HashiCorp

Revelando el modelo operativo en la nube

Encontrar el camino más rápido al valor
en un centro de datos moderno y multinube

ARTÍCULO TÉCNICO

Contenido

Resumen ejecutivo

Ahora es el momento en que la nube debe funcionar. Para progresar en una era de arquitectura multinube, impulsada por la transformación digital, la TI empresarial debe evolucionar y pasar del control de acceso basado en ITIL a facilitar procesos de autoservicio compartidos para la excelencia de DevOps.

Para la mayoría de las empresas, los objetivos de las iniciativas de transformación digital significan generar nuevo valor tanto para la empresa como para el cliente de una forma más rápida y a gran escala. La implicación para la TI empresarial es entonces el cambio de la optimización de costos a la optimización de velocidad. La nube es una parte inevitable de este cambio, ya que presenta la oportunidad de implementar rápidamente servicios bajo demanda a una escala ilimitada.

Para encontrar el camino más rápido hacia el valor de la nube, las empresas deben pensar en cómo industrializar el proceso de entrega de aplicaciones en cada capa de la nube: adoptando el modelo operativo en la nube y poniendo en sintonía a las personas, los procesos y las herramientas con él.

En este artículo técnico, analizamos las implicaciones del modelo operativo en la nube y presentamos soluciones para que los equipos de TI adopten este modelo en toda la capa de aprovisionamiento de infraestructura.

Transición a un centro de datos multinube

La transición a entornos de nube y multinube es una transición generacional para la TI. Esta transición significa cambiar de servidores mayormente dedicados en un centro de datos privado a un conjunto de capacidades informáticas disponibles bajo demanda. Aunque la mayoría de las empresas comenzaron con un solo proveedor de nube, hay buenos motivos para usar los servicios de otros proveedores e, inevitablemente, la mayoría de las organizaciones en la lista Global 2000 usará más de uno, ya sea intencionadamente o mediante fusiones y adquisiciones.

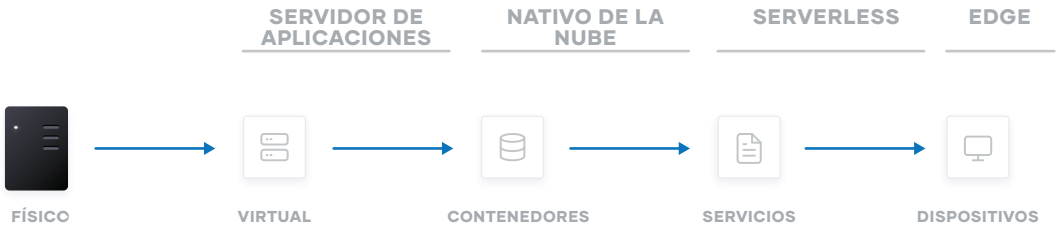
La nube presenta una oportunidad para la optimización de velocidad y escala para nuevos "sistemas de interacción": aplicaciones creadas para atraer clientes y usuarios. Estas nuevas aplicaciones son la interfaz principal para que el cliente interactúe con una empresa y son ideales para la entrega en la nube ya que tienden a:

- tener características de uso dinámico, cuando se necesita escalar las cargas hacia arriba y hacia abajo por orden de magnitud durante períodos de tiempo cortos.
- estar bajo presión para crear e iterar rápidamente. Muchos de estos nuevos sistemas pueden ser de naturaleza efímera y ofrecen una experiencia de usuario específica en torno a un evento o campaña.

Sin embargo, para la mayoría de las empresas, estos sistemas de interacción deben conectarse a los "sistemas de registro" existentes —las bases de datos comerciales y aplicaciones internas principales— que a menudo continúan residiendo en la infraestructura de los centros de datos existentes. Como resultado, las empresas terminan con un híbrido, una combinación de múltiples entornos de nube pública y privada.

Entonces, el desafío para la mayoría de las empresas es cómo entregar estas aplicaciones a la nube con coherencia y al mismo tiempo garantizar la menor fricción posible entre los diversos equipos de desarrollo.

A este desafío se suma que los aspectos básicos subyacentes han pasado de manipular máquinas virtuales en un entorno autónomo a manipular "recursos" en la nube en un entorno compartido. Entonces, las empresas tienen modelos operativos contrapuestos para mantener su patrimonio existente, mientras desarrollan la nueva infraestructura en la nube.



Para que la informática en la nube funcione, es necesario que haya flujos de trabajo coherentes que se puedan reutilizar a escala en múltiples proveedores de nube. Esto requiere:

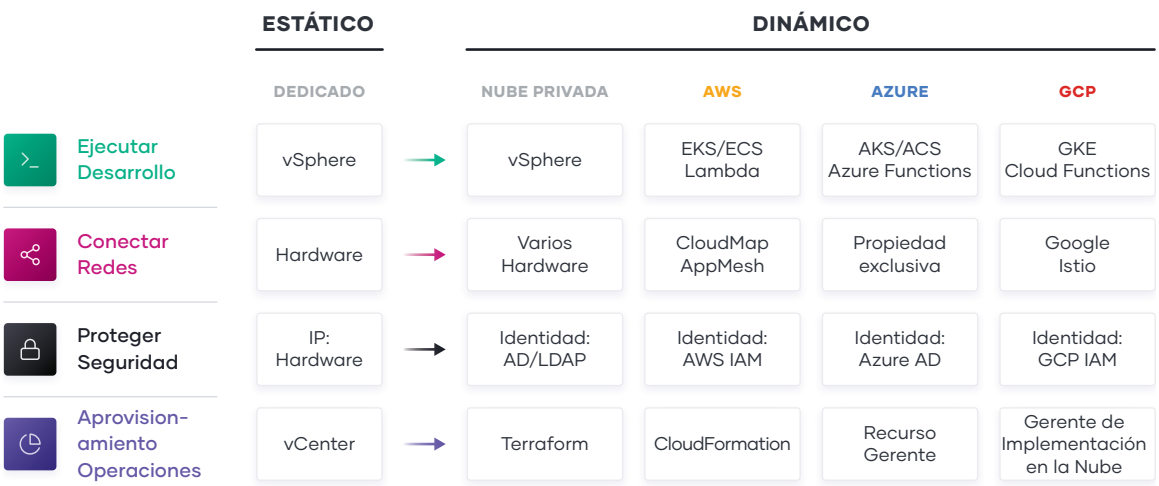
- Conjuntos de instrucciones coherentes para el aprovisionamiento
- Identidad para la seguridad y para las conexiones de red
- Privilegios y derechos para que puedan implementarse y ejecutarse

Implicaciones del modelo operativo en la nube

Las principales implicaciones de la transición a la nube yacen en el cambio de la infraestructura "estática" a la infraestructura "dinámica": de un enfoque en la configuración y la gestión de una flota estática de recursos de TI, a aprovisionar, proteger, conectar y ejecutar recursos dinámicos bajo demanda.

