L'ARCHITECTURE DE RÉFÉRENCE INFOBLOX® ET LES MEILLEURES PRATIQUES POUR NIOS DDI

UNE VISION PLUS CONCRÈTE DU DÉPLOIEMENT DES SERVICES DNS ET DHCP À L'AIDE DES PRODUITS INFOBLOX NIOS DDI ET INFOBLOX THREAT DEFENSE™ SUR UN RÉSEAU, POUR GAGNER EN SIMPLICITÉ, SÉCURITÉ ET ÉVOLUTIVITÉ.

TABLE DES MATIÈRES

RÉSUMÉ

Ce guide, élaboré à partir de livres blancs rédigés par Cricket Liu et Infoblox® Architecture Review Board (ARB), souligne les efforts de collaboration de notre organisme interne chargé de valider toutes les conceptions importantes produites par les architectes de solutions d'Infoblox. Aux côtés de l'ARB, divers experts techniques d'Infoblox apportent leurs connaissances spécialisées pour garantir que nos solutions sont robustes, innovantes et conformes aux bonnes pratiques du secteur.

Les appliances NIOS sont un moyen idéal pour fournir des services DNS (Domain Name System) et DHCP (Dynamic Host Configuration Protocol), et ont ensuite présenté une architecture permettant de prendre en charge ces services ainsi que les services de sécurité de manière efficace, fiable et sécurisée. Ce guide s'appuie sur ces livres blancs pour inclure plusieurs nouvelles avancées dans le domaine des technologies de l'information :

- L'utilisation du DNS en tant qu'outil de sécurité essentiel
- L'essor des clouds publics et du cloud computing
- L'importance croissante de l'informatique en libre-service, stimulée par des services tels que ServiceNow
- La croissance des réseaux d'entreprise pour inclure davantage de petits bureaux à distance
- La nécessité d'une intégration avec les systèmes de gestion des informations et des événements de sécurité (SIEM) et d'autres technologies de sécurité

Pour montrer comment prendre en charge ces nouveaux développements, nous présenterons l'étude de cas d'une entreprise et de son réseau professionnel, et nous développerons une architecture DDI (DNS, DHCP et gestion des adresses IP) adaptée à ses besoins en suivant les meilleures pratiques de l'industrie. Cette conception tiendra compte des exigences de l'entreprise en matière de disponibilité, de performance, de sécurité et de reprise après sinistre, ainsi que de la prise en charge de l'informatique et des applications dans le cloud, et l'intégration avec les systèmes internes et ceux basés dans le cloud.

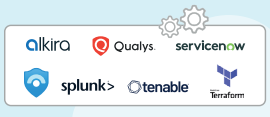
Durant la lecture de ce livre blanc, réfléchissez à votre propre infrastructure DDI. Offre-t-elle le même niveau de résilience, de performance et de sécurité ? Pourriez-vous adapter certains éléments de cette conception à votre propre usage ?

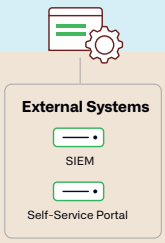
ACME ROBOTICS

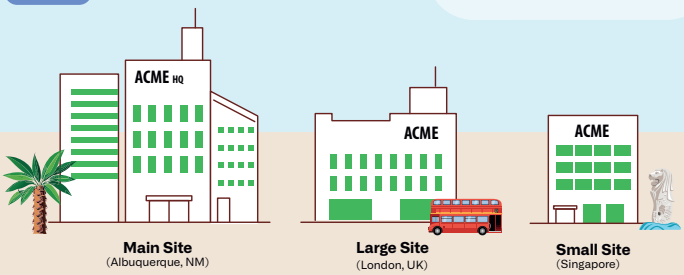
infoblox.

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.







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.

