

# vNIOS para DNS, DHCP y administración de direcciones IP en Microsoft Azure

Servicios de red virtualizados líderes en la industria para Azure

## EL DESAFÍO

### IMPLEMENTACIONES COHERENTES Y SEGURAS DE SERVICIOS DE RED CRÍTICOS EN ENTORNOS HÍBRIDOS Y DE NUBE PÚBLICA

Las organizaciones están modernizando sus redes para aprovechar las ventajas de la arquitectura en la nube: costes más bajos, mayor agilidad y flexibilidad, mayor seguridad y acceso global. Sin embargo, muchos administradores de red siguen luchando con procesos manuales, laboriosos y propensos a errores para gestionar sus direcciones IP (IPAM) y operaciones de DNS. Las herramientas heredadas y el software gratuito a menudo presentan desafíos complejos de arquitectura e implementación. Debido a que estas herramientas carecen de capacidades de detección de cambios en la configuración de DNS, verificación y herramientas de auditoría, tareas como la detección de activos, la replicación de Active Directory, la autenticación, el procesamiento de archivos y la impresión se ven afectadas negativamente. Estas complicaciones dan lugar a una mala visibilidad, operaciones ineficientes, conflictos e interrupciones, compromisos de la seguridad e incapacidad para atender los requisitos de cumplimiento normativo y auditoría.

## LA SOLUCIÓN

### GESTIÓN DE DIRECCIONES IP Y DNS DE NIVEL EMPRESARIAL LÍDER EN EL MERCADO PARA NUBES HÍBRIDAS Y MULTINUBE

#### Aproveche DNS e IPAM de Infoblox en Microsoft Azure

DNS e IPAM de Infoblox para Azure amplía las capacidades de su software líder del sector, totalmente integrado con Infoblox Grid, como NIOS virtual (vNIOS) o plataforma de dispositivos en la nube. La opción de máquina virtual (VM) ofrece servicios centralizados y distribuidos de DNS, IPAM y protocolos FTP, TFTP y HTTP.

#### Habilite DHCP para Azure

Las organizaciones con iniciativas que priorizan la nube o interesadas en desmantelar los centros de datos físicos y simplificar la migración a la nube pueden implementar DHCP para Azure. Esta funcionalidad garantiza la coherencia del servicio, ya que permite configurar los servicios DHCP en instancias vNIOS en Azure y servir DHCP a los clientes in situ.

#### Aumente la flexibilidad y la escalabilidad para Azure Stack Hub

Las organizaciones pueden operar dispositivos virtuales tanto en Azure como en Azure Stack. Dentro de Azure Stack, los equipos pueden ejecutar DNS e IPAM, servicios DHCP y vDiscovery de Infoblox para detectar recursos y endpoints en la nube. Azure Stack Government también es compatible. Esta integración en la nube in situ ofrece la máxima flexibilidad y escalabilidad para despliegues de Azure.

## BENEFICIOS

### Obtenga un DNS más rápido para Azure

Mejore el soporte de aplicaciones de Azure con DNS más rápido y fiable

### Habilite DHCP para Azure

Configure servicios DHCP en instancias de Azure en vNIOS y ofrezca DHCP a los clientes in situ

### Amplíe el rendimiento y la fiabilidad

Aumente el rendimiento y garantice el tiempo de actividad con las opciones de implementación de DNS e IPAM para la nube híbrida pública

### Garantice coherencia de DNS

Mejore la coherencia de DNS e IPAM con la sincronización de lectura de NIOS para aplicaciones DNS nativas de la nube de Azure a través de redes de Azure y tradicionales, a fin de ofrecer mayor precisión y una mejor experiencia de usuario.

### Ofrezca alta disponibilidad (HA)

Configure los dispositivos NIOS para la redundancia HA y así mejorar el tiempo de actividad y evitar puntos únicos de fallo en Azure

### Mejore la detección y la visibilidad

Elimine puntos ciegos con la detección automatizada y la visibilidad unificada y forense de las redes y máquinas virtuales en Azure

## Garantice la coherencia del DNS y la experiencia del usuario

Los administradores pueden configurar la sincronización de lectura a fin de que coincida con las aplicaciones DNS nativas de la nube de Azure, para objetos de Infoblox y la interfaz de usuario. Esta capacidad mejora la experiencia del usuario y la coherencia en las plataformas en la nube.

## Ofrezca resiliencia, alta disponibilidad (HA) y óptimo tiempo de actividad

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. Se ve afectado por el mantenimiento planificado y 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.

