infoblox®

ARQUITECTURA DE REFERENCIA DE INFOBLOX® Y MEJORES PRÁCTICAS PARA NIOS DDI

ANÁLISIS PRÁCTICO DE LA IMPLEMENTACIÓN DE LOS SERVICIOS DNS Y DHCP CON LOS PRODUCTOS INFOBLOX NIOS DDI E INFOBLOX THREAT DEFENSE™ EN UNA RED PARA AUMENTAR LA SENCILLEZ, LA SEGURIDAD Y LA ESCALABILIDAD.

ÍNDICE

RESUMEN

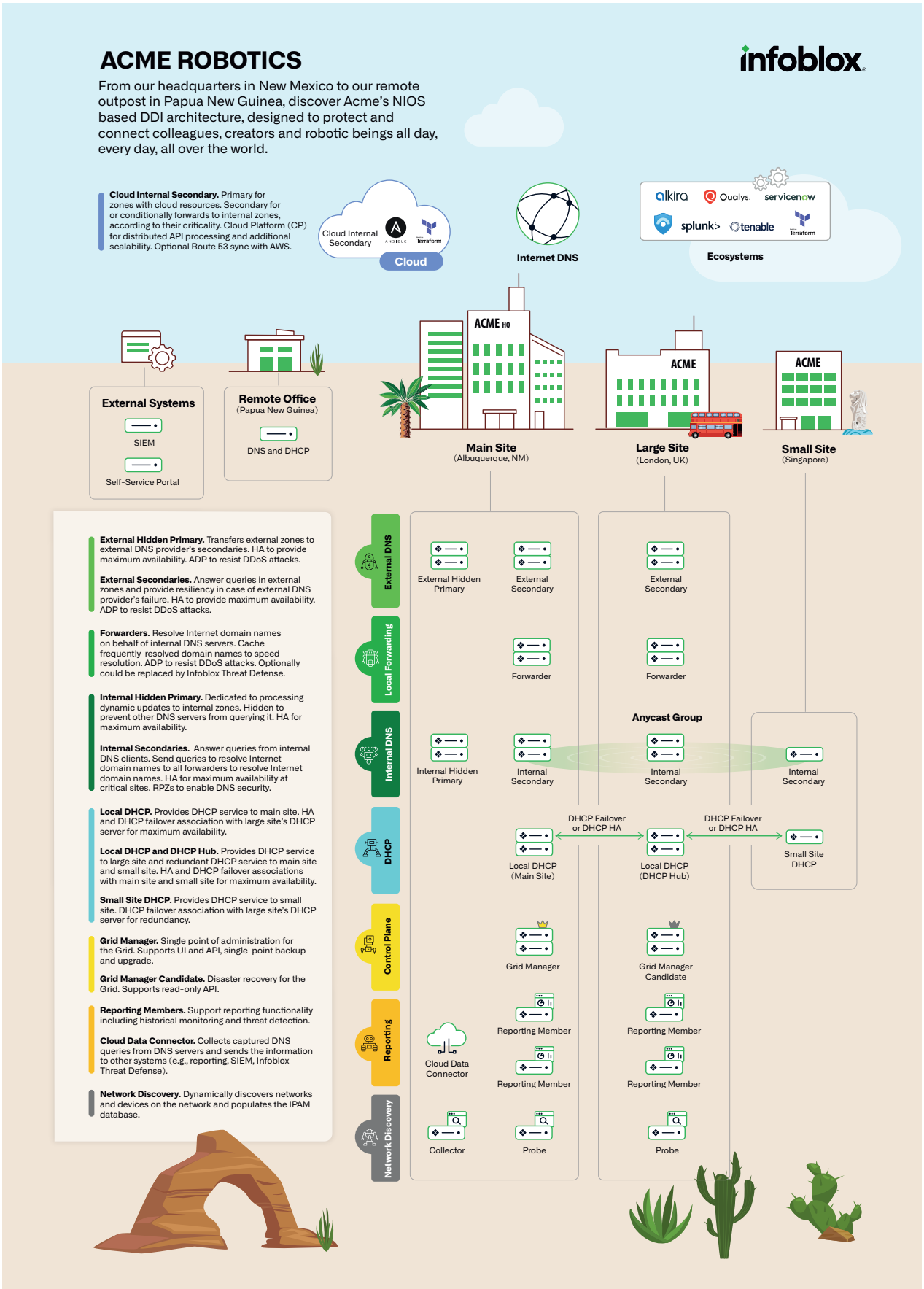
Esta guía, desarrollada a partir de documentos técnicos redactados por Cricket Liu y la Junta de Revisión de Arquitectura de Infoblox® (ARB), destaca los esfuerzos colaborativos de nuestro organismo interno responsable de examinar todos los diseños no triviales producidos por los arquitectos de soluciones de Infoblox. Además de la ARB, varios expertos técnicos de Infoblox aportan sus conocimientos especializados para garantizar que nuestras soluciones sean sólidas, innovadoras y estén alineadas con las mejores prácticas del sector.

