

# VISIBILIDAD SIN PRECEDENTES PARA LA GESTIÓN DE REDES CON NETWORK INSIGHT DE INFOBLOX

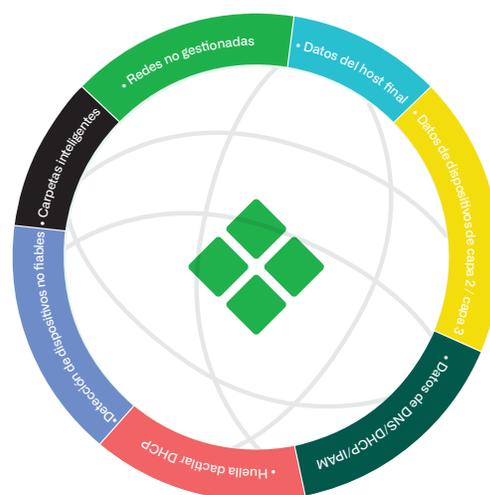
## RESUMEN DEL PRODUCTO

**Network Insight de Infoblox ofrece inteligencia de red procesable al integrar datos de DNS, DHCP e IPAM con datos de infraestructura de red, lo que proporciona una visibilidad sin precedentes en toda la red.**

Automatiza la recopilación de información en todos los dispositivos de capa 2 y capa 3 conectados a la red, lo que permite a los administradores de red recopilar, correlacionar y ver fácilmente los datos de la red para aumentar la agilidad, reducir el riesgo y disminuir los costes.

Los ingenieros, administradores y arquitectos de redes reciben grandes cantidades de datos e información a través de infinidad de registros, informes, alertas y notas anecdóticas. Tienen que priorizar rápidamente los problemas del día a día y llevar a cabo una variedad de tareas operativas, además de resolver problemas tanto notificados como supuestos, todo ello frente al escalado dinámico que respalda una amplia gama de servicios. Estas tareas se complican aún más a causa de la disparidad de los datos, a veces contradictorios, dado que cada uno de los silos operativos utiliza su propio conjunto de herramientas para recopilar y analizar datos, y planificar acciones con ellos.

Para afrontar estos desafíos, Network Insight de Infoblox ofrece inteligencia de red procesable mediante la integración de datos del Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) y la gestión de direcciones IP (IPAM) con los datos de la infraestructura de red, lo que ofrece una visibilidad de toda la red sin precedentes. Los administradores de red pueden recopilar información fácilmente, analizarla y tomar las medidas adecuadas para administrar mejor sus redes y prestar servicios de red. Network Insight también mejora la seguridad, reduce el riesgo de interrupciones del servicio y desmantela los silos operativos en TI.



## RECOPILAR. ANALIZAR. ¡TOMAR MEDIDAS!

### Recopilar la información adecuada

Network Insight automatiza la recopilación de información en todos los dispositivos de capa 2 y capa 3 —como enrutadores, conmutadores, cortafuegos y equilibradores de carga— conectados a la red y puede ajustarse a intervalos, calendarios, redes objetivo, rangos de IP y direcciones IP individuales. Si bien la tarea de recopilación de información está automatizada, también está disponible un mecanismo a demanda. Los datos recopilados contienen:

- Datos de dispositivos de infraestructura de red
- Datos de la interfaz de infraestructura de red
- VMware ESXi/datos de virtualización

Para garantizar que los datos de los dispositivos se recopilen correctamente, se utilizan varias técnicas, entre ellas:

- Protocolo simple de administración de redes (SNMP)
- Barridos de ping inteligentes de subredes IPv4
- Análisis de NetBIOS
- Recopilación de datos de puertos de conmutación
- Análisis de puertos
- Barridos de ping completos
- Actualización automática de ARP antes del sondeo del puerto del conmutador

Los intervalos de sondeo para la recopilación de datos de los puertos de conmutación son definidos por el usuario y pueden configurarse con una frecuencia horaria, diaria, semanal o mensual con varios parámetros, como «l sondeo horario comienza 10 minutos después de la hora en punto» o «cada 2 días». Los equipos de redes pueden utilizar este mecanismo de programación flexible para optimizar la recopilación de datos en función de sus necesidades específicas, así como para controlar el uso del ancho de banda en horas pico de servicio. Los administradores de redes también pueden acelerar la detección de activos para ahorrar tiempo o reducir la frecuencia de detección para no sobrecargar el sistema.

Los datos de IPAM, junto con los datos de DNS y DHCP en tiempo real, se integran con los datos de los dispositivos de infraestructura y se presentan en Network Insight. En el mercado actual, hay productos que recopilan datos de dispositivos y otros que proporcionan datos de IPAM, DNS y DHCP; Network Insight de Infoblox hace ambas cosas, con lo que ofrece datos de IPAM inteligentes y flujos de trabajo integrados en una misma GUI.