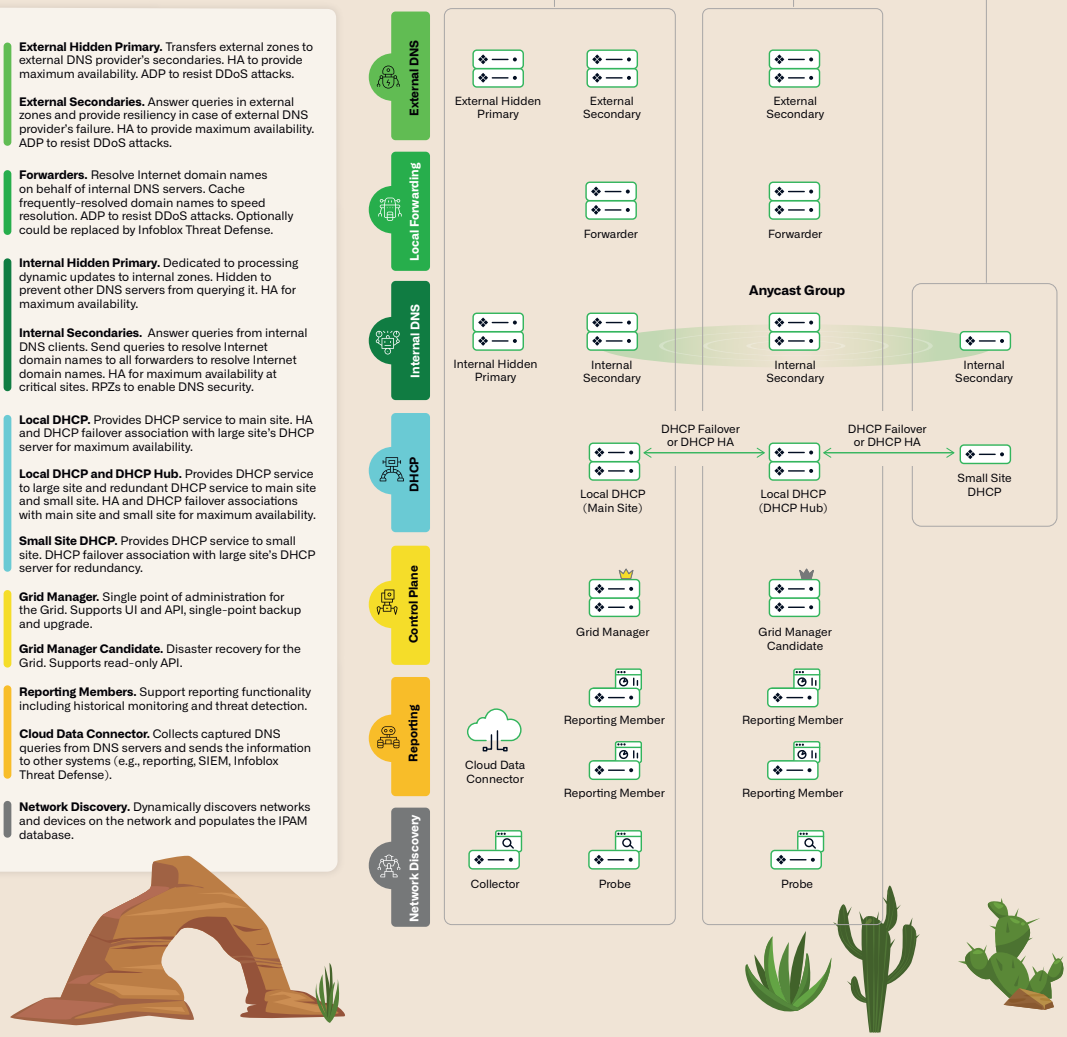
Grid Manager. Single point of administration for the Grid. Supports UI and API, single-point backup and upgrade.

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.



L'ENTREPRISE

Nous avons récemment été chargés de concevoir une nouvelle architecture DNS pour une entreprise multinationale, ACME Robotics. ACME est un fournisseur renommé de dispositifs robotiques qui assurent un large éventail de fonctions. ACME Robotics fabrique, commercialise et distribue des produits. Elle possède également un service des ventes et un service d'assistance.

L'entreprise évolue sur un marché mondial, bien que principalement concentré dans le Sud-Ouest des États-Unis.

Elle possède quatre catégories de sites connectés à son réseau d'entreprise :

1. Le siège d'ACME à Albuquerque, au Nouveau-Mexique, abrite le plus grand nombre d'utilisateurs (environ 2 000). C'est également là que se trouve le centre de données principal de l'entreprise.
2. Un grand site à Londres, en Angleterre, accueille environ 500 utilisateurs locaux.
3. Des petits sites, dont le site de Singapour, accueille généralement 100 utilisateurs ou moins. Ils sont divisés par régions géographiques, chacune étant rattachée à un bureau régional. Chaque petit site est connecté au réseau de l'entreprise via un lien avec la branche régionale dont il dépend.
4. En général, les sites à distance comptent moins de 24 utilisateurs. Ils sont connectés à Internet et au réseau d'entreprise via une connexion VPN ou SD-WAN.

L'entreprise est très présente en ligne, notamment pour commercialiser ses produits. Pour ce faire, elle utilise deux clouds publics : AWS et Azure. Elle exécute plusieurs applications dans chaque cloud et certaines nécessitent un accès aux ressources internes. Le provisionnement dans le cloud est automatisé par Terraform ou Ansible, en fonction de l'application.

L'entreprise utilise ServiceNow pour permettre aux employés de demander des modifications informatiques, y compris pour le DNS et le DHCP. Elle exécute un SIEM interne et, en raison du secteur dans lequel elle opère, elle est dans l'obligation de capturer et d'archiver les données DNS passives (pDNS).