Los dispositivos NIOS son un vehículo ideal para proporcionar servicios de Domain Name System (DNS) y Dynamic Host Configuration Protocol (DHCP), y posteriormente presentaron una arquitectura para respaldar esos servicios y servicios de seguridad de manera eficiente, confiable y segura. Esta guía amplía esos documentos técnicos para abarcar varios nuevos desarrollos en el mundo de la tecnología de la información:

- El uso de DNS como una herramienta crítica de seguridad
- El auge de las nubes públicas y la informática en la nube
- La creciente importancia de la TI de autoservicio, impulsada por servicios como ServiceNow
- La expansión de las redes corporativas para incluir más oficinas pequeñas y remotas
- La necesidad de integración con los sistemas de gestión de eventos e información de seguridad (SIEM) y otras tecnologías de seguridad

Para demostrar cómo dar soporte a estos nuevos desarrollos, presentaremos un caso práctico de una empresa y su red corporativa, y desarrollaremos una arquitectura de DNS, DHCP y gestión de direcciones IP (DDI) para satisfacer sus requisitos basándonos en las mejores prácticas del sector. El diseño tendrá en cuenta los requisitos de la empresa en cuanto a disponibilidad, rendimiento, seguridad y recuperación ante desastres, compatibilidad con la computación y las aplicaciones basadas en la nube, y la integración con los sistemas internos y basados en la nube.

Mientras lee este documento, piense en su propia infraestructura de DDI. ¿Ofrece el mismo nivel de resiliencia, rendimiento y seguridad? ¿Hay aspectos de este diseño que podría adaptar para su propio uso?


ACME ROBOTICS
infoblox.
From our headquarters in New Mexico to our remote outpost in Papua New Guinea, discover Acme's NIOS based DDI architecture, designed to protect and connect colleagues, creators and robotic beings all day, every day, all over the world.
Cloud Internal Secondary. Primary for zones with cloud resources. Secondary for or conditionally forwards to internal zones, according to their criticality. Cloud Platform (CP) for distributed API processing and additional scalability. Optional Route 53 sync with AWS.
Cloud Internal Secondary
Cloud
Internet DNS
alkira
Qualys.
servicenow
splunk>
tenable
Terraform
Ecosystems
External Systems
SIEM
Self-Service Portal
Remote Office
(Papua New Guinea)
DNS and DHCP
ACME HQ
Main Site
(Albuquerque, NM)
ACME
Large Site
(London, UK)
ACME
Small Site
(Singapore)
External Hidden Primary. Transfers external zones to external DNS provider's secondaries. HA to provide maximum availability. ADP to resist DDoS attacks.
External Secondaries. Answer queries in external zones and provide resiliency in case of external DNS provider's failure. HA to provide maximum availability. ADP to resist DDoS attacks.
Forwarders. Resolve Internet domain names on behalf of internal DNS servers. Cache frequently-resolved domain names to speed resolution. ADP to resist DDoS attacks. Optionally could be replaced by Infoblox Threat Defense.
Internal Hidden Primary. Dedicated to processing dynamic updates to internal zones. Hidden to prevent other DNS servers from querying it. HA for maximum availability.
Internal Secondaries. Answer queries from internal DNS clients. Send queries to resolve Internet domain names to all forwarders to resolve Internet domain names. HA for maximum availability at critical sites. RPZs to enable DNS security.
Local DHCP. Provides DHCP service to main site. HA and DHCP failover association with large site's DHCP server for maximum availability.
Local DHCP and DHCP Hub. Provides DHCP service to large site and redundant DHCP service to main site and small site. HA and DHCP failover associations with main site and small site for maximum availability.
Small Site DHCP. Provides DHCP service to small site. DHCP failover association with large site's DHCP server for redundancy.
Grid Manager. Single point of administration for the Grid. Supports UI and API, single-point backup and upgrade.
Grid Manager Candidate. Disaster recovery for the Grid. Supports read-only API.
Reporting Members. Support reporting functionality including historical monitoring and threat detection.
Cloud Data Connector. Collects captured DNS queries from DNS servers and sends the information to other systems (e.g., reporting, SIEM, Infoblox Threat Defense).
Network Discovery. Dynamically discovers networks and devices on the network and populates the IPAM database.
External DNS
Local Forwarding
Internal DNS
DHCP
Control Plane
Reporting
Network Discovery
External Hidden Primary
External Secondary
External Secondary
Forwarder
Forwarder
Anycast Group
Internal Hidden Primary
Internal Secondary
Internal Secondary
Internal Secondary
DHCP Failover or DHCP HA
DHCP Failover or DHCP HA
Local DHCP (Main Site)
Local DHCP (DHCP Hub)
Small Site DHCP
Grid Manager
Grid Manager Candidate
Reporting Member
Reporting Member
Cloud Data Connector
Reporting Member
Reporting Member
Collector
Probe
Probe

LA EMPRESA

Recientemente se nos solicitó diseñar una nueva arquitectura del DNS para una empresa multinacional, ACME Robotics. ACME es un conocido proveedor de dispositivos robóticos que desempeñan una amplia gama de funciones. ACME Robotics se dedica a la fabricación, comercialización y distribución, y cuenta con una organización de ventas y asistencia técnica.

