NOTAS DE LA SOLUCIÓN

TRINZIC X6 RESUELVE PROBLEMAS DE AUTOMATIZACIÓN, SEGURIDAD Y TIEMPO DE ACTIVIDAD EN REDES HÍBRIDAS Y MULTINUBE

NIOS 9.0.1

Las ventajas de la conectividad en la nube están llevando a organizaciones de prácticamente todos los sectores del mercado a migrar sus plataformas de datos y aplicaciones desde centros de datos físicos y heredados a entornos híbridos y multinube.

El tiempo de actividad de las aplicaciones, la resiliencia, la recuperación ante desastres, la automatización de los flujos de trabajo, la escalabilidad, la agilidad y las posibles ventajas en cuanto a costes de TI son algunas de las razones más convincentes, si no urgentes, para modernizar la infraestructura empresarial. Sin embargo, a lo largo del proceso de migración híbrida y multinube, las organizaciones se enfrentan a innumerables retos que pueden retrasar o incluso paralizar los esfuerzos de modernización del entorno laboral y la obtención de las ventajas de la nube. Como líder en servicios unificados de redes y seguridad, Infoblox se ha anticipado a estos retos y ha colaborado con empresas líderes a nivel mundial para comprender y desarrollar soluciones que simplifiquen y resuelvan las principales dificultades de la migración a la nube. Con NIOS 9.0.1 y Trinzic X6, la plataforma de dispositivos físicos y de software diseñada específicamente, Infoblox ayuda a las empresas a evitar los errores más comunes, a obtener más rápidamente las ventajas de la nube y a implementar soluciones mejores y más sólidas para optimizar la relación tiempo-valor.

DESAFÍOS EMPRESARIALES

Con NIOS 9.0.1, Infoblox resuelve algunos de los desafíos empresariales más frecuentes y permite modernizar el lugar de trabajo, al incluir tres licencias generales que ahorran costes (antes se vendían por separado) como parte de la plataforma Trinzic X6: automatización de la API de Cloud Platform (CP), el cortafuegos de DNS (DFW) y el equilibrio de la carga global de servidores de DNS Traffic Control (DTC). Estas soluciones abordan problemas empresariales como escalar la automatización de las cargas de trabajo y la capacidad de supervivencia en entornos con silos y multinube; la protección de la empresa en el perímetro mediante el uso de zonas de políticas de respuesta (RPZ) para interceptar y bloquear la resolución en el DNS de direcciones IP o dominios maliciosos de la red; y la mejora del tiempo de actividad de las aplicaciones y la experiencia del usuario mediante la eliminación de la latencia y la facilitación de la recuperación ante desastres. Estas Notas de la solución examinan cada una de estas características y capacidades por separado e incluyen casos de uso clave, cómo funciona la solución y sus posibles ventajas para entornos híbridos y multinube.

Trinzic X6 resuelve retos apremiantes de la modernización en la nube, al incluir licencias generales para la automatización de la API de Cloud Platform (CP), el cortafuegos de DNS (DFW) y el equilibrio de la carga global de servidores de DNS Traffic Control (DTC).

AUTOMATIZACIÓN DE LA API DE CLOUD PLATFORM (CP)

CASOS DE USO

- Ampliar la automatización de DDI con API
- Evitar el retorno de llamadas a la API
- Extender DDI a entornos multinube
- Simplificar el control de acceso para los equipos de redes y de la nube
- Reducir la complejidad de las operaciones de red
- Ahorrar costes y ofrecer un retorno de la inversión sólido

BENEFICIOS

- **Procesamiento distribuido de la API:** La licencia CP mejora el rendimiento de DDI y distribuye las cargas de la API en el plano local.
- **Administración delegada y multiinquilino:** Los administradores pueden delegar objetos de DDI para la gestión programática mediante

AUTOMATIZACIÓN DE LA API DE CLOUD PLATFORM (CP)

ESCALAR Y AUTOMATIZAR LA INFRAESTRUCTURA DE DDI PARA ENTORNOS EN LA NUBE

A medida que las empresas adoptan despliegues en la nube, las funciones de orquestación y automatización resultan críticas. La licencia de la API CP de Infoblox mejora la escalabilidad y la resiliencia de los despliegues de centros de datos, al distribuir el procesamiento de la API y mantener las llamadas a la API y los servicios del protocolo DNS/DHCP localizados en cada centro de datos o entorno en la nube. Este tipo de ubicación permite a las empresas escalar sus servicios de red críticos con una arquitectura que optimiza las necesidades de las implementaciones en la nube distribuidas de hoy y permite topologías de despliegue futuras.

