NOTAS DE LA SOLUCIÓN

CONTROL Y SEGURIDAD SIN INTERRUPCIONES PARA IMPLEMENTACIONES DE NUBE HÍBRIDA CON AMAZON ROUTE 53 E INFOBLOX

RESUMEN

El servicio DNS de Amazon Route 53 ofrece soporte limitado más allá de los entornos puros de Amazon Web Services (AWS).

Estas limitaciones implican que las empresas no pueden crear una solución unificada de DNS, DHCP y gestión de direcciones IP (DDI) para atender a toda la organización, incluidas redes de campus empresariales y nubes híbridas, solo con Route 53, ya que Route 53 se centra exclusivamente en las nubes privadas virtuales (VPC) de AWS, lo que limita la conectividad, la visibilidad y la seguridad cuando se aplica a plataformas en la nube ajenas a AWS.

Infoblox integra su plataforma DDI líder del sector con AWS y el DNS de Amazon Route 53, con lo que ofrece una solución unificada, apta a nivel comercial, empresarial y de proveedor de servicios, para implementaciones en AWS y en la nube híbrida. La integración de Infoblox con Amazon Route 53 cierra la brecha entre el personal de TI empresarial y los equipos de la nube. Reduce la complejidad y ayuda a lograr un estado de seguridad óptimo, puesto que proporciona un único plano de control para gestionar los despliegues in situ, en nube privada y en la nube pública de AWS, con lo que aumenta la seguridad de esos despliegues. Esta solución resuelve las necesidades de los clientes actuales y futuros de Infoblox que incorporan AWS y utilizan Amazon Route 53 como DNS.

LA FALTA DE VISIBILIDAD, AUTOMATIZACIÓN Y COHERENCIA PUEDE MERMAR LAS IMPLEMENTACIONES DE AMAZON ROUTE 53

Amazon Route 53 ofrece funcionalidad de DNS privada dentro de las VPC de AWS. Sin embargo, una empresa que utiliza una nube híbrida enfrenta desafíos operativos incluso al usar Amazon Route 53, incluidos:

- **DNS limitado:** La resolución de DNS —o las respuestas a las consultas— está aislada en la red de AWS, lo que da problemas cuando se necesita comunicación fuera de una zona alojada privada de AWS en particular. Para subsanar este problema, los equipos de TI suelen iniciar múltiples servidores BIND que remiten el tráfico DNS fuera de las zonas aisladas de AWS, método que suma complejidad y ofrece escasa coherencia entre implementaciones de DNS dispares.
- **Sin IPAM:** AWS no dispone de una solución de gestión de direcciones IP (IPAM) y, a menudo, tiene una visibilidad limitada de las instancias virtuales, lo que perjudica la gestión diaria e incrementa el tiempo necesario para las auditorías y el cumplimiento normativo.

CONSTRUCCIÓN DE UNA SOLUCIÓN UNIFICADA DE DNS E IPAM CON AMAZON ROUTE 53

DDI de Infoblox para AWS se integra con el servicio de DNS de Amazon Route 53 y proporciona una consola centralizada para implementaciones de AWS y nube híbrida que proporciona visibilidad, una gestión coherente y seguridad. La solución de Infoblox y Amazon Route 53, al no estar restringida a las zonas alojadas privadas de Amazon Route 53, permite efectuar despliegues de nube híbrida fiables que se extienden más allá de AWS.

- **Falta de visibilidad en la nube híbrida:** Sin una solución coherente de DNS e IPAM en toda la nube híbrida, el personal de TI empresarial debe recurrir a varias herramientas para acceder a los datos del DNS y las direcciones IP. Esta falta de visibilidad da lugar a tiempos de resolución de problemas más largos, reduce la capacidad de planificación en la red y aumenta los riesgos de seguridad. También incrementa las incoherencias en la gestión de DNS y el espacio de direcciones IP a nivel empresarial.
- **Seguridad de DNS limitada:** Route 53 proporciona una seguridad de DNS limitada y poca capacidad de detección avanzada de amenazas en implementaciones de AWS y nube híbrida. La exfiltración de datos mediante la tunelización del DNS y el malware que utiliza el DNS son amenazas comunes que pueden paralizar las redes tecnológicas.

