HashiCorp

Habilitação do modelo operacional em nuvem

Como escolher o caminho mais rápido para alcançar valor em um datacenter moderno e multinuvem

ARTIGO TÉCNICO (WHITEPAPER)

Conteúdo

Sumário executivo

Agora é o momento em que a nuvem precisa funcionar. Para prosperar em uma era de arquitetura multinuvem, impulsionada pela transformação digital, a TI empresarial deve evoluir a partir do controle baseado em ITIL para permitir processos de autoatendimento compartilhados para a excelência de DevOps.

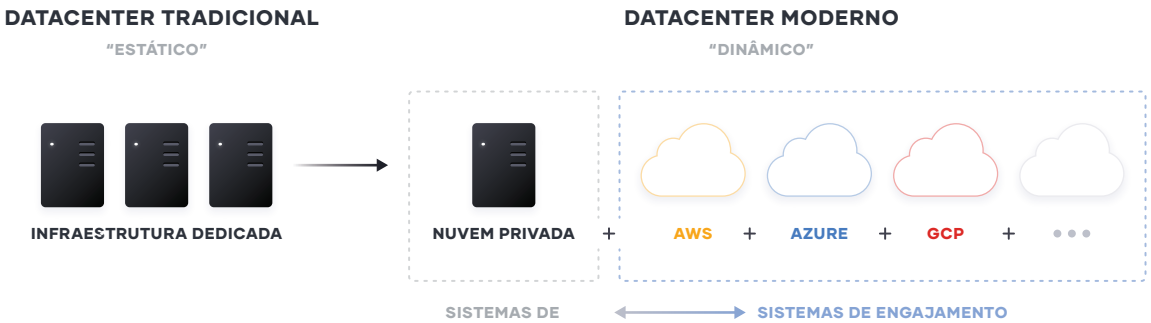
Para a maioria das empresas, os esforços de transformação digital significam entregar novos negócios e valor ao cliente mais rapidamente e em uma escala muito grande. A implicação para a TI empresarial é uma mudança da otimização de custos para a otimização de velocidade. A nuvem é uma parte inevitável dessa mudança, pois apresenta a oportunidade de implantar rapidamente serviços sob demanda com escala ilimitada.

Para desbloquear o caminho mais rápido para o valor da nuvem, as empresas devem considerar como industrializar o processo de entrega de aplicações em cada camada da nuvem: adotar o modelo operacional da nuvem e ajustar pessoas, processos e ferramentas a ele.

Neste artigo técnico, analisamos as implicações do modelo operacional em nuvem e apresentamos soluções para as equipes de TI adotarem esse modelo em todo o fornecimento de infraestrutura, segurança, rede e aplicações.

Transição para um datacenter multinuvem

A transição para ambientes em nuvem e multinuvem é uma transição geracional para a TI. Essa transição significa mudar de servidores amplamente dedicados em um datacenter privado para um banco de recursos de computação disponível sob demanda. Embora a maioria das empresas tenha começado com um provedor de nuvem, há bons motivos para usar serviços de outros e, inevitavelmente, a maioria das organizações da lista Global 2000 usará mais de um, seja por design ou por meio de fusões e aquisições.



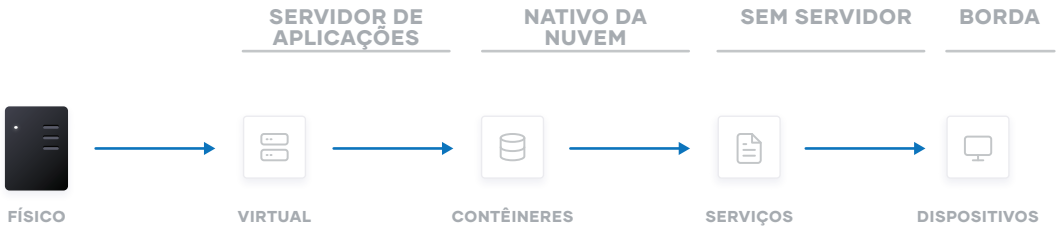
A nuvem apresenta uma oportunidade de otimização de velocidade e escala para novos "sistemas de engajamento", as aplicações criadas para a interação de clientes e usuários. Essas novas aplicações são a interface principal para o cliente se envolver com uma empresa e são ideais para entrega na nuvem, pois tendem a:

- Ter características de uso dinâmicas, com a necessidade de ampliar ou reduzir a escala por ordens de magnitude durante curtos períodos de tempo.
- Estar sob pressão para construir e reiterar rapidamente. Muitos desses novos sistemas podem ser de natureza efêmera, oferecendo uma experiência de usuário específica em torno de um evento ou campanha.

No entanto, para a maioria das empresas, esses sistemas de engajamento devem se conectar aos "sistemas de registro" existentes, os principais bancos de dados de negócios e aplicações internas, que muitas vezes continuam a ser hospedados na infraestrutura em data centers existentes. Como resultado, as empresas acabam com uma combinação híbrida de vários ambientes de nuvem pública e privada.

O desafio para a maioria das empresas é como entregar essas aplicações na nuvem com consistência, garantindo também o menor atrito possível entre as várias equipes de desenvolvimento.

Para aumentar esse desafio, as primitivas subjacentes mudaram, da manipulação de máquinas virtuais em um ambiente autônomo para a manipulação de "recursos" de nuvem em um ambiente compartilhado. Em seguida, as empresas têm modelos operacionais concorrentes para manter seus bens existentes, enquanto desenvolvem a nova infraestrutura de nuvem.



Para que a computação em nuvem funcione, é preciso haver fluxos de trabalho consistentes que possam ser reutilizados em escala em vários provedores de nuvem. Isso exige:

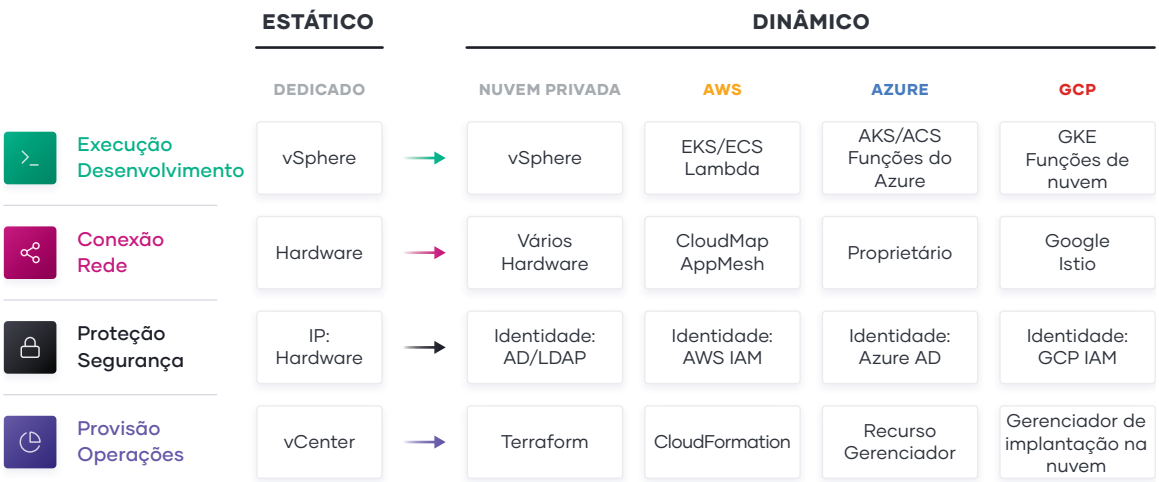
- Conjuntos de instruções consistentes para provisionamento
- Identidade para segurança e para conexões de rede
- Privilégios e direitos para que possam ser implantados e executados

Implicações do Modelo Operacional em nuvem

A implicação essencial da transição para a nuvem é a mudança da infraestrutura "estática" para a infraestrutura "dinâmica": do foco na configuração e gerenciamento de uma frota estática de recursos de TI para o provisionamento, a segurança, a conexão e a execução de recursos dinâmicos sob demanda.

