infoblox®

NO CONSTRUYA SU MAÑANA SOBRE SERVICIOS CRÍTICOS DE RED DE AYER

La modernización, la automatización y la seguridad requieren DDI de nivel empresarial

Junio de 2025

TABLA DE CONTENIDOS

LOS COSTES OCULTOS DE UNOS SERVICIOS CRÍTICOS DE RED DISPARES

En la empresa hiperconectada de hoy, DNS, DHCP y la gestión de direcciones IP (DDI) no son meros servicios de fondo, sino la base de operaciones digitales seguras y escalables. Y sin embargo, muchas organizaciones aún confían en una infraestructura envejecida y fragmentada, con la suposición de que es «suficientemente buena».

Lo que a menudo se pasa por alto es cuánto les cuesta mantener soluciones anticuadas, no solo en pagos, sino también en tiempo de inactividad, exposición al riesgo y pérdidas de productividad. Según una investigación reciente*, las organizaciones que utilizan DDI de nivel no empresarial son significativamente más vulnerables a las interrupciones operativas, experimentan tiempos de recuperación más largos tras las interrupciones, se enfrentan a tasas más altas de fallos de auditoría y sufren costes más elevados.

* 9 errores de no utilizar un DDI de nivel empresarial, Enterprise Strategy Group, febrero de 2025

A MEDIDA QUE AUMENTAN LAS DEMANDAS DE SERVICIOS DE IDENTIDAD, EN LA NUBE Y PERIMETRALES, EL DDI DE NIVEL EMPRESARIAL NO ES SOLO UNA MEJORA, SINO UN IMPERATIVO DE LA MODERNIZACIÓN.

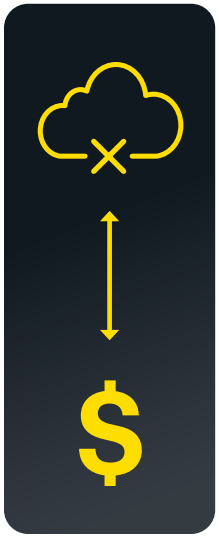
SI EL DNS EMPRESARIAL FALLA, EL MUNDO MODERNO SE DETIENE:
NO HAY COMERCIO, NO HAY VUELOS, NO HAY ENERGÍA. TODO SE PARALIZA.

DESAFÍOS CLAVE CON EL DNS, DHCP E IPAM TRADICIONALES EN SILOS:

- Tiempo de inactividad no planificado
- Falta de visibilidad y control
- Pérdida de productividad
- Costes más elevados
- Problemas de escalabilidad
- Puntos únicos de fallo
- Vulnerabilidades de seguridad más graves

LOS SERVICIOS DE RED CRÍTICOS SON SU SALVAVIDAS DIGITAL

Es posible que su organización se modernice en lo que respecta a la capa de aplicaciones y la nube, pero sin DNS y DHCP de nivel empresarial, toda la infraestructura está en riesgo. Casi todas las aplicaciones modernas, desde los sistemas de planificación de recursos empresariales (ERP) hasta las plataformas de identidad, dependen del DNS como punto de entrada digital. Un solo ámbito de DHCP mal configurado puede hacer que departamentos enteros queden sin acceso a la red.