Cuando se desglosan estas implicaciones y se elabora la pila, se observan varios cambios de enfoque:

- **Aprovisionamiento.** La capa de infraestructura pasa de ejecutar servidores dedicados con escala limitada a un entorno dinámico donde las organizaciones pueden adaptarse fácilmente a una mayor demanda al poner en funcionamiento miles de servidores y reducirlos cuando no están en uso. A medida que las arquitecturas y los servicios están más distribuidos, el volumen total de los nodos de ejecución aumenta significativamente.
- **Proteger.** La capa de seguridad pasa de un entorno fundamentalmente de "alta confianza" que depende de un perímetro y firewall potentes a un entorno de "nivel de confianza bajo" o de "cero confianza" que no tiene un perímetro claro o estático. Como resultado, la premisa básica para la seguridad pasa de estar basada en IP a usar un acceso a recursos basado en la identidad. Este cambio es altamente disruptivo para los modelos de seguridad tradicionales.
- **Conectar.** La capa de red pasa de depender en gran medida de la ubicación física y la dirección IP de los servicios y las aplicaciones a utilizar un registro dinámico de servicios para la detección, segmentación y composición. El equipo de TI empresarial no tiene el mismo control sobre la red, o las ubicaciones físicas de los recursos informáticos, y debe pensar en la conectividad basada en servicios.
- **Ejecutar.** La capa de tiempo de ejecución pasa de implementar artefactos en un servidor de aplicaciones estático a implementar aplicaciones con un planificador en un conjunto de infraestructura que se aprovisiona bajo demanda. Además, las nuevas aplicaciones se han convertido en conjuntos de servicios que se aprovisionan dinámicamente y se empaquetan de múltiples maneras: desde en máquinas virtuales hasta en contenedores.



Para abordar estos desafíos, los equipos deben hacerse las siguientes preguntas:

- **Personas.** ¿Cómo podemos capacitar a un equipo para una realidad multinube, donde las habilidades se pueden aplicar de manera coherente independientemente del entorno objetivo?
- **Proceso.** ¿Cómo posicionamos los servicios centrales de TI como facilitadores de autoservicio para lograr velocidad, en oposición a un controlador de acceso basado en tickets, al mismo tiempo que mantenemos el cumplimiento y la gobernanza?
- **Herramientas.** ¿Cómo aprovechamos mejor el valor de las capacidades disponibles de los proveedores de nube con el fin de obtener mayor valor empresarial y para el cliente?

Revelando el modelo operativo en la nube

Dado que las implicaciones del modelo operativo en la nube impactan en los equipos de infraestructura, seguridad, redes y aplicaciones, vemos un patrón que se repite en las empresas que consta en establecer servicios centrales compartidos (centros de excelencia) para brindar la infraestructura dinámica necesaria en cada capa para una entrega exitosa de aplicaciones.

A medida que los equipos usan cada servicio compartido en el modelo operativo en la nube, la velocidad de la TI aumenta. Mientras más madura sea la nube de una organización, más veloz será.

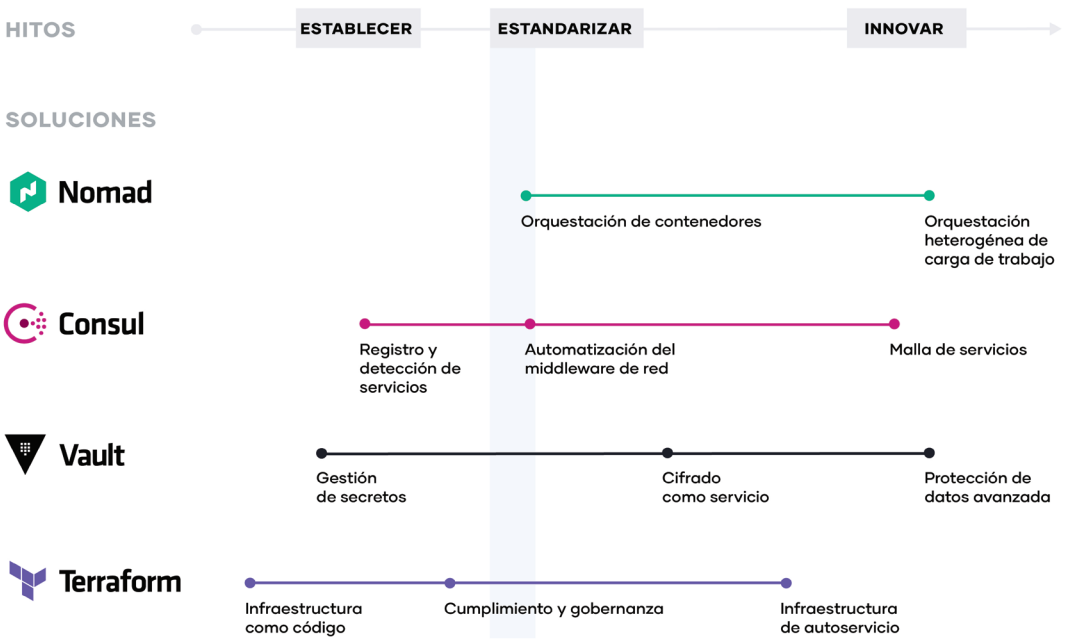
El recorrido típico que hemos visto adoptar a los clientes cuando comienzan a aprovechar el modelo operativo en la nube, tiene tres hitos principales:

1. **Establecer los aspectos fundamentales de la nube**: a medida que comienza su recorrido hacia la nube, los requisitos inmediatos son aprovisionar la infraestructura de la nube, generalmente, adoptando el marco de infraestructura como código y asegurarse de que esté protegida con una solución de gestión de secretos. Estos son los aspectos indispensables que le permitirán crear una arquitectura de nube escalable y verdaderamente dinámica que esté preparada para el futuro.

2. **Estandarizar un conjunto de servicios compartidos**: a medida que el consumo de la nube comience a aumentar, deberá implementar y estandarizar un conjunto de servicios compartidos para aprovechar al máximo lo que la nube tiene para ofrecer. Esto también presenta desafíos en torno a la gobernanza y el cumplimiento a medida que la necesidad de establecer reglas de control de acceso y requisitos de seguimiento se vuelve cada vez más importante.

3. **Innovar utilizando una arquitectura lógica común**: a medida que adopte completamente la nube y emplee los servicios y aplicaciones de la nube como los principales sistemas de interacción, surgirá la necesidad de crear una arquitectura lógica común. Esto requiere un plano de control que se conecte con el ecosistema extendido de soluciones de nube y proporcione de manera inherente seguridad avanzada y orquestación de todos los servicios y múltiples nubes.