Ao decompor essa implicação, e trabalhar na pilha, várias mudanças de abordagem estão implícitas:

- **Provisão.** A camada de infraestrutura passa de servidores dedicados em escala limitada para um ambiente dinâmico, no qual as organizações podem facilmente se ajustar ao aumento da demanda acionando milhares de servidores e reduzindo a escala quando não estiverem em uso. À medida que arquiteturas e serviços se tornam mais distribuídos, o grande volume de nós de computação aumenta significativamente.
- **Proteção.** A camada de segurança passa de um mundo fundamentalmente "de alta confiança" imposto por um forte perímetro e firewall para um ambiente "de baixa confiança" ou "confiança zero" sem perímetro claro ou estático. Como resultado, a suposição fundamental para a segurança muda, o que antes era baseado em IP passa a usar o acesso aos recursos baseado em identidade. Essa mudança é altamente impactante para os modelos de segurança tradicionais.
- **Conexão.** A camada de rede deixa de ser altamente dependente da localização física e do endereço IP de serviços e aplicações para usar um registro dinâmico de serviços de descoberta, segmentação e composição. Uma equipe corporativa de TI não tem o mesmo controle sobre a rede, ou os locais físicos dos recursos de computação, e deve pensar sobre a conectividade baseada em serviço.
- **Execução.** A camada de tempo de execução muda da implantação de artefatos para um servidor de aplicações estáticas para a implantação de aplicações com um programador no topo de um grupo de infraestrutura que é provisionado sob demanda. Além disso, novas aplicações se tornaram coleções de serviços que são provisionados dinamicamente e empacotados de várias maneiras: de máquinas virtuais a contêineres.



Para abordar esses desafios, essas equipes devem fazer as seguintes perguntas:

- **Pessoas.** Como podemos capacitar uma equipe para uma realidade multinuvem, onde as habilidades podem ser aplicadas consistentemente, independentemente do ambiente alvo?
- **Processo.** Como posicionamos os serviços centrais de TI como um facilitador de autoatendimento de velocidade, em vez de um mantenedor de controle baseado em tíquetes, mantendo a conformidade e a governança?
- **Ferramentas.** Qual é a melhor forma de revelar o valor das capacidades disponíveis dos provedores de nuvem em busca de melhor valor para o cliente e os negócios?

Habilitação do modelo operacional em nuvem

À medida que as implicações do modelo operacional em nuvem impactam as equipes em infraestrutura, segurança, rede e aplicações, vemos um padrão repetido entre as empresas de estabelecer serviços compartilhados centrais, centros de excelência, para fornecer a infraestrutura dinâmica necessária em cada camada para uma entrega de aplicação bem-sucedida.

À medida que as equipes entregam cada serviço compartilhado para o modelo operacional em nuvem, a velocidade de TI aumenta. Quanto maior a maturidade em nuvem que uma organização tem, maior é a sua velocidade.

A jornada típica que temos visto os clientes adotarem, à medida que habilitam o modelo operacional em nuvem, envolve três marcos principais:

1. **Estabelecer os fundamentos da nuvem**: ao iniciar sua jornada para a nuvem, os requisitos imediatos são provisionar a infraestrutura de nuvem, normalmente adotando a infraestrutura como código e garantindo que ela seja segura com uma solução de gerenciamento de segredos. Essas são as necessidades básicas que permitirão que você construa uma arquitetura de nuvem escalável e verdadeiramente dinâmica, preparada para o futuro.

2. **Padronizar em um conjunto de serviços compartilhados**: à medida que o consumo de nuvem começa a aumentar, você precisará implementar e padronizar em um conjunto de serviços compartilhados para aproveitar ao máximo o que a nuvem tem a oferecer. Isso também apresenta desafios relacionados à governança e à conformidade, pois a necessidade de definir regras de controle de acesso e requisitos de rastreamento se torna cada vez mais importante.

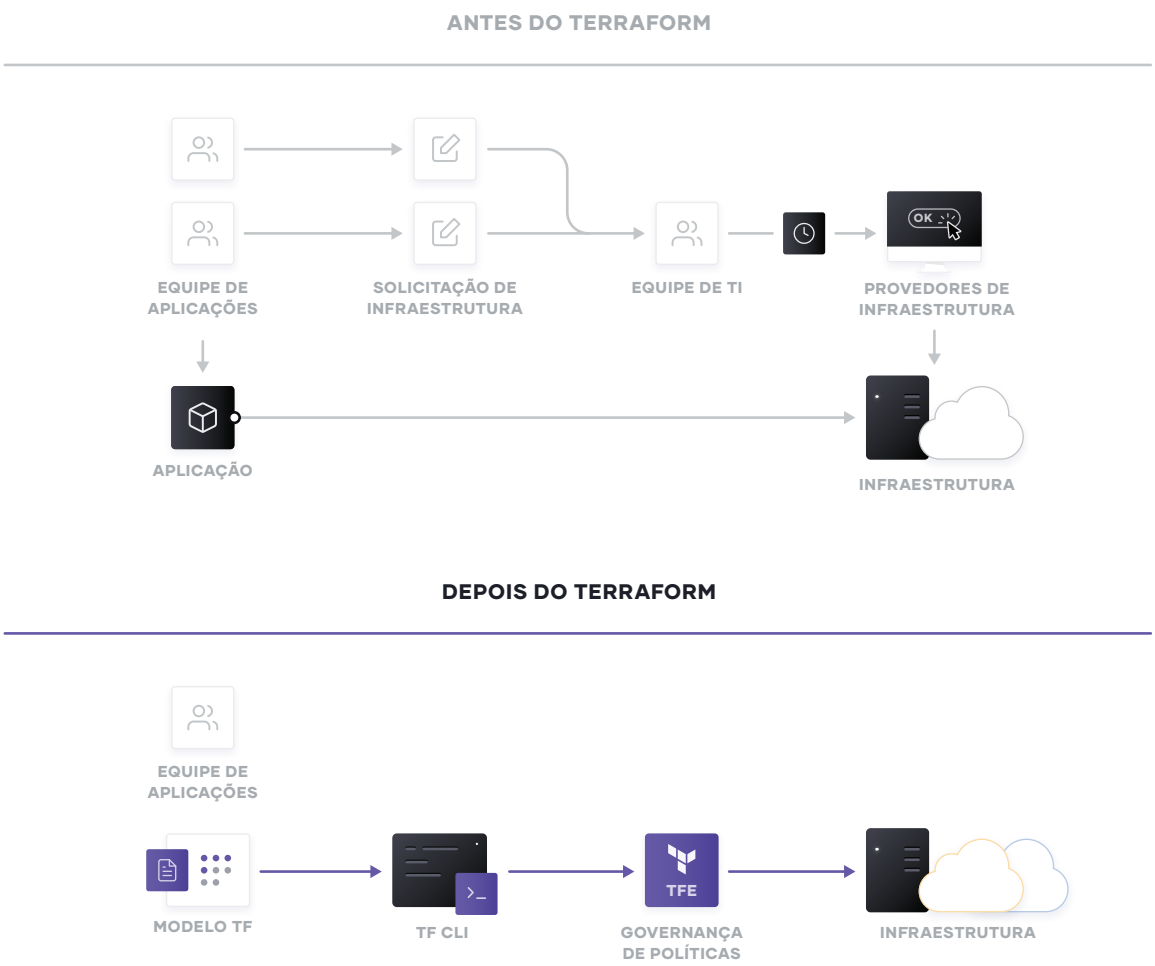
3. **Inovar usando uma arquitetura lógica em comum**: conforme ocorre a adoção completa da nuvem e a dependência de serviços e aplicações em nuvem como os principais sistemas de engajamento, haverá a necessidade de criar uma arquitetura lógica em comum. Isso requer um plano de controle que se conecte ao ecossistema estendido de soluções em nuvem e inerentemente forneça segurança e orquestração avançadas entre serviços e várias nuvens.