EL COSTE REAL DE LAS INTERRUPCIONES

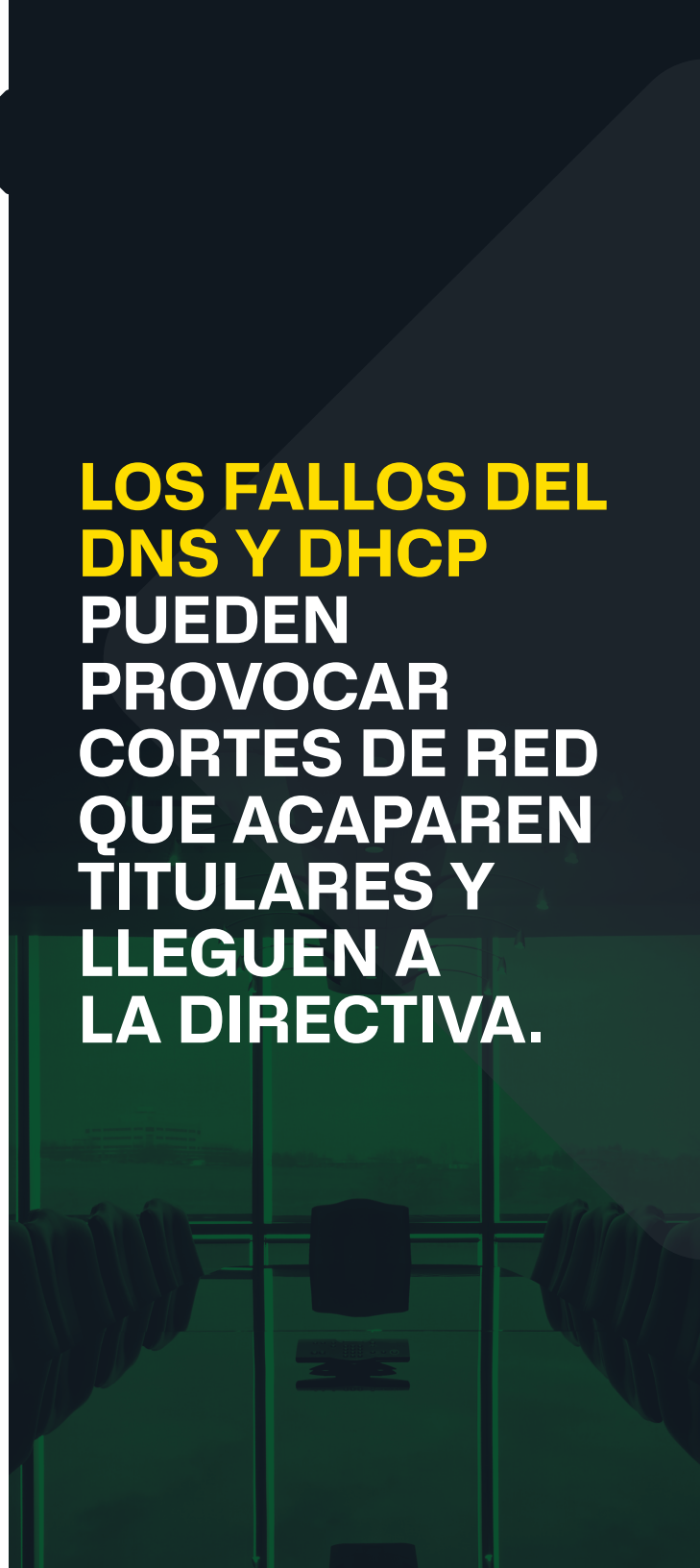
Las interrupciones del DNS y DHCP no son solo problemas de TI, sino riesgos empresariales. El coste medio de una interrupción de la red ha ido aumentando poco a poco hasta alcanzar los 9.000 dólares por minuto* en las grandes organizaciones; esa cifra se dispara cuando las interrupciones afectan a sistemas de atención al cliente o a procesos críticos para la misión.

CASO DESTACADO:

Un minorista global que dependía de la infraestructura obsoleta de Microsoft DNS tuvo un problema de sincronización que paralizó los terminales de punto de venta (TPV) en más de 100 tiendas durante tres horas.

¿PÉRDIDA ESTIMADA DE INGRESOS? 7,5 MILLONES DE DÓLARES. ¿LA CONFIANZA DEL CLIENTE? AÚN MÁS DIFÍCIL DE RECUPERAR.

LOS FALLOS DEL DNS Y DHCP PUEDEN PROVOCAR CORTES DE RED QUE ACAPAREN TITULARES Y LLEGUEN A LA DIRECTIVA.



* El verdadero coste del tiempo de inactividad, Forbes, David Flower, Forbes Technology Council, 10 de abril de 2024

UNA TRANSFORMACIÓN DIGITAL SIN DDI EMPRESARIAL EN LA BASE ES UN RASCACIELOS SOBRE ARENAS MOVEDIZAS.