Además, el software de dispositivos virtuales de Infoblox para Azure ofrece todas las características de redundancia, alta disponibilidad, control de acceso y recuperación ante desastres de los dispositivos de hardware de Infoblox. Los usuarios cuentan con las ventajas demostradas de fiabilidad y tiempo de actividad de una solución de Infoblox y, por otra parte, se benefician de los costes reducidos que ofrece la nube de Azure. Dado que una única base de datos IPAM con autoridad actúa como repositorio centralizado para todos los dispositivos físicos y virtuales y las conexiones de red, los metadatos de red contextuales enriquecidos en tiempo real son fácilmente visibles a través de un único plano de control y cuentan con respaldo y disponibilidad para garantizar la resiliencia de la red y el tiempo de actividad.

## Mejore la visibilidad y el control de IPAM para instancias de nube pública

IPAM de Infoblox permite una detección de red avanzada (recursos virtuales incluidos), mapeo de redes e IP y filtrado avanzado, a través de funciones innovadoras como las carpetas inteligentes. Una interfaz gráfica de usuario fácil de usar proporciona configuración basada en plantillas, prevención automática de errores y visibilidad en tiempo real para la supervisión y la generación de informes. Acorte el tiempo de detección y respuesta gracias a la visibilidad en IPAM, que abarca desde redes tradicionales hasta despliegues de nube híbrida.

## Amplíe los miembros de informes y Network Insight en Azure

La visibilidad de la red es fundamental en los entornos multinube híbridos de hoy. Infoblox ofrece la capacidad de implementar los dispositivos de software de Informes y Análisis y detección de Network Insight en nubes públicas de Azure. Esta capacidad es compatible con las iniciativas que dan prioridad a la nube y simplifica la migración de los centros de datos físicos a la nube. También permite la detección de activos y la visibilidad de los metadatos de DDI con vistas a auditorías históricas, cumplimiento normativo, alertas en tiempo real, rendimiento de la red y planificación de la capacidad.

## Delegue las tareas de DNS e IPAM en los propietarios pertinentes

Con las herramientas de Infoblox, el equipo de red puede colaborar de manera efectiva con los equipos de servidores y centros de datos a través de recursos tradicionales y virtuales. Infoblox ofrece capacidades seguras de auditoría y administración basada en roles para facilitar la delegación efectiva de responsabilidades en un entorno virtualizado.

## Simplifique los procesos y aumente la productividad con Infoblox PayGo en Microsoft Azure Marketplace

Infoblox PayGo es un modelo de licencia flexible, de autoservicio y basado en el uso para desarrollar e implementar servicios de DNS, DHCP y administración de direcciones IP en entornos multinube. A través de PayGo, disponible en Microsoft Azure Marketplace, las organizaciones pueden acceder e implementar rápidamente

### Habilite políticas dinámicas de seguridad y redes

Conéctese con Azure AD a fin de proporcionar datos de identidad y directivas de seguridad dinámicas para sus usuarios y grupos

### Detecte, bloquee y corrija amenazas

Evite interrupciones con la protección de DNS avanzada (vADP) virtual para que Azure detecte y mitigue la más amplia gama de ataques de DNS

### Aproveche la potente Threat Intelligence para reforzar la seguridad

Combine Threat Intelligence con BloxOne® Threat Defense para disfrutar de seguridad en todo momento y lugar en Azure

### Abarate costes con soluciones respetuosas con el medioambiente

Reduzca el coste total de propiedad por medio de disminuir el gasto en hardware, energía, refrigeración e inmuebles

### Acelere los procesos con una implementación sencilla

Implemente fácilmente utilizando sus prácticas de virtualización estándar

### Amplíe la flexibilidad

Combine un dispositivo físico y múltiples opciones de dispositivos virtuales en una única implementación

### Acceda a Infoblox PayGo en Azure Marketplace

Explore las nuevas capacidades de DDI, resuelva los desafíos, reduzca el gasto comprometido, acceda rápidamente a la capacidad escalable, acelere el despliegue y simplifique la complejidad

## PRESTACIONES CLAVE

### Dispositivos virtuales en la nube

Agilice el tiempo de obtención de valor con la integración total de DNS e IPAM de Infoblox en nubes híbridas o públicas

servicios de red críticos sin los procesos de ventas tradicionales ni grandes compromisos de infraestructura. PayGo permite a las empresas explorar nuevas capacidades y solventar dificultades de la red, la nube y la seguridad. Reduce el compromiso de gasto, proporciona acceso inmediato a una capacidad escalable, acelera la implementación y simplifica la complejidad, con lo que se consigue una mayor productividad y un tiempo de generación de valor acertado. Para obtener más información, visite [Infoblox en Microsoft Azure Marketplace](#).

### **Amplíe la seguridad para detectar, bloquear y corregir amenazas**

NIOS añade protección de DNS avanzada (vADP) virtual a la nube pública de Azure 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.