POR QUÉ CAMBIAR: MODERNIZAR LA INFRAESTRUCTURA DE DNS E IPAM

La automatización y distribución de servicios críticos de DDI (DNS, DHCP e IPAM) son esenciales en las infraestructuras modernas y dinámicas. Las aplicaciones pueden desplegarse in situ en nubes privadas, de forma externa en nubes públicas o en un entorno híbrido con solo cambiar las configuraciones en la plataforma de orquestación o gestión de la nube. Del mismo modo, las aplicaciones pueden trasladarse para optimizar el uso de los recursos de infraestructura como servicio (IaaS). Por tanto, es fundamental que la solución DDI sea flexible, automatizada y distribuida entre estos entornos.

Como parte del flujo de trabajo de aprovisionamiento, es necesaria la integración entre los equipos de servidor/nube para preparar los requisitos de computación, almacenamiento y red que requiere cada máquina virtual:

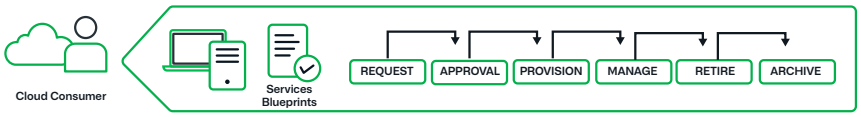

Figura 1: La creación de máquinas virtuales (VM) pasa a través de los equipos de servidor/nube y red para aprovisionar, gestionar y retirar máquinas virtuales.

POR QUÉ AHORA: AUTOMATICE Y ESCALE DDI DE NIVEL EMPRESARIAL PARA REDES HÍBRIDAS Y MULTINUBE

La licencia de la API CP resuelve la complicación de los servicios DDI distribuidos, al proporcionar protocolos de DNS y DHCP con gestión de registros DDI a través de API en una única plataforma de Trinzic X6, integrada directamente en la Grid de Infoblox. A medida que se aprovisionan VM, la licencia CP asigna direcciones IP y crea registros del DNS automáticamente para cada VM, eliminando los cuellos de botella debidos a un aprovisionamiento manual de direcciones IP y registros del DNS individuales. Además, la licencia CP permite la supervivencia de la API, el procesamiento distribuido de la API y la delegación de autoridad.

Infoblox se integra con las principales plataformas de gestión de la nube mediante API RESTful para mejorar la agilidad, dado que proporciona gestión de direcciones IP y aprovisionamiento de DNS automatizado para las cargas de trabajo. Las plataformas de orquestación en la nube utilizan llamadas a la API para aprovisionar servicios de red destinados a la automatización del DNS y las direcciones IP. Mantener estas llamadas a la API resulta crucial para aprovisionar VM y requiere una solución escalable y resiliente, sin un punto único de fallo.

proyectos específicos en la nube o de automatización. También pueden segmentar y gestionar los objetos por inquilino sin renunciar a una visibilidad centralizada.

- **Mejora de la capacidad de supervivencia:** Como la automatización de la API se efectúa a nivel del dispositivo local, la creación de la virtualización y la nube puede continuar, aun si se pierde la conectividad con el gestor de la red Grid.
- **Integración total con DDI de Infoblox:** La funcionalidad de CP es compatible con los dispositivos de DDI tradicionales en una red Grid de Infoblox y con la seguridad interna del DNS de Infoblox.
- **Integración directa con las principales plataformas:** Infoblox incorpora integraciones con VMware vRA/vRO, AWS EC2, GCP, Azure, OpenStack y otras plataformas optimizadas para un despliegue rápido y la rápida obtención de valor.

Visibilidad y gestión centralizadas para implementaciones de nube híbrida

Las capacidades de sincronización de datos y de base de datos distribuida de la red Grid de Infoblox facilitan la gestión centralizada de todos los datos de DDI, al tiempo que distribuyen la compatibilidad con los protocolos DNS y DHCP. La licencia CP lleva este concepto un paso más allá, al permitir actualizaciones de la API en los mismos miembros de Infoblox que prestan servicios de DNS/DHCP. La red Grid de Infoblox lleva a cabo una sincronización bidireccional de todos los datos que contiene en tiempo casi real, lo que proporciona la exclusiva capacidad de permitir la actualización de los registros críticos de DDI a través del gestor de la red Grid o a través de los miembros Trinzic X6 de CP. Esta capacidad ofrece a las empresas las mismas ventajas del procesamiento de la API distribuido y de alta disponibilidad que obtendrían al mantener los protocolos DNS/DHCP desde su red Grid de Infoblox.