LOS SERVICIOS DE RED HEREDADOS NO PUEDEN AFRONTAR LAS NECESIDADES ACTUALES

Las empresas no pueden permitirse el riesgo de utilizar herramientas del DNS y DHCP heredadas, especialmente a medida que se acelera la transformación digital. Lo que funcionaba hace una década sencillamente no responde a las necesidades de hoy.

RIESGO OPERATIVO

Los sistemas heredados suelen basarse en interdependencias frágiles entre DNS, DHCP y Microsoft Active Directory, todos desplegados en el mismo servidor de Windows. Y, como hemos mencionado, un único punto de fallo puede dar lugar a interrupciones en cascada.

INEFICIENCIAS DE COSTES

Atender la infraestructura heredada a menudo requiere personal específico para el mantenimiento, la aplicación de parches y la resolución de problemas. A ello se suman los costosos ciclos de renovación de hardware, con lo que la curva de costes de DDI se vuelve insostenible.

VISIBILIDAD FRAGMENTADA

La mayoría de los despliegues de DDI heredados no permiten una visualización en tiempo real, autoritativa y consolidada del uso de direcciones IP o del estado de los activos en entornos híbridos y multinube. Esta falta de visibilidad provoca retrasos en la identificación y el aislamiento de los puntos finales comprometidos, obliga al seguimiento y la conciliación manual de las direcciones IP en hojas de cálculo y crea dificultades para el cumplimiento normativo y los registros de auditoría, además de conflictos y superposiciones de direcciones IP.

CUELLOS DE BOTELLA DE LA INNOVACIÓN

Los sistemas de DDI heredados ralentizan la automatización, limitan las integraciones y obligan a los equipos de DevOps a depender de tickets manuales o scripts obsoletos.

EN RESUMEN, LAS HERRAMIENTAS HEREDADAS NO ESTÁN A LA ALTURA

Características como los retrasos en la sincronización de DNS, la falta de una papelera de reciclaje y el control de acceso basado en roles (RBAC) limitado hacen que los sistemas heredados sean poco fiables a gran escala. Peor aún, muchos requieren una consola de gestión por servidor, lo que crea silos operativos y aumenta la posibilidad de desviaciones en la configuración.

EL STATU QUO LLEVA A LA RUINA EMPRESARIAL

Los servicios críticos de red en silos presentan infinidad de retos para los gestores de redes, la nube y la seguridad, así como más ocasiones para los actores malintencionados. Sea cual sea su campo, si aún trata de construir su futuro digital con servicios de red obsoletos, está abriendo la puerta a los problemas.

Cómo el ransomware paralizó la atención al paciente

- Una banda de ransomware atacó un importante sistema hospitalario
- DNS/DHCP y los servicios de directorio compartían un mismo servidor, lo que impidió acceder a él cuando más urgía solucionar problemas
- Una descarga de un solo empleado comprometió servidores críticos
- Las operaciones de atención médica colapsaron: los registros, los teléfonos y los portales de pacientes dejaron de funcionar
- Hubo 5,6 millones de registros de pacientes afectados e interrupciones durante semanas

Coste total: 1.300 millones USD

Los costes ocultos de parchear servidores

- Un proveedor de energía gestionaba 400 servidores que requerían 4.800 parches al año
- Una tasa de fallos del 1 % suponía 48 incidencias al año
- Se estimaba que aproximadamente 50 empleados estarían inactivos cuatro horas cada vez
- 100 $ de coste medio por hora y empleado

Impacto anual del tiempo de inactividad: 960.000 USD

Una incidencia en julio de 2024 ' resonó en todo el mundo

- El mayor apagón informático de la historia
- Millones de servidores se cayeron
- Los servicios críticos de DNS/DHCP están caídos en todo el mundo
- 10.000 vuelos cancelados
- Innumerables hospitales afectados

Miles de empresas comprometidas

Según una investigación reciente de Forrester, el DDI de nivel empresarial ahorra tiempo y dinero considerables:

Ahorro de 7,1 millones USD

al pasar de una infraestructura heredada a un DDI moderno*

De 2 días a 1 hora

en tiempo ahorrado para el despliegue de máquinas virtuales en 1.000 centros**

14.000 horas

en tiempo ahorrado en toda la red con DDI moderno

* The Total Economic Impact™ del DDI de Infoblox, Forrester Consulting, octubre de 2023

** Resultados de una empresa

POR QUÉ EL DDI DE NIVEL EMPRESARIAL ES EL PRIMER PASO PARA LA MODERNIZACIÓN DE TI

El recorrido hacia la nube híbrida, la confianza cero y la computación perimetral no comienza con nuevas aplicaciones o interfaces de usuario deslumbrantes, sino con unos servicios de red críticos que sean fiables, escalables y seguros.

DNS, DHCP E IPAM UNIFICADOS = DDI

Para transformar su red, primero debe transformar su despliegue y gestión. Un DDI de grado empresarial combina la implementación y gestión del DNS, DHCP y gestión de direcciones IP (IPAM) en un mismo flujo de gestión. Esta combinación simplifica la complejidad de los servicios de red tradicionales y agiliza las operaciones empresariales. También mejora la visibilidad de la nube híbrida y entre distintas nubes, lo que facilita la automatización de procesos y permite ejecutar servicios de red tanto in situ como en la nube. Está diseñada específicamente para proporcionar la resiliencia, visibilidad y automatización que requieren las empresas actuales.

De hecho, las organizaciones que utilizan DDI de nivel empresarial han comunicado un aumento de más del 60 % en la productividad de las tareas del DDI, con menos pasos manuales y menos errores de configuración. Una empresa logró retirar el 100 % de las herramientas DDI anticuadas que no eran de Microsoft y reducir en más del 50 % la infraestructura de Microsoft requerida.

EL DDI DE NIVEL EMPRESARIAL ES LA BASE DE LA TI MODERNA

GESTIÓN CENTRALIZADA Y UNIFICADA

Las soluciones DDI de nivel empresarial ofrecen automatización y orquestación centralizadas para las funciones de DNS, DHCP e IPAM en diversos entornos: in situ, híbridos y multinube. Al unificar estos servicios básicos de red en un único panel de administración, los equipos de TI obtienen:

- Operaciones simplificadas
- Mejor aplicación de políticas
- Eficiencia operativa

MAYOR VISIBILIDAD

Una plataforma DDI empresarial proporciona visibilidad en tiempo real de todos los dispositivos y servicios con IP habilitadas en la red, algo esencial tanto para el control operativo como para la seguridad. Las prestaciones clave incluyen también:

- Detección dinámica de activos
- Seguimiento de asignaciones y utilización de IP
- Análisis integrado

OPCIONES DE DESPLIEGUE FLEXIBLES

El DDI de nivel empresarial le permite desplegar servicios en concordancia con los objetivos empresariales y las estrategias de TI, en lugar de limitarse a diseños de producto rígidos. Esta flexibilidad logra:

- Soporte nativo en la nube e híbrido
- DNS/DHCP sin infraestructuras, que se presta como servicio
- Opciones de dispositivos virtuales y físicos
- Arquitectura escalable

ADMINISTRACIÓN BASADA EN ROLES

Las plataformas de DDI empresariales incorporan controles de acceso más estrictos para apoyar la colaboración entre los equipos de NetOps, SecOps y CloudOps, manteniendo las responsabilidades de cada uno. Esta administración colaborativa permite:

- Acceso basado en permisos
- Auditabilidad y seguimiento de cambios
- Administración delegada

POSTURA DE SEGURIDAD MÁS SÓLIDA

Las soluciones de DDI de nivel empresarial refuerzan la seguridad, puesto que usan el DNS como elemento fundamental de la ciberseguridad. Esta seguridad adicional incluye el bloqueo proactivo del tráfico dirigido a dominios maliciosos y la detención de ataques basados en el DNS. Gracias a las capacidades de seguridad integradas, el DDI moderno ofrece:

- Seguridad preventiva
- Visibilidad en tiempo real del tráfico del DNS y sus anomalías
- Políticas de seguridad coherentes en entornos híbridos y multinube

LA MODERNIZACIÓN NO CONSISTE EN CAMBIAR POR CAMBIAR.
SE BASA EN LA RESILIENCIA, VISIBILIDAD Y CORDURA OPERATIVA.