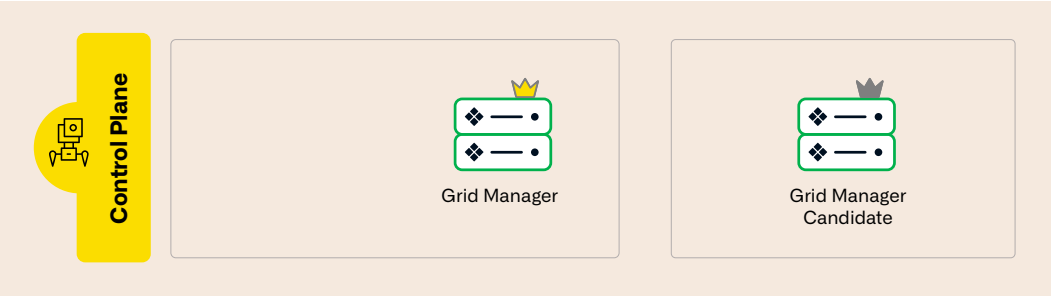
L'équipe de support informatique de l'entreprise est répartie entre le siège social et les grands sites. Chaque bureau régional dispose d'un membre du personnel informatique, principalement pour fournir un support local pour les postes de travail et les ordinateurs portables, et pour agir comme un support à distance pour le personnel du siège.

L'entreprise permet à ses employés d'apporter leurs propres appareils au travail, mais les isole sur des réseaux pour les visiteurs. Notre conception tient compte d'un nombre moyen d'appareils par employé et de la charge transactionnelle générée par ceux-ci.

UNE NOTE IMPORTANTE SUR LE DIMENSIONNEMENT

Il existe un élément important de l'architecture que nous n'abordons pas dans cette conception ou ce document : le dimensionnement. Afin de garantir que les serveurs DNS et DHCP sont suffisamment performants pour couvrir les besoins de l'entreprise, celle-ci doit évaluer ou, du moins, estimer les taux de transaction DNS et DHCP pour chaque serveur de la conception, et spécifier les appareils capables de gérer cette charge. Par ailleurs, l'entreprise doit calculer une « marge de manœuvre » adéquate : une capacité de serveur supplémentaire pour faire face aux pics de charge imprévus (par exemple, en raison d'une panne puis du rétablissement de l'alimentation électrique sur un site). Enfin, l'entreprise doit estimer et planifier sa croissance au fil du temps : en effet, si elle prévoit d'embaucher massivement, d'acquérir d'autres sociétés ou de fusionner avec une autre entreprise, cela peut avoir un impact significatif sur la charge du DNS et du DHCP.

PLAN DE CONTRÔLE



Commençons par le plan de contrôle DDI, qui dans cette conception, se compose d'un Grid Manager (GM) au siège à Albuquerque et d'un Candidat au poste de Grid Manager (GMC) basé au grand site de Londres.

Au sein d'un Grid NIOS Infoblox, le GM prend en charge l'interface utilisateur web utilisée par les administrateurs et l'API utilisée par les développeurs pour automatiser les tâches DDI.[1] Le GM gère également la communication et la synchronisation avec tous les membres Infoblox[2] dans le Grid ; ces appareils prennent en charge le DNS, le DHCP et d'autres services. Compte tenu de son rôle essentiel, le GM devrait toujours être déployé sous la forme d'une paire d'appareils à grande disponibilité (HA) du Virtual Router Redundancy Protocol (VRRP) sur le même site physique. Le GM peut également servir à mettre à jour ou maintenir les règles de Protection DNS avancée (ADP) et les modules Threat Insight.

Le GMC est une réplique du GM, qui se synchronise avec le GM en temps réel. Si les deux appareils qui remplissent le rôle de GM échouent, un administrateur peut promouvoir le GMC au rôle de GM à l'aide d'une simple commande. Le GM nouvellement promu informera les autres appareils du Grid et assumera les fonctions de l'ancien GM. Comme pour le GM, le GMC doit toujours être déployé en tant que paire d'appareils HA VRRP sur le même site physique.

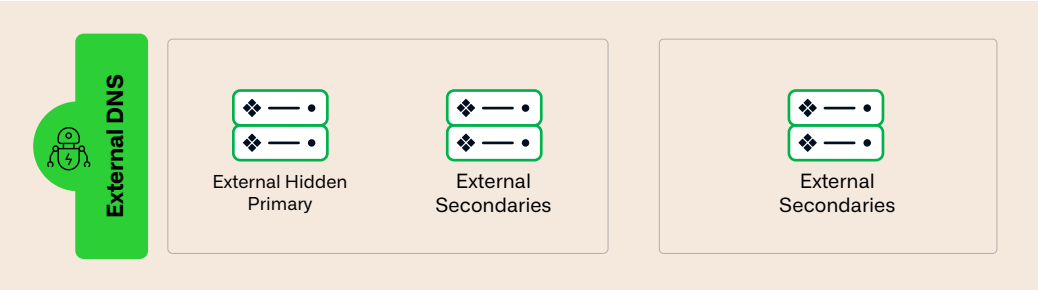
Les Grids Infoblox prennent en charge la désignation de nombreux GMC, mais cette entreprise ayant identifié Londres comme son site de reprise après sinistre, elle n'y hébergera qu'un seul GMC.