Gestión mejorada de la API con plataformas de gestión en la nube

Sin la licencia CP, las llamadas a la API se envían al gestor de la red Grid de Infoblox como parte del despliegue de automatización de redes en la nube de Infoblox. Este enfoque funciona bien si la comunicación con el gestor de la red Grid está disponible. No obstante, si se interrumpe la conectividad de la red entre la plataforma de gestión de la nube u orquestador y el centro de datos principal que aloja el gestor de la red Grid, el DNS y la gestión de direcciones IP se verán afectados, lo que aumentará el riesgo de cortes del servicio.

La licencia CP de Infoblox presta servicios de DNS y DHCP igual que los miembros tradicionales de la red Grid, pero también es capaz de sincronizar y gestionar registros de IPAM. Estas funciones garantizan que todas las llamadas a la API se mantengan dentro del mismo centro de datos o entorno en la nube, al mismo tiempo que se producen los cambios de DNS/DHCP. Como consecuencia, se eliminan los problemas de disponibilidad y latencia, incluso si se pierde la conectividad con el gestor de la red Grid. Cuando se reanuda la conexión, los datos se sincronizan automáticamente entre el gestor de la red Grid y los miembros de la plataforma en la nube. Este paso de sincronización garantiza la supervivencia local, a la vez que proporciona visibilidad y gestión centralizadas. En entornos de nube extendidos donde las VM se ejecutan en varias ubicaciones, la capacidad de la API local mejora la fiabilidad general del sistema y evita la latencia de las llamadas a la API que se envían a través de una WAN.

Gestión distribuida de DDI y compatibilidad con múltiples inquilinos

La licencia CP de Infoblox admite un modelo de delegación que permite a las organizaciones segmentar su solución DDI para delegar la gestión de registros de zonas, subzonas, redes/subredes o rangos a organizaciones o proyectos específicos dentro de una organización. Cuando se utiliza con la automatización de redes en la nube de Infoblox, la licencia CP permite a los administradores de red delegar y aislar la gestión de registros DDI específicos para inquilinos de OpenStack o vRA de VMware, o las VPC de las instancias EC2 en AWS, lo que facilita la gestión de entornos multiinquilino.

Se pueden desplegar licencias CP adicionales a demanda para aumentar la capacidad de la API y los protocolos o para proporcionar servicios de red críticos para nuevos entornos de nube a medida que se aprovisionan. Esta capacidad mejora el tiempo general de servicio, al mismo tiempo que proporciona escalabilidad y resiliencia adicionales para las implementaciones en la nube. La capacidad de CP es esencial para proporcionar los servicios de DDI dinámicos y escalables que requieren los despliegues híbridos y multinube.

POR QUÉ INFOBLOX: ESCALAR LA AUTOMATIZACIÓN FIABLE DE DDI, EL RENDIMIENTO Y LA CAPACIDAD DE SUPERVIVENCIA PARA LAS EMPRESAS MULTINUBE

La licencia CP de Infoblox optimiza una solución DDI de nivel empresarial para lograr un rendimiento y una capacidad de supervivencia fiables y escalables en la automatización de redes en la nube. Proporciona visibilidad completa de los recursos físicos y virtuales con gestión desde un plano único de control. También aprovecha las sólidas integraciones de la API con AWS, Azure, GCP, OpenStack, VMware y otras plataformas para escalar la automatización en toda la empresa híbrida y multinube.

CORTAFUEGOS DE DNS (DFW)

PROTEGER EL DNS HASTA EL PERÍMETRO DE LA EMPRESA

El cortafuegos de DNS de Infoblox es un servicio del Domain Name System (DNS) que utiliza zonas de políticas de respuesta (RPZ) con un servicio de threat intelligence (fuente de software malicioso) para proteger el DNS mediante la detección, contención y control del malware. Este tipo de software malicioso utiliza el DNS para comunicarse con servidores de comando y control (C&C) y botnets con fines de intrusión, exfiltración de datos u otras actividades maliciosas. Las RPZ ofrecen un método para entender la reputación de los servidores y servicios que consultan los clientes, y de establecer políticas y acciones para impedir que los usuarios y sistemas de la red se conecten a ubicaciones maliciosas conocidas en internet. Al incluir la licencia DFW en NIOS para dispositivos físicos y de software, Infoblox le ayuda a proteger su empresa en entornos in situ, centros de datos y la nube hasta el perímetro de la red.