INFOBLOX UNIVERSAL DDI™ PRODUCT SUITE PROPORCIONA SERVICIOS DE RED CRÍTICOS DE NIVEL EMPRESARIAL INCOMPARABLES

El conjunto de productos Infoblox Universal DDI™ Product Suite es la solución DDI de nivel empresarial más potente del sector, que combina gestión y control centralizados, automatización, escalabilidad y seguridad en entornos híbridos, multinube e in situ. Unifica DNS, DHCP e IPAM en una única plataforma integrada, que proporciona visibilidad en tiempo real, automatización inteligente y alta disponibilidad para los servicios de red críticos que se ejecutan in situ o en sistemas de DNS nativos de la nube, como AWS, Google Cloud y Azure. También permite a las organizaciones seguir utilizando su DNS nativo de la nube y combinarlo con la gestión de Universal DDI.

La arquitectura nativa de la nube de Infoblox también permite opciones de implementación flexibles que se alinean con las estrategias modernas de TI empresarial, mientras que características avanzadas como la integración de threat intelligence y la extensibilidad impulsada por API permiten a las organizaciones optimizar las operaciones, mejorar la postura de seguridad y respaldar la transformación digital a gran escala. Con una fiabilidad demostrada y adopción global por parte de las empresas, Universal DDI es la referencia para gestionar y proteger las redes complejas y dinámicas de hoy.

GESTIÓN UNIFICADA Y CENTRALIZADA EN TODAS LAS NUBES E IN SITU

En su núcleo, Universal DDI consolida DNS, DHCP e IPAM en un plano de control unificado, lo que permite una gestión simplificada de estos servicios de red críticos en la infraestructura in situ y en los tres principales proveedores de la nube: AWS, Azure y Google Cloud. Al centralizar el control, Universal DDI:

- Elimina los silos
- Simplifica las operaciones
- Mejora la seguridad
- Reduce el riesgo de configuraciones erróneas
- Permite aprovisionar servicios de red más rápidamente

LA VISIBILIDAD EXHAUSTIVA PERMITE MEJORAR TANTO LA SEGURIDAD COMO EL CUMPLIMIENTO

Con una visibilidad en tiempo real de los rangos de IP configurados, el uso, el estado del asignación y más, los equipos de TI pueden detectar anomalías de forma proactiva, hacer cumplir las políticas y evitar sorpresas costosas. Algunas empresas han logrado:

- **60 %** identificación más rápida de dispositivos comprometidos en incidentes de seguridad
- **>70 %** reducción del tiempo dedicado a preparar informes de cumplimiento

OPCIONES DE IMPLEMENTACIÓN FLEXIBLES PARA ADAPTARSE A SU ARQUITECTURA

Ya necesite un modelo de DDI como servicio, físico o virtual in situ o híbrido, Infoblox se adapta a sus requisitos. Despliegue servicios en el perímetro, en la nube o en ambos, y gestione las políticas de los servicios distribuidos con coherencia y automatización integrada.

PUNTO DE PRUEBA: Una empresa de logística global redujo el aprovisionamiento de sitios perimetrales de siete días a dos horas gracias a las plantillas de despliegue automatizado de Infoblox.

LA ADMINISTRACIÓN BASADA EN ROLES SIMPLIFICA LA GOBERNANZA.

Asigne roles fácilmente según la función, la geografía o el ámbito de cumplimiento. Olvídese del acceso de todo o nada y de arriesgadas excepciones manuales.