Nous avons annoncé que nous n'aborderions pas la question du dimensionnement dans ce document, mais une remarque sur le dimensionnement des GMC s'impose : les GMC offrent la possibilité (très pratique) de gérer des appels API en lecture seule, ce qui peut s'avérer utile, par exemple, pour prendre en charge l'intégration avec ServiceNow, qu'ACME utilise. Lors du dimensionnement des GMC, tenez compte à la fois de la charge exercée sur le GM **et** de la charge exercée sur le GMC par tout appel API en lecture seule qu'il traite. En cas de sinistre, si vous promouvez le GMC au rôle de GM, celui-ci doit être capable de gérer la charge cumulée du GM et de son ancien rôle de GMC. Vous pouvez également ajouter un ou plusieurs GMC qui se consacreraient au traitement des appels API en lecture seule.

1 Sauf exception. Consultez la section « Cloud » pour en savoir plus.

2 Remarque : nous utilisons le terme « appareil » pour désigner à la fois les appareils physiques et les appareils virtuels. Ces derniers sont exécutés sur presque toutes les plateformes de virtualisation et dans les clouds publics.

DNS AUTORITAIRE EXTERNE



Les serveurs DNS autoritaires externes publient les zones de l'entreprise sur Internet, ce qui permet aux clients et partenaires présents en ligne d'envoyer des e-mails aux adresses de l'entreprise, de visiter le site Web de l'entreprise, d'accéder aux applications Web et bien plus encore. Ils possèdent un rôle crucial, car leur disponibilité se répercute directement sur les revenus, la satisfaction des clients et la réputation de l'entreprise.

L'infrastructure DNS autoritaire externe se compose de trois membres. Un membre principal caché sur le site du siège social à Albuquerque et deux membres secondaires ; un au siège social et un sur le grand site de Londres. Chaque membre correspond à une paire d'appareils VRRP HA. Cette configuration permet aux administrateurs de mettre à niveau les serveurs DNS sans interruption de service, ce qui pourrait s'avérer nécessaire si un bogue ou une vulnérabilité était découvert dans BIND, par exemple, ou s'il fallait passer à des appareils de plus grande taille pour suivre la croissance de l'entreprise.

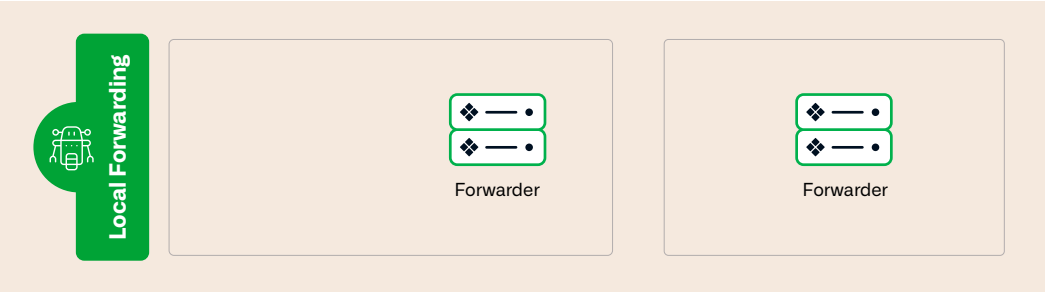
L'infrastructure DNS autoritaire externe **étendue** inclut également les serveurs DNS exécutés par un fournisseur d'hébergement DNS basé sur Internet. Les fournisseurs d'hébergement DNS, tels que Cloudflare et UltraDNS de Neustar, fournissent de nombreux serveurs DNS sur l'infrastructure DNS largement distribuée sur Internet, que l'entreprise aurait du mal à gérer et dont l'exploitation lui coûterait cher. Cependant, les fournisseurs d'hébergement DNS subissent parfois des pannes,[3] c'est pourquoi exploiter deux serveurs DNS secondaires sur le réseau de l'entreprise et sur d'autres emplacements peut constituer une police d'assurance efficace et peu coûteuse. Évidemment, cela dépend de la charge de requête attendue. Si vous envisagez un grand nombre de serveurs secondaires, alors utiliser Anycast pourrait vous rendre un grand service.