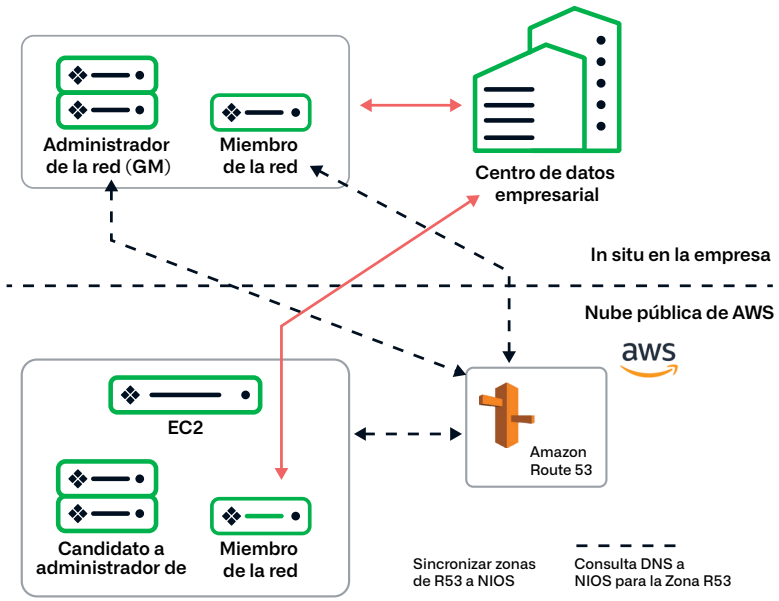


Figura 1: Gestión unificada a través de una nube híbrida

Mejore la visibilidad contextual en AWS y las implementaciones híbridas

La visibilidad contextual de la red es fundamental en los entornos multinube híbridos de hoy. Dado que Route 53 se centra exclusivamente en los recursos virtuales de AWS, la visibilidad se limita solo a esas instancias de la nube pública. La solución de Infoblox y AWS ofrece detección automatizada, visibilidad mejorada y seguimiento de VPC e instancias EC2 en una misma plataforma, lo que facilita la integración de los activos de la nube pública en un mismo servicio de DNS y gestión de direcciones IP. Infoblox simplifica la creación de registros y su borrado cuando se destruyen las instancias. Detecta e incluye o excluye recursos de red utilizando el enrutamiento entre dominios sin clases (CIDR o IP privada) de vDiscovery para garantizar una distribución eficiente de las direcciones IP en AWS.

A los equipos que necesitan gestionar y sincronizar múltiples cuentas en Amazon Route 53, Infoblox les ahorra un tiempo significativo. También reduce las tarifas de uso de AWS, al eliminar implementaciones de miembros de vNIOS en cada cuenta y sincronizar todas las zonas alojadas de Route 53 con la red Grid. vDiscovery reduce múltiples tareas de detección a un solo proceso que abarca diversas regiones y cuentas de AWS. También retiene los filtros de cuenta para permitir la selección de regiones y la migración de trabajos de vDiscovery en curso sin pérdida de datos, lo que mejora la experiencia del usuario, la eficiencia de las cargas de trabajo y el control administrativo.

A clientes federales y de otras administraciones, Infoblox les ofrece mayor visibilidad y control, ya que posibilita la sincronización de Route 53 y vDiscovery a través de múltiples regiones y cuentas de AWS GovCloud. Esta capacidad consigue un DNS altamente disponible y escalable, que conecta las solicitudes de los usuarios con las aplicaciones web de AWS mediante políticas de enrutamiento personalizadas para reducir la latencia.

Los equipos de TI reducen sensiblemente el tiempo necesario para auditar la información del DNS y las direcciones IP gracias a una vista coherente de los parámetros de AWS y ajenos a AWS en un mismo plano de control, que permite elaborar informes de cumplimiento normativo, operativos y ejecutivos.

Alta disponibilidad, tiempo de actividad y resiliencia

NIOS permite a los clientes que utilizan dispositivos de plataforma en la nube (CP) configurar dos dispositivos NIOS para contar con alta disponibilidad (HA) y tiempo de actividad. El valor HA indica con qué fiabilidad pueden acceder los usuarios al sistema y si este se ve afectado por el mantenimiento planificado o el tiempo de inactividad no programado. El tiempo de actividad indica el tiempo que un sistema está operativo. Con NIOS, los administradores pueden controlar ambos extremos y evitar puntos únicos de error en Azure y otros entornos de nube pública, especialmente para cargas de trabajo y aplicaciones críticas.

