Conclusão 19

 © 2020 Elasticsearch B.V. Todos os direitos reservados.

Introdução

Uma mudança de plataforma de software pode parecer uma tarefa assustadora. A migração para novos sistemas requer definição do design certo, aquisição de recursos de nuvem ou hardware para software autogerenciado, análise e implementação de segurança, implantação e teste, políticas de governança, transferência de dados e outros conteúdos, suporte para as partes interessadas, contratação de pessoal, treinamento e muito mais. E mesmo quando há o reconhecimento e a aceitação de objetivos como melhoria nos insights dos dados, tecnologia com mais capacidade de ampliação e redução do custo total de propriedade (TCO), o próprio processo de migração para uma nova plataforma pode interromper até mesmo o melhor dos planos.

A intenção deste guia é simplificar a sua migração para o Elastic Stack. Veremos estratégias para sair de plataformas legadas como Splunk® e ArcSight®, minimizando interrupções, riscos e custos.

eb-introtoAPM-2020-2566 | elastic.co/pt | © 2020 Elasticsearch B.V. Todos os direitos reservados.

Por que a Elastic?

A Elastic é uma empresa de busca, o que significa que disponibilizamos o poder da busca — a capacidade de encontrar informações e insights relevantes em grandes quantidades de dados instantaneamente — para um conjunto diversificado de aplicações.

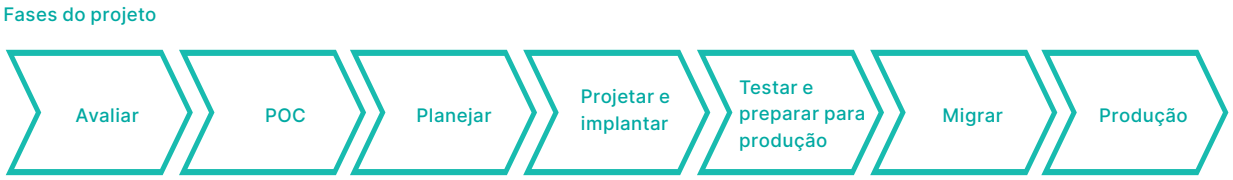
O Elastic Stack é um poderoso conjunto de produtos para ingestão e armazenamento de dados de qualquer fonte, em qualquer formato, realizando buscas, análises e visualizações em milissegundos. Nós também criamos soluções com base no Elastic Stack para uma ampla variedade de casos de uso: Elastic Enterprise Search para busca no local de trabalho, em apps e em websites; Elastic Observability para logging, métricas e monitoramento de performance de aplicação (APM); e Elastic Security para gerenciamento de eventos e informações de segurança (SIEM) e segurança de endpoint.

O Elastic Stack e nossas soluções foram desenvolvidos para serem executados em nuvens públicas ou privadas, em ambientes híbridos ou em ambientes locais tradicionais. Conforme o panorama da tecnologia muda, nossos produtos crescem e se adaptam. Nesse sentido, acreditamos que a nossa empresa é verdadeiramente elástica.

Planejamento de uma migração

Em qualquer projeto de migração, é importante demonstrar o sucesso para os negócios desde o início. Ao migrar para o Elastic Stack, isso significa que devemos nos concentrar primeiro nas fontes de dados e insights de maior prioridade, e criar visualizações e dashboards para atender aos objetivos de negócios. Com o tempo, outras fontes de dados podem ser adicionadas. A natureza distribuída do Elastic Stack facilita a ampliação e a adição de nós de dados a qualquer momento.
Recomendamos dividir a sua jornada de migração nas fases a seguir. O dono do projeto ou a parte interessada do negócio deve estar ciente de que, embora cada uma dessas fases possa ser diferente quanto à duração e aos detalhes, é importante garantir que cada marco seja concluído no nível certo para a sua organização:

- Avaliação
- Prova de conceito
- Planejamento
- Design e implantação
- Testes e preparo para produção
- Migração
- Produção



Avaliação

A fase de avaliação do projeto deve incluir a identificação e a priorização das fontes de dados, das visualizações e das necessidades da equipe e da organização. Essa fase pode ser dividida em:

- **Avaliação de negócios:** reúna-se com cada uma das equipes de negócios para determinar a prioridade e as necessidades do usuário final, incluindo resultados, funcionalidade e treinamento. Também inclui requisitos como conformidade regulamentar, políticas, requisitos de retenção de dados e RTO/RPO de recuperação de desastres.
- **Avaliação técnica:** reúna-se com as partes interessadas técnicas de várias equipes para descobrir o ambiente, a arquitetura e as fontes de dados existentes (tipo e formato da fonte, complexidade). Use essas informações para começar a projetar o novo ambiente e descartar possíveis obstáculos.
- **Entregáveis:** um documento que lista os fatores de sucesso e os objetivos de negócios, contendo uma descrição do ambiente atual, seguido de uma lista detalhada de requisitos técnicos e de negócios.