El mercado de la empresa es mundial, pero se concentra especialmente en el suroeste de Estados Unidos.

Esta empresa dispone de cuatro tipos de centros conectados a su red corporativa:

1. La sede de ACME en Albuquerque, Nuevo México, alberga el mayor número de usuarios (unos 2000). La sede también aloja el principal centro de datos de la empresa.
2. Un centro de grandes dimensiones en Londres, Inglaterra, alberga aproximadamente a 500 usuarios locales.
3. Los centros pequeños, incluido el de Singapur, suelen dar servicio a 100 usuarios o menos. Los centros pequeños se dividen en regiones geográficas, cada una respaldada por una oficina regional. Cada centro pequeño está conectado a la red corporativa a través de un enlace a la oficina regional que lo respalda.
4. Los centros remotos suelen admitir a menos de 24 usuarios. Los centros remotos están conectados a internet y a la red corporativa a través de una conexión VPN o SD-WAN.

La empresa tiene una presencia sustancial en internet, ya que utiliza la red para comercializar sus productos. Para ofrecer sus servicios, utiliza dos nubes públicas, AWS y Azure. En cada nube se ejecutan varias aplicaciones, algunas de las cuales requieren acceso a recursos internos. El aprovisionamiento en la nube se automatiza mediante Terraform o Ansible, según laaplicación.

La empresa utiliza ServiceNow para que los empleados soliciten cambios de TI, incluidos los de DNS y DHCP. Ejecuta un SIEM interno y, debido a la industria en la que opera, tiene la obligación de registrar y archivar datos de DNS pasivos (pDNS).

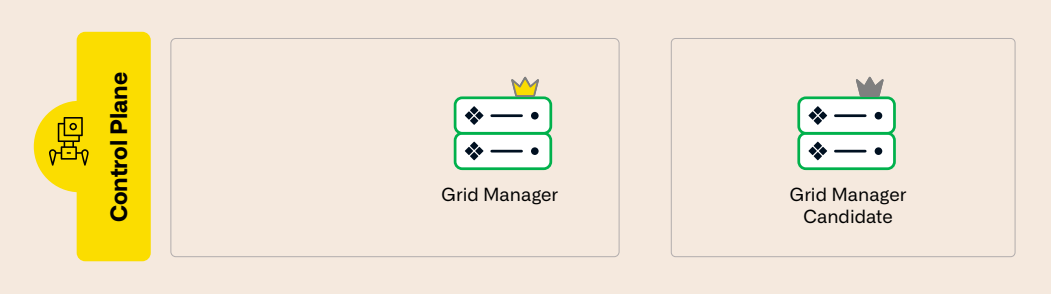
El personal de soporte de TI de la empresa está distribuido entre la sede central y los centros grandes. Cada oficina regional cuenta con un empleado de TI, que proporciona principalmente asistencia local para ordenadores de sobremesa y portátiles, y actúa como «ojos y manos» remotos del personal de la sede central.

La empresa permite a los empleados llevar dispositivos propios al trabajo, pero los segrega en redes de invitados. En el diseño se ha tenido en cuenta el número medio de dispositivos por empleado y la carga transaccional que generan.

UNA NOTA IMPORTANTE ACERCA DEL TAMAÑO

Un aspecto importante de la arquitectura que no cubrimos en este diseño ni en este documento es el dimensionamiento. Para garantizar que los servidores DNS y DHCP ofrezcan el rendimiento necesario para atender la carga de la empresa, esta tendría que medir o al menos estimar las tasas de transacción de DNS y DHCP de cada uno de los servidores del diseño y especificar los dispositivos que puedan soportar esa carga. Además, la empresa debería diseñar un «margen de maniobra» adecuado: capacidad adicional de los servidores para acomodar picos de carga imprevistos (p. ej., debido a una pérdida y posterior restablecimiento del suministro eléctrico en un centro). Por último, la empresa tendría que estimar y planificar el crecimiento a lo largo del tiempo: si planea llevar a cabo contrataciones agresivas, adquirir otras empresas o fusionarse con otro negocio, ello puede tener un impacto material en la carga de DNS y DHCP.

PLANO DE CONTROL



Comencemos con el plano de control de DDI, que en este diseño consta de un gestor de la red Grid (GM) en la sede central de Albuquerque y un candidato a gestor (GMC) en el centro de grandes dimensiones de Londres.