POR QUÉ CAMBIAR: LA INFRAESTRUCTURA DEL DNS ESTÁ BAJO ATAQUE

Los ataques a la infraestructura DNS siguen siendo una de las principales causas de las miles de violaciones de datos que se producen a diario en todos los sectores en todo el mundo. El DNS es objeto de ataques a través de una amplia gama de ataques volumétricos al DNS, DDoS o de amplificación/reflexión del DNS y exploits, como el envenenamiento de la caché del DNS, la suplantación de identidad y el secuestro de sesiones, que eluden o incluso interrumpen el funcionamiento de los cortafuegos de próxima generación (NGFW) actuales. La mayoría de los NGFW no pueden identificar ni gestionar estas amenazas, porque permiten que el tráfico pase por el puerto 53, el protocolo a través del cual se envían las consultas y respuestas al DNS.

POR QUÉ AHORA: PREVENIR LA EXFILTRACIÓN DE DATOS Y LA CONEXIÓN A UBICACIONES MALICIOSAS

El DNS se utiliza cada vez más como vía para la exfiltración de datos mediante el túnel del protocolo IP a través del puerto 53, ya sea de forma inadvertida, a través de dispositivos infectados con software malicioso no detectado, o de forma intencionada por parte de actores maliciosos. Para empeorar aún más las cosas, la mayoría del software malicioso no se detecta hasta más de 200 días después de la infección, lo que expone a las empresas a la pérdida de datos confidenciales de clientes, información financiera, propiedad intelectual y otros datos críticos.

POR QUÉ INFOBLOX: UNIFICAR REDES Y SEGURIDAD PARA LOGRAR PROTECCIÓN Y RENDIMIENTO

DFW de Infoblox es la solución líder en seguridad de redes basada en el DNS. Con DFW, Infoblox unifica redes y seguridad, al contener y controlar el software malicioso de exfiltración de datos en implementaciones locales hasta el perímetro de la red en la nube. DFW funciona integrando las RPZ del DNS, BloxOne Threat Defense de Infoblox (opcional), Threat Insight o fuentes forenses externas de indicadores de compromiso (IoC) para detectar, bloquear y redirigir el software malicioso. Infoblox combina DFW con datos de IPAM en la red Grid para aislar los dispositivos infectados y permitir su corrección. Al aprovechar la huella digital de DHCP y el mapeo de identidades, los administradores pueden captar el nombre de usuario vinculado a un dispositivo infectado y reducir el impacto de las amenazas en una fase temprana de la cadena de ciberataque. Además, DFW habilita la redirección del DNS, lo que permite a los administradores bloquear o reenviar dominios a un «jardín vallado» u otras ubicaciones designadas. DFW también se puede utilizar como desencadenante para integraciones del ecosistema de seguridad en clientes con la licencia Ecosystem. DFW también se integra con Informes y análisis de Infoblox para proporcionar informes resumidos y datos contextuales enriquecidos, incluidos los principales accesos a RPZ, los principales nombres de host maliciosos, los principales usuarios maliciosos y muchas otras métricas de seguridad.

CORTAFUEGOS DE DNS (DFW)

CASOS DE USO

- Lleve la detección de IOC al borde de la red (en las instalaciones o en la nube)
- Habilite DFW en un dispositivo de hardware o software
- Permita la protección contra amenazas con Infoblox o fuentes de terceros
- Garantice la protección contra el software malicioso en el DNS
- Mejore la pila de seguridad existente

BENEFICIOS

- **Detectar, contener y controlar el software malicioso:** Combine herramientas y datos de redes y seguridad para permitir la detección temprana de comunicaciones infectadas o maliciosas.
- **Reducir el impacto de las amenazas al DNS empresarial:** Combine las RPZ con fuentes de threat intelligence opcionales para proteger su empresa tanto en despliegues in situ como en la nube.
- **Mejorar la visibilidad, la automatización y el control:** Permita que los administradores vean datos contextuales enriquecidos, automaticen la respuesta a amenazas, redirijan el tráfico y corrijan amenazas de seguridad.
- **Activar las integraciones del ecosistema de seguridad:** Mejore los conocimientos sobre amenazas, la visibilidad, el intercambio y la respuesta a través de extensas integraciones del ecosistema.