Prova de conceito (POC)

Caso ainda não tenha sido executada, recomendamos incluir uma fase de POC na sua jornada de migração como parte do processo de avaliação. Um ambiente de POC com um pequeno número de fontes de dados que representem as necessidades de negócios de alta prioridade pode ser benéfico para o desenvolvimento inicial e a validação, além de agilizar as fases futuras. O ambiente de POC também pode ser útil para apresentar e demonstrar valor para executivos e patrocinadores, e pode ser usado para testar a inclusão de novas fontes de dados mais adiante.

Planejamento

A fase de planejamento deve incluir:

- Definição das tarefas de implementação e marcos
- Estimativa do esforço para cada tarefa e marco
- Descrição das dependências (técnicas, de negócios, de pessoas)
- Identificação das funções das principais partes interessadas no projeto e alocação de tarefas
- Criação e compartilhamento de um plano de projeto

Ao longo da duração do projeto, a equipe de gestão de projetos (GP) deve validar os requisitos de planejamento frente ao andamento do projeto. Entre as tarefas comuns e os pontos de verificação do GP, incluem-se:

- Avaliações contínuas de marcos de consultoria
- Informações sobre as dependências
- Escalações de riscos
- Gerenciamento de solicitações de alteração
- Relatório de status do projeto para as partes interessadas
- Gerenciamento de recursos e orçamento
- Transferência, treinamento do usuário e integração de dados

Design e implantação

Práticas recomendadas de design

A primeira etapa é arquitetar uma plataforma do Elastic Stack que seja limitada em seu tamanho inicial, mas que seja projetada para ser ampliável. Inicialmente, não há necessidade de arquitetar com muita complexidade uma plataforma distribuída — o Elastic Stack ou o Elastic Cloud pode ser configurado para crescimento futuro usando alguns princípios de design simples:

- Use uma arquitetura com práticas recomendadas desde o início, na qual nós dedicados e qualificados para se tornarem nós master possibilitem a adição futura de nós de dados conforme necessário para o crescimento
- Implemente armazenamento local por nó que não dependa de um sistema de armazenamento centralizado
- Estabeleça diretrizes antecipadas para os requisitos de desempenho relativo dos dados atuais em contraste com os dados históricos em uma estratégia de índice congelado hot-warm — onde os dados atuais residem em armazenamento SSD de alto desempenho, enquanto os dados mais antigos são armazenados em um disco rígido mais denso —, a fim de minimizar o TCO e maximizar a densidade dos dados
- Use o Elastic Common Schema (ECS) com o Elastic Security e os Beats para padronizar o mapeamento de dados e simplificar o processo de ingestão por meio de modelos do Filebeat.
- Use um fluxo de dados que centralize todos os dados primeiro em pipelines do Logstash de alto volume ou outras ferramentas, como Kafka ou Redis. Então, permita que as várias plataformas de destino acessem alguns desses dados ou todos, proporcionando flexibilidade e crescimento futuro. A bifurcação do fluxo de dados poderá então ser usada para migrar incrementalmente as cargas de trabalho para o Elastic Stack.

- Use nós de ingestão para enriquecer ou transformar os dados durante a ingestão. Um pipeline com vários processadores pode ser configurado por fonte de dados conforme necessário para garantir a consistência dos dados desde a migração até o streaming de dados de produção normal.
- Projete para alta disponibilidade e tolerância a falhas com disponibilidade de várias zonas, usando zonas de disponibilidade do Elastic Cloud, ou distribuição de vários clusters, usando replicação entre clusters e/ou busca entre clusters.
- Crie um ambiente de teste/provisório (mesmo que seja apenas para um único nó) onde as equipes de negócios possam testar a ingestão e o mapeamento. As configurações de mapeamento poderão então ser movidas para sua instância de produção por meio dos modelos de índice do Elasticsearch, permitindo que você desabilite o mapeamento dinâmico na produção, mas o deixe habilitado no ambiente de teste ou preparação. O mapeamento dinâmico é uma ótima ferramenta para experimentar ou desenvolver com o Elastic Stack e facilita a obtenção de uma compreensão inicial de seus dados, mas, em geral, não deve ser usado na produção devido a problemas em potencial com explosão de campos ou degradação de desempenho.