En una red Grid de Infoblox NIOS, el GM da soporte a la interfaz de usuario basada en web que utilizan los administradores y a la API que utilizan los desarrolladores para automatizar las tareas de DDI.[1] El GM también gestiona la comunicación y la sincronización con todos los miembros de Infoblox[2] en la red Grid; esos dispositivos admiten DNS, DHCP y otros servicios. Dada su función crítica, el GM debe desplegarse siempre mediante una pareja de dispositivos de alta disponibilidad (HA) del Protocolo de Redundancia de Enrutador Virtual (VRRP) en un mismo emplazamiento físico. El GM también puede utilizarse para actualizar o mantener las reglas de Protección avanzada del DNS (ADP) y los módulos de Threat Insight.

El GMC es una réplica del GM, que se sincroniza con el GM en tiempo real. Si los dos dispositivos que respaldan el rol del GM fallan, un administrador puede asignar al GMC el rol de GM con un simple comando. El nuevo GM asignado informará a los demás dispositivos de la red Grid y asumirá las funciones del anterior GM. Al igual que sucede con el GM, el GMC siempre debe desplegarse mediante una pareja de dispositivos HA VRRP en un mismo emplazamiento físico.

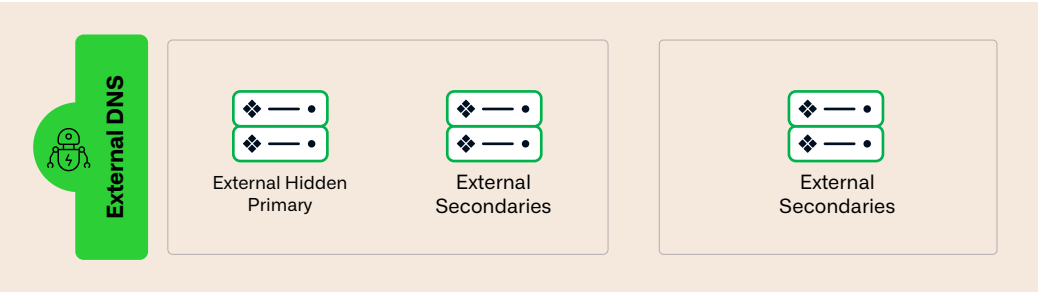
Las redes Grid de Infoblox admiten la designación de muchos GMC, pero esta empresa ha identificado Londres como su centro de recuperación ante desastres y, por lo tanto, solo alojará un GMC allí.

Hemos dicho que no abarcaríamos el dimensionamiento en el presente documento, pero es necesario añadir una nota sobre el dimensionamiento de los GMC: los GMC admiten la capacidad (muy útil) de gestionar llamadas API de solo lectura, lo cual puede ser útil, por ejemplo, para dar soporte a la integración con ServiceNow, que utiliza ACME. Al dimensionar los GMC, hay que tener en cuenta tanto la carga sobre el GM como la carga sobre el GMC de cualquier llamada API de solo lectura que gestionen. En caso de desastre, si asigna el GMC como GM, deberá poder gestionar la carga agregada del GM y su función anterior como GMC. Como alternativa, puede añadir uno o más GMC y dedicarlos a gestionar las llamadas API de solo lectura.

1 Con ciertas excepciones: consulte la sección «Nube» para obtener más detalles.

2 Tenga en cuenta que usamos el término «dispositivo» para hacer referencia a todos los dispositivos, ya sean físicos o virtuales. Estos últimos se ejecutan en casi todas las plataformas de virtualización y en nubes públicas.

DNS AUTORITATIVO EXTERNO



Los servidores del DNS autoritativo externo publicitan las zonas de la empresa en internet, permitiendo a los clientes y socios enviar correos electrónicos a las direcciones de la empresa, visitar el sitio web, acceder a las aplicaciones públicas, etc. Su papel es fundamental, ya que su disponibilidad se traduce directamente en ingresos, satisfacción del cliente y reputación corporativa.

La infraestructura del DNS autoritativo externo consta de tres miembros: uno primario oculto en la sede de Albuquerque, uno secundario en la sede y otro en el centro de grandes dimensiones de Londres. Cada miembro está compuesto por una pareja de dispositivos HA VRRP. Esto permite a los administradores actualizar los servidores DNS sin provocar tiempo de inactividad, lo cual podría ser necesario si se encontrara un error o una vulnerabilidad en BIND, por ejemplo, o si se necesitan dispositivos de mayor tamaño a medida que crezca la empresa.

