NOTE DE SYNTHÈSE

CONTRÔLE ET SÉCURITÉ TRANSPARENTS POUR LES DÉPLOIEMENTS DE CLOUD HYBRIDE AVEC AMAZON ROUTE 53 ET INFOBLOX

RÉSUMÉ

Le service DNS Amazon Route 53 offre un support limité au-delà des environnements Amazon Web Services (AWS) exclusifs.

Ces limitations signifient que les sociétés ne peuvent pas créer une solution unique et unifiée de gestion DNS, DHCP et des adresses IP (DDI) pour desservir l'ensemble de leur entreprise, y compris les réseaux de campus d'entreprise et les clouds hybrides, avec uniquement Route 53. Route 53 se concentre uniquement sur les clouds privés virtuels (VPC) d'AWS, ce qui limite la connectivité, la visibilité et la sécurité lorsqu'il est utilisé pour des plateformes cloud autres qu'AWS.

Infoblox intègre sa plateforme DDI leader du secteur avec AWS et Amazon Route 53 DNS, offrant une solution unifiée de niveau commercial, entreprise et fournisseur de services pour les déploiements AWS et cloud hybride. L'intégration d'Infoblox avec Amazon Route 53 comble le fossé entre les équipes informatiques d'entreprise et les équipes cloud. Il réduit la complexité et aide à atteindre une sécurité optimale en fournissant un plan de contrôle unique pour gérer les déploiements sur site, dans le cloud privé et dans le cloud public AWS, tout en renforçant la sécurité de ces déploiements. Cette solution répond aux besoins des clients actuels et futurs d'Infoblox qui s'étendent vers AWS et utilisent Amazon Route 53 pour le DNS.

LE MANQUE DE VISIBILITÉ, D'AUTOMATISATION ET DE COHÉRENCE PEUT ENTRAVER LES DÉPLOIEMENTS D'AMAZON ROUTE 53

Amazon Route 53 offre une fonctionnalité DNS privée au sein des VPC AWS. Cependant, une entreprise utilisant un cloud hybride rencontre des défis opérationnels, même en utilisant Amazon Route 53, tels que :

- **DNS limité :** La résolution DNS ou les réponses aux requêtes sont isolées au sein de leur réseau AWS, ce qui pose des problèmes lorsque la communication est nécessaire en dehors d'une zone privée hébergée AWS particulière. Pour contourner ce problème, les équipes informatiques mettent souvent en place plusieurs serveurs BIND pour transmettre le trafic DNS en dehors des zones AWS isolées. Cette approche ajoute de la complexité et manque de cohérence entre des déploiements DNS disparates.
- **Pas d'IPAM :** AWS ne dispose pas de solution de gestion des adresses IP (IPAM) et a souvent une visibilité limitée des instances virtuelles, ce qui impacte négativement la gestion quotidienne et augmente le temps nécessaire pour l'audit et la conformité.

CRÉER UNE SOLUTION UNIFIÉE DE DNS ET IPAM AVEC AMAZON ROUTE 53

Infoblox DDI pour AWS s'intègre au service DNS Amazon Route 53, fournissant une console centralisée pour les déploiements AWS et cloud hybride, assurant visibilité, gestion cohérente et sécurité. Sans être limité aux zones d'hébergement privées d'Amazon Route 53, la solution Infoblox et Amazon Route 53 permet des déploiements de cloud hybride fiables qui s'étendent au-delà d'AWS.

- **Manque de visibilité sur le cloud hybride :** Sans une solution DNS et IPAM cohérente à travers le cloud hybride, le service informatique de l'entreprise doit utiliser plusieurs outils pour accéder aux données DNS et aux adresses IP. Ce manque de visibilité entraîne des délais de dépannage plus longs, réduit la capacité de planification du réseau et augmente les risques de sécurité. Il accroît également les incohérences dans la gestion à l'échelle de l'entreprise de l'espace d'adresses DNS et IP.
- **Sécurité DNS limitée :** Route 53 offre une sécurité DNS limitée et une capacité avancée de détection des menaces pour les déploiements AWS et de cloud hybride. L'exfiltration de données via le DNS tunneling et les logiciels malveillants utilisant le DNS sont des menaces courantes qui peuvent paralyser les réseaux informatiques.