Otimização para o seu caso de uso

Uma decisão importante que surge em todas as plataformas de clientes é a de projetar para os requisitos específicos da organização. Parâmetros como custo e taxa de resposta à consulta podem ser ajustados às suas necessidades específicas. A arquitetura hot-warm da Elastic e os modelos de implantação do Elastic Cloud são baseados em padrões comprovados e reproduzíveis, facilitando a seleção da arquitetura certa para a sua implantação.

Como exemplo, talvez você precise otimizar para um ambiente com uso intensivo de gravação, com vários terabytes por dia de ingestão de log e endpoint, mas o número de buscas na plataforma seja moderado. Nessa situação, você pode optar por aumentar a quantidade de dados armazenados por nó para maximizar a densidade dos dados, embora reconheça que buscas complexas podem levar minutos em vez de segundos. Um exemplo oposto seria um ambiente de busca para um catálogo de comércio eletrônico: você pode dar suporte a milhões de consultas de busca por minuto, mas os dados mudam diariamente e, portanto, essa é uma plataforma com uso intensivo de leitura, que requer mais recursos de computação de CPU e memória, mas utiliza entrada/saída (E/S) apenas moderada. Ou talvez você tenha uma plataforma multiuso que dê suporte a vários casos de uso e exija um equilíbrio entre as operações de leitura e gravação, com vários clusters no mesmo centro de excelência (CoE).

Esses requisitos, identificados no início, podem levar a boas decisões que permitirão que a plataforma seja ampliada no futuro. Altos requisitos de E/S e expectativas de busca quase em tempo real exigem investimento na camada hot de armazenamento, com menos de 4 TB por nó. Para consultas mais intermitentes ou ao permitir tempos de resposta mais longos, é possível ter uma densidade de dados mais alta, de 8 a 16 TB por nó, com nós warm ou congelados. Nós sempre podem ser adicionados para ampliação, e diferentes tipos de nós proporcionam a combinação certa de nós hot, warm e congelados para manter um equilíbrio aceitável entre custo e desempenho. Rollups podem ser utilizados para armazenar resultados de dados importantes, ao mesmo tempo reduzindo o volume de dados de alta frequência. Finalmente, a gestão de ciclo de vida do índice (ILM) pode ser usada para definir políticas de ciclo de vida do índice, como transferir índices mais antigos para um armazenamento de custo mais baixo ou excluir dados antigos de forma predefinida.

Design pensando na simplicidade operacional

Existem muitas opções para simplificar a administração de longo prazo e o crescimento da sua plataforma Elastic Stack. Embora este guia não se aprofunde na parte de administração e operações, apresentamos algumas opções de implantação que são comumente usadas para facilitar a administração, melhorar a eficiência das equipes, reduzir o TCO atual e habilitar o ambiente para crescimento futuro.

- O Elastic Cloud elimina a necessidade de executar servidores localmente. Adicionar novos nós é tão simples quanto aumentar os recursos totais de memória, armazenamento e computação, e ele pode ser otimizado para uma arquitetura hot-warm e os requisitos da sua solução. O armazenamento de backend no Google Cloud, no Microsoft Azure ou na Amazon Web Services (AWS) pode ser selecionado no momento da criação do cluster.
- O Elastic Cloud Enterprise (ECE) fornece um produto de orquestração local ou na nuvem com a mesma base de tecnologia usada no Elastic Cloud. O ECE fornece o Elasticsearch, o Kibana e uma UI administrativa para containers baseados em Docker.
- O Elastic Cloud on Kubernetes (ECK) simplifica a configuração e a administração com o Elasticsearch, o Kibana e uma UI administrativa para o Kubernetes. Ele é baseado no padrão Operador do Kubernetes e é otimizado para gerenciar uma ou mais implantações no Kubernetes.