Un serveur DNS principal caché détient une copie faisant autorité des zones externes, mais ne répond pas aux requêtes des serveurs DNS sur Internet. À la place, il transfère ces zones au fournisseur d'hébergement DNS.

Pour vous protéger contre les dangers liés à la communication directe avec Internet, les serveurs DNS autoritaires externes utilisent l'ADP, qui détecte, atténue et signale différents types d'attaques contre des serveurs DNS.

3 Voir l'attaque DDoS sur Dyn en octobre 2016, https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn.

TRANSFERT LOCAL

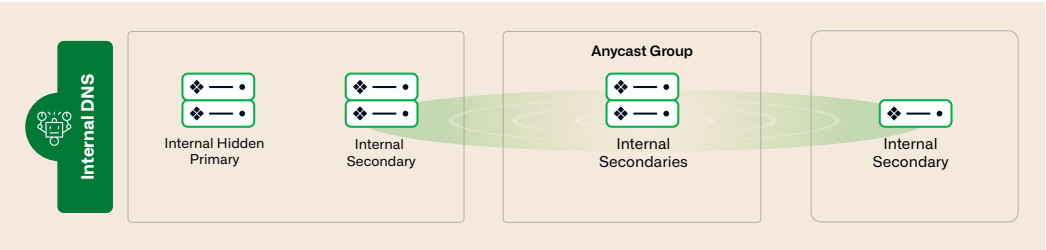


Les serveurs de redirection locaux (parfois appelées serveurs de redirection de mise en cache) sont des serveurs DNS internes dont le rôle est de résoudre les noms de domaine Internet au nom des serveurs DNS internes en envoyant des requêtes aux serveurs DNS sur Internet. En autorisant seulement un petit nombre de serveurs DNS internes à communiquer directement avec les serveurs DNS sur Internet, l'entreprise réduit son exposition à certains types de vulnérabilités potentielles, telles que les dépassements de tampon causés par des réponses mal formatées.

L'entreprise dispose de deux serveurs de redirection : l'un au siège et l'autre sur le grand site, qui est destiné à la reprise après sinistre. Tous deux se composent d'une paire d'appareils HA VRRP. Bien qu'il soit désigné comme dispositif de reprise après sinistre, le serveur de redirection du grand site est utilisé même lorsque le serveur de redirection du siège est disponible, afin d'offrir un débit supplémentaire, en plus d'une redondance. Les serveurs DNS internes choisissent quel serveur de redirection utiliser en fonction du temps de réponse des requêtes envoyées à ce serveur. Si le temps de réponse est équivalent, un serveur est sélectionné au hasard. Par conséquent, ces serveurs DNS internes utiliseront les deux serveurs de redirection en fonction de leur réactivité. Ce fonctionnement aura tendance à équilibrer la charge entre eux.

Pour vous protéger contre les dangers liés à la communication directe avec Internet, les serveurs de redirection utilisent l'ADP, qui détecte et bloque différents types d'attaques contre les serveurs DNS et le trafic à haut volume généré par certains outils de DNS Tunneling bien connus. Vous pouvez déployer Threat Insight sur ces membres pour gérer le DNS Tunneling à faible volume (faible et lent). La fonctionnalité Threat Insight est également disponible sur le portail Infoblox et le proxy de redirection DNS (DFP) d'Infoblox. Au sein d'un déploiement NIOS, Threat Insight utilise des zones de politique de réponse (RPZ) pour la mise en application.

DNS INTERNE



Le DNS étant un service réseau essentiel, tous les sites internes de l'entreprise nécessitent un serveur DNS local. Le siège social en possède deux, sous forme de paires d'appareils HA, le premier servant de serveur principal caché pour les zones internes. Un serveur principal caché est un serveur dédié au traitement des mises à jour dynamiques des zones qu'il gère, plutôt qu'à la réponse aux requêtes des clients. L'autre serveur gère les requêtes des clients et fonctionne comme serveur secondaire pour les zones internes. Pour résoudre d'autres noms de domaine, il envoie des requêtes à l'un des serveurs de redirection.