EJEMPLO DE RECORRIDO EMPRESARIAL PARA EXPLOTAR UN MODELO OPERATIVO EN LA NUBE

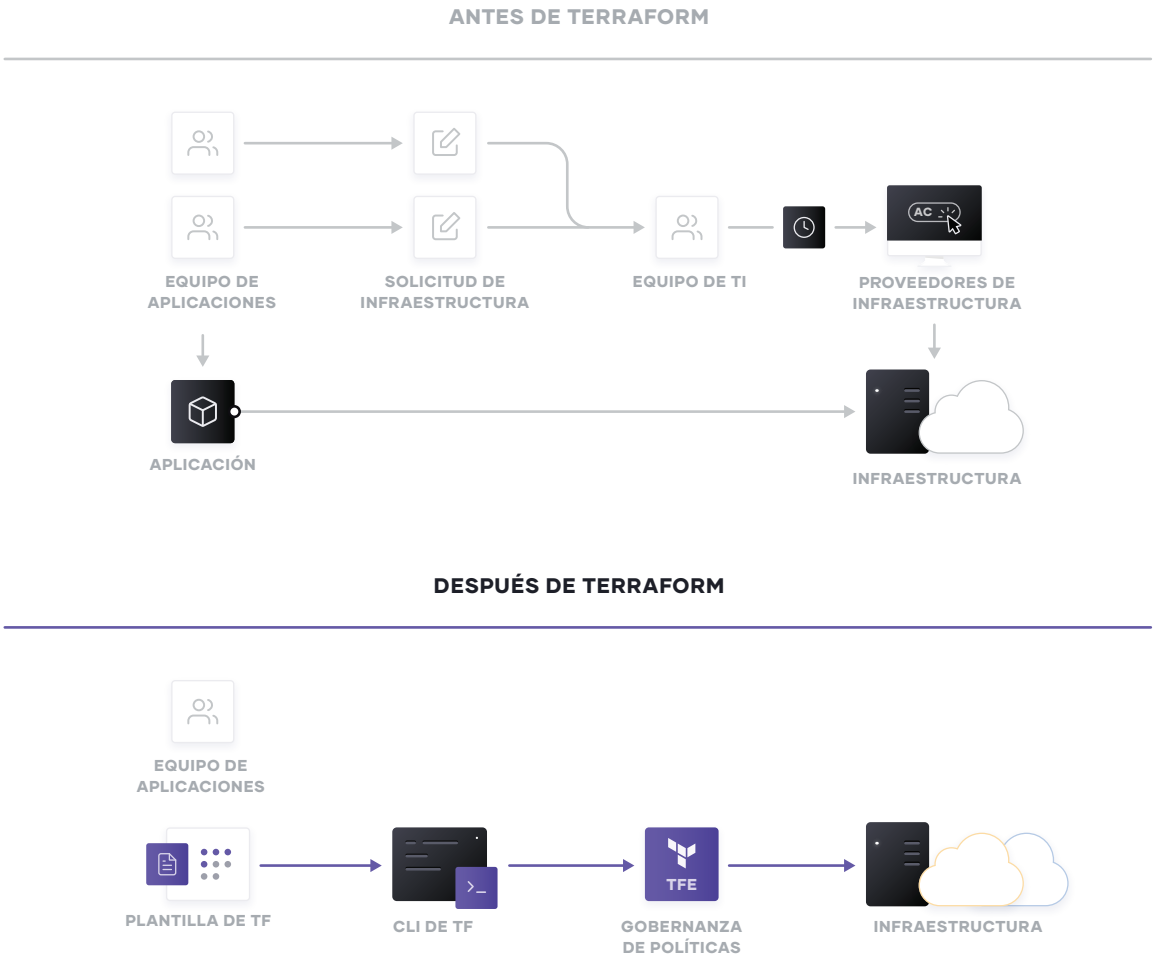


A continuación, se encuentra el recorrido paso a paso que hemos visto que las organizaciones realizan con éxito.

Paso 1: Aprovisionamiento de infraestructura multinube

La base para adoptar la nube es el aprovisionamiento de infraestructura. HashiCorp Terraform es el producto de aprovisionamiento para la nube más utilizado del mundo y se puede emplear para aprovisionar infraestructura para cualquier aplicación utilizando una variedad de proveedores para cualquier plataforma objetivo.

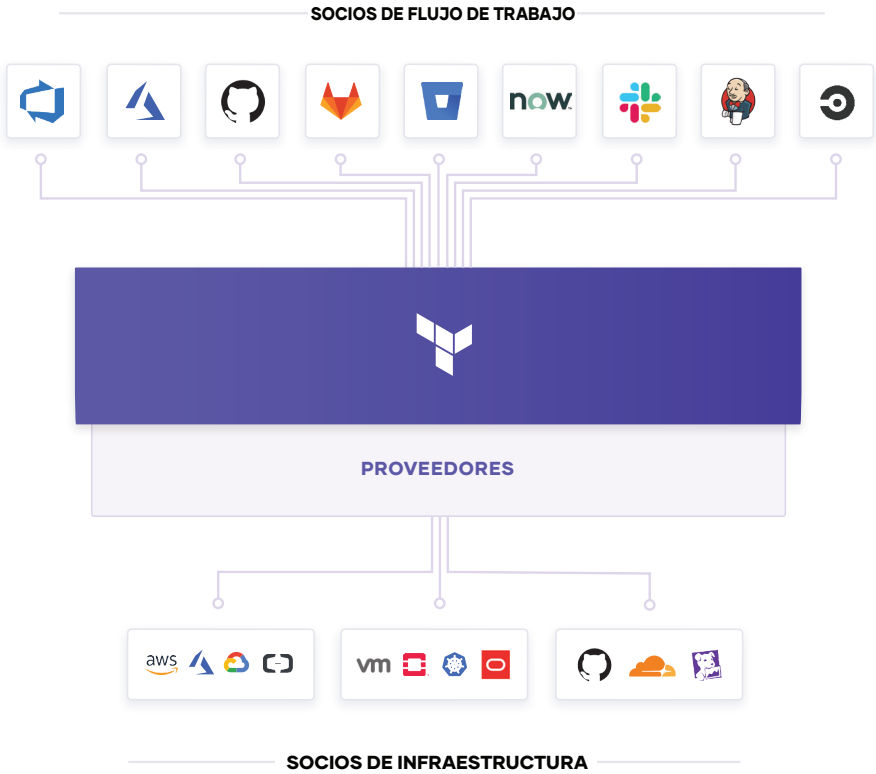
Para crear servicios compartidos para el aprovisionamiento de infraestructura, los equipos de TI deben comenzar por implementar prácticas de infraestructura como código reproducible y luego disponer en capas los flujos de trabajo de cumplimiento y gobernanza para garantizar los controles adecuados.



Infraestructura como código reproducible

El primer objetivo de un servicio compartido para el aprovisionamiento de infraestructura es permitir la entrega de infraestructura como código reproducible, lo cual proporciona a los equipos de DevOps una manera de planificar y aprovisionar recursos dentro de los flujos de trabajo de CI/CD utilizando herramientas conocidas en todo el proceso.

Los equipos de DevOps pueden crear plantillas de Terraform que expresen la configuración de los servicios de una o más plataformas en la nube. Terraform se integra con todas las principales herramientas de gestión de configuración para permitir que se realice un aprovisionamiento detallado después del aprovisionamiento de los recursos subyacentes. Finalmente, las plantillas se pueden ampliar con servicios de muchos otros proveedores de ISV para incluir agentes de monitoreo, sistemas de monitoreo de rendimiento de aplicaciones (application performance monitoring, APM), herramientas de seguridad, DNS y redes de distribución de contenidos, y más. Una vez definidas, las plantillas se pueden aprovisionar según sea necesario de manera automática. Cuando se hace esto, Terraform se convierte en la *lengua franca* y en el flujo de trabajo común para los equipos que aprovisionan recursos en la nube pública y privada.



Para la TI de autoservicio, el desacoplamiento del proceso de creación de plantillas y del proceso de aprovisionamiento reduce en gran medida el tiempo que tarda cualquier aplicación en lanzarse, porque los desarrolladores ya no necesitan esperar la aprobación de Operaciones, siempre y cuando utilicen una plantilla preaprobada.

Cumplimiento y gestión

Para la mayoría de los equipos, también existe la necesidad de aplicar políticas sobre el tipo de infraestructura creada, sobre la forma en que se utiliza y sobre los equipos que pueden usarla. El marco de política como código de Sentinel de HashiCorp proporciona cumplimiento y gobernanza sin requerir un cambio en el flujo de trabajo general del equipo, y también está definido como código, lo que permite la colaboración y la comprensión por parte de DevSecOps.

Sin el marco de políticas como código, las organizaciones recurren al uso de un proceso de revisión basado en tickets para aprobar los cambios. Esto hace que los desarrolladores esperen semanas o más para aprovisionar la infraestructura y se produzca un cuello de botella. El marco de política como código nos permite resolver esto al separar la definición de la política de la ejecución de la política.

Los equipos centralizados codifican políticas que aplican seguridad, cumplimiento y mejores prácticas operativas en todo el aprovisionamiento en la nube. La aplicación automatizada de políticas garantiza que los cambios mantengan el cumplimiento sin crear un cuello de botella para la revisión manual.