DNS e IPAM de Infoblox como dispositivo virtual para Azure también es compatible con BloxOne® Threat Defense, la solución de seguridad híbrida fundamental de Infoblox. BloxOne Threat Defense permite a las organizaciones detectar y bloquear malware moderno, C&C, exfiltración de datos y amenazas de DGA, consolidar y distribuir la información sobre amenazas a todo el ecosistema y mejorar la eficiencia del SOC mediante la automatización y la integración de los ecosistemas.

### **Utilice Azure Sentinel para la defensa adaptativa de SIEM y SOAR**

Maximice los datos de consulta de DNS ampliados que genera BloxOne con Azure Sentinel, la solución en la nube de Microsoft para la gestión de eventos e información de seguridad (SIEM) y la orquestación, automatización y respuesta de seguridad (SOAR). Conecte sus datos de BloxOne a Sentinel en un clic para ver los registros de DNS sin procesar en un formato legible. Visualice los datos en paneles interactivos y detecte e investigue anomalías y más con las herramientas Sentinel personalizables y listas para usar, desarrolladas y diseñadas específicamente para BloxOne.

### **Opciones de implementación flexibles**

vNIOS for DDI de Infoblox se integra plenamente con los principales dispositivos locales, virtuales y en la nube del sector. Infoblox es compatible con Microsoft Azure, entornos de nube privada (incluidos VMware, OpenStack, Microsoft y otros) y redes tradicionales, o cualquier combinación 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 Trinzi 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 comerciales, empresariales y de nivel de proveedor de servicios que ofrecen una experiencia de red crítica y coherente, con la fiabilidad y la flexibilidad necesarias para escalar su entorno según las necesidades empresariales.

### **Reduzca los requisitos de espacio de rack, alimentación y refrigeración**

Al aprovechar Microsoft Azure, el software de dispositivos virtuales de Infoblox se ejecuta en recursos de la nube pública, que ahorran espacio en los racks de equipos y reducen los costes de alimentación y refrigeración. De esta forma, las organizaciones pueden reducir su coste total de propiedad y construir una infraestructura respetuosa con el medioambiente.

#### **Plano de control único**

Obtenga visibilidad del espacio de direcciones de su red a través de un plano de control único

#### **Implementación flexible de DNS**

Amplíe su red con DNS externos o internos a fin de mejorar la experiencia de usuario con DNS más rápidos para las aplicaciones de Azure

#### **Sincronización de lectura de NIOS para aplicaciones DNS nativas de la nube de Azure**

Asocie los objetos de NIOS y la interfaz de usuario con DNS nativo de la nube de Azure para obtener coherencia y mejorar la experiencia de usuario en distintas plataformas en la nube

#### **Alta disponibilidad (HA) en Azure**

Garantice la fiabilidad de aplicaciones de misión crítica, configurando dos dispositivos NIOS de Cloud Platform (CP) para disfrutar de alta disponibilidad y maximizar el tiempo de actividad de la red

#### **Detección y sincronización IPAM**

Automatice la detección, la visibilidad y la sincronización multirred de IPAM, así como la conversión en masa de direcciones IP en activos gestionados para aumentar la precisión y mejorar la experiencia de usuario y la eficiencia

#### **Políticas dinámicas de seguridad y redes**

Proporcione datos de identidad y políticas dinámicas de red y seguridad para los usuarios y grupos de Azure

#### **Rendimiento de la aplicación DNS**

Ofrezca mejores experiencias de usuario con un DNS más rápido para las aplicaciones de Azure

#### **Tolerancia a fallos y recuperación ante desastres**

Garantizar resiliencia con NIOS ofrece tolerancia a los fallos y respaldo para la recuperación ante desastres con vistas a garantizar la resiliencia de la plataforma