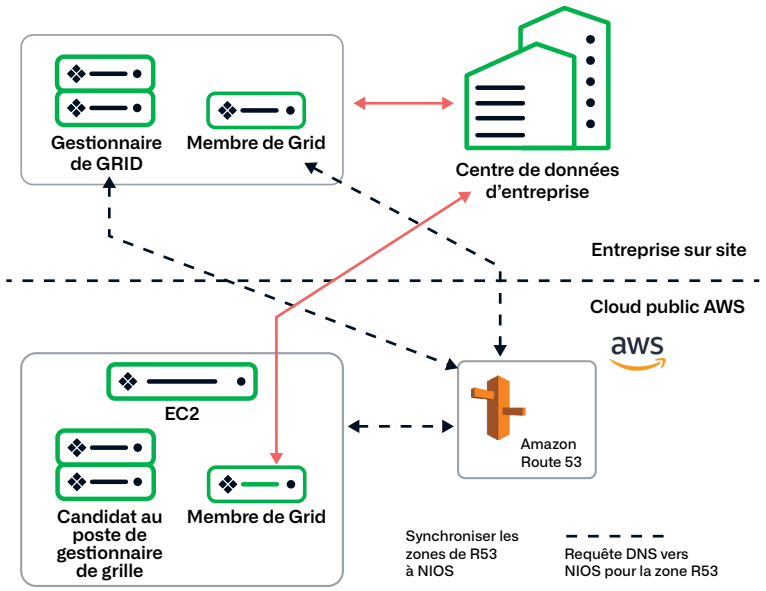


Figure 1 : Gestion unifiée à travers un cloud hybride

Améliorer la visibilité contextuelle sur les déploiements AWS et hybrides

La visibilité contextuelle du réseau est essentielle dans les environnements hybrides multi-cloud modernes. Étant donné que Route 53 se concentre exclusivement sur les ressources virtuelles AWS, la visibilité est limitée uniquement à ces instances de cloud public. La solution Infoblox et AWS offre une découverte automatisée, une visibilité améliorée et un suivi des VPC et des instances EC2 sur une plateforme unique, ce qui simplifie l'intégration des actifs du cloud public sous une gestion commune des DNS et des adresses IP. Infoblox simplifie la création et le nettoyage des enregistrements après la suppression des instances. Il détecte et inclut ou exclut des ressources réseau en utilisant le routage inter-domaine sélectif (CIDR ou IP privée) vDiscovery pour assurer une distribution efficace des adresses IP dans AWS.

Pour les équipes ayant besoin de gérer et synchroniser plusieurs comptes dans Amazon Route 53, Infoblox économise un temps considérable et des frais d'utilisation AWS en éliminant les déploiements de membres vNIOS dans chaque compte et en synchronisant toutes les zones hébergées de Route 53 avec le Grid. vDiscovery réduit les tâches de découverte multiples en un seul travail de découverte sur plusieurs régions et comptes AWS. Il conserve également les filtres de compte pour permettre la sélection de régions et la migration des tâches vDiscovery existantes sans perte de données, afin d'améliorer l'expérience utilisateur, l'efficacité des charges de travail et le contrôle administratif.

Pour les clients fédéraux et autres clients gouvernementaux, Infoblox permet d'améliorer la visibilité et le contrôle en fournissant une prise en charge de la synchronisation Route 53 et de vDiscovery pour plusieurs régions et comptes AWS GovCloud. Cette fonctionnalité fournit un DNS hautement disponible et évolutif et connecte les requêtes des utilisateurs aux applications Internet AWS ainsi qu'à des politiques de routage personnalisées pour réduire la latence.

Les équipes informatiques peuvent considérablement réduire le temps nécessaire pour auditer les informations DNS et adresses IP en obtenant une vue cohérente des paramètres AWS et non AWS dans un plan de contrôle unique pour la conformité, les rapports opérationnels et exécutifs.