Por último, DFW proporciona una base fiable para la protección contra el software malicioso del DNS y mejora el impacto y el ROI de la infraestructura de seguridad existente del cliente.

¿Cómo funciona?

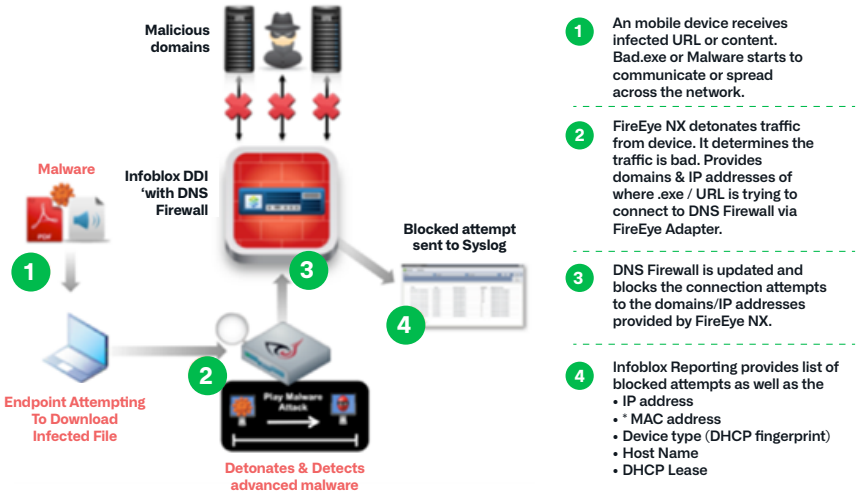

Figura 2: Cómo funciona el cortafuegos de DNS para bloquear intentos de conexión maliciosos.

CONTROL DE TRÁFICO DE DNS (DTC)

MEJORAR LA GESTIÓN DEL TRÁFICO, EL TIEMPO DE ACTIVIDAD DE LAS APLICACIONES Y LA EXPERIENCIA DEL USUARIO

La licencia DTC de Infoblox es una solución integrada para el equilibrio de carga global de servidores (GSLB), que ofrece gestión del tráfico de red, tiempo de actividad fiable para las aplicaciones, resiliencia de los servicios y recuperación ante desastres para redes locales, híbridas y multinube. DTC integra datos de IPAM autoritarios con métricas de estado de los servidores DNS y GSLB, geo-IP y atributos ampliables («EA» o metaetiquetas de usuario) para redirigir de forma inteligente el tráfico de los usuarios a los servidores óptimos y garantizar así el máximo tiempo de actividad y la mejor experiencia de usuario.

POR QUÉ CAMBIAR: LA MODERNIZACIÓN GLOBAL ESTÁ TRANSFORMANDO EL PANORAMA DE LA RED

La modernización regional y global del lugar de trabajo transforma la empresa local y multinube híbrida. El acceso directo a las aplicaciones en la nube desde cualquier lugar ha aumentado las expectativas de la experiencia del cliente, que debe ser rápida, eficiente y estar siempre disponible. SD-WAN habilita el acceso directo a internet para las sucursales locales. Surgen las capacidades 5G y el IoT incrementa las demandas de conectividad para los recursos de red. Estos retos se intensifican a medida que las organizaciones adoptan nuevas plataformas y tecnologías. Los usuarios esperan obtener rendimiento en tiempo real, especialmente en portales de comercio electrónico e internos. La gestión de aplicaciones heredadas y modernas resulta más compleja, sobre todo en caso de fusiones y adquisiciones. La normativa de privacidad se intensifica y su incumplimiento conlleva sanciones elevadas. Las tendencias cambiantes en los trabajadores móviles y remotos y las sucursales, la globalización, la consolidación de los centros de datos, las continuas limitaciones de recursos y la expansión del DNS, el software malicioso y los ataques sigilosos ejercen una presión aún mayor sobre los equipos encargados de gestionar el tráfico de red, el tiempo de actividad y la continuidad empresarial de forma responsable y sostenible.

- **Integrar informes y análisis:** Obtenga informes a demanda resumidos, forenses y visualizados con datos de red enriquecidos.
- Mejorar la pila de seguridad existente: refuerce el impacto, el valor y el retorno de la inversión de las herramientas de seguridad e integraciones existentes.