PUNTO DE PRUEBA: Una agencia federal estadounidense utilizó el RBAC de Infoblox para dar soporte a más de 1.200 usuarios, con estricta separación de las redes clasificadas y las no clasificadas.

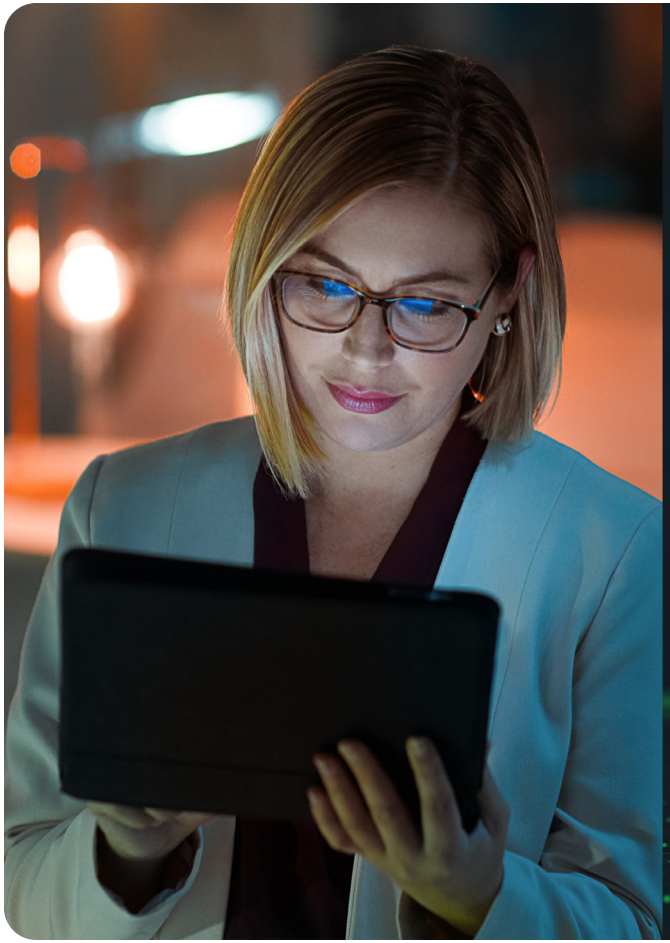
SEGURIDAD DEL DNS QUE DETIENE LAS AMENAZAS ANTES

Universal DDI de Infoblox proporciona seguridad integrada de nivel empresarial mediante Infoblox Threat Defense™. Al integrar las capacidades del DNS protector con la solución de DNS, DHCP e IPAM en una plataforma unificada, los equipos de seguridad pueden detener las amenazas con carácter preventivo, más de 63 días antes (de media) que otras soluciones. Universal DDI:

- Bloquea preventivamente el tráfico hacia dominios maliciosos y de phishing
- Bloquea amenazas basadas en el DNS, incluidas las de comando y control (C2), exfiltración de datos y algoritmos de generación de dominios (DGA), en tiempo real
- Identifica dominios similares para proteger la reputación de la marca
- Aplica políticas de seguridad coherentes desde el perímetro del punto final hasta la nube
- Acelera la respuesta a incidentes mediante la priorización de eventos del DNS y la atribución de puntos finales

DESACOPLAR LOS SERVICIOS CRÍTICOS PARA LA MISIÓN EQUIVALE A UNA MAYOR RESILIENCIA

El DDI de nivel empresarial desacopla los servicios de red de la identidad, lo que garantiza el tiempo de actividad, la visibilidad y la seguridad en entornos híbridos. Infoblox moderniza los servicios de red críticos mediante un DDI resiliente, diseñado específicamente para el nivel empresarial, el control de accesos basado en roles, la seguridad y la automatización.



NIST

Instituto Nacional de Estándares y Tecnología SP 800-81

2.3.1. Servicios DNS dedicados: Los ciberdelincuentes y otros actores tratarán de amplificar y maximizar la interrupción de cualquier ciberincidente atacando los sistemas de misión crítica, especialmente los objetivos que alojan múltiples componentes críticos.