O que vem a seguir é o passo a passo da jornada que vimos as organizações adotarem com sucesso.

Etapa 1: Provisionamento de infraestrutura multinuvem

A base para adotar a nuvem é o provisionamento de infraestrutura. O HashiCorp Terraform é o produto de provisionamento de nuvem mais amplamente usado no mundo e pode ser usado para provisionar infraestrutura para qualquer aplicação usando uma variedade de provedores para qualquer plataforma de destino.

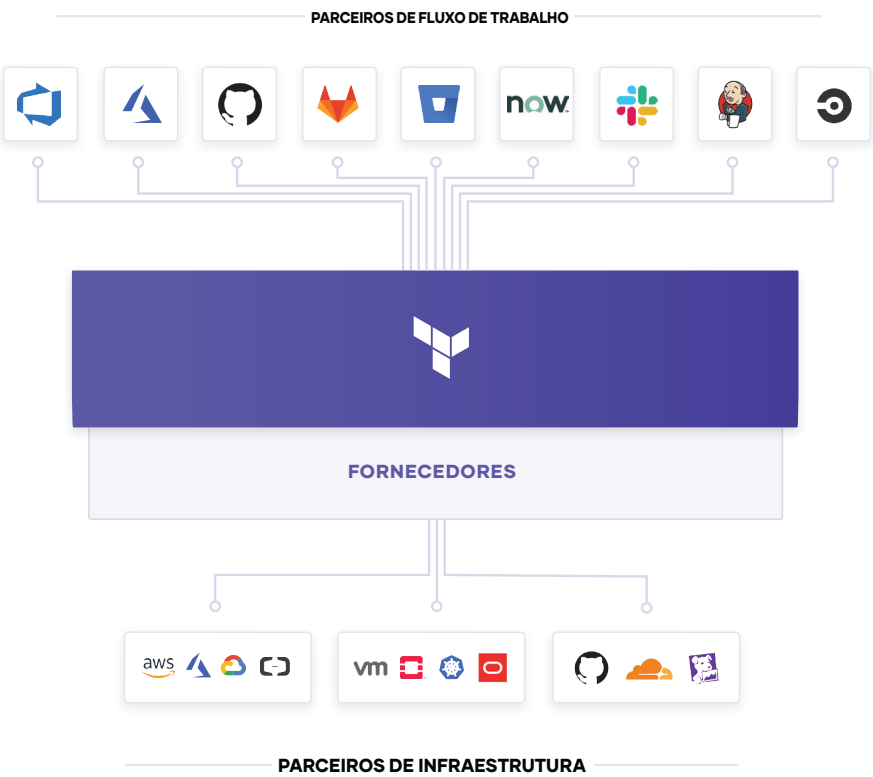
Para obter serviços compartilhados para provisionamento de infraestrutura, as equipes de TI devem começar implementando a infraestrutura reproduzível como práticas de código e, em seguida, dispor os fluxos de trabalho de conformidade e governança em camadas para garantir controles apropriados.



Infraestrutura reproduzível como código

O primeiro objetivo de um serviço compartilhado para provisionamento de infraestrutura é permitir a entrega de infraestrutura reproduzível como código, fornecendo às equipes de DevOps uma maneira de planejar e provisionar recursos dentro de fluxos de trabalho de CI/CD usando ferramentas conhecidas em todo o processo.

As equipes de DevOps podem criar modelos do Terraform que expressam a configuração de serviços de uma ou mais plataformas de nuvem. O Terraform se integra a todas as principais ferramentas de gerenciamento de configuração para permitir que o provisionamento refinado seja tratado após o provisionamento dos recursos subjacentes. Por fim, os modelos podem ser estendidos com serviços de muitos outros provedores de ISV para incluir agentes de monitoramento, sistemas de monitoramento de desempenho de aplicação (application performance monitoring, APM), ferramentas de segurança, DNS e redes de entrega de conteúdo e muito mais. Depois de definidos, os modelos podem ser provisionados conforme necessário de maneira automatizada. Ao fazer isso, o Terraform se torna a *língua franca* e o fluxo de trabalho em comum para equipes que provisionam recursos em nuvem pública e privada.



Para TI de autoatendimento, a dissociação do processo de criação de modelo e o processo de provisionamento reduzem muito o tempo necessário para que qualquer aplicação entre em operação, pois os desenvolvedores não precisam mais esperar pela aprovação das operações, desde que usem um modelo pré-aprovado.

Conformidade e gerenciamento

Para a maioria das equipes, também há a necessidade de impor políticas sobre o tipo de infraestrutura criada, como ela é usada e quais equipes podem usá-la. A estrutura da política como código Sentinel da HashiCorp fornece conformidade e governança sem exigir uma mudança no fluxo de trabalho geral da equipe, e também é definida como código, permitindo colaboração e compreensão para DevSecOps.

Sem a política como código, as organizações recorrem ao uso de um processo de análise baseado em tíquete para aprovar alterações. O resultado são desenvolvedores que precisam esperar semanas ou mais para provisionar a infraestrutura, o que se torna um gargalo. A política como código nos permite resolver isso por meio da divisão entre definição da política e execução da política.

Equipes centralizadas codificam políticas que impõem segurança, conformidade e melhores práticas operacionais em todo o provisionamento de nuvem. A aplicação automatizada de políticas garante que as alterações estejam em conformidade sem criar um gargalo de revisão manual.