Paso 2: Seguridad multinube

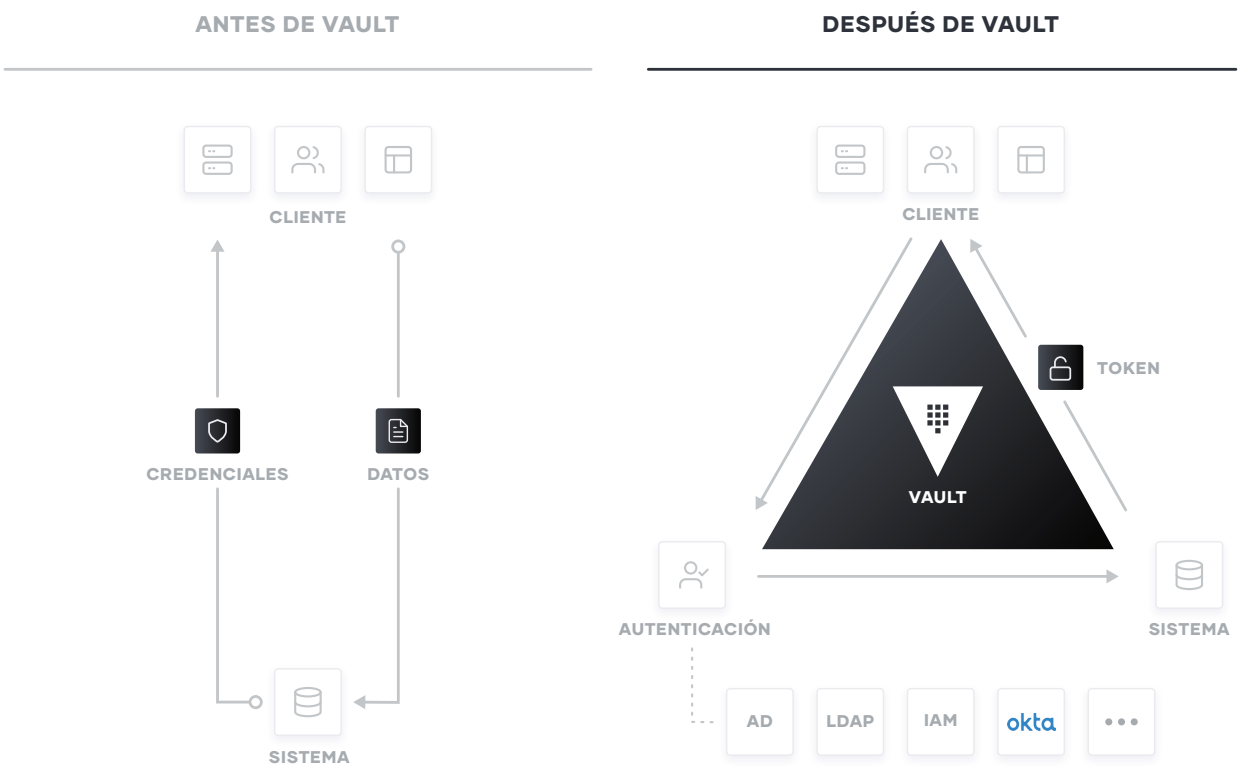
Infraestructura dinámica en la nube significa un cambio de identidad basada en host a identidad basada en aplicación, con redes de confianza baja o cero en múltiples nubes sin un perímetro de red claro.

En el entorno de la seguridad tradicional, adoptamos redes internas de alto nivel de confianza, lo que resultó en una capa exterior rígida y en un interior blando. Con el enfoque moderno de "confianza cero", trabajamos para fortalecer el interior también. Esto requiere que las aplicaciones se autentiquen explícitamente, se autoricen para obtener secretos y realizar operaciones delicadas, y se auditen de forma estricta.

HashiCorp Vault permite a los equipos almacenar de forma segura y controlar estrictamente el acceso a tokens, contraseñas, certificados y claves de cifrado para proteger máquinas y aplicaciones. Esto proporciona una solución integral de gestión de secretos. Además, Vault ayuda a proteger los datos en reposo y los datos en tránsito. Vault ofrece una API de alto nivel de criptografía para que los desarrolladores protejan los datos confidenciales sin exponer claves de cifrado. Vault también puede actuar como una entidad de certificación, para proporcionar certificados dinámicos de corta duración para proteger las comunicaciones con SSL/TLS. Por último, Vault ofrece servicios de administración de identidades entre diferentes plataformas, como Active Directory local y AWS IAM, para permitir que las aplicaciones funcionen independientemente de los límites de las plataformas.

Vault se utiliza ampliamente en sectores que van desde bolsas de valores y grandes organizaciones financieras hasta cadenas hoteleras y muchos otros para proporcionar seguridad en el modelo operativo en la nube.

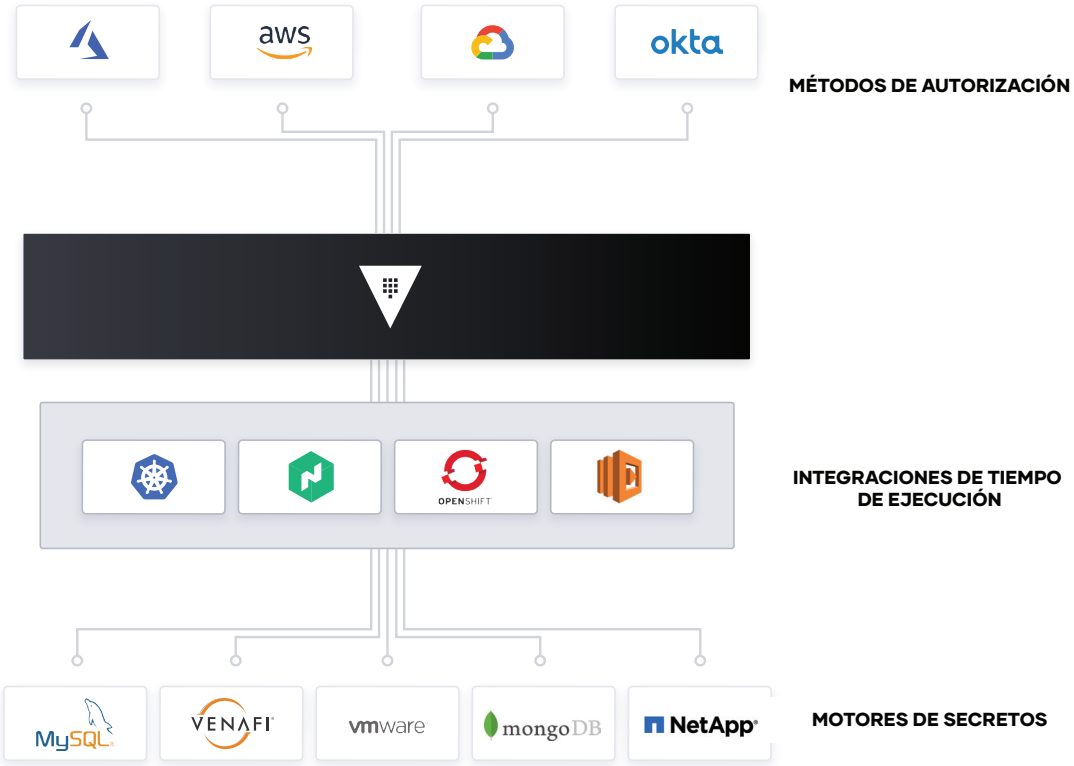
Para lograr servicios compartidos de seguridad, los equipos de TI deben contar con servicios de gestión de secretos centralizados y luego usar esos servicios para ofrecer casos de uso de cifrado como servicio más sofisticados, como certificados y rotaciones de claves, y cifrado de datos en tránsito y en reposo.