Para garantizar la resiliencia cibernética, debe limitarse la coexistencia de múltiples servicios de misión crítica en un mismo sistema (es decir, separarse las funciones).

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81r3.ipd.pdf

INFOBLOX UNIVERSAL DDI FACILITA ESTAS PIEDRAS ANGULARES DE LA MODERNIZACIÓN

MODERNIZACIÓN DE LA IDENTIDAD

Desafío
Una empresa estaba migrando a plataformas híbridas de gestión de identidades (Okta y Azure AD), pero su DNS y DHCP seguían vinculados a Microsoft Active Directory in situ.

Solución:
Universal DDI de Infoblox desacopló los servicios de red críticos de la infraestructura heredada y aportó DNS y DHCP nativos de la nube y escalables, con visibilidad y gestión unificadas.

Resultado:
- ✔ Migración sin problemas de la plataforma de gestión de identidades híbridas
- ✔ Mayor tiempo de actividad y capacidad de gestión
- ✔ Reducción de la dependencia del Microsoft Active Directory heredado

Universal DDI garantizó una transformación de identidad fluida, segura y escalable, sin interrupciones.

TRANSFORMACIÓN EN LA NUBE

Desafío
Un destacado proveedor de atención médica había trasladado las cargas de trabajo a AWS y Azure, pero tenía dificultades para gestionar el DNS en entornos fragmentados tanto locales como en la nube.

Solución:
Universal DDI de Infoblox proporcionó una plataforma centralizada para gestionar el DNS entre múltiples proveedores de nube e infraestructura privada.

Resultado:
- ✔ Visibilidad de 360° en entornos híbridos
- ✔ Mayor tiempo de actividad y capacidad de gestión
- ✔ Automatización simplificada para DevOps
- ✔ Prestación de servicios segura y resiliente

100 % retirada de herramientas de seguridad del DNS heredadas

>30 % Aumento de la productividad del SOC

MODERNIZACIÓN DE LOS SERVICIOS EDGE

Desafío
Con el auge del trabajo remoto, el IoT y el procesamiento perimetral, una empresa de logística necesitaba un DNS/DHCP fiable en decenas de nodos perimetrales, sin presencia de TI.

Solución:
Universal DDI de Infoblox automatizó el aprovisionamiento de DNS/DHCP perimetrales mediante servicios resilientes de gestión remota.

Resultado:
- ✔ Configuración instantánea de sitios con aprovisionamiento sin contacto
- ✔ Un 70 % menos de interrupciones en los sitios remotos
- ✔ Postura de seguridad reforzada, con control centralizado

Infoblox trasladó los servicios de red de nivel empresarial al perímetro, sin tener que desplegar personal de TI sobre el terreno.

PORQUE CUANDO EL DNS FALLA, SU EMPRESA SE PARA.
ASÍ DE SENCILLO.

infoblox.

UNIVERSAL DDI DEINFOBLOX
CONSTRUYA PARA EL FUTURO

Para las empresas que navegan la transformación digital y necesitan servicios de red críticos fiables, seguros y escalables, Universal DDI es una plataforma de DDI nativa de la nube que unifica la gestión, automatiza las operaciones y asegura el perímetro. A diferencia de las herramientas DNS y DHCP heredadas y aisladas, Infoblox proporciona una infraestructura de red moderna que facilita la agilidad empresarial, la resiliencia, la seguridad y el ahorro de costes.

Universal DDI de Infoblox no es solo una mejora, sino un requisito fundamental para las empresas modernas. Es la forma de construir una red resiliente, receptiva y preparada para afrontar cualquier eventualidad.

¿ESTÁ LISTO PARA DEJAR ATRÁS EL STATU QUO?
Infórmese en: infoblox.com/es/networkmodernization

infoblox.

Infoblox aúna redes, seguridad y la nube para formar una base que sea tan resiliente como ágil. Integramos, protegemos y automatizamos los servicios críticos de red sin contratiempos para que las empresas puedan avanzar rápido y sin sobresaltos.

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

+1.408.986.4000
www.infoblox.com/es