Etapa 2: Segurança multinuvem

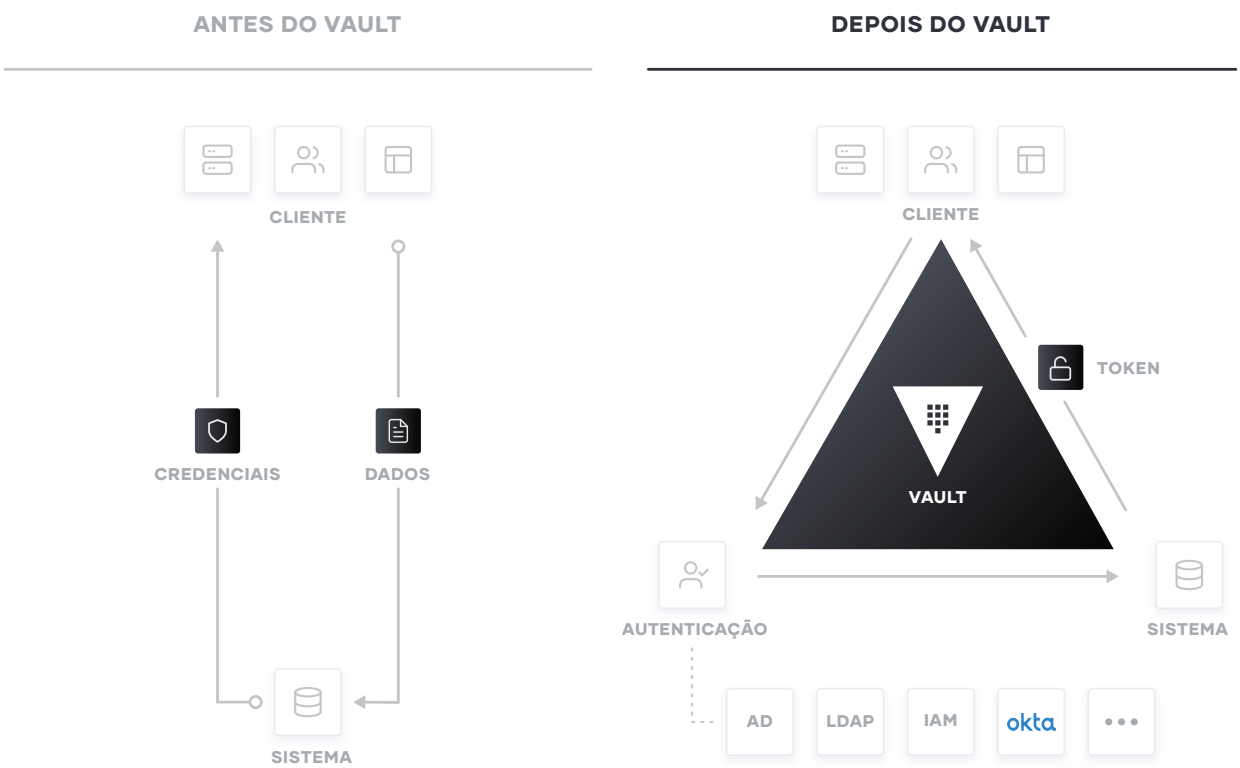
Infraestrutura de nuvem dinâmica significa uma mudança de identidade baseada em host para identidade baseada em aplicação, com redes de confiança baixa ou zero em várias nuvens sem um perímetro de rede claro.

No mundo da segurança tradicional, pressupomos redes internas de alta confiança, o que resultou em um exterior sólido e um interior frágil. Com a abordagem moderna de "confiança zero", trabalhamos para fortalecer também o interior. Isso exige que as aplicações sejam explicitamente autenticadas, autorizadas a buscar segredos e executar operações confidenciais e auditadas rigorosamente.

O HashiCorp Vault permite que as equipes armazenem e controlem com segurança o acesso a tokens, senhas, certificados e chaves de criptografia para proteger máquinas e aplicações. Isso fornece uma solução abrangente de gerenciamento de segredos. Além disso, o Vault ajuda a proteger os dados em repouso e os dados em trânsito. O Vault expõe uma API de alto nível para criptografia para desenvolvedores protegerem dados confidenciais sem expor chaves de criptografia. O Vault também pode atuar como uma autoridade de certificação, para fornecer certificados dinâmicos de curta duração para proteger as comunicações com SSL/TLS. Por fim, o Vault permite uma intermediação de identidade entre diferentes plataformas, como o Active Directory no local e o AWS IAM, para permitir que as aplicações trabalhem além dos limites da plataforma.

O Vault é amplamente usado, inclusive em bolsas de valores, grandes organizações financeiras, redes hoteleiras e tudo o mais para fornecer segurança no modelo operacional em nuvem.

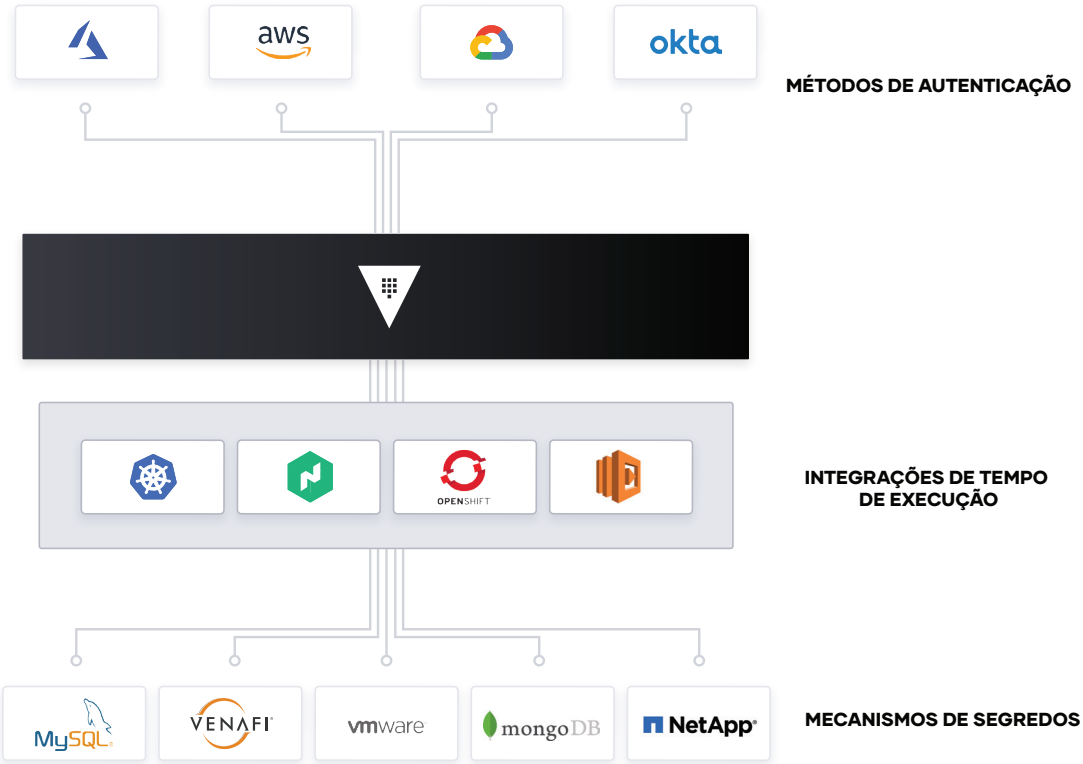
Para obter serviços compartilhados para segurança, as equipes de TI devem habilitar serviços de gerenciamento de segredos centralizados e, em seguida, usar esse serviço para fornecer casos de uso de criptografia como serviço mais sofisticados, como rotações de certificados e chaves, e criptografia de dados em trânsito e em repouso.



Gerenciamento de segredos

O primeiro passo na segurança de nuvem é normalmente o gerenciamento de segredos: o armazenamento central, o controle de acesso e a distribuição de segredos dinâmicos. Em vez de depender de endereços IP estáticos, é crucial a integração com sistemas de acesso baseados em identidade, como AWS IAM e Azure AAD, para autenticar e acessar serviços e recursos.

