NOTAS DE LA SOLUCIÓN

CREACIÓN DE UNA INFRAESTRUCTURA DE RED ÁGIL Y RESILIENTE

Las organizaciones están modernizando sus redes para hacer frente a los retos que plantean el panorama normativo en constante crecimiento y las amenazas en constante evolución. Muchas empresas confían en entornos Microsoft para sus operaciones críticas, pero es difícil garantizar la seguridad de la red y la disponibilidad de las aplicaciones con capacidades limitadas. Las frecuentes interrupciones e infracciones causadas por las limitaciones del sistema con la infraestructura de Microsoft subrayan la necesidad de soluciones DNS específicas para redes críticas.

MODERNIZACIÓN CRÍTICA DE LA RED

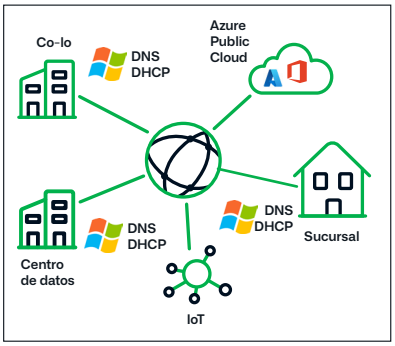
La infraestructura de red consta de muchos componentes: cortafuegos, enrutadores, conmutadores, dispositivos Wi-Fi, servidores de nombres de dominio, servidores DHCP y otros. La mayoría de los elementos de las infraestructuras críticas ya se están actualizando a versiones modernas de hardware o software. ¿Qué pasa con los servidores de nombres de dominio y los servidores DHCP? ¿Sus servicios de red centrales siguen siendo heredados? Los servicios de red heredados, los programas gratuitos como los de Microsoft o las soluciones "hágalo usted mismo" (DIY) son inconexos, lentos y están expuestos a riesgos de seguridad, lo que provoca interrupciones masivas.

HOY EN DÍA, LO GRATIS SALE CARO

Una infraestructura de red crítica típica está distribuida en centros de datos, muchas sucursales, entornos multinube y centros de servicios de coubicación. Es difícil gestionar este tipo de infraestructura diversa con herramientas de bajo coste debido a las limitaciones del sistema, la visibilidad fragmentada y la ineficacia. Aunque los gastos de capital iniciales puedan parecer menores, los gastos operativos en los que incurriría con la infraestructura de Microsoft o cualquier otra herramienta gratuita compensarán las ventajas "gratuitas". Estas herramientas aumentan el riesgo de errores e interrupciones debido a las configuraciones y soluciones manuales.

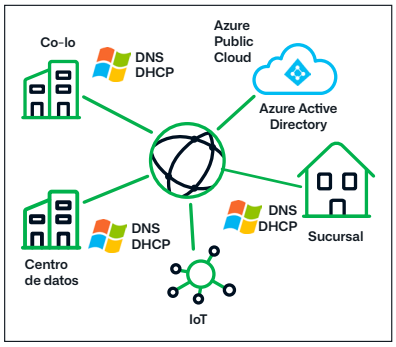
- **Limitaciones de escala:** no hay un único punto de gestión y no puede escalar para crecer debido a las limitaciones del sistema; la consola de gestión de Microsoft no puede escalar más allá de 8-10 servidores por perfil.
- **Sin vista centralizada:** la consolidación de registros (auditoría y servicio) requiere la creación de scripts y, sin la integración de DNS y DHCP, el IPAM no tiene autoridad.
- **Falta de funciones avanzadas:** no requiere DNS Anycast ni recursión por configuración de servidor, lo que aumenta el tiempo de configuración.
- **Configuración por servidor:** la gestión de zonas de los servidores miembros no está disponible en la integración de Azure, y es necesario borrar la caché para nuevas actualizaciones o solución de problemas.
- **Impacto en el rendimiento:** la replicación de DNS y la activación del registro de depuración retrasan y degradan el rendimiento.

> Coste anual estimado de 3300 dólares por servidor, es decir, más de **1,3 millones** al año
>
> - Arquitecto de redes, empresa multinacional de petróleo y gas.



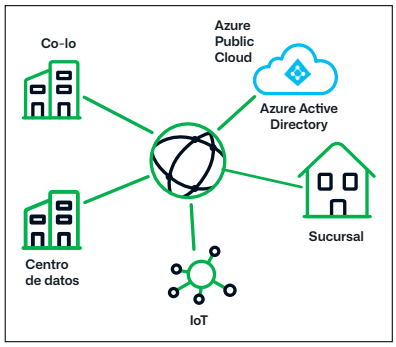
Microsoft AD Enterprise presenta limitaciones de escalabilidad, falta de funciones avanzadas y lagunas de seguridad.

Figura 1: Microsoft AD Enterprise



Azure AD Enterprise tiene una visibilidad fragmentada, una seguridad limitada y carece de gestión centralizada.

Figura 2: Azure AD Enterprise



Infoblox DDI Enterprise ofrece funciones completas, como visibilidad, automatización y control, además de escalabilidad, seguridad y resistencia.

Figura 3: Infoblox DDI Enterprise

LA SOLUCIÓN DE INFOBLOX PARA UNA VERDADERA RESILIENCIA Y AGILIDAD

RACIONALIZA LAS OPERACIONES DE MISIÓN CRÍTICA

Aproveche la solución DDI (DNS, DHCP e IPAM) especialmente diseñada de Infoblox y obtenga visibilidad, automatización y control centralizados completos para sus redes críticas.

Utilizar Infoblox implica:

- La eliminación del tiempo de inactividad causado por parches, actualizaciones y errores de configuración
- La ausencia de pruebas periódicas, eliminando los errores humanos y reduciendo significativamente el riesgo de interrupciones
- La presencia de seguridad "shift-left", que proporciona una sólida protección de la capa DNS y detecta los ciberataques en las fases iniciales del ciclo
- La detención de la exfiltración de datos DNS y de otras vulnerabilidades, como los algoritmos de generación de dominios y los dominios de imitación

> "La solución Infoblox supuso un ahorro del **40%** respecto a nuestra implementación de Microsoft".
>
> Arquitecto de redes, empresa multinacional de petróleo y gas.

Según un estudio de clientes basado en el ROI realizado por una empresa analista externa, el ahorro anual con Infoblox incluye:

Reducción del **69%** del tiempo dedicado a los cambios típicos de configuración de DNS/DHCP	Reducción del **70%** del tiempo dedicado a solucionar problemas de interrupciones de DNS/DHCP	Reducción de más del **90%** del tiempo de recopilación de datos de dispositivos de red	Reducción del **98%** de la formación inicial y continua de los equipos de red

CONCLUSIÓN

El DDI es fundamental para cualquier empresa que dependa de una red para sus operaciones. Aunque la infraestructura de Microsoft puede parecer una opción atractiva para gestionar los servicios DDI debido a su rentabilidad, puede resultar una propuesta arriesgada para las empresas que dependen de estos servicios para sus operaciones críticas. Infoblox ofrece una solución DDI resistente, fiable y especialmente diseñada para su empresa.

infoblox.

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

+1.408.986.4000
www.infoblox.com

Versión: 20230803v1