## Analizar: mejores datos significan mejores decisiones

La interfaz gráfica de usuario (GUI) de Network Insight, de navegación sencilla con datos integrados, permite a los administradores de redes obtener conclusiones rápidas sobre las tareas y los problemas de red. Las redes, los dispositivos y los servidores finales —gestionados actualmente o no— son visibles en la GUI de Network Insight. La información sobre la administración de los puertos y su estado operativo, las características de la interfaz, el estado de los troncales, las redes de área local virtual asignadas y las redes de área local virtuales extensibles (VXLAN) también están disponibles. Los datos del host final proporcionan información sobre el tipo de activo, la interfaz a la que se conecta, sus direcciones MAC e IP y las VLAN asignadas.

Las visualizaciones transversales de datos se logran mediante carpetas inteligentes, que reducen el alcance de los datos presentados a través de filtros y criterios lógicos. Se pueden aplicar más de 50 filtros diferentes con un número prácticamente infinito de combinaciones. La segmentación de los datos en carpetas inteligentes crea una lógica eficaz, ya que llega al núcleo de lo que supervisan y controlan los equipos de red.

## ¡Tomar medidas!

Cuando los datos de la red se presentan de forma lógica en la GUI y se envían automáticamente a carpetas inteligentes, los profesionales de redes pueden tomar las medidas necesarias para ejecutar las tareas en curso. Las vistas de datos y los flujos de trabajo integrados ofrecen ventajas empresariales críticas, como mayor agilidad, menores riesgos y una reducción de costes gracias a las mejoras procedimentales, además de desmantelar silos operativos.

IP Address	Name	Device Type	Model	Vendor	Device Version	Location	Description	Discover Now	Managed	Active Use
198.18.16.129	unknown	Power Controller		HP				No	0	
198.18.16.127	unknown	Power Controller		HP				No	0	
10.66.100.1	core-dems-01	Router		Cytera		Cytera	VyOS 1.3-rollin...	Yes	0	
198.18.0.254	i05-rb-discov...	Switch-Router	N3K23048TP1GE	Cisco	7.0(3)77(1)		*Not so secret... Cisco NX-OS2...	No	0	
198.18.200.30	int27-primary-a...	Security Manager	IntVnIQ	Cisco			Linknow Cisco Identity S...	No	0	
192.168.1.82	gm1p2	vN10S	ND-V805	Infoblox	8.6.2-49947		Sunnyvale Infoblox ND-V8...	Yes	0	
192.168.1.5	demagn1	vN10S	IB-V825	Infoblox	8.6.2-49947		Santa Clara Infoblox IB-V82...	Yes	0	
198.18.16.122	unknown	Power Controller		HP				No	0	
198.18.0.252	PA-VM	Firewall	PA-VM	PaloAltoNetworks	11.0.1		isolated environ... Palo Alto Netw...	No	0	
198.18.200.15	int1_switch	Switch	PowerConnect ...	Dell	3.3.3.9		PowerConnect ...	No	0	
198.18.200.20	me-3060-48-p...	Router	WS-C3660X-48...	Cisco	12.2(53)SE2		Cisco IOS Soft...	No	0	
192.168.1.81	gm1p1	vN10S	ND-V805	Infoblox	8.6.2-49947		Santa Clara Infoblox ND-V8...	Yes	0	
192.168.1.10	demagn1	vN10S	IB-V4025	Infoblox	8.6.2-49947		Santa Clara Infoblox IB-V40...	Yes	0	
198.18.194.110	PA-3020	Firewall	PA-3020	PaloAltoNetworks	9.1.11-A2		colo Palo Alto Netw...	No	0	
10.66.100.91	unknown	Router						No	0	
192.168.1.25	demagn3	vN10S	IB-V1425	Infoblox	8.3.8		INFO-SC-rbJ4 Infoblox IB-V14...	Yes	0	
198.18.300.16	unknown	Switch	Powerconnect	Dell	4.9.1.4		Powerconnect	No	0	

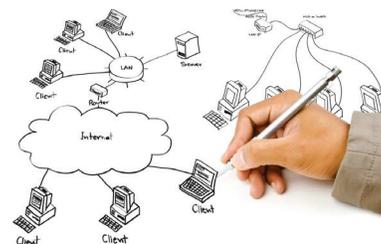
Figura 1: Datos de infraestructura de red en la pestaña «Dispositivos»

## Mejoras de los flujos de trabajo

Network Insight reduce el riesgo, el tiempo y el coste asociados a tareas específicas en varias áreas.