Há outras ferramentas de orquestração de plataforma disponíveis. A orquestração, ou automação da instalação, da configuração e do provisionamento de nós ou clusters, pode melhorar muito a velocidade e a consistência da administração de um grande ambiente do Elastic Stack, bem como a eficiência da equipe de operações do CoE. Existem alguns diferentes métodos legados para orquestrar o Elastic Stack:

- Manual oficial do Ansible para Elasticsearch, fornecido pela Elastic
- Módulo oficial do Puppet para Elasticsearch, fornecido pela Elastic
- Cookbook oficial do Chef para Elasticsearch, fornecido pela Elastic
- Imagens do Docker para Elastic

Implantação do Elastic Stack

Projetar e otimizar a implantação do Elastic Stack para atender às suas necessidades desde o início ajudará a evitar que você tenha de refazer o trabalho em estágios posteriores. Nesta seção, compartilharemos várias práticas simples e considerações que ajudarão você a se preparar para crescer com escalabilidade.

- Implante um ambiente de desenvolvimento — uma plataforma de pré-produção que espelhe a produção e esteja pronta para ingestão de pipeline, criação de modelos de mapeamento e tarefas de desenvolvimento de casos de uso. O ambiente de desenvolvimento é uma valiosa plataforma provisória para integrar cada nova fonte de dados, bem como implementar

- e testar novos recursos, dashboards, plugins ou desenvolvimento. A vasta coleção de integrações da Elastic, plugins do Elasticsearch, plugins do Kibana e bibliotecas de API de DSL de consulta do Elasticsearch podem simplificar a etapa de integração de dados.
- Implante o ambiente de produção — uma plataforma pronta para dar suporte à carga de produção que possa ser facilmente ampliada ao longo do tempo com a simples adição de nós de dados e ingestão.
- Implante a plataforma de streaming de dados — um pipeline que seja facilmente controlado e seja suficientemente flexível para atender às necessidades de várias equipes, com largura de banda para ingerir eventos, logs ou dados de observabilidade por meio do modelo PUSH x PULL.
- Use trabalhos de machine learning e detecção automatizada de anomalia em todas as soluções para automatizar o monitoramento, aumentar a visibilidade e reduzir o tempo necessário para identificar anomalias e ameaças e responder a elas.

Automação

Os recursos de machine learning da Elastic podem identificar anomalias e gerar alertas para reduzir sua dependência de dashboards, enquanto o alerta pode ser integrado a sistemas de terceiros como e-mail, PagerDuty e Slack para permitir o envio e recebimento de notificações de forma proativa. As REST APIs da Elastic e a DSL de consulta do Elasticsearch permitem a automação de muitas áreas do Elastic Stack:

- Orquestração/construção
- Atualização
- Integridade operacional/diagnóstico
- Controle de fontes/implantação de casos de uso
- Machine learning
- Alertas
- Gestão de ciclo de vida de índices
- Enriquecimento de dados por meio de processadores de ingestão ou do Logstash
- Modelos de índice
- Uso do ECE e do ECK para rápida implantação de cluster e gerenciamento de zona
- Disponibilidade de várias zonas com ECE e ECK
- Detecção e resposta de endpoint (EDR)

Testes e preparo para produção

O teste deve acontecer em todo o projeto em vários níveis.

- Teste do usuário para cada caso de uso de alta prioridade: o teste do usuário geralmente inclui o carregamento de dados de amostra representativos na plataforma. O resultado esperado é que os modelos, o mapeamento de dados, os dashboards e os alertas para dados de alta prioridade estejam prontos no lançamento.
- Comparativo de referência de pipeline de dados: com a transmissão do pipeline de dados completo para o Elastic Stack, o pipeline de ingestão pode ser testado quanto à taxa de transferência e à resiliência. Esses dados podem ser facilmente excluídos antes da transição de migração. O resultado esperado é um relatório de utilização do pipeline de dados que pode ser usado como linha de base para crescimento futuro (taxa de transferência máxima, EPS máximo, CPU média, memória, consumo de disco com base nas fontes de log do cliente).
- Comparativo de referência de desempenho do Elasticsearch: embora o dimensionamento de referência tradicional não seja obrigatório em um sistema altamente distribuído, já que os nós podem ser adicionados conforme a necessidade para ampliar acompanhando o crescimento, um comparativo de referência pode ser utilizado para otimizar o volume de dados por nó e reduzir o TCO de longo prazo. Os resultados de referência da Elastic estão disponíveis aqui, ou você pode testar a capacidade em seu próprio ambiente com o Rally, o framework de referência open source da Elastic.
- Teste de um plano de recuperação de desastres que incorpore falha no nível da zona ou do local: o resultado esperado é que a equipe tenha um plano bem documentado e entenda as etapas necessárias para se recuperar da perda de uma zona crítica ou de um datacenter.