Les grands sites de l'entreprise disposent également de paires d'appareils HA qui font office de serveurs DNS secondaires. Les petits sites disposent d'appareils uniques (c'est-à-dire, non HA). Pour fournir une redondance supplémentaire du service DNS, tous les serveurs DNS du siège, des grands sites et des petits sites font partie d'un des deux groupes Anycast. Les serveurs DNS du groupe A ont une adresse IP virtuelle associée à leur service DNS ; les serveurs du groupe B

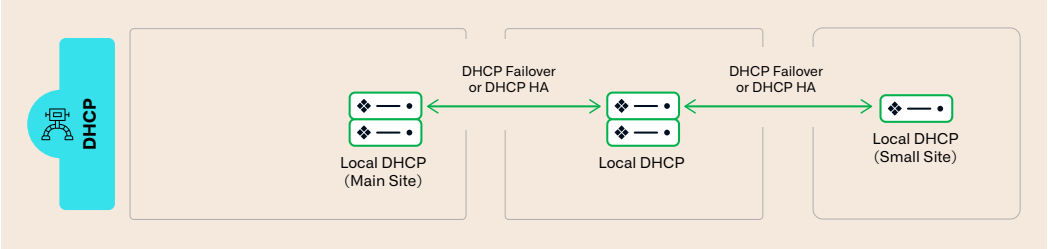
ont une adresse IP virtuelle différente. Appareils internes[4] sont configurés pour interroger une adresse IP virtuelle, puis l'autre. C'est une manière de garantir en quelque sorte que les appareils internes envoient leur première requête à un serveur DNS réactif.

Tous les serveurs DNS récursifs internes sont « raccordés » avec des RPZ. Les RPZ sont transférés depuis des fournisseurs RPZ basés sur Internet (y compris Infoblox) et contiennent des flux de données sur les menaces en temps réel, dont des noms de domaine connus pour être utilisés de manière malveillante et des adresses IP de serveurs de noms autoritaires reconnus comme malveillants sur Internet. Ces RPZ empêchent les clients DNS de résoudre des noms de domaine malveillants et repèrent rapidement les appareils qui tentent de les résoudre, permettant ainsi à l'équipe de sécurité informatique de l'entreprise d'identifier et d'isoler les appareils infectés. L'une de ces RPZ peut être alimentée par Threat Insight lorsque la fonctionnalité découvre des tunnels DNS.

En interne, l'entreprise dispose également d'applications basées sur la zone géographique, que n'importe quelle personne qui a accès au réseau d'entreprise peut utiliser. Elle souhaite aussi équilibrer la charge et fournir une redondance. La solution DNS Traffic Control (DTC) d'Infoblox pour équilibrer la charge optimise les délais de réponse et les performances des applications en dirigeant intelligemment le trafic DNS en fonction de l'emplacement du client, de la disponibilité du serveur et de la topologie du réseau. DTC est configurée sur les serveurs DNS autoritaires internes.

Nous avons dédié une section distincte au DNS pour les bureaux à distance, intitulée « Bureaux distants ».

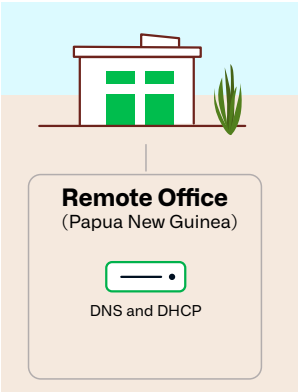
DHCP



Comme le DNS, le DHCP est un service réseau essentiel et tous les sites internes de l'entreprise doivent posséder un serveur DHCP local. Et tout comme le DNS, le DHCP est pris en charge par les paires d'appareils HA présents au siège social et sur les grands sites, ainsi que par des appareils individuels sur les petits sites. Cependant, pour fournir une redondance supplémentaire, les serveurs DHCP sont configurés en associations de basculement DHCP : chaque serveur DHCP est associé à un serveur DHCP pair avec lequel il partage des informations sur les groupements de baux DHCP, et tous deux peuvent attribuer des baux aux clients à partir de ces groupements. Ainsi, même les sites dotés d'un seul appareil disposent d'un service DHCP redondant. Ces serveurs DHCP exploitent le DNS dynamique (DDNS) pour mettre à jour les enregistrements DNS sur le serveur principal caché pour les zones internes.

BUREAUX DISTANTS

Les bureaux distants de l'entreprise sont, par définition, de petite taille et n'accueillent chacun qu'un nombre modeste d'employés. Toutefois, ces bureaux sont nombreux et leur connexion à Internet ainsi qu'au reste du réseau d'entreprise demeure cruciale. La plupart des bureaux distants disposent d'un accès Internet à haut débit, mais pas d'une connexion dédiée au réseau de l'entreprise. Ils peuvent cependant envoyer du trafic vers le réseau de l'entreprise via un VPN pour les services DNS et DHCP. Dans le cas présent, l'entreprise utilise Infoblox Universal DDI™, la solution DDI gérée dans le cloud d'Infoblox, pour fournir un DNS et un DHCP à ces



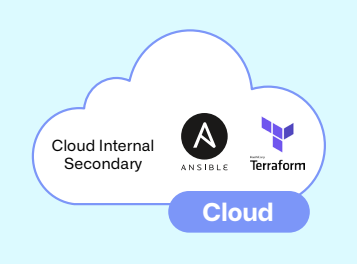
4 À l'exception de ceux qui se trouvent dans les bureaux à distance : voir la section « Bureaux distants » pour connaître leur configuration.

bureaux. Chaque appareil géré dans le cloud NIOS-X fournit des services DNS et DHCP au bureau à distance. Les serveurs DNS des bureaux à distance ne font pas partie de l'infrastructure Anycast de l'entreprise. Les clients des bureaux distants envoient d'abord des requêtes au serveur DNS local, puis se rabattent sur les adresses IP des deux groupes Anycast.