### 1. Validación de la implementación de nuevas redes y activos

Las redes ya no son conexiones estáticas de cobre, fibra y hardware. La introducción de la nube, la virtualización y la movilidad provocan que las redes actuales sean más dinámicas que nunca. Construir redes y luego desmantelarlas es una práctica común entre los administradores de redes. Estas actividades respaldan a las empresas en rápido crecimiento a medida que amplían su presencia geográfica mediante sucursales, crean entornos DevOps y dan soporte a una amplia variedad de usuarios externos con necesidades distintas. Los equipos que diseñan estas redes tienen en cuenta una serie de consideraciones, como el uso específico, la capacidad, los flujos de tráfico de red esperados, los requisitos de redundancia y otros parámetros de diseño. El despliegue final puede verse fácilmente mediante Network Insight, lo que facilita a los administradores de redes confirmar que la red desplegada coincide con el diseño original.



### 2. Localización y reparación de posibles brechas de seguridad

Casi el 60% de las organizaciones encuestadas creen que la falta de visibilidad de la red supone un riesgo alto o muy alto para la organización.<sup>1</sup> Esta falta de visibilidad permite a los usuarios personalizar su entorno de trabajo de cualquier modo, desde impresoras privadas hasta routers domésticos, y también encubre a cualquiera con intenciones maliciosas que acceda a la red. Una visibilidad clara de toda la red permite mejorar la seguridad y reduce las interrupciones del servicio.

Veamos, por ejemplo, una empresa en la que, en dos ocasiones distintas, dos sucursales perdieron la conectividad con el centro de datos principal y el único síntoma fue que los usuarios de sedas sucursales no podían acceder a las aplicaciones corporativas del centro de datos de la sede.

Para solucionar este problema, se reunió a un equipo de profesionales de TI durante todo un día para comparar sus datos operativos en silos, hacer conjeturas y señalar posibles culpables. Cada equipo se centró en excluir su responsabilidad como causa raíz, en lugar de colaborar para resolver el problema.

El equipo determinó que los ordenadores de las sucursales tenían direcciones IP que no pertenecían a las redes definidas en los enrutadores que prestaban servicio a esas oficinas. Todas las direcciones IP de los dispositivos comenzaban por 192.168 en vez de por el valor 10.10 esperado. Al final, se detectó un router doméstico conectado, que utilizaba su propio DHCP para conceder direcciones IP en la sucursal. Este problema se habría detectado de inmediato con Network Insight.

### 3. Gestión de fusiones, adquisiciones y otras expansiones

Cuando las corporaciones se fusionan a través de la adquisición de empresas, adoptar una nueva red puede ser una tarea complicada, plagada de direcciones IP superpuestas, carencias de documentación del diseño original y otras lagunas de información. Sin las herramientas y la visibilidad adecuadas, en algunas adquisiciones, descifrar los pormenores y ejecutar un plan de fusión de redes en una sola red cohesiva puede llevar más de nueve meses. Las empresas que han adquirido otras periódicamente y han adoptado sus redes tienen el lujo de contar con la experiencia pasada para guiar sus procesos y perfeccionar los pasos necesarios, pero incluso para ellas, no todas las situaciones son iguales. En empresas que tal vez afronten este proceso solo una o dos veces, se insiste demasiado en sacar adelante el trabajo dedicando poco o nada



**“** Network Insight nos ha resultado muy útil para descubrir múltiples redes. También nos da cierta perspectiva en lo que respecta a la seguridad. Cuando recibo preguntas de seguridad sobre lo que se sabe de una dirección IP, puedo ir a buscarla y ver qué información de identificación del host de DHCP está registrada y qué información de la infraestructura de red revela el agente de detección.

**Brent Hetherwick,**  
Ingeniero sénior de sistemas,  
Adobe Systems

de tiempo a desarrollar un proceso eficiente y funcional. Network Insight integra el proceso de recopilación de datos y reasignación en un mismo conjunto de soluciones, con flujos de trabajo que permiten desglosar y reintroducir una red adquirida, todo desde un solo panel. Esta integración puede reducir un proyecto de nueve meses a dos semanas.

#### 4. Mejorar la detección, la visibilidad y la gestión de SDN y SD-WAN

Network Insight amplía la detección, la visibilidad y el control con integraciones para las principales redes definidas por software (SDN, como Cisco ACI, Juniper Mist y Silver Peak) y las redes de área extensa definidas por software (SD-WAN, como Cisco Meraki y Viptela). Al integrar las API de Infoblox con el software de los proveedores, Network Insight unifica la visibilidad de las direcciones IP, flexibiliza la implementación y mejora la coherencia, la experiencia del usuario y la gestión de redes remotas y sucursales.