Migração

Com a implantação do Elastic pronta, agora é hora de começar a migrar o conteúdo.

- Dados de observabilidade: usando Beats lightweight e/ou o Logstash, fontes de eventos de log e métricas no formato do ECS podem ser ingeridas para mapear os dados de maneira rápida e previsível em um formato padronizado de fácil visualização no Elastic Stack. Agentes do Elastic APM fornecem monitoramento e traces no nível da aplicação.
- Dados de segurança: logs tradicionais de firewalls e roteadores de rede ingeridos pelo Elastic Security e pelos Beats, além de dados de captura de pacotes do Packetbeat, permitem a correlação de eventos de segurança e ameaças. O mecanismo de detecção do Elastic Security fornece regras prontas para uso para ameaças comuns. Com isso, é possível ter todos os dados relacionados à segurança em uma única janela, com correlação em todos os nós de host e rede.
- Dados de agentes legados: você pode usar agentes de envio legados, como encaminhadores da Splunk ou ArcSight SmartConnectors, para redirecionar os dados diretamente para o Elastic Stack. Esse é um método rápido para transmitir dados do seu pipeline para o Elasticsearch.

Abordagens de migração

Em geral, uma migração de uma plataforma legada é mais eficaz quando é feita diretamente dos dados brutos originais (logs, métricas, eventos de segurança etc.). A migração de dados processados ou rollups de resumo de plataformas legadas é muito mais complexa e menos útil. Com base na duração da retenção de dados necessária, a migração dos logs de dados brutos originais determinará o período de transição quando ambos os ambientes estiverem ativos em paralelo, o que reduz o impacto para a plataforma legada e reduz o risco geral e a complexidade da migração. Várias abordagens de migração com base no acesso e ingestão de dados brutos são descritas abaixo.

Abordagem de bifurcação

Com a abordagem de bifurcação, o tráfego de agentes legados é redirecionado para mecanismos do Logstash ou do Syslog para interceptar os eventos para o Elasticsearch. Depois que os casos de uso sob o gerenciamento da Elastic forem aprovados, poderá ser feita a mudança dos agentes legados para os Beats.

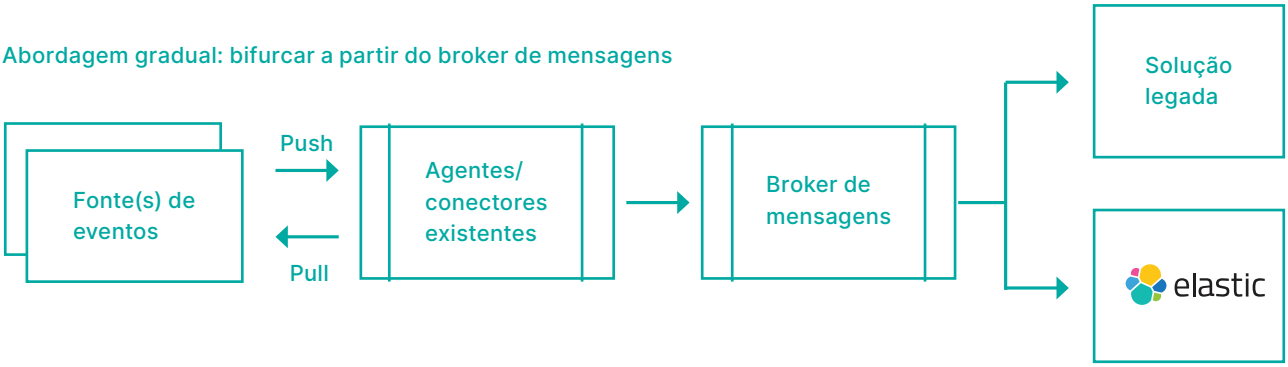
Vantagens:

- Dá tempo para entender as implicações da substituição de agentes legados (como os Universal Forwarders ou os Heavy Forwarders da Splunk)

Desvantagens:

- Requer configuração/alterações no destino dos agentes legados
- O licenciamento de ambos os serviços continua durante a transição

Abordagem gradual: bifurcar a partir do broker de mensagens



Abordagem de transição

A abordagem de transição introduz a instalação de todos os eventos de segurança ou coletores de log com o Elastic Security ou os Beats para encaminhar eventos para o Elasticsearch.