CONTROL DE TRÁFICO DE DNS (DTC)

CASOS DE USO

- Gestión rentable del tráfico global en nubes internas y externas, locales e híbridas
- Tiempo de actividad para aplicaciones locales y SaaS basadas en subred, GeoIP y Atributos Extensibles
- Recuperación ante desastres (DR) para garantizar la resiliencia tras interrupciones catastróficas
- Consolidación de zonas de dominio y replicación de servidores y recursos
- Escalado de aplicaciones basado en API en entornos privados, híbridos y multinube
- Conciencia a nivel de sitio para clientes de MS AD
- Informes y análisis completamente integrados

BENEFICIOS

- **DNS/Equilibrio de carga global de servidores (GSLB) integrado:** Integra la gestión de direcciones IP (IPAM) autoritativa con DNS y GSLB para proporcionar rendimiento y un tiempo de actividad de aplicaciones de intranet e internet de alta disponibilidad (99,999%) sin depender de una plataforma de DNS adicional.

¿POR QUÉ AHORA? TIEMPO DE ACTIVIDAD GLOBAL ASEQUIBLE Y FIABLE, Y CONTINUIDAD EMPRESARIAL

DTC de Infoblox proporciona una solución asequible en comparación con otros controladores de entrega de aplicaciones (ADC) de la competencia para resolver los retos cambiantes de la gestión del tráfico global. DTC ofrece una gran satisfacción al usuario gracias a la fiabilidad del tiempo de actividad de las aplicaciones, su rendimiento y la conmutación por error sin interrupciones. Utiliza una interfaz de usuario sencilla y API robustas para distribuir las cargas de tráfico de red en entornos geográficamente diversos, in situ e híbridos, y multinube para comercio electrónico, portales de atención al cliente, la web y aplicaciones internas empresariales críticas. También garantiza la continuidad del negocio y la recuperación ante desastres en caso de que se produzca un evento catastrófico, con el fin de restablecer la normalidad operativa.

POR QUÉ INFOBLOX: UNIFICAR REDES Y SEGURIDAD PARA LOGRAR PROTECCIÓN Y RENDIMIENTO

DTC de Infoblox integra datos de IPAM autoritarios con el DNS y GSLB para dirigir de forma inteligente el tráfico de los usuarios a los servidores óptimos. A diferencia de los ADC de la competencia, es una solución de DNS totalmente integrada, más rápida y fiable que la adición de protocolos de capa 2 y capa 3. Proporciona múltiples algoritmos de equilibrio de carga y comprobaciones de estado flexibles y automatizadas para garantizar la disponibilidad de los servidores. DTC es escalable para adaptarse a los cambiantes volúmenes de tráfico de datos y necesidades empresariales. Para lograr una visibilidad óptima, DTC utiliza una sencilla interfaz de usuario y un visualizador que muestra los nombres de dominio con equilibrio de carga (LBDN), las relaciones y los atributos de grupos y servidores. Además, a diferencia de otros ADC, permite realizar pruebas en tiempo real y preproducción de LBDN, grupos y servidores para garantizar la preparación previa a la fase de producción. DTC puede utilizar GeoIP y datos de atributos ampliables («EA», metaetiquetas definidas por el usuario) para controlar el tráfico a zonas específicas de una región para el cumplimiento de la normativa y la privacidad, junto con la optimización de las aplicaciones. Una herramienta integrada de informes y análisis basada en Splunk que ofrece paneles de control, informes, búsquedas, alertas y distribución automatizada de informes DTC preconstruidos y personalizables está disponible por separado. Por último, DTC se integra con las fuentes de detección de Infoblox para actualizar automáticamente las topologías basándose en datos de subredes IP, GeoIP y AE. Las API pueden utilizarse para añadir rápidamente nuevas instancias de servidor, aprovisionar nuevas aplicaciones, integrarse con otros sistemas y automatizar tareas rutinarias. Dado que DTC está integrado directamente en la red Grid, no es necesario gestionar la implementación, configuración y actualización del software de una plataforma independiente.