O Vault usa políticas para codificar como as aplicações autenticam, quais credenciais estão autorizadas a usar e como a auditoria deve ser realizada. Ele pode ser integrado a uma variedade de provedores de identidade confiáveis, como plataformas de identidade em nuvem e gerenciamento de acesso (IAM), Kubernetes, Active Directory e outros sistemas baseados em SAML para autenticação. O Vault gerencia centralmente e impõe o acesso a segredos e sistemas com base em fontes confiáveis de aplicações e identidade de usuários.



As equipes de TI empresarial devem criar um serviço compartilhado que permita a solicitação de segredos para qualquer sistema por meio de um fluxo de trabalho consistente, auditado e seguro.

Criptografia como serviço

Além disso, as empresas precisam criptografar dados de aplicações em repouso e em trânsito. O Vault pode fornecer criptografia como serviço para oferecer uma API consistente para gerenciamento de chaves e criptografia. Isso permite que os desenvolvedores executem uma única integração e protejam os dados em vários ambientes.

Usar o Vault como base para criptografia como serviço resolve problemas difíceis enfrentados por equipes de segurança, como certificado e rotação de chaves. O Vault permite o gerenciamento centralizado de chaves para simplificar a criptografia de dados em trânsito e em repouso em nuvens e datacenters. Esse gerenciamento ajuda a reduzir custos relacionados a módulos de segurança de hardware (Hardware Security Modules, HSM) caros e aumenta a produtividade com fluxos de trabalho de segurança e padrões criptográficos consistentes em toda a organização.

Embora muitas organizações atribuam aos desenvolvedores a criptografia de dados, muitas vezes elas não fornecem o "como", o que faz com que os desenvolvedores criem soluções personalizadas sem uma compreensão adequada da criptografia. O Vault proporciona aos desenvolvedores uma API simples que pode ser facilmente usada e, ao mesmo tempo, oferece às equipes de segurança centralizadas os controles de política e as APIs de gerenciamento de ciclo de vida de que precisam.

Proteção avançada de dados

As organizações que migram para a nuvem ou abrangem ambientes híbridos ainda mantêm e oferecem suporte a serviços e aplicações no local que precisam executar operações criptográficas, como criptografia de dados para armazenamento em repouso. Esses serviços não necessariamente querem implementar a lógica em torno do gerenciamento dessas chaves criptográficas e, portanto, buscam delegar a tarefa de gerenciamento de chaves a provedores externos. A Proteção avançada de dados permite que as organizações conectem, controlem e integrem com segurança chaves de criptografia avançadas, operações e gerenciamento entre a infraestrutura e o Vault Enterprise, incluindo a proteção automática de dados no MySQL, MongoDB, PostgreSQL e outros bancos de dados usando transparent data encryption (TDE).

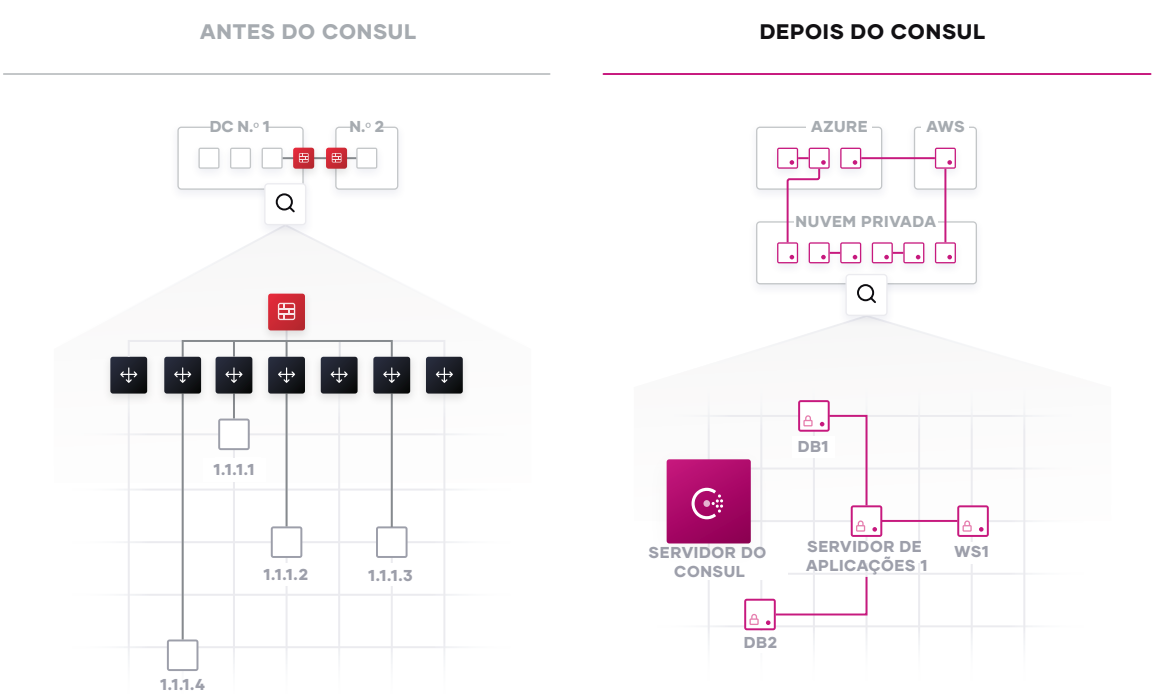
Para organizações que têm requisitos de alta segurança para conformidade de dados (PCI=SS, HIPAA etc.), proteção de dados e anonimato protegido por criptografia para informações pessoalmente identificáveis (personally identifiable information, PII), a Proteção avançada de dados fornece às organizações funcionalidade para tokenização de dados, como o mascaramento, para proteger dados confidenciais, como cartões de crédito, informações pessoais confidenciais, dados bancários etc.

Etapa 3: Rede de serviços multinuvem

Os desafios da implantação de rede na nuvem são muitas vezes um dos aspectos mais difíceis para as empresas na adoção do modelo operacional em nuvem. A combinação de endereços IP dinâmicos, um crescimento significativo no tráfego leste-oeste à medida que o padrão de microsserviços é adotado e a falta de um perímetro de rede claro são um desafio formidável.

A HashiCorp Consul fornece uma camada de rede de serviço multinuvem para conectar e proteger serviços. O Consul é um produto amplamente implantado, com muitos clientes executando significativamente mais de 100.000 nós em seus ambientes.

Os serviços de rede devem ser fornecidos centralmente, em que as equipes de TI fornecem recursos de registro de serviço e descoberta de serviço. Ter um registro em comum fornece um "mapa" de quais serviços estão sendo executados, onde estão e o status de integridade atual. O registro pode ser consultado de maneira programática para permitir a descoberta de serviços ou impulsionar a automação de rede de gateways de API, balanceadores de carga, firewalls e outros componentes críticos de middleware. Esses componentes de middleware podem ser movidos para fora da rede usando uma abordagem de malha de serviço, onde proxies são executados na borda para fornecer funcionalidade equivalente. As abordagens de malha de serviço permitem que a topologia de rede seja simplificada, especialmente para topologias multinuvem e multidatacenter.



Descoberta de serviço

O ponto de partida para a implantação de rede no modelo operacional em nuvem normalmente é um registro de serviço comum, que fornece um diretório em tempo real de quais serviços estão sendo executados, onde eles estão e seu status de integridade atual. As abordagens tradicionais para redes dependem de balanceadores de carga e IPs virtuais para fornecer uma abstração de nomenclatura para representar um serviço com um IP estático. O processo para rastrear a localização da rede de serviços muitas vezes assume a forma de planilhas, painéis de balanceador de carga ou arquivos de configuração, todos processos manuais desarticulados que não são ideais.