## DNS E IPAM DE INFOBLOX PARA MICROSOFT AZURE

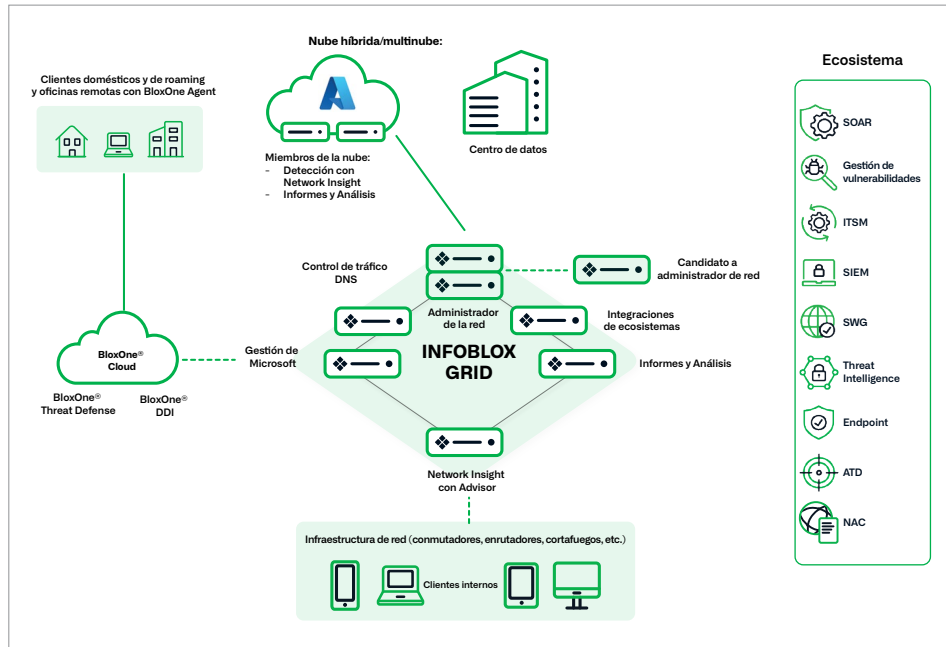


Figura 1: Los servicios de red virtualizados de Infoblox para Azure se implementan en entornos de nube híbrida o multinube

### Defensa adaptativa

Utilice Azure Sentinel SIEM y SOAR para obtener datos contextuales y una respuesta de seguridad más rápida

### Detección y corrección de amenazas

Integre BloxOne® Threat Defense para detectar, bloquear y resolver amenazas de seguridad

### Inteligencia de red contextual

Reciba alertas, datos históricos y actuales, y análisis para controlar mejor la red

### Implementación flexible y actualizaciones sencillas

Garantice la flexibilidad, la escalabilidad y el tiempo de actividad del servicio con actualizaciones de software optimizadas en dispositivos diseñados específicamente para implementaciones in situ, virtuales y en la nube.

### Soluciones ecológicas

Ahorre energía y proteja el medio ambiente reduciendo el número de servidores y dispositivos

## ESPECIFICACIONES DE LA PLATAFORMA DE DNS E IPAM DE INFOBLOX PARA MICROSOFT AZURE

Modelo de software	Consultas DNS por segundo* (QPS)	Concesiones DHCP por segundo*(LPS)	Tipo de instancia de Azure	Modelo de detección de redes (ND)	Informes (RPT)	
TE-926	33 750	225	Standard_E4s_v3	ND-906	✓	N/A
TE-1516	67 500	400	Standard_E8s_v3	ND-1516	N/A	N/A
TE-1526	112 500	675	Standard_E16s_v3	ND-1526	✓	N/A
TE-2326	250 000	1200	Standard_E20s_v3	ND-2326	✓	N/A
TE-4126	450 000	1500	Standard_E32s_v3	ND-4126	✓	N/A
TR-v5005	N/A	N/A	Personalizar	N/A	✓	

## ESPECIFICACIONES DE LA PLATAFORMA DE DNS E IPAM DE INFOBLOX PARA MICROSOFT AZURE HUB

Modelo de software	Consultas DNS por segundo* (QPS)	Concesiones DHCP por segundo*(LPS)	Tipo de instancia de Azure Hub	Modelo de detección de redes (ND)	Informes (RPT)	
TE-926	33 750	225	Standard_E4_v3	ND-906	⊖	N/A
TE-1516	67 500	400	Standard_E8_v3	ND-1516	N/A	N/A
TE-1526	112 500	675	Standard_E16_v3	ND-1526	⊖	N/A
TE-2326	250 000	1200	⊖	ND-2326	⊖	N/A
TE-4126	450 000	1500	⊖	ND-4126	⊖	N/A
TR-v5005	N/A	N/A	N/A	N/A	⊖	

\*Los números de rendimiento indicados son solo de referencia. Representan los resultados de las pruebas de laboratorio en un entorno controlado centrado en los servicios de protocolo individuales. La habilitación de protocolos, servicios, porcentaje de aciertos de caché adicionales para DNS recursivo y variables de entorno del cliente afectará al rendimiento. Para diseñar y dimensionar una solución para un entorno de producción, póngase en contacto con su arquitecto de soluciones Infoblox local.

☑ Compatible / incluido

⊖ Esta función es compatible con este modelo, pero no con esta plataforma.

N/A La función no es compatible con este modelo o plataforma

## CONTACTAR CON NOSOTROS

Para obtener más información o respuestas sobre DDI, DNS, IPAM y otros servicios de red de Infoblox para Microsoft Azure, póngase en contacto con el equipo de su cuenta en Infoblox, consulte nuestras [integraciones de red crítica](#) o [contáctenos](#) en Infoblox.com.



Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

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

+1.408.986.4000  
[www.infoblox.com](http://www.infoblox.com)