Plus grande disponibilité, temps de fonctionnement et résilience

NIOS permet aux clients exécutant des appareils de plateforme cloud (CP) de configurer deux appareils NIOS pour la haute disponibilité (HA) et la disponibilité. La haute disponibilité (HA) mesure la fiabilité avec laquelle les utilisateurs peuvent accéder au système, et si le système est affecté par la maintenance planifiée ou les temps d'arrêt imprévus. Le temps de fonctionnement mesure le temps pendant lequel un système est opérationnel. Avec la haute disponibilité (HA), les administrateurs peuvent éviter les points de défaillance uniques dans Azure et d'autres environnements de cloud public, surtout pour les applications et charges de travail critiques.

Sécurité DNS et contrôle renforcés

Ces dernières années, les attaques par déni de service distribué (DDoS) contre le fournisseur de services Internet Dyn et d'autres organisations ont démontré la nécessité d'une protection contre les menaces basées sur le DNS pour minimiser les interruptions d'activité coûteuses, les pertes de revenus et les atteintes à la réputation de la marque. NIOS ajoute la protection DNS avancée virtuelle (vADP) pour le cloud public AWS afin de détecter et d'atténuer la plus large gamme d'attaques DNS, y compris les attaques volumétriques, NXDOMAIN, le détournement de DNS et d'autres exploits. Avec vADP, les administrateurs peuvent rapidement détecter les attaques, maintenir l'intégrité du DNS, améliorer le temps de fonctionnement et étendre la protection DNS externe des environnements locaux sur site aux environnements de cloud public.

Pour renforcer davantage la sécurité du système, Infoblox permet la synchronisation de vNIOS avec les listes de sous-ensembles multi-comptes d'Amazon Route 53 pour accroître la posture de sécurité et améliorer le contrôle. Les administrateurs peuvent étendre la découverte et la synchronisation de Route 53 à partir d'une seule instance NIOS vers une liste de plusieurs comptes AWS. Les administrateurs peuvent choisir entre 1) NIOS fournissant une découverte automatique des comptes, ou 2) spécifier une liste de comptes à découvrir et à synchroniser à partir des environnements Route 53. Cette capacité renforce la sécurité en 1) empêchant les comptes enfants d'accéder à la racine ; 2) bloquant l'accès des administrateurs délégués ; 3) inhibant la découverte de tous les comptes des unités organisationnelles (OU) ; et 4) utilisant l'accès par autorisation Assume-Role. Ces dispositions de sécurité DNS renforcent les services réseau essentiels contre les attaques et maintiennent les applications disponibles et performantes, permettant ainsi aux organisations de se concentrer sur le service à la clientèle et la gestion de leur entreprise.

Maintenir une plateforme DDI cohérente pour le cloud hybride

De nombreuses organisations déploient un environnement hybride combinant des infrastructures sur site, privées virtuelles, hybrides et publiques, multi-cloud, y compris AWS. Au lieu de recourir à des feuilles de calcul manuelles obsolètes ou à la complexité de solutions disparates, Infoblox réduit la nécessité de mettre en place des serveurs DNS polyvalents et permet des communications entre les sites et AWS, en intégrant les enregistrements DNS de plusieurs plateformes au sein d'un seul plan de contrôle afin d'améliorer la cohérence et la gestion.

Infoblox prend également en charge les types d'instances EC2 R6, ce qui améliore les performances tout en réduisant le coût total de possession. Infoblox permet une connexion directe à AWS Nitro Systems et à la console série EC2 pour un dépannage plus rapide, avec une meilleure expérience utilisateur et un meilleur contrôle. vNIOS améliore encore la cloud security et le contrôle du cloud en permettant le chiffrement Elastic Block Store (EBS) pour les données au repos, les données en transit et toutes les sauvegardes de volumes.

Les options de déploiement flexibles

Infoblox DDI pour AWS est étroitement intégré aux appareils virtuels et physiques sur site de pointe. La plateforme DDI complète peut prendre en charge le cloud public AWS, les environnements de cloud privé (par exemple, y compris VMware, OpenStack, Microsoft et autres) et les réseaux traditionnels, ou toute combinaison dans un déploiement hybride. La solution unifiée garantit un maximum de flexibilité, d'évolutivité et de disponibilité des services.