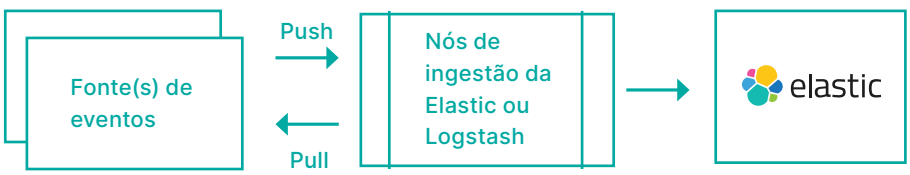
Vantagens:

- Processo limpo sem dependências do serviço legado
- Pode usar os Beats para implementação rápida ou ferramentas existentes como o Syslog com Logstash; estes ocasionalmente podem ser implantados em paralelo com agentes legados

Desvantagens:

- Requer alterações em todos os coletores de log de borda desde o início

Abordagem direta: transição a partir de fonte(s) de eventos



Abordagem de replicação

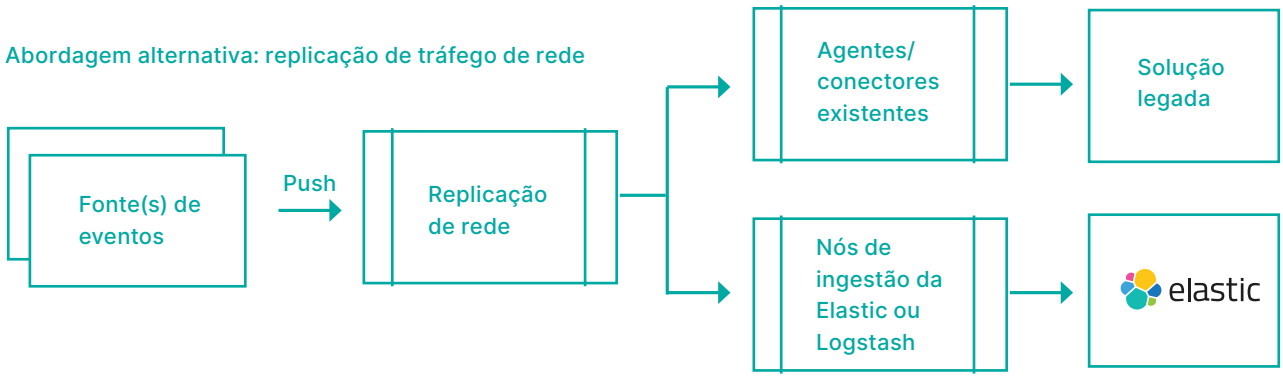
Com a abordagem de replicação, o tráfego dos agentes legados é redirecionado para um balanceador de carga ou broker de mensagens com recursos de replicação de tráfego.

Vantagens:

- Nenhuma alteração em hosts ou aplicações que já têm agentes legados

Desvantagens:

- Implica mais despesas operacionais (gastos com licenciamento/hardware em recursos de replicação de tráfego)
- Requer alterações no destino dos agentes legados



Priorização de fontes de dados

Uma organização pode ter centenas ou milhares de fontes de dados. Sua organização sabe melhor do que ninguém quais dados são mais importantes, e é fundamental identificar as fontes de maior prioridade para que possam ser implementadas primeiro.
É comum que certas fontes de dados sejam simplesmente mais importantes do que outras. Dividindo o processo de migração de fontes de dados com base na prioridade ou volume e padronizando o mapeamento de dados com o ECS, pode-se implementar um processo de migração contínua, permitindo que uma fonte de dados ou um pequeno subconjunto de fontes de dados seja movido por sprint. Isso segue um padrão comum, desta forma:

1. Mapeie a fonte de dados primeiro em um ambiente de teste ou desenvolvimento e verifique se ela funciona
2. Copie o modelo de índice para o ambiente de produção e faça a ingestão da fonte de dados na produção
3. Crie visualizações e dashboards para a nova fonte de dados e confirme se os dados estão mapeados corretamente e se os dashboards resultantes fornecem os insights necessários
4. Descomissione o sistema legado que fornecia as ferramentas de dados para essa fonte de dados (e reutilize os nós ou o hardware se possível — eles poderiam até mesmo ser apagados, reconstruídos e adicionados ao cluster da Elastic para capacidade adicional)
5. Confira e repita para as fontes de dados restantes

Migração de buscas, dashboards e alertas

Uma grande organização pode manter centenas ou milhares de visualizações, dashboards, alertas e buscas salvas. Muitos deles são criados por equipes individuais voltadas para seus próprios requisitos de dados ou área de monitoramento. Existem algumas estratégias comumente usadas para migrar essas consultas padrão:

- Como falamos anteriormente, a priorização é uma técnica fundamental. Muitas visualizações ou alertas existentes foram necessários em algum momento, mas podem não ser usados com frequência ou ser atuais. Deve-se pedir que cada equipe de dados priorize os dashboards consultados com mais frequência.
- As visualizações podem ser desenvolvidas com relativa rapidez pelas equipes de analistas. O Kibana Lens oferece um criador de visualizações com recurso de arrastar e soltar, possibilitando que novos dashboards sejam implementados de forma rápida e intuitiva.
- Os alertas do Elastic Stack podem ser criados rapidamente na seção Alerts and Actions (Alertas e Ações) do Kibana. Alertas menos precisos e sofisticados também podem ser desenvolvidos usando a DSL de consulta do Elasticsearch via Watcher. Para muitos casos de uso comuns, a seção Alerts and Actions fornece uma implementação mais rápida.
- Dashboards validados, alertas e relatórios criados em um ambiente de teste também podem ser migrados usando uma REST API ou por meio de exportação para o ambiente de produção.
- Dada a amplitude das necessidades de monitoramento, é fundamental que as suas equipes possam desenvolver seus próprios dashboards e alertas. O curso Data Analysis with Kibana (Análise de dados com o Kibana) abrange as habilidades de que suas equipes precisam para criar dashboards avançados rapidamente.

Produção

A fase de produção é resultado do sucesso das etapas anteriores. A operação de longo prazo para estabilidade e crescimento requer monitoramento e adição de novos nós de dados conforme a necessidade, além de gerenciamento do ambiente usando boas técnicas de integração, como planejamento para volume adicional e modelos de índice estático.

Dicas operacionais

É possível alcançar a eficiência operacional por meio de técnicas simples para assegurar a consistência para seus usuários, usando automação e abstração:

- Monitoramento da stack centralizado no ambiente Elastic para entender a capacidade de uso e o desempenho, incluindo o rastreamento da porcentagem de dados integrados/migrados
- Rollover automatizado de índice usando ILM
- Gerenciamento centralizado de pipeline para entrada, processamento e saída
- Caracteres curinga (*) em padrões de indexação para consultar vários índices
- Aliases de índice para abstrair nomes de índice

Centro de excelência (CoE)

O segredo para construir um CoE de produção é uma equipe de operações bem treinada e comprometida, com foco na estabilidade e previsibilidade da plataforma, mas permitindo que as equipes de dados aprimorem consistentemente o uso da plataforma e tenham suas necessidades de negócios atendidas. O baixo TCO é obtido aumentando a capacidade da plataforma conforme necessário para manter os tempos de resposta exigidos e adicionando nós de dados ao longo do tempo. Com a natureza distribuída do Elastic Stack, não há necessidade de construir a plataforma com grande complexidade inicialmente — novos nós de dados podem ser adicionados ao cluster em tempo real para aumentar os recursos de capacidade. Esse é o conceito central dos preços baseados em recursos da Elastic. Você pode otimizar para as necessidades da sua organização com base no volume total de dados armazenados, na retenção de dados e nos requisitos de tempo de resposta.

Para montar a sua equipe Elastic

Ao construir e administrar o ambiente do Elastic Stack, normalmente vemos algumas funções ou personas importantes nas equipes. Em uma equipe pequena, certamente é possível ter uma pessoa só fazendo todas as tarefas a seguir; em um ambiente maior, há otimização e escala que vem com a especialização por função.