Seguridad y control reforzados de DNS

En los últimos años, los ataques de denegación de servicio distribuido (DDoS) al proveedor de servicios de internet Dyn y otras organizaciones han demostrado la necesidad de protegerse contra amenazas basadas en el DNS para minimizar costosas interrupciones comerciales, pérdidas de ingresos y daños a la reputación de la marca. NIOS añade protección de DNS avanzada (vADP) virtual a la nube pública de AWS para detectar y mitigar la más amplia gama de ataques de DNS, incluidos los volumétricos, NXDOMAIN, el secuestro de DNS y otros exploits. Mediante vADP, los administradores pueden detectar rápidamente ataques, mantener la integridad de DNS, mejorar el tiempo de actividad y ampliar la protección de DNS externa desde las instancias locales in situ hasta los entornos de la nube pública.

Para fortalecer aún más la seguridad del sistema, Infoblox habilita la sincronización de vNIOS con las listas de subconjuntos multicuenta de Amazon Route 53 a fin de incrementar la postura de seguridad y mejorar el control. Los administradores pueden hacer extensivas la detección y la sincronización de Route 53 a una lista de múltiples cuentas en AWS, desde una única instancia de NIOS. Pueden elegir entre: 1) dejar que NIOS detecte automáticamente las cuentas, o 2) especificar una lista de cuentas que detectar y sincronizar desde los entornos de Route 53. Esta capacidad refuerza la seguridad por medio de: 1) impedir que las cuentas secundarias accedan a la principal; 2) bloquear el acceso de administrador delegado; 3) inhibir la detección de todas las cuentas de la unidad organizativa, y 4) utilizar el acceso de permisos "Asumir un rol". Estas medidas de seguridad del DNS refuerzan los servicios críticos de la red frente a los ataques y mantienen las aplicaciones disponibles y operativas, de modo que la organización puede centrarse en atender a los clientes y gestionar sus actividades.

Mantener una plataforma DDI consistente para la nube híbrida

Muchas organizaciones implementan un entorno híbrido que combina infraestructuras locales, privadas virtuales, híbridas, públicas y multinube, incluido AWS. En lugar de utilizar hojas de cálculo manuales y obsoletas o la complejidad de soluciones dispares, Infoblox reduce la necesidad de crear servidores de DNS de uso general y hace posible la comunicación entre entornos in situ y en AWS, al integrar los registros de DNS de múltiples plataformas en un mismo plano de control que mejora la coherencia y la capacidad de gestión.

Infoblox también admite los tipos de instancias EC2 R6, lo que mejora el rendimiento y reduce el coste total de propiedad. Infoblox permite conectar directamente con AWS Nitro Systems y la consola serie EC2 para disfrutar de una resolución de problemas más rápida, con una mejor experiencia de usuario y más control. vNIOS mejora aún más la seguridad y el control de la nube, al permitir el cifrado de Elastic Block Store (EBS) para datos en reposo, datos en tránsito y todas las copias de seguridad de volúmenes.

Opciones de implementación flexibles

DDI de Infoblox para AWS se integra plenamente con los principales dispositivos in situ, virtuales y físicos del sector. La plataforma de DDI integral es compatible con la nube pública de AWS, entornos de nube privada (por ejemplo, VMware, OpenStack, Microsoft y otros) y redes tradicionales, o una combinación de ellos en una implementación híbrida. La solución unificada garantiza la máxima flexibilidad, escalabilidad y disponibilidad del servicio.