Para o Consul, cada serviço é registrado programaticamente e interfaces DNS e API são fornecidas para permitir que qualquer serviço seja descoberto por outros serviços. A verificação de integridade integrada monitorará o status de integridade de cada instância de serviço para que a equipe de TI possa fazer a triagem da disponibilidade de cada instância e o Consul consiga ajudar a evitar o roteamento de tráfego para instâncias de serviço não íntegras.

O Consul pode ser integrado a outros serviços que gerenciam o tráfego norte-sul existente, como balanceadores de carga tradicionais e plataformas de aplicações distribuídas, como Kubernetes, para fornecer um serviço consistente de registro e descoberta em ambientes de multidatacenter, nuvem e plataforma.

Automação de middleware de rede

O próximo passo é reduzir a complexidade operacional com middleware de rede existente por meio da automação de rede. Em vez de um processo manual baseado em tíquetes para reconfigurar balanceadores de carga e firewalls sempre que houver uma mudança nos locais ou configurações da rede de serviço, o Consul pode automatizar essas operações de rede. Isso é conseguido permitindo que os dispositivos de middleware de rede assinem alterações de serviço do registro de serviço, permitindo uma infraestrutura altamente dinâmica que pode ser dimensionada significativamente mais alta do que as abordagens estáticas.

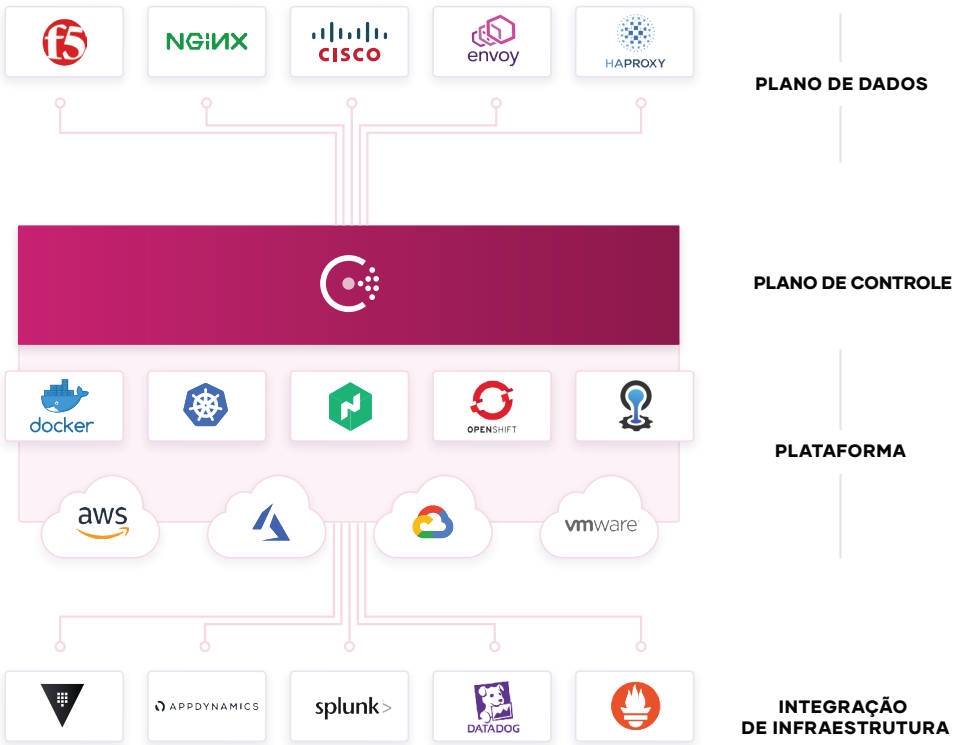
Isso desvincula o fluxo de trabalho entre equipes, pois os operadores podem implantar aplicações de maneira independente e publicar no Consul, enquanto as equipes de NetOps podem assinar o Consul para lidar com a automação downstream.

Rede de confiança zero com malha de serviço

À medida que as organizações continuam a escalar com aplicações baseadas em microsserviços ou nativos da nuvem, a infraestrutura subjacente se torna maior e mais dinâmica com uma explosão de tráfego leste-oeste. Isso causa uma proliferação de middleware de rede caro com pontos únicos de falha e despesas gerais significativa expostas às equipes de TI.

O Consul fornece uma malha de serviços distribuídos que envia roteamento, autorização e outras funcionalidades de rede para os endpoints na rede, em vez de imposição por meio de middleware. Isso torna a topologia de rede mais simples e fácil de gerenciar, elimina a necessidade de middleware caro dentro dos caminhos de tráfego leste-oeste e torna a comunicação entre serviços muito mais confiável e escalável.

O Consul é um plano de controle acionado por API que se integra a proxies sidecar ao lado de cada instância de serviço (proxies como Envoy, HAProxy e NGINX). Esses proxies fornecem o plano de dados distribuído. Juntos, esses dois planos permitem um modelo de rede de confiança zero que protege a comunicação entre serviços com criptografia TLS automática e autorização baseada em identidade. As equipes de operação e segurança de rede podem definir as políticas de segurança por meio de intenções com serviços lógicos em vez de endereços IP.