- **Executivo da empresa ou parte interessada:** direciona os principais objetivos de negócios e o financiamento para a solução. Se o ambiente do Elastic Stack dá suporte a vários casos de uso, cada equipe de negócios pode ter seu próprio executivo ou principal parte interessada.
- **Analista de dados:** consome os insights de dados fornecidos pelo Elastic Stack. A certificação Elastic Certified Analyst foi desenvolvida para preparar e validar esses membros da equipe.
- **Embaixador:** trabalha diretamente com as equipes de negócios no planejamento da integração e na ingestão inicial de dados no Elastic Stack e as ajuda a criar dashboards ou desenvolver com base nas APIs.
- **Arquiteto-chefe:** cuida do projeto e do planejamento de capacidade da infraestrutura, do ambiente e das funções consultivas para melhor uso da plataforma. Recomendamos que os arquitetos-chefes obtenham a certificação para estarem preparados para responder a questões relacionadas a crescimento, práticas recomendadas, escala e desempenho.
- **Chefe de operações e equipe de operações:** são responsáveis pelo provisionamento da infraestrutura e das operações da plataforma. Esse trabalho poderá ser feito por uma equipe de DevOps se sua organização também estiver usando as REST APIs da Elastic ou a DSL de consulta do Elasticsearch por meio de uma biblioteca cliente na sua linguagem favorita e automação via ferramentas.
- **Chefe de busca ou relevância:** nas equipes do Enterprise Search, é o profissional responsável por otimizar a qualidade dos resultados da busca e trabalhar com as equipes de negócios para garantir que as expectativas dos usuários e da empresa quanto à busca sejam atendidas.

A equipe de Serviços da Elastic oferece uma variedade de serviços para auxiliar nossos clientes no desenvolvimento de conhecimentos e habilidades. Nós nos concentramos na transferência de conhecimento e em ajudar os clientes a se tornar autossuficientes na tecnologia da Elastic. Veja alguns dos nossos principais recursos de consultoria:

Gerente de engajamento

Faz a supervisão operacional no projeto. Auxilia no cronograma, recursos e navegação do seu plano de sucesso

Gerente técnico da conta

Consultor com função de consultoria de longo prazo

Arquiteto de incorporação

Orientação técnica de longo prazo e práticas recomendadas

Engenheiro de incorporação

Especialista técnico responsável pela entrega prática

Gerente de consultoria

Faz a supervisão da gestão e a alocação de engenheiros/especialistas

O treinamento e certificação da Elastic também ajuda a preparar sua equipe para trabalhar em projetos e operações do Elastic Stack. Temos muitos cursos que podem ajudar suas equipes a ganhar experiência e conhecimento sobre os produtos e soluções da Elastic, qualquer que seja seu perfil ou familiaridade com a nossa tecnologia.

- As assinaturas de treinamento da Elastic fornecem acesso a todo o nosso catálogo de cursos por um ano — a melhor opção para o aprendizado de longo prazo. As assinaturas Standard e Professional também incluem exames de certificação.
- Os cursos Elasticsearch Engineer I e Elasticsearch Engineer II, voltados para engenheiros e desenvolvedores de DevOps que trabalham em infraestrutura ou com APIs, preparam os alunos para a certificação Elastic Certified Engineer.
- O curso Data Analysis with Kibana (Análise de dados com Kibana), voltado para analistas e operadores que usam o Kibana para visualização de dados e dashboards, prepara os alunos para a certificação Elastic Certified Analyst.
- ECE Fundamentals (Fundamentos do ECE) é um curso gratuito que oferece treinamento básico para a instalação e a operação do ECE.
- Nosso curso Private Elastic Endpoint Security (Segurança de endpoint privada da Elastic) oferece a administradores e equipes de resposta a detecção de ameaças experiência prática no uso dos recursos de segurança de endpoint do Elastic Security.
- Por fim, existem vários outros cursos gratuitos para novos usuários do Elastic Stack.

Referências adicionais

Migração da Splunk para o Elastic Stack: migração de dados (blog)
Kibana for Splunk SPL Users (Kibana para usuários do Splunk SPL) (treinamento)

Conclusão

O Elastic Stack oferece velocidade, escala e relevância por meio de uma arquitetura distribuída nativa e decisões de design simples que possibilitam crescimento e flexibilidade no futuro. Esperamos que você tenha achado esta visão geral dos princípios de design útil, para que possa fazer uma migração tranquila e comece a trabalhar na sua nova plataforma rapidamente, evitando os riscos e os custos de uma migração complexa.