Pour fournir un DHCP redondant, chaque serveur DHCP du bureau à distance s'inscrit dans une relation active-passive avancée avec un serveur DHCP d'un autre bureau distant voisin. Cela permet aux deux serveurs de fournir des services DHCP aux clients de l'un ou l'autre des bureaux à distance, assurant ainsi des services DHCP redondants même pour les bureaux distants.

La solution cloud d'Infoblox, NIOS-X en tant que service, est une alternative pour les bureaux dont le fonctionnement dépend entièrement d'Internet, qui fournit des services DDI en tant que service géré. Elle offre une évolutivité, une flexibilité et une sécurité renforcée en hébergeant ces services réseau essentiels dans le cloud, éliminant ainsi la nécessité de posséder du matériel sur site. NIOS-X en tant que service s'intègre parfaitement aux autres solutions Infoblox. Elle offre une approche unifiée et simplifiée de la gestion et de la sécurité du réseau, pour garantir des opérations réseau fiables et efficaces.

LE CLOUD



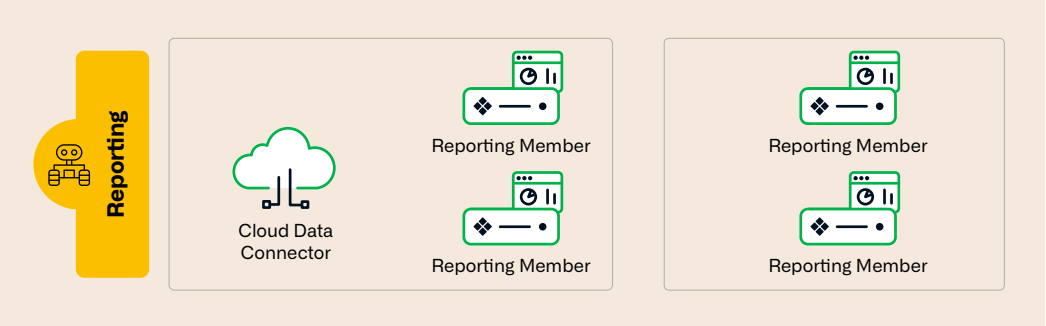
L'entreprise utilise plusieurs clouds publics pour prendre en charge aussi bien les applications internes que celles accessibles en ligne. Chaque cloud héberge un ou plusieurs dispositifs de plateforme cloud virtuelle au statut secondaire pour les zones internes dans lesquelles les applications cloud et les charges de travail doivent résoudre des noms de domaine. Cette méthode offre une meilleure résilience que le recours à la redirection conditionnelle pour diriger les requêtes vers les serveurs DNS internes afin de résoudre les noms de domaine internes.

Le dispositif de plateforme cloud est également configuré comme dispositif principal pour les zones cloud dans lesquelles les systèmes de provisionnement de l'entreprise, Terraform et Ansible, doivent gérer des enregistrements de ressources. Pour intégrer Terraform et Ansible au Grid, Terraform utilise Infoblox Terraform Provider, tandis qu'Ansible utilise Infoblox NIOS Collection pour l'automatisation Ansible.

L'automatisation du réseau cloud (CNA) d'Infoblox offre également une visibilité sur l'environnement du réseau cloud. Elle affiche les ressources cloud utilisées, telles que les clouds privés virtuels/réseaux virtuels, les sous-réseaux et les machines virtuelles. En outre, la CNA est capable de créer automatiquement des enregistrements DNS pour les nouveaux éléments découverts par le processus de découverte virtuel.