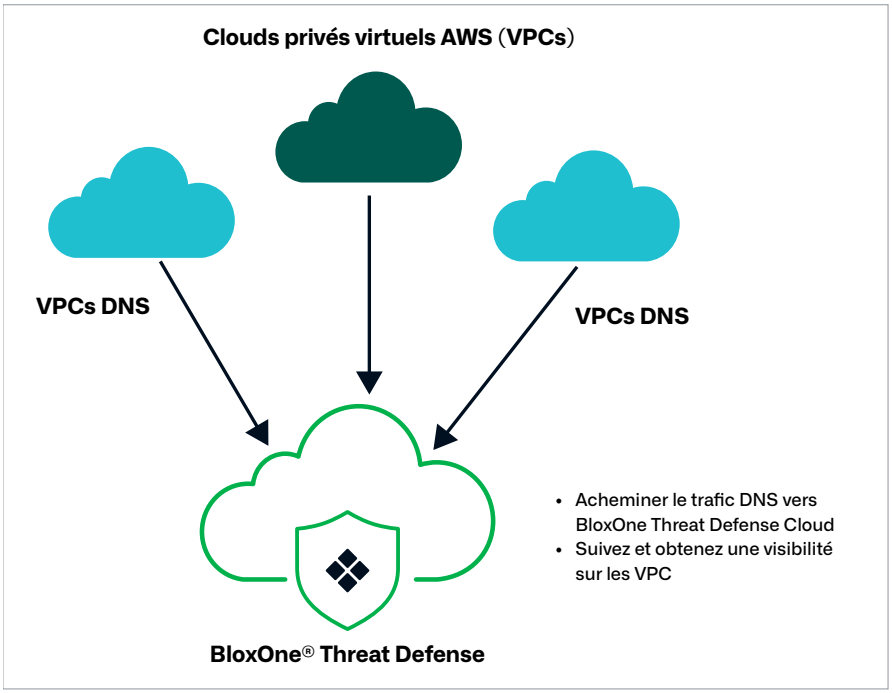
Infoblox propose une gamme complète d'options de déploiement via des appareils physiques et logiciels sécurisés et spécialement conçus pour les petits bureaux à distance et les succursales, les organisations de taille moyenne et les grandes entreprises et les fournisseurs de services avec des centres de données et des sites distribués. La plateforme physique et logicielle de l'appliance Trinzic X6 offre des performances DNS et DHCP jusqu'à 50 % supérieures à celles des modèles précédents. Elle inclut également des licences économiques pour l'automatisation des API de la plateforme Cloud, le pare-feu DNS et l'équilibrage de charge global des serveurs de contrôle du trafic DNS. Quels que soient les besoins de votre organisation, Infoblox propose des solutions commerciales, d'entreprise et de fournisseur de services qui offrent une solution réseau cohérente et essentielle avec la fiabilité et la flexibilité nécessaires pour faire évoluer votre environnement en fonction des besoins de votre entreprise.

Infoblox permet la migration vers le cloud en autorisant les administrateurs à déployer les appliances de découverte et de création de rapports et d'analyse Network Insight dans les clouds publics AWS. Network Insight offre une découverte intégrée des couches 2 et 3, une synchronisation IPAM avec les appareils, les hôtes finaux et les ports réseau, la gestion des ports de commutation, ainsi que des notifications de cycle de vie et de conformité. En outre, la solution Infoblox Reporting and Analytics, construite sur Splunk, le leader du marché de la recherche de données, fournit des capacités de surveillance, de visualisation et de SIEM. L'installation d'appliances optimisant les solutions dans AWS soutient les initiatives « cloud-first », simplifie la migration des centres de données physiques vers le cloud, réduit les ressources des centres de données physiques et offre une visibilité mono et multisite sur les métadonnées DDI pour l'audit historique/la conformité, l'alerte en temps réel, la performance du réseau et la planification de la capacité. Par conséquent, les organisations obtiennent une visibilité complète à la demande, simplifient les rapports de conformité et permettent des audits détaillés des informations DNS et des adresses IP pour les ressources AWS à travers les réseaux et les régions géographiques.