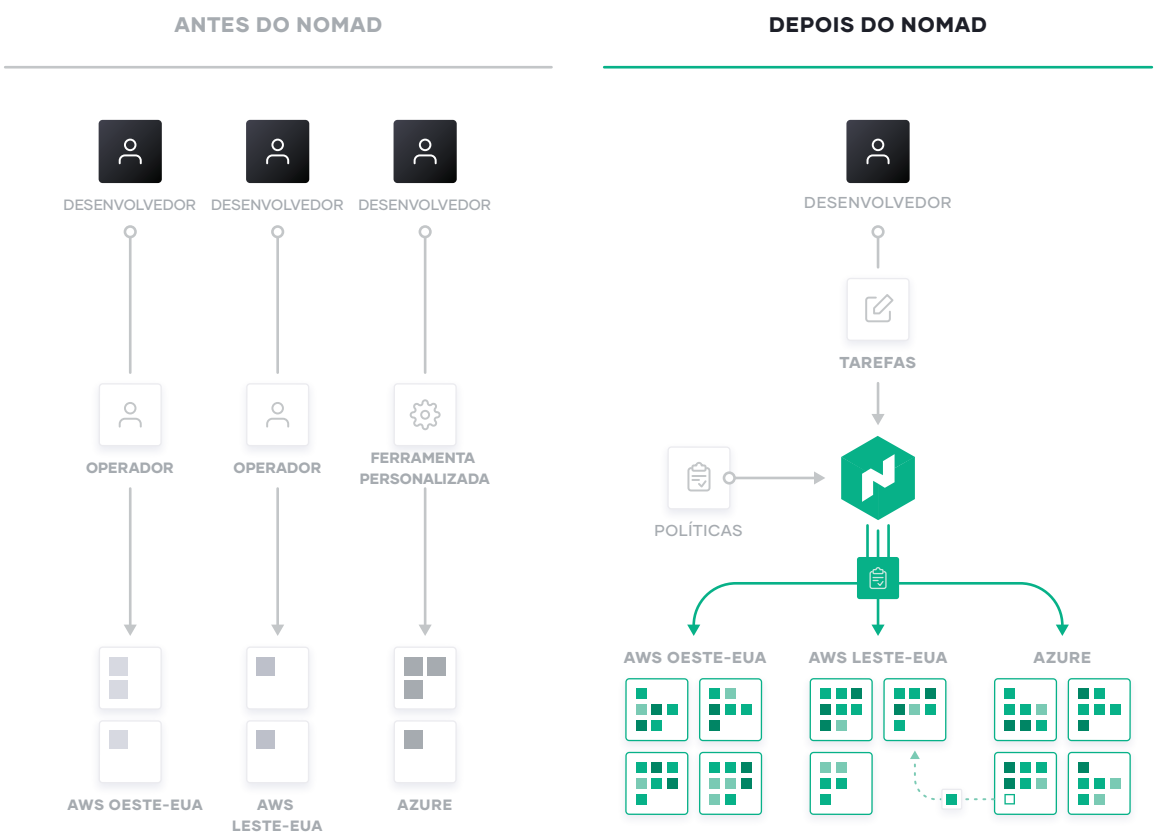


O Consul permite a segmentação de serviços refinados para proteger a comunicação entre serviços com criptografia TLS automática e autorização baseada em identidade. O Consul pode ser integrado ao Vault para gerenciamento centralizado de PKI e certificados. A configuração de serviço é obtida por meio de armazenamento de chave/valor acionado por API que pode ser usado para configurar facilmente serviços em tempo de execução em qualquer ambiente.

Etapa 4: Entrega de aplicações multinuvem

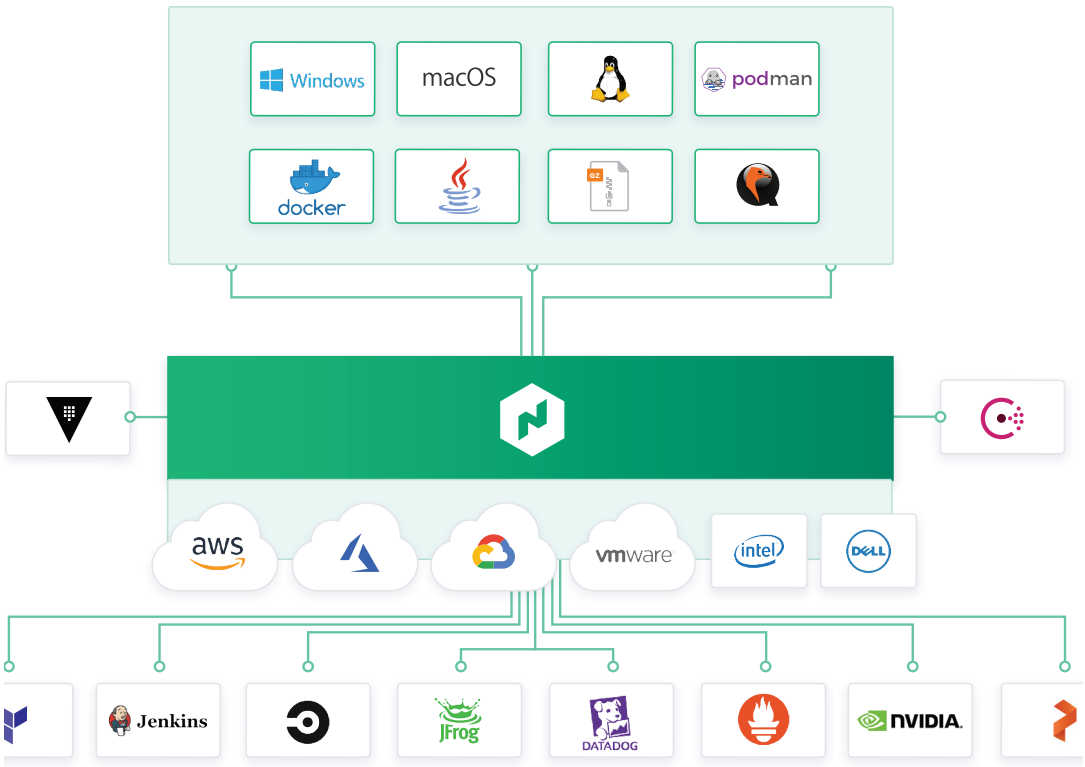
Finalmente, na camada de aplicações, novas aplicações são cada vez mais distribuídas, enquanto aplicações herdadas também precisam ser gerenciadas de maneira mais flexível. O HashiCorp Nomad fornece um orquestrador flexível para implantar e gerenciar aplicações herdadas e modernas, para todos os tipos de cargas de trabalho: de serviços de longa duração a lotes de curta duração e agentes de sistema.

Para obter serviços compartilhados para a entrega de aplicações, as equipes de TI devem usar o Nomad em conjunto com o Terraform, Vault e Consul para permitir a entrega consistente de aplicações em infraestrutura de nuvem, incorporando os requisitos necessários de conformidade, segurança e rede, bem como a orquestração e o agendamento da carga de trabalho.



Orquestração de carga de trabalho mista

Muitas novas cargas de trabalho são desenvolvidas com empacotamento de contêineres com a intenção de implantar no Kubernetes ou em outras plataformas de gerenciamento de contêineres. Mas muitas cargas de trabalho herdadas não serão transferidas para essas plataformas, nem as futuras aplicações sem servidor. O Nomad fornece um processo consistente para a implantação de todas as cargas de trabalho de máquinas virtuais, por meio de binários e contêineres independentes, e oferece benefícios de orquestração essenciais em todas essas cargas de trabalho, como automação de lançamento, várias estratégias de atualização, empacotamento e resiliência.



Para aplicações modernas, normalmente contêineres integrados, o Nomad fornece o mesmo fluxo de trabalho consistente em escala em qualquer ambiente. O foco do Nomad é a simplicidade e a eficácia na orquestração e programação, e ele evita a complexidade de plataformas como Kubernetes, que exigem habilidades de operação especializadas e resolvem apenas cargas de trabalho em contêineres.

O Nomad integra-se aos fluxos de trabalho de CI/CD existentes para fornecer implantações de aplicações rápidas e automáticas para cargas de trabalho herdadas e modernas.

Computação de alto desempenho

O Nomad foi projetado para programar aplicações com baixa latência em clusters muito grandes. Isso é fundamental para clientes com grandes trabalhos em lote, como é comum com cargas de trabalho de computação de alto desempenho (High Performance Computing, HPC). No desafio de um milhão de contêineres, o Nomad conseguiu programar um milhão de instâncias do Redis em 5.000 máquinas em três data centers, em menos de 5 minutos. Várias implantações grandes do Nomad são executadas em escalas ainda maiores.

O Nomad permite que aplicações de alto desempenho usem facilmente uma API para consumir capacidade dinamicamente, permitindo o compartilhamento eficiente de recursos para aplicações de análise de dados, como o Spark. O agendamento de baixa latência garante que os resultados estejam disponíveis em tempo hábil e minimiza o desperdício de recursos ociosos.