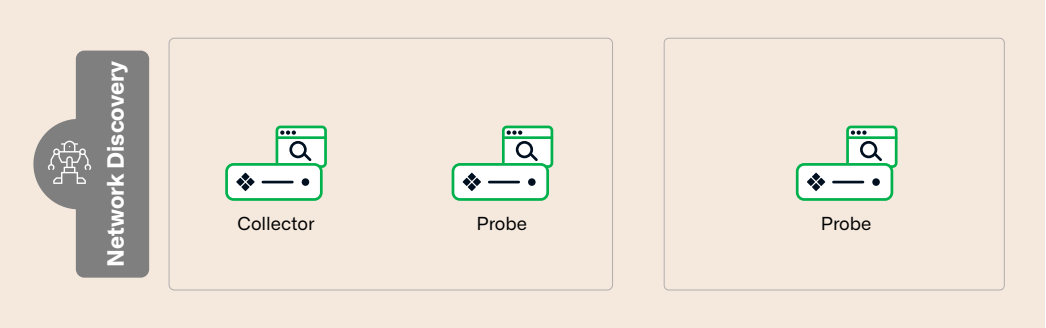
Si l'entreprise a recours à des services DNS spécifiques au cloud, tels qu'Amazon Route 53 ou Azure DNS, elle peut les intégrer au Grid grâce à la synchronisation. Elle garde ainsi un point de visibilité et de contrôle unique de toutes les données DNS par le biais de l'interface et de l'API du Grid.

RAPPORT



Pour prendre en charge les fonctionnalités de création de rapports du Grid, l'entreprise utilise quatre serveurs de rapports : deux au siège et deux sur le site désigné pour la reprise après sinistre. L'utilisation de quatre serveurs, bien qu'elle ne soit pas strictement nécessaire, offre à la fois une redondance et des performances accrues. Ainsi, si un ou les deux serveurs de rapports situés au siège tombent en panne, les données de rapport ne seront pas perdues. Ces données continueront d'être indexées, les rapports pourront toujours être générés et des recherches pourront être exécutées sur les données de rapport. Dans une configuration à quatre serveurs de rapports, le placement optimal consisterait à installer deux serveurs auprès du GM et deux autres auprès du GMC, que vous utiliseriez lors d'un événement de reprise après sinistre.

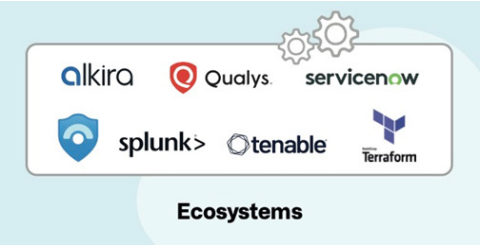
LA DÉCOUVERTE DU RÉSEAU



La découverte du réseau est un élément essentiel d'une solution de gestion des adresses IP : elle garantit que la base de données DDI reflète l'état réel du réseau et non une version idéalisée de celui-ci. La fonctionnalité de découverte virtuelle offre une capacité de découverte dans les environnements virtuels et cloud sur site de l'entreprise, mais c'est aussi quelque chose dont le réseau d'entreprise a besoin.

La découverte du réseau s'appuie sur plusieurs appareils : deux au siège et un sur chaque grand site. L'un des appareils du siège est désigné comme outil de consolidation : il reçoit toutes les données découvertes par les différentes sondes, les consolide et les duplique dans le GM afin de les inclure dans la base de données DDI. Les autres appareils jouent le rôle de sondes, qui envoient les requêtes et réalisent les opérations de sondage nécessaires à la découverte des appareils sur le réseau.

SYSTÈMES EXTERNES ET INTÉGRATIONS DE L'ÉCOSYSTÈME



L'entreprise utilise à la fois des systèmes basés dans le cloud et des systèmes internes pour exécuter diverses fonctionnalités, y compris leur système SIEM, leur système de gestion des tickets (rappelons qu'elle utilise ServiceNow) et un portail en libre-service mis à disposition des employés pour qu'ils puissent demander à apporter des modifications simples à la base de

données DDI. Les appareils du Grid envoient les données enregistrées directement au SIEM. Les journaux DNS, tels que les données pDNS, sont envoyés à Infoblox Data Connector, ce qui permet de réduire la surcharge imposée aux serveurs DNS pour envoyer les données et de filtrer ces données avant de les envoyer aux systèmes externes (pour éviter d'enregistrer des requêtes purement internes, par exemple, si besoin).

Grâce à son intégration au Grid, ServiceNow permet aux utilisateurs de demander des modifications de la base de données DDI, comme la réservation, l'ajout et la suppression d'adresses IP. Le Grid peut également envoyer des notifications à ServiceNow pour avertir le système lorsque des appareils rejoignent ou quittent le réseau, et lorsque des problèmes de sécurité sont détectés.

En offrant une visibilité précoce des menaces, des adresses IP faisant autorité et des données réseau contextuelles avec les outils existants, Infoblox met fin au cloisonnement et renforce l'ensemble de la pile de sécurité informatique, garantissant ainsi un meilleur retour sur investissement et une efficacité opérationnelle accrue. L'écosystème Infoblox s'intègre parfaitement à une large gamme d'outils de sécurité, de réseau et de cloud pour améliorer la détection des menaces, automatiser les flux de travail et renforcer les capacités de réponse dans les environnements sur site, hybrides et multi-cloud.

Siège social
2390 Mission College Boulevard,
Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version : 20250221v2