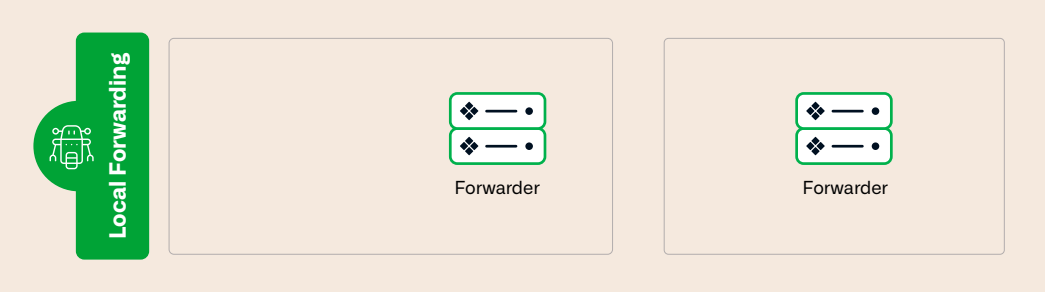
La infraestructura externa autoritativa de DNS **ampliada** también incluye los servidores DNS gestionados por un proveedor de alojamiento de DNS basado en Internet. Los proveedores de alojamiento de DNS, como Cloudflare y UltraDNS de Neustar, proporcionan muchos servidores DNS en Internet, una infraestructura de DNS ampliamente distribuida que sería difícil de gestionar para la empresa y costosa de operar. Sin embargo, los proveedores de alojamiento de DNS también experimentan interrupciones a veces,[3] por lo que ejecutar dos servidores DNS secundarios en la red propia de la empresa y en otros puntos de presencia puede actuar como una póliza de seguro económica y eficaz. Obviamente, depende de la carga de consultas esperada. Si se considera la posibilidad de usar un mayor número de servidores secundarios, Anycast puede resultar particularmente útil.

Un servidor DNS primario oculto mantiene una copia autoritativa de las zonas externas, pero no responde a las consultas de los servidores DNS en internet. En su lugar, este servidor DNS transfiere esas zonas al proveedor de alojamiento de DNS.

Como protección adicional contra los peligros de la comunicación directa con internet, los servidores DNS autoritativos externos utilizan ADP, que detecta, mitiga y alerta de una serie de ataques contra servidores DNS.

3 Vea el ciberataque DDoS contra Dyn de octubre de 2016, https://es.wikipedia.org/wiki/Ciberataque_a_Dyn_de_octubre_de_2016.

REENVÍO LOCAL

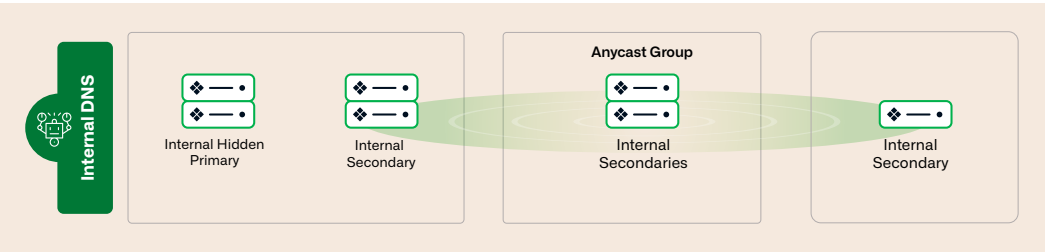


Los reenviadores locales, a veces llamados reenviadores de caché, son servidores DNS internos designados para resolver nombres de dominio de internet en representación de los servidores DNS internos, mediante la consulta de servidores DNS en internet. Al permitir que solo un pequeño número de servidores DNS internos se comuniquen directamente con los servidores DNS en internet, la empresa reduce su exposición a ciertos tipos de vulnerabilidades potenciales, como los desbordamientos de búfer provocados por respuestas mal formateadas.

La empresa cuenta con dos reenviadores, uno en la sede central y otro en el centro de grandes dimensiones, designado para la recuperación ante desastres. Ambos son parejas HA VRRP. Pese a su designación como dispositivo de recuperación ante desastres, el reenviador en el centro de grandes dimensiones se utiliza aun cuando el reenviador de la sede central está disponible, lo que no solo proporciona redundancia, sino también un mayor rendimiento. Los servidores DNS internos eligen qué reenviador utilizar según el tiempo de ida y vuelta de las consultas enviadas a ese reenviador y, cuando el tiempo de ida y vuelta es aproximadamente igual, eligen aleatoriamente; por tanto, esos servidores DNS internos utilizarán ambos reenviadores en función de su capacidad de respuesta, lo que tenderá a equilibrar la carga entre ellos.

Como protección adicional contra los peligros de la comunicación directa con internet, los reenviadores utilizan ADP, que detecta y detiene una serie de ataques contra los servidores DNS y el tráfico de gran volumen que generan ciertas herramientas bien conocidas de tunelización de DNS. En casos de tunelización de DNS de bajo volumen (lenta), Threat Insight puede desplegarse en estos miembros. La función Threat Insight también está disponible a través del portal de Infoblox y del proxy de reenvío de DNS (DFP) de Infoblox. En un despliegue de NIOS, Threat Insight utiliza zonas de políticas de respuesta (RPZ) para aplicar las normas.