Gestión de secretos

El primer paso para la seguridad en la nube es generalmente la gestión de secretos: el almacenamiento central, el control de acceso y la distribución de secretos dinámicos. En lugar de depender de direcciones IP estáticas, es fundamental integrarse con sistemas de acceso basado en la identidad como AWS IAM y Azure AAD para la autenticación y el acceso a servicios y recursos.

Vault utiliza políticas para codificar cómo se autentican las aplicaciones, qué credenciales están autorizadas a usar y cómo se debe realizar la auditoría. Puede integrarse con una variedad de proveedores de identidades de confianza, como plataformas de gestión de acceso e identidad en la nube (IAM), Kubernetes, Active Directory y otros sistemas basados en SAML para autenticación. Vault entonces gestiona y aplica de manera centralizada el acceso a secretos y sistemas con base en fuentes confiables de identidades de aplicaciones y usuarios.



Los equipos de TI empresarial deben crear un servicio compartido que permita la solicitud de secretos para cualquier sistema a través de un flujo de trabajo coherente, auditado y protegido.

Cifrado como servicio

Además, las empresas deben cifrar los datos de las aplicaciones en reposo y en tránsito. Vault puede ofrecer cifrado como servicio para proporcionar una API coherente con la gestión de claves y la criptografía. Esto permite a los desarrolladores realizar una sola integración y luego proteger los datos en múltiples entornos.

Usar Vault como base para el cifrado como servicio resuelve problemas difíciles que enfrentan los equipos de seguridad, como la rotación de certificados y de claves. Vault permite la gestión centralizada de claves para simplificar el cifrado de datos en tránsito y en reposo en nubes y centros de datos. Esto ayuda a reducir los costos en torno a los módulos caros de seguridad de hardware (Hardware Security Module, HSM) y aumenta la productividad con flujos de trabajo de seguridad coherentes y estándares criptográficos en toda la organización.

Si bien muchas organizaciones establecen la orden de que los desarrolladores cifren los datos, no suelen proporcionarles la forma de hacerlo, por lo cual los desarrolladores quedan sin una comprensión adecuada de la criptografía para crear soluciones personalizadas. Vault proporciona a los desarrolladores una API simple que se puede usar fácilmente, al mismo tiempo que brinda a los equipos de seguridad central los controles de políticas y las API de gestión del ciclo de vida que necesitan.

Protección de datos avanzada

Las organizaciones que se trasladan a la nube o que utilizan entornos híbridos continúan manteniendo y dando soporte a servicios y aplicaciones locales que necesitan realizar operaciones criptográficas, como el cifrado de datos para almacenamiento en reposo. Estos servicios no necesariamente quieren implementar la lógica en torno a la gestión de estas claves criptográficas y, por lo tanto, buscan delegar la tarea de gestión de claves a proveedores externos. Advanced Data Protection permite a las organizaciones conectar, controlar e integrar de forma segura claves de cifrado avanzado, operaciones y gestión entre la infraestructura y Vault Enterprise, lo cual incluye protección automática de datos en MySQL, MongoDB, PostgreSQL y otras bases de datos que utilizan cifrado de datos transparente (transparent data encryption, TDE).

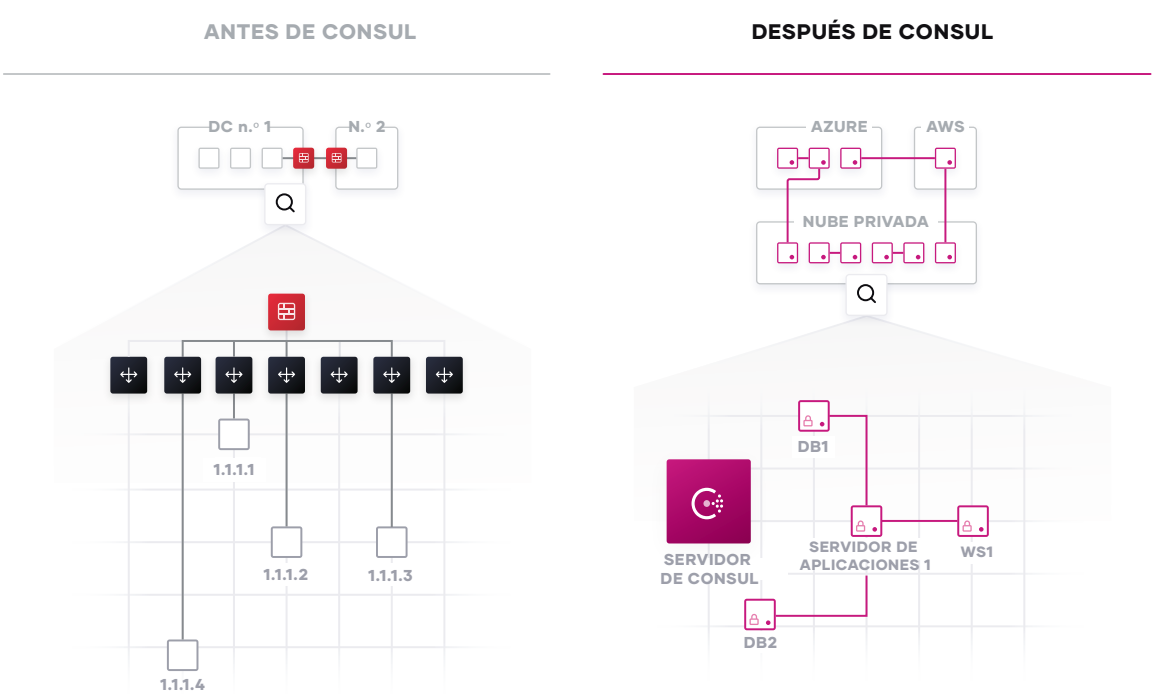
En el caso de organizaciones con requisitos de seguridad altos para el cumplimiento de datos (PCI=SS, HIPAA, etc.), la protección de datos y el anonimato mediante protección con criptografía para información de identificación personal (o PII [personally identifiable information]), Advanced Data Protection les proporciona funcionalidad para tokenización de datos, como enmascaramiento de datos, para proteger datos confidenciales, por ejemplo, tarjetas de crédito, información personal confidencial, números bancarios, etc.

Paso 3: Redes de servicios multinube

Los desafíos de las redes en la nube a menudo son uno de los aspectos más difíciles en la adopción del modelo operativo en la nube para las empresas. La combinación de direcciones IP dinámicas, un crecimiento significativo en el tráfico este-oeste cuando se adopta el patrón de microservicios y la falta de un perímetro de red claro representan un desafío enorme.

HashiCorp Consul proporciona una capa de red de servicios multinube para conectar y proteger servicios. Consul es un producto ampliamente implementado, con muchos clientes que emplean una cantidad considerablemente superior a 100 000 nodos en sus entornos.

Los servicios de redes deben prestarse de una forma centralizada, donde los equipos de TI proporcionen capacidades de registro de servicios y detección de servicios. Tener un registro común proporciona un "mapa" de los servicios que se están ejecutando, el lugar donde se encuentran y su estado actual. El registro se puede consultar programáticamente para habilitar la detección de servicios o impulsar la automatización de red de puertas de enlace de API, equilibradores de carga, firewalls y otros componentes de middleware críticos. Estos componentes de middleware se pueden trasladar fuera de la red utilizando un enfoque de malla de servicios, en el que los proxies se ejecutan en el perímetro para proporcionar funcionalidad equivalente. Los enfoques de malla de servicios permiten simplificar la topología de red, especialmente para topologías de múltiples nubes y múltiples centros de datos.