#### 5. Desmantelar silos operativos en las tecnologías de la información

En las organizaciones de TI actuales, surgen silos operativos de forma natural. Estos silos se crean en respuesta al nivel de conocimientos que deben tener los expertos en la materia para llevar a cabo el trabajo complicado en sus áreas respectivas. Sin embargo, la naturaleza dinámica de las redes actuales requiere cohesión de los servicios de TI, por lo que es preciso compartir datos fidedignos. En el plano operativo, la empresa debe pagar un «precio» por estos silos sintéticos. Sin embargo, Network Insight puede desmantelar los silos, ya que proporciona una administración molecular basada en roles, de modo que diferentes equipos pueden usar la misma herramienta y los mismos datos integrados. Así, los administradores de redes responsables de IPAM cuentan con visibilidad completa del uso de las direcciones IP asignadas en otros equipos, mientras que los equipos propios disponen de los permisos y capacidades para administrar su propio rango de IP en Network Insight. La colaboración y la visibilidad entre equipos son algunas de las ventajas sencillas, pero potentes, que ofrece Network Insight.

## IMPLEMENTACIÓN DE LA SOLUCIÓN

### La Fundación: Infoblox Grid

Infoblox Grid permite que una colección de dispositivos funcione y se administre como un solo sistema unificado. Un dispositivo de Infoblox asignado como Grid Manager envía datos de configuración global y actualiza a los Grid Members, supervisa las operaciones de estos miembros y sincroniza sus cambios con la base de datos central.

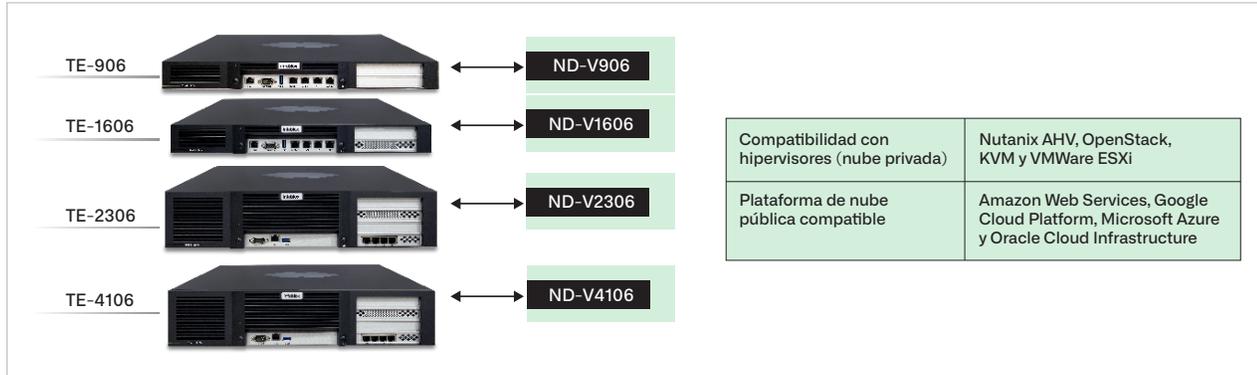
Network Insight aprovecha la tecnología Infoblox Grid™ para proporcionar opciones de implementación flexibles. Tanto si utiliza un enfoque centralizado como una arquitectura distribuida, Network Insight puede configurarse en dispositivos TrinziC X6 en función de su estrategia de red.

### Detección de direcciones IP a través de SDN y SD-WAN

Integre las principales redes definidas por software (SDN) y redes de área extensa (SD-WAN) para detectar y administrar direcciones IP en sucursales y oficinas remotas, lo que ofrece mayor flexibilidad de implementación, visibilidad unificada, control y una experiencia de usuario uniforme.

## Opciones de plataformas

Los dispositivos Trinzi X6 con Network Insight ofrecen una amplia gama de modelos diseñados para ofrecer mayor rendimiento, capacidad y disponibilidad. También proporcionan flexibilidad de despliegue como dispositivos físicos o de software.



## Network Insight de Infoblox mejora la agilidad y reduce riesgos y gastos operativos

Network Insight ofrece inteligencia de red procesable por medio de integrar, en tiempo real, datos de DNS, DHCP e IPAM con datos de infraestructura de red para proporcionar una visibilidad sin precedentes en toda la red. Recoger y correlacionar estos datos permite a los administradores de redes recopilar fácilmente la información necesaria, analizarla y luego tomar las medidas adecuadas para administrar mejor sus redes, validar diseños, efectuar un aprovisionamiento eficaz, solucionar problemas y prestar servicios de red. Network Insight mejora la toma de decisiones, reduce riesgos de seguridad e interrupción del servicio, y desmantela silos operativos en TI.

Para obtener más información, visite [www.infoblox.com/NetworkInsight](http://www.infoblox.com/NetworkInsight) o póngase en contacto con [sales@infoblox.com](mailto:sales@infoblox.com).

1 2020 SANS Network Visibility and Threat Detection Survey



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)