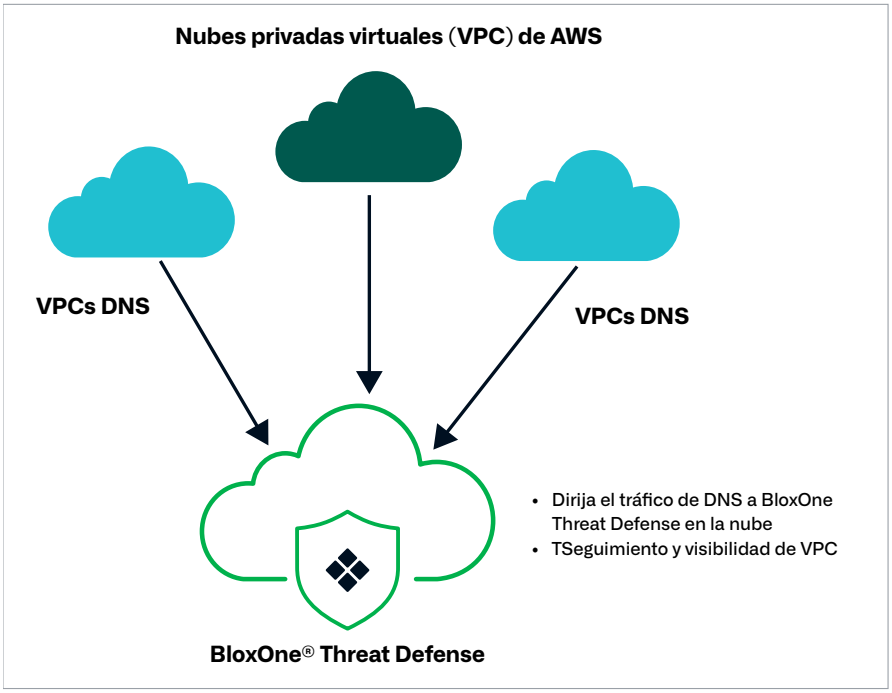
Infoblox ofrece una gama completa de opciones de despliegue a través de dispositivos físicos y de software seguros y diseñados especialmente para pequeñas oficinas remotas y sucursales, medianas y grandes empresas y proveedores de servicios con centros de datos y sitios distribuidos. La plataforma de dispositivos físicos y de software Trinzic X6 ofrece un rendimiento de DNS y DHCP hasta un 50% mejor que los modelos anteriores. También incluye licencias que ahorran costes en automatización con API de Cloud Platform, cortafuegos de DNS y equilibrio de carga global de servidores con DNS Traffic Control. Sea lo que sea lo que necesite su organización, Infoblox ofrece soluciones de nivel comercial, empresarial y de proveedor de servicios que proporcionan una experiencia de red crítica y coherente, con la fiabilidad y la flexibilidad necesarias para escalar su entorno según las necesidades de su empresa.

Infoblox facilita la migración a la nube, al permitir a los administradores desplegar los dispositivos de detección de Network Insight y de Informes y análisis en nubes públicas de AWS. Network Insight ofrece detección integrada de capa 2 y capa 3, sincronización de IPAM con dispositivos, hosts finales y puertos de red, gestión de puertos de conmutación, y notificaciones de ciclo de vida y cumplimiento. Además, la solución Informes y análisis de Infoblox, construida sobre Splunk, líder del mercado en búsqueda de datos, ofrece capacidades de monitorización, visualización y gestión de eventos e información de seguridad (SIEM). Colocar en AWS dispositivos que optimizan soluciones respalda las iniciativas de prioridad en la nube y simplifica la migración de centros de datos físicos a la nube. También reduce los recursos físicos de los centros de datos y ofrece visibilidad de metadatos DDI en entornos únicos y múltiples para auditoría histórica o cumplimiento, alertas en tiempo real, rendimiento de red y planificación de capacidad. Como resultado, las organizaciones obtienen visibilidad completa a demanda, simplifican la elaboración de informes de cumplimiento y pueden auditar en detalle la información del DNS y las direcciones IP de los recursos de AWS en todas las redes y regiones geográficas.