Detección de servicios

El punto de partida para las redes en el modelo operativo en la nube es generalmente un registro de servicios común, que proporciona un directorio en tiempo real de los servicios que se están ejecutando, el lugar donde se encuentran y su estado actual. Los enfoques tradicionales de las redes emplean equilibradores de carga e IP virtuales para proporcionar una abstracción de nomenclatura con el fin de representar un servicio con una IP estática. El proceso para realizar un seguimiento de la ubicación de los servicios de red a menudo es mediante hojas de cálculo, paneles de equilibradores de carga o archivos de configuración, de los cuales todos son procesos manuales desarticulados que no son ideales.

En Consul, cada servicio se registra programáticamente y se proporcionan interfaces de DNS y API para permitir que cualquier servicio sea detectado por otros servicios. La comprobación de estado integrada monitoreará el estado de cada instancia de servicio para que el equipo de TI pueda evaluar la disponibilidad de cada instancia y Consul pueda ayudar a evitar el enrutamiento del tráfico a instancias de servicio incorrectas.

Consul se puede integrar con otros servicios que gestionan el tráfico norte-sur existente, como los equilibradores de carga tradicionales y plataformas de aplicaciones distribuidas, como Kubernetes, para proporcionar un servicio de registro y detección coherente en entornos de múltiples centros de datos, de nube y de plataforma.

Automatización del middleware de red

El siguiente paso es reducir la complejidad operativa con el middleware de red existente a través de la automatización de la red. En lugar de emplear un proceso manual basado en tickets para reconfigurar los equilibradores de carga y los firewalls cada vez que hay un cambio en las ubicaciones o configuraciones de la red de servicios, Consul puede automatizar estas operaciones de red. Esto se logra al permitir que los dispositivos del middleware de red apliquen los cambios de servicio del registro de servicios, lo que da lugar a una infraestructura altamente dinámica que puede escalar significativamente más alto que los enfoques estáticos.

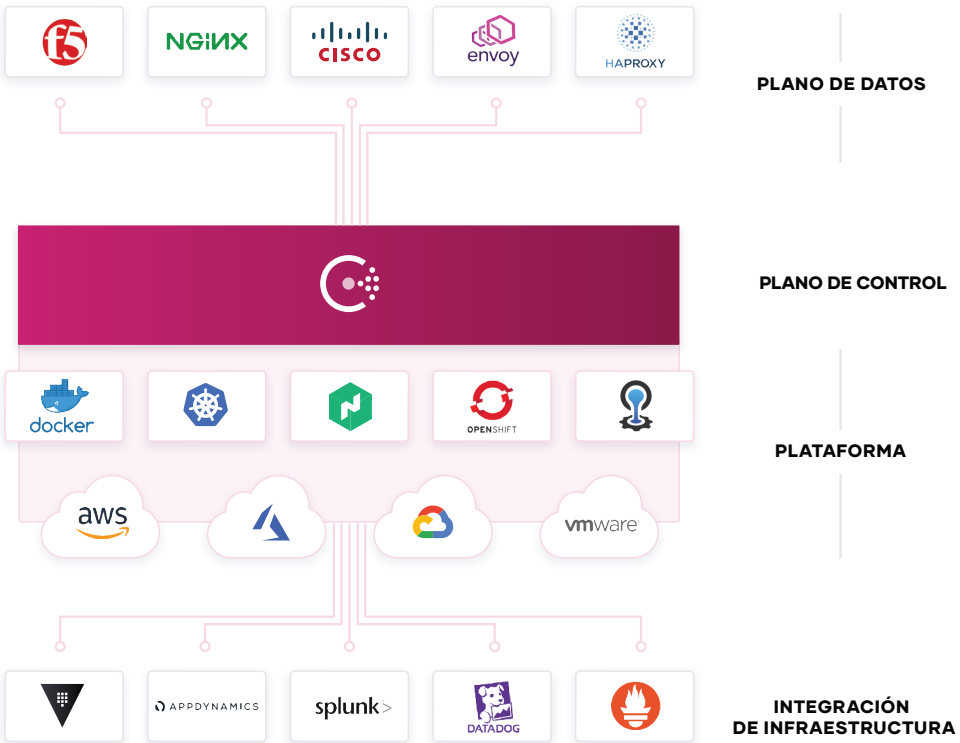
Esto desacopla el flujo de trabajo entre equipos, ya que los operadores pueden implementar aplicaciones y publicar en Consul de manera independiente, mientras que los equipos de NetOps pueden utilizar Consul para manejar la automatización descendente.

Redes de confianza cero con malla de servicios

A medida que las organizaciones continúan escalando con aplicaciones basadas en microservicios o nativas de la nube, la infraestructura subyacente se vuelve más grande y dinámica con una explosión de tráfico este-oeste. Esto provoca una proliferación de costoso middleware de red con puntos únicos de falla y una importante sobrecarga operativa a cargo de los equipos de TI.

Consul proporciona una malla de servicios distribuida que impulsa el enrutamiento, la autorización y otras funcionalidades de red a los extremos de la red, en lugar de imponerlos a través del middleware. Esto hace que la topología de red sea más simple y fácil de gestionar, elimina la necesidad de un middleware costoso dentro de las rutas de tráfico este-oeste y hace que la comunicación de servicio a servicio sea mucho más confiable y escalable.

Consul es un plano de control impulsado por API que se integra con proxies sidecar junto con cada instancia de servicio (proxies como Envoy, HAProxy y NGINX). Estos proxies proporcionan el plano de datos distribuidos. Juntos, estos dos planos dan lugar a un modelo de red de confianza cero que protege la comunicación de servicio a servicio con cifrado TLS automático y autorización basada en la identidad. Los equipos de operación y seguridad de red pueden definir las políticas de seguridad a través de intenciones con servicios lógicos en lugar de direcciones IP.