DNS INTERNO



Dado que el DNS es un servicio de red tan crítico, todos los centros internos de la empresa necesitan un servidor DNS local. La sede central tiene dos, ambos formados por una pareja HA, ya que uno sirve como primario oculto para las zonas internas. Un servidor primario oculto es un servidor dedicado a procesar actualizaciones dinámicas de las zonas que gestiona, en lugar de a responder consultas de clientes. El otro servidor gestiona las consultas de los clientes y actúa como secundario para las zonas internas; para resolver otros nombres de dominio, consulta a uno de los reenviadores.

Los centros de grandes dimensiones de la empresa también cuentan con parejas HA que actúan como servidores DNS secundarios. Los centros pequeños tienen dispositivos simples (es decir, no HA). Para proporcionar redundancia adicional del servicio DNS, todos los servidores DNS de la sede, los centros de grandes dimensiones y los centros pequeños forman parte de uno de los dos grupos de Anycast. Los servidores DNS del Grupo A cuentan con una dirección IP

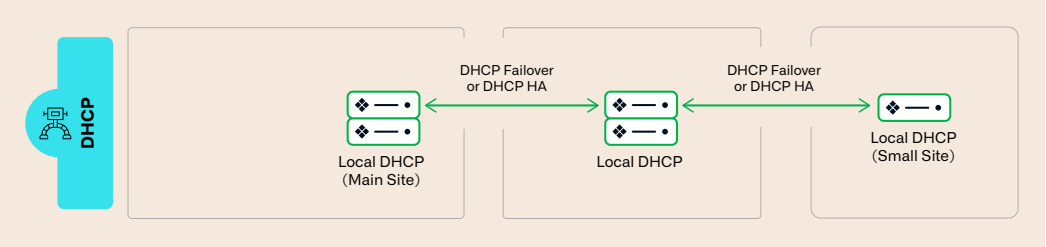
virtual asociada a su servicio de DNS; los servidores del Grupo B tienen una dirección IP virtual distinta. Los dispositivos internos[4] tienen sus resolvedores stub de DNS configurados para consultar primero una dirección IP virtual y luego la otra. Así prácticamente se garantiza que los dispositivos internos envíen su primera consulta a un servidor DNS receptivo.

Todos los servidores DNS recursivos internos están «conectados» con RPZ. Las RPZ se transfieren desde proveedores de RPZ basados en internet, entre ellos Infoblox, y contienen fuentes en tiempo real de datos sobre amenazas, incluidos los nombres de dominio que se sabe que se utilizan de forma maliciosa y las direcciones IP de servidores de nombres autoritativos maliciosos conocidos en internet. Estas RPZ impiden la resolución de nombres de dominio maliciosos por parte de los clientes de DNS y localizan rápidamente los dispositivos que intentan resolverlos, lo que permite al equipo de seguridad informática de la empresa identificar y poner en cuarentena rápidamente los dispositivos infectados. Una de estas RPZ puede ser poblada por Threat Insight a medida que descubre túneles de DNS.

La empresa también dispone de aplicaciones con base geográfica dentro de la organización, y cualquier persona de la red corporativa puede utilizarlas. También existe el deseo de equilibrar la carga y proporcionar redundancia. DNS Traffic Control (DTC) de Infoblox es una solución de equilibrio de carga que optimiza los tiempos de respuesta y el rendimiento de las aplicaciones, dirigiendo de forma inteligente el tráfico DNS en función de la ubicación del cliente, la disponibilidad de los servidores y la topología de la red. DTC se configura en los servidores DNS autoritativos internos.

Trataremos el DNS para oficinas remotas en una sección separada llamada «Oficinas remotas».

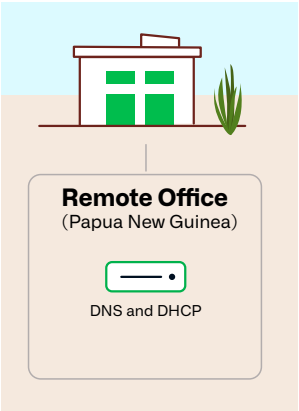
DHCP



Al igual que DNS, DHCP es un servicio de red crítico, por lo que todos los centros internos de la empresa necesitan disponer de un servidor DHCP local. De manera similar a DNS, DHCP se sustenta en parejas HA en la sede central y los centros de grandes dimensiones, y en dispositivos individuales en los centros pequeños. Sin embargo, para proporcionar redundancia adicional, los servidores DHCP se configuran en asociaciones de conmutación por error de DHCP: cada servidor DHCP tiene un servidor DHCP asociado con el que comparte información sobre los grupos de asignación de DHCP, y ambos pueden ofrecer asignaciones a los clientes de esos grupos. De esta manera, incluso los centros con un solo dispositivo cuentan con un servicio DHCP redundante. Estos servidores DHCP utilizan DNS dinámico (DDNS) para actualizar los registros de DNS en el servidor primario oculto para las zonas internas.