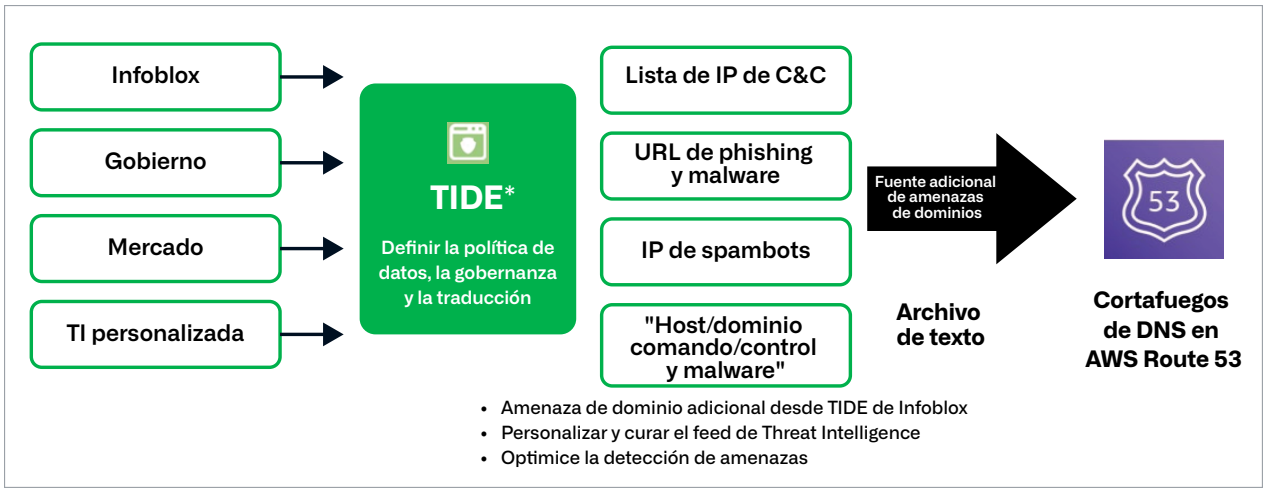
Extienda la seguridad de la capa DNS y la detección de amenazas a AWS

Los usuarios también pueden aprovechar la seguridad de DNS, la gestión de direcciones IP (IPAM) y la cuidada threat intelligence de de Infoblox para obtener visibilidad en las VPC de AWS y optimizar la detección de amenazas en el cortafuegos de DNS de Amazon Route 53. Implementar BloxOne® Threat Defense de Infoblox como parte de una estrategia integral reduce significativamente el riesgo de ataques avanzados y exploits, así como la exfiltración de datos del DNS.

A través de las amplias integraciones del ecosistema, los usuarios pueden automatizar la respuesta a los eventos detectados y utilizar el contexto de la red para priorizar la respuesta. Los usuarios pueden gestionar y minimizar de forma eficaz las amenazas en las VPC de AWS por medio de redirigir el tráfico de DNS de las VPC a BloxOne Threat Defense Cloud, que rastrea y obtiene visibilidad de las instancias en la nube, además de reducir el riesgo de ciberamenazas.



Por otra parte, las organizaciones pueden aprovechar la plataforma TIDE (intercambio de datos de inteligencia sobre amenazas) de Infoblox para enviar indicadores de compromiso (IOC) tanto al dispositivo del DNS en AWS de Infoblox como al cortafuegos de DNS de Amazon Route 53, lo que proporciona seguridad uniforme en todos los entornos y favorece la precisión, al elegir las fuentes de Threat Intel en función de las necesidades específicas. El acceso a decenas de fuentes de amenazas adicionales de la plataforma TIDE de Infoblox complementa las proporcionadas por el cortafuegos de DNS de Route 53. La capacidad de detectar y bloquear las amenazas existentes mediante una potente fuente personalizada refuerza la pila de seguridad y mejora las capacidades de defensa, investigación y respuesta.



CONCLUSIÓN

El enfoque aislado de Amazon Route 53 en AWS presenta deficiencias de gestión y lagunas en los servicios de red centrales —entre otras, falta de visibilidad, incoherencia y seguridad entre plataformas—, puesto que gestiona infraestructuras in situ e híbridas multinube. DDI de Infoblox para AWS solventa tales problemas gracias a la plataforma DDI líder del sector y reduce la complejidad, ya que utiliza una única consola para gestionar instancias in situ, la nube pública de AWS y los componentes críticos de DNS. BloxOne Threat Defense proporciona seguridad fundamental del DNS para proteger entornos híbridos mediante la detección de amenazas, la respuesta y la integración de ecosistemas para optimizar el rendimiento en materia de seguridad.

CONTACTAR CON NOSOTROS

Para obtener más información o respuestas sobre DNS e IPAM de Infoblox y otros servicios de red para Amazon Web Services (AWS), póngase en contacto con el equipo de su cuenta en Infoblox, consulte nuestras integraciones de red críticas o contáctenos en Infoblox.com.

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

+1.408.986.4000
www.infoblox.com

Versión: 20240529v2