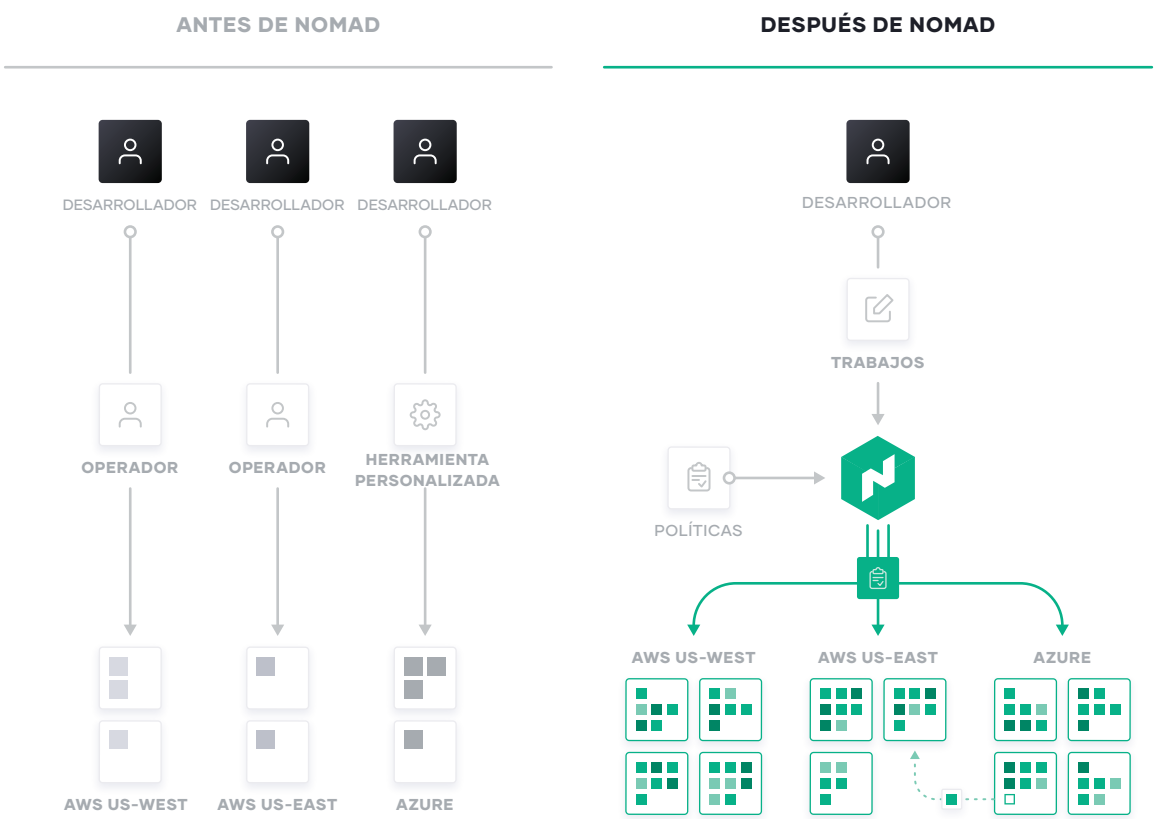


Consul permite la segmentación detallada de servicios para asegurar la comunicación de servicio a servicio con cifrado TLS automático y autorización basada en la identidad. Consul se puede integrar con Vault para la gestión centralizada de PKI y certificados. La configuración de servicios se realiza mediante un almacén de claves/valores impulsados por API que se puede utilizar para configurar fácilmente los servicios en tiempos de ejecución en cualquier entorno.

Paso 4: Entrega de aplicaciones multinube

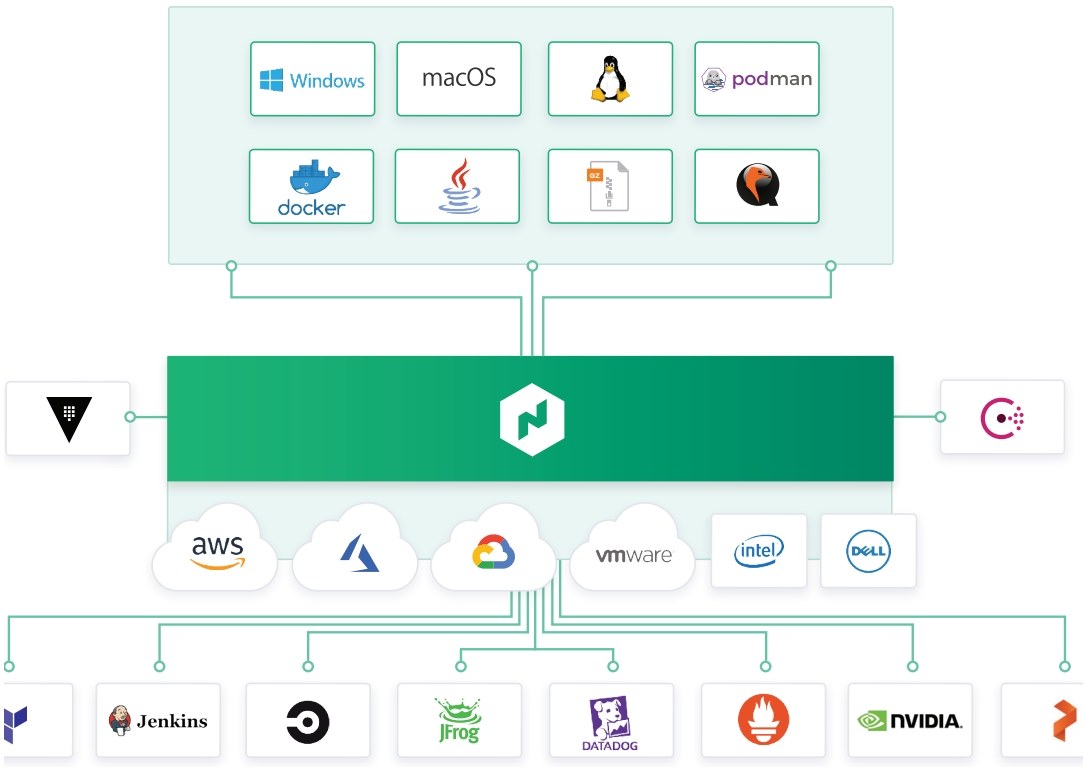
Por último, en la capa de aplicaciones, las nuevas aplicaciones están cada vez más distribuidas, mientras que las aplicaciones heredadas también deben gestionarse de manera más flexible. HashiCorp Nomad proporciona un orquestador flexible para implementar y gestionar aplicaciones heredadas y modernas, para todo tipo de cargas de trabajo: desde servicios de larga ejecución hasta lotes de corta duración y agentes de sistemas.

Para lograr servicios compartidos para la entrega de aplicaciones, los equipos de TI deben usar Nomad junto con Terraform, Vault y Consul para permitir una entrega coherente de aplicaciones en la infraestructura de nube, que incorpore los requisitos necesarios de cumplimiento, seguridad y redes, así como orquestación y planificación de carga de trabajo.



Orquestación de carga de trabajo combinada

Muchas cargas de trabajo nuevas se desarrollan con empaquetado en contenedores con la intención de implementarlos en Kubernetes u otras plataformas de gestión de contenedores. Sin embargo, muchas cargas de trabajo heredadas no se trasladarán a esas plataformas, ni tampoco lo harán en el futuro las aplicaciones Serverless. Nomad proporciona un proceso coherente para la implementación de todas las cargas de trabajo desde máquinas virtuales, a través de archivos binarios y contenedores independientes, y proporciona beneficios de orquestación central en todas esas cargas de trabajo, como automatización de versiones, múltiples estrategias de actualización, bin packing y resiliencia.



Para aplicaciones modernas, generalmente contenedores integrados, Nomad proporciona el mismo flujo de trabajo uniforme a escala en cualquier entorno. Nomad se centra en la simplicidad y la efectividad de la orquestación y planificación, y evita la complejidad de plataformas como Kubernetes que requieren habilidades especializadas para operar y resolver únicamente cargas de trabajo de contenedores.

Nomad se integra en los flujos de trabajo de CI/CD existentes y proporciona implementaciones de aplicaciones automáticas y rápidas para cargas de trabajo heredadas y modernas.

Informática de alto rendimiento

Nomad está diseñado para programar aplicaciones con baja latencia en clústeres muy grandes. Esto es fundamental para clientes que tienen grandes trabajos por lotes, como suele suceder con las cargas de trabajo de informática de alto rendimiento (High Performance Computing, HPC). En el desafío del millón de contenedores, Nomad fue capaz de planificar un millón de instancias de Redis en 5000 máquinas en tres centros de datos, en menos de 5 minutos. Varias implementaciones grandes de Nomad se ejecutan a escalas aún mayores.

Nomad permite que las aplicaciones de alto rendimiento utilicen fácilmente una API para consumir capacidad de manera dinámica, lo que permite compartir recursos de manera eficiente para aplicaciones de análisis de datos como Spark. La planificación de baja latencia asegura que los resultados estén disponibles de manera oportuna y minimiza el desperdicio de recursos inactivos.