OFICINAS REMOTAS

Las oficinas remotas de la empresa son, por definición, pequeñas y solo tienen capacidad para un número modesto de empleados. Sin embargo, hay bastantes oficinas remotas y su conectividad a internet y al resto de la red corporativa es importante. La mayoría de las oficinas remotas cuentan con acceso a internet de alta velocidad, pero no con una conexión dedicada a la red corporativa; en su lugar, pueden enviar tráfico a través de una VPN a la red corporativa para los servicios de DNS y DHCP. En este caso, para proporcionar DNS y DHCP a estas oficinas, la empresa utiliza



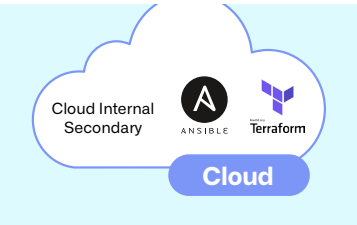
4 Salvo en las oficinas remotas: consulte la sección «Oficinas remotas» para informarse acerca de su configuración.

Infoblox Universal DDI™, la solución DDI gestionada en la nube de Infoblox. Cada dispositivo gestionado en la nube, NIOS-X, proporciona servicios de DNS y DHCP a la oficina remota. Los servidores DNS de las oficinas remotas no forman parte de la infraestructura Anycast de la empresa; los clientes de las oficinas remotas consultan primero el servidor DNS local y luego recurren a las direcciones IP de los dos grupos Anycast.

Para proporcionar DHCP redundante, el servidor DHCP de cada oficina remota mantiene una relación activa-pasiva avanzada con el servidor DHCP de una oficina remota cercana. De este modo, ambos servidores pueden ofrecer DHCP a los clientes en cualquiera de las oficinas remotas, proporcionando servicios DHCP redundantes incluso a las oficinas remotas.

Una alternativa para las oficinas que dependen totalmente de internet para su funcionamiento es NIOS-X como servicio, una solución de Infoblox basada en la nube que proporciona servicios DDI gestionados. Ofrece escalabilidad, flexibilidad y seguridad mejorada al alojar estos servicios de red críticos en la nube y eliminar la necesidad de hardware local. NIOS-X como servicio se integra a la perfección con otras soluciones de Infoblox para ofrecer un enfoque unificado y simplificado en cuanto a gestión y seguridad de redes, lo que garantiza operaciones de red fiables y eficientes.

NUBE



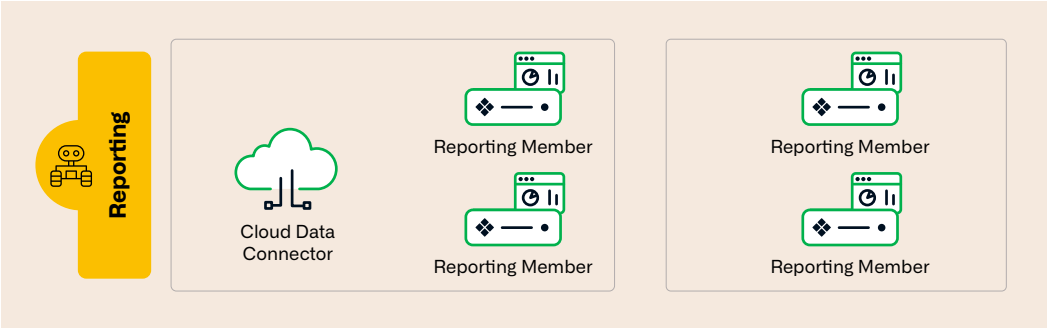
La empresa utiliza varias nubes públicas para dar soporte a aplicaciones tanto internas como públicas con acceso desde internet. Cada nube aloja uno o más dispositivos de plataforma de nube virtual configurados como secundarios para las zonas internas en las que las aplicaciones y cargas de trabajo de la nube necesitan resolver los nombres de dominio. Esto proporciona una mayor resiliencia que utilizar el reenvío condicional para dirigir las consultas a servidores DNS internos con el fin de resolver nombres de dominio internos.

El dispositivo de la plataforma en la nube también está configurado como primario para las zonas de nube en las que los sistemas de aprovisionamiento de la empresa, Terraform y Ansible, necesitan gestionar los registros de recursos. Para integrar Terraform y Ansible con la red Grid, Terraform utiliza Terraform Provider de Infoblox, mientras que Ansible utiliza NIOS Collection de Infoblox para la automatización de Ansible.

La Automatización de Red en la Nube (CNA) de Infoblox también proporciona visibilidad del entorno de la red en la nube, mostrando los recursos de nube en uso, como nubes privadas virtuales/redes virtuales, subredes y máquinas virtuales. Además, CNA puede crear automáticamente registros DNS para los nuevos elementos que se descubran mediante el proceso de detección virtual.