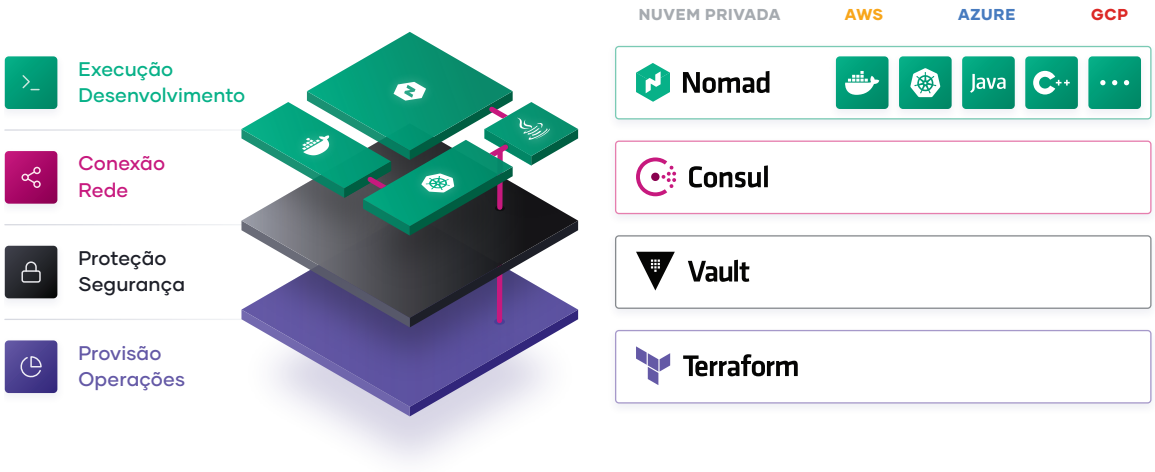
Orquestração de vários data centers

O Nomad é multirregião e multinuvem por design, com um fluxo de trabalho consistente para implantar qualquer carga de trabalho. À medida que as equipes implantam aplicações globais em vários data centers ou através dos limites da nuvem, o Nomad oferece orquestração e programação para essas aplicações, com suporte de recursos e políticas de infraestrutura, segurança e rede para garantir que as aplicações sejam implantadas com sucesso.

Etapa 5: Processo de entrega de aplicação industrializada

Em última análise, esses serviços compartilhados em infraestrutura, segurança, rede e tempo de execução de aplicações apresentam um processo industrializado para a entrega de aplicações, tudo isso aproveitando a natureza dinâmica de cada camada da nuvem.

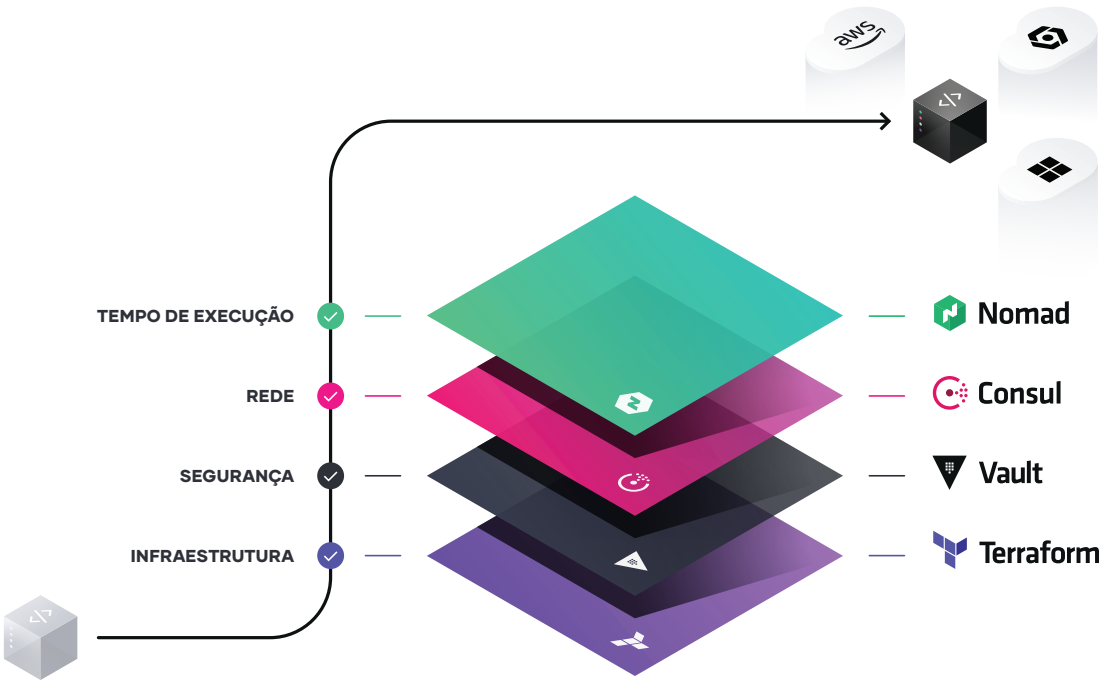
Adotar o modelo operacional em nuvem permite a TI de autoatendimento, que é totalmente compatível e governada, para que as equipes entreguem aplicações em velocidade crescente.



Conclusão

Um modelo operacional de nuvem comum é uma mudança inevitável para as empresas com o objetivo de maximizar seus esforços de transformação digital. O conjunto de ferramentas da HashiCorp busca fornecer soluções para cada camada da nuvem para permitir que as empresas façam essa mudança para o modelo operacional da nuvem.

A TI corporativa precisa evoluir de pontos de controle baseados em ITIL com seu foco na otimização de custos, para se tornar facilitadora de autoatendimento focada na otimização de velocidade. Isso pode ser feito por meio do fornecimento de serviços compartilhados em cada camada da nuvem projetada para ajudar as equipes a fornecer novos negócios e valor para o cliente rapidamente.



Desbloquear o caminho mais rápido para o valor em um data center multinuvem moderno através da adoção de um modelo operacional em nuvem comum significa mudar as características da TI corporativa:

- **Pessoas: Mudança para habilidades multinuvem**
    - Reutilize as habilidades de gerenciamento de data centers internos e fornecedores de nuvem única e aplique-as consistentemente em qualquer ambiente.
    - Adote o DevSecOps e outras práticas ágeis para fornecer continuamente sistemas cada vez mais efêmeros e distribuídos.

- **Processo: Mudança para TI de autoatendimento**
    - Posicione a TI central como um serviço compartilhado de habilitação focado na velocidade de entrega de aplicações: software de remessa cada vez mais rapidamente com risco mínimo.
    - Estabeleça centros de excelência em cada camada da nuvem para a entrega de recursos de autoatendimento.
- **Ferramentas: Mudança para ambientes dinâmicos**
    - Use ferramentas que suportem a crescente transitoriedade e distribuição de infraestrutura e aplicações e que suportem os fluxos de trabalho críticos em vez de estarem vinculados a tecnologias específicas.
    - Forneça ferramentas de política e governança para combinar a velocidade de entrega com a conformidade para gerenciar o risco em um ambiente de autoatendimento.

Sobre a HashiCorp

A HashiCorp é líder em software de automação de infraestrutura multinuvem. O pacote de software da HashiCorp permite que as organizações adotem fluxos de trabalho consistentes para provisionar, proteger, conectar e executar qualquer infraestrutura para qualquer aplicação. As ferramentas de código aberto da HashiCorp, Vagrant, Packer, Terraform, Vault, Consul e Nomad são baixadas dezenas de milhões de vezes por ano e são amplamente adotadas pelas empresas da Global 2000. As versões empresariais desses produtos aprimoram as ferramentas de código aberto com recursos que promovem colaboração, operações, governança e funcionalidade de vários data centers. A empresa tem sede em São Francisco e é apoiada por Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP e Bessemer Venture Partners. Para obter mais informações, acesse www.hashicorp.com ou siga a HashiCorp no Twitter @HashiCorp.


HashiCorp