- **Gestión inteligente del tráfico global:** Utiliza GSLB basado en el DNS para dirigir de manera inteligente el tráfico de usuarios al servidor óptimo en función de la ubicación del cliente y del servidor, y del estado y la disponibilidad de cada servidor.
- **Visualizador de DTC:** Muestra los nombres de dominio con equilibrio de carga (LBDN), relaciones y atributos de grupos y servidores a través de una única visualización en la GUI.
- **Pruebas de preproducción:** Permite probar LBDN, grupos y servidores nuevos y actualizados de forma rápida y en tiempo real para asegurar la preparación en preproducción antes de la puesta en marcha.
- **Cumplimiento:** Permite el uso de GeoIP y datos de atributos ampliables (EA) para restringir el tráfico a zonas específicas de la región para LBDN y grupos, lo que contribuye a cumplir los requisitos de privacidad.
- **Informes y análisis integrados:** Proporciona paneles de control, informes, búsquedas, alertas y distribución automatizada de informes basados en Splunk, prediseñados y personalizables para ofrecer más visibilidad y control.
- **Automatización de API:** Añada nuevas instancias de servidores, aprovisione nuevas aplicaciones rápidamente, integre otros sistemas y automatice las tareas rutinarias de gestión de GSLB; ahorre tiempo y dinero con esta API fácil de usar y bien documentada, que refleja la funcionalidad de la GUI web.

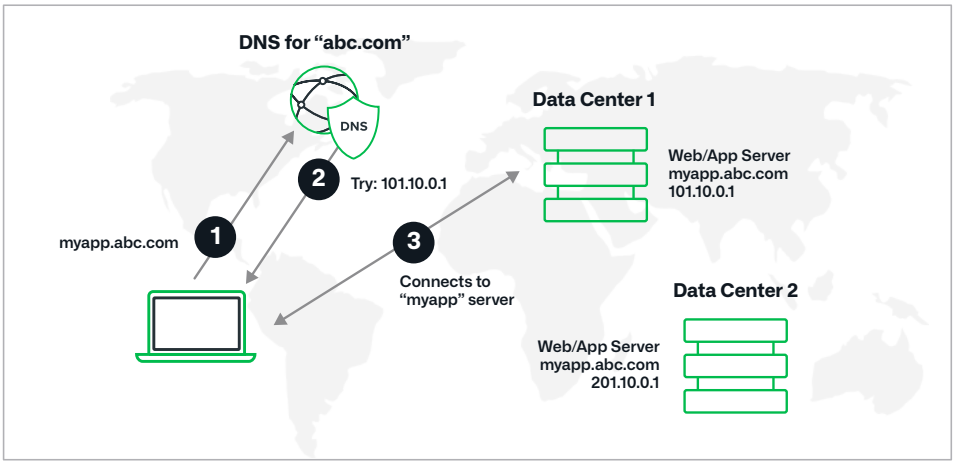

Figura 3: Aprovisionamiento de DTC que muestra 1) la iniciación del despliegue de una aplicación, 2) la conexión al DNS de la empresa y 3) el aprovisionamiento de servidores mi_app en centros de datos distribuidos.

RESUMEN Y PRÓXIMOS PASOS

Con NIOS 9.0.1 y la plataforma Trinzic X6, Infoblox aporta valor por medio de resolver desafíos de modernización de la nube con licencias generales, que antes se vendían por separado, para la automatización de la API de Cloud Platform (CP), el cortafuegos de DNS (DFW) y el equilibrio de la carga global de servidores de DNS Traffic Control (DTC). Estas soluciones abordan problemas empresariales comunes, como escalar la automatización de cargas de trabajo y la supervivencia en silos y entornos multinube; proteger la empresa hasta el perímetro mediante el uso de zonas de políticas de respuesta (RPZ) para interceptar y bloquear la resolución en el DNS de dominios o IP de red maliciosos; y mejorar la gestión del tráfico, el tiempo de actividad de las aplicaciones y la experiencia del usuario. Para obtener más información o comenzar una prueba, póngase en contacto con su equipo de cuentas en Infoblox.com/es.

CONTACTE CON NOSOTROS

Para obtener información técnica adicional, consulte las notas de la versión NIOS 9.0.1 (disponibles en GA, 21/8/2023) que se encuentran en el portal de soporte de Infoblox en https://support.infoblox.com.

Para obtener respuestas específicas sobre la plataforma NIOS o Trinzic X6 de Infoblox, o sobre la amplia gama de integraciones híbridas y multinube para la modernización del lugar de trabajo, póngase en contacto con su equipo de cuentas de Infoblox o con nosotros en Infoblox.com/es.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es

Versión: 20230731v1