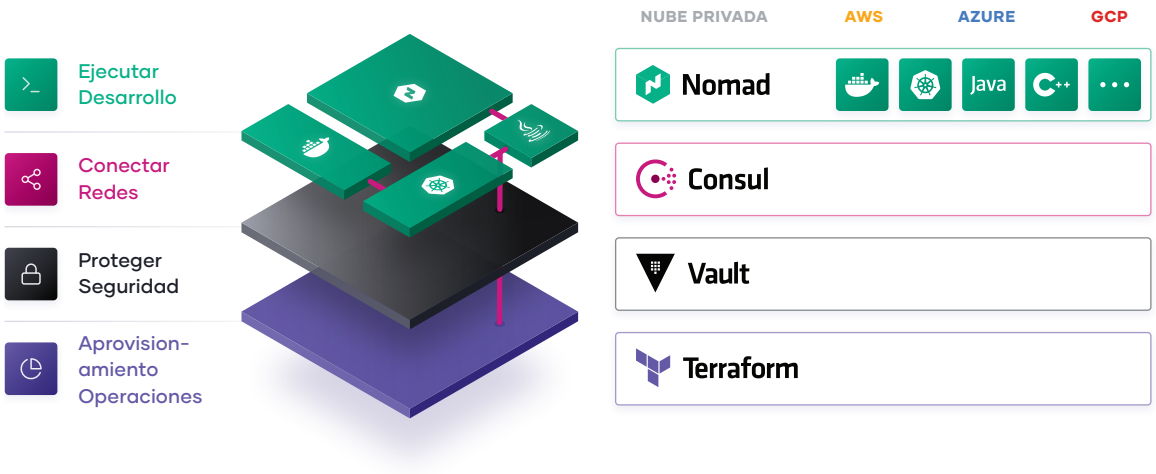
Orquestación de carga de trabajo de múltiples centros de datos

Nomad tiene un diseño multiregional y multinube, con un flujo de trabajo coherente en la implementación de cualquier carga de trabajo. A medida que los equipos implementan aplicaciones globales en múltiples centros de datos, o en diferentes nubes, Nomad proporciona organización y planificación para esas aplicaciones, con el respaldo de la infraestructura, la seguridad y los recursos y las políticas de red para garantizar que las aplicaciones se implementen con éxito.

Paso 5: Proceso de entrega de aplicaciones industrializado

Por último, estos servicios compartidos en infraestructura, seguridad, redes y tiempo de ejecución de aplicaciones presentan un proceso industrializado para la entrega de aplicaciones, al mismo tiempo que se aprovecha la naturaleza dinámica de cada capa de la nube.

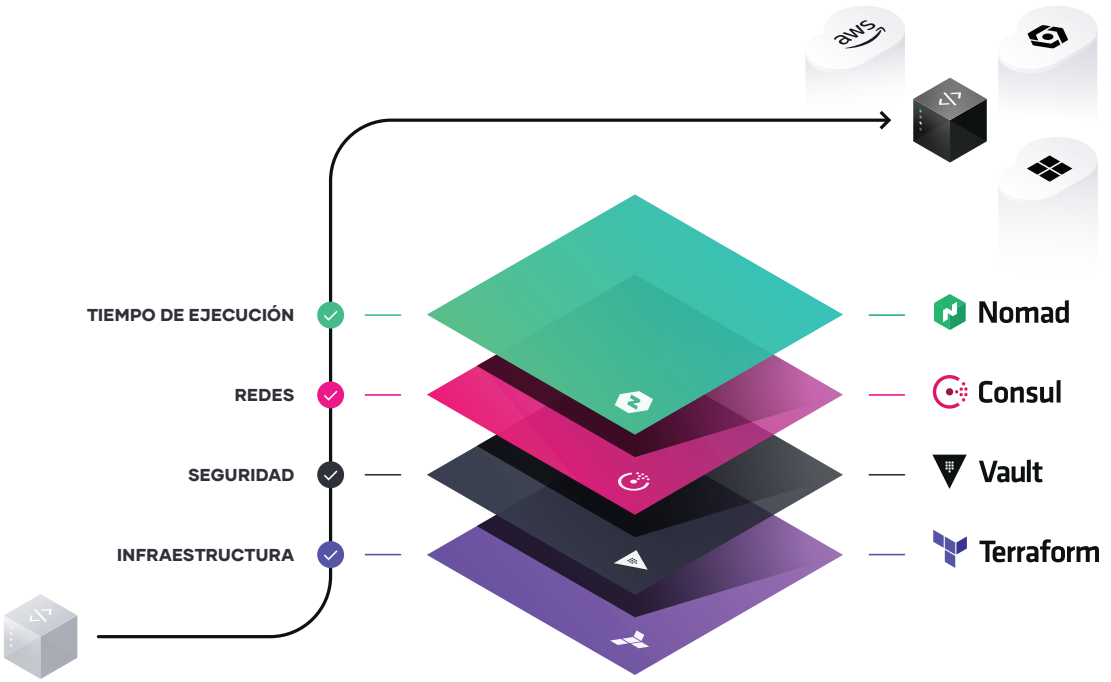
Adoptar el modelo operativo en la nube da lugar a una TI de autoservicio, que cumple completamente con las políticas y la gobernanza, para que los equipos entreguen aplicaciones a una velocidad cada vez mayor.



Conclusión

Un modelo operativo en la nube común es un cambio inevitable para las empresas que buscan maximizar sus iniciativas de transformación digital. El conjunto de herramientas de HashiCorp busca proporcionar soluciones para cada capa de la nube con el objetivo de permitir a las empresas hacer este cambio al modelo operativo en la nube.

La TI empresarial debe evolucionar y alejarse de los puntos de control basados en ITIL y de su enfoque en la optimización de costos, para convertirse en facilitadores de autoservicio enfocados en la optimización de velocidad. Esto puede lograrse mediante la oferta de servicios compartidos en cada capa de la nube, diseñados para ayudar a los equipos a brindar nuevo valor empresarial y para el cliente de forma rápida.



Encontrar el camino más rápido hacia el valor en un centro de datos multinube mediante la adopción de un modelo operativo en la nube significa cambiar características de la TI empresarial:

- **Personas: cambiar a habilidades multinube**
    - Reutilice las habilidades de la gestión interna del centro de datos y de los proveedores de una sola nube y aplíquelas de manera coherente en cualquier entorno.
    - Adopte DevSecOps y otras prácticas ágiles para generar continuamente sistemas cada vez más efímeros y distribuidos.

- **Proceso: cambiar a una TI de autoservicio**
    - Posicione la TI central como un servicio compartido habilitante enfocado en la velocidad de la entrega de aplicaciones, que despache software cada vez más rápido con un riesgo mínimo.
    - Establezca centros de excelencia en cada capa de la nube para la entrega de capacidades de autoservicio.
- **Herramientas: cambiar a entornos dinámicos**
    - Utilice herramientas que respalden la creciente efimeridad y distribución de la infraestructura y las aplicaciones y que respalden los flujos de trabajo críticos en lugar de estar vinculados a tecnologías específicas.
    - Proporcione herramientas de política y gobernanza que ajusten la velocidad de la entrega con el cumplimiento para gestionar el riesgo en un entorno de autoservicio.

Acerca de HashiCorp

HashiCorp es el líder en software de automatización de infraestructura multinube. El conjunto de software de HashiCorp permite a las organizaciones adoptar flujos de trabajo coherentes para aprovisionar, proteger, conectar y ejecutar cualquier infraestructura para cualquier aplicación. Las herramientas de código abierto de HashiCorp Vagrant, Packer, Terraform, Vault, Consul y Nomad se descargan decenas de millones de veces al año y son ampliamente adoptadas por las empresas de la lista Global 2000. En las versiones Enterprise de estos productos las herramientas de código abierto están mejoradas con características que promueven la colaboración, las operaciones, la gobernanza y la funcionalidad de los múltiples centros de datos. La compañía tiene su sede central en San Francisco y cuenta con el respaldo de Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP y Bessemer Venture Partners. Para obtener más información, visite www.hashicorp.com o siga a HashiCorp en Twitter @HashiCorp.


HashiCorp