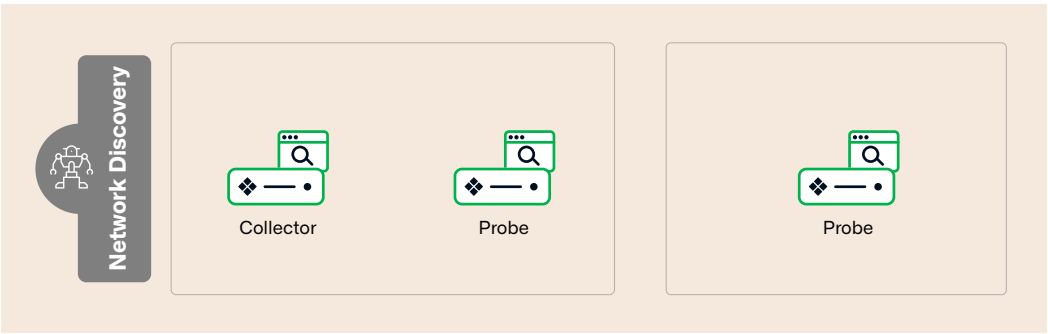
Si la empresa utiliza servicios DNS específicos de la nube, como Amazon Route 53 o Azure DNS, esos servicios pueden integrarse con la red Grid mediante sincronización. Así se mantiene un único punto de visibilidad y control de todos los datos de DNS a través de la interfaz y la API de la red Grid.

GENERACIÓN DE INFORMES



Para respaldar las capacidades de elaboración de informes de la red Grid, la empresa utiliza cuatro servidores, dos de ellos en la sede central y dos en el lugar designado para la recuperación ante desastres. El uso de cuatro servidores, aunque no sea estrictamente necesario, proporciona tanto redundancia como un mayor rendimiento: uno o los dos servidores de informes de la sede pueden fallar sin que se pierdan datos de informes. Los datos de los informes se seguirán indexando, se podrán seguir generando informes y se podrán realizar búsquedas en los datos de los informes. Con cuatro servidores de informes, la ubicación óptima sería tener dos con el GM y dos con el GMC que se asignaría durante un evento de recuperación ante desastres.

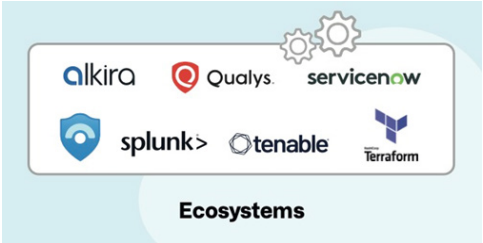
DETECCIÓN DE LA RED



La detección de la red es un componente crítico de una solución para la gestión de direcciones IP: la detección garantiza que la base de datos de DDI refleje el estado real de la red y no una versión idealizada de ella. La función de detección virtual proporciona detección en los entornos de nube y virtuales in situ de la empresa, pero la red empresarial también necesita detección.

Varios dispositivos admiten la detección de la red: dos en la sede central y uno en cada centro de grandes dimensiones. Uno de los dispositivos en la sede se designa como consolidador: recibe todos los datos detectados en los diversos sondeos, los consolida y los replica en el GM para incluirlos en la base de datos de DDI. Los demás dispositivos son sondas, que efectúan las consultas, pruebas y sondeos necesarios para detectar dispositivos en la red

SISTEMAS EXTERNOS E INTEGRACIONES DEL ECOSISTEMA



La empresa utiliza tanto sistemas basados en la nube como internos para una amplia gama de funciones, en especial el sistema SIEM, el sistema de gestión de tickets (recordemos que utilizan ServiceNow) y un portal de autoservicio que permite a los empleados solicitar cambios simples en la base de datos de DDI. Los dispositivos en la red Grid envían la salida registrada directamente al SIEM. Los registros de

DNS, como los datos de pDNS, se envían al conector de datos de Infoblox, porque se reduce la sobrecarga impuesta a los servidores de DNS al enviar los datos y permite filtrar dichos datos antes de enviarlos a los sistemas externos (para no registrar consultas puramente internas, por ejemplo, si así se desea).

Gracias a su integración con la red Grid, ServiceNow permite a los usuarios solicitar cambios en la base de datos de DDI, como reservar, añadir y eliminar direcciones IP. Por ejemplo, la red Grid también puede enviar notificaciones a ServiceNow y avisar al sistema cuando los dispositivos se conectan o desconectan de la red y si se detectan problemas de seguridad.

Al compartir la visibilidad temprana de las amenazas, las direcciones IP autorizadas y los datos de red contextuales con las herramientas existentes, Infoblox rompe los silos y refuerza toda la pila de seguridad de TI, lo que garantiza un mejor ROI y eficiencia operativa. El ecosistema de Infoblox se integra a la perfección con una amplia gama de herramientas de seguridad, redes y nube para reforzar la detección de amenazas, automatizar los flujos de trabajo y mejorar las capacidades de respuesta en los entornos in situ, híbridos y multinube.

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

+1.408.986.4000
www.infoblox.com/es

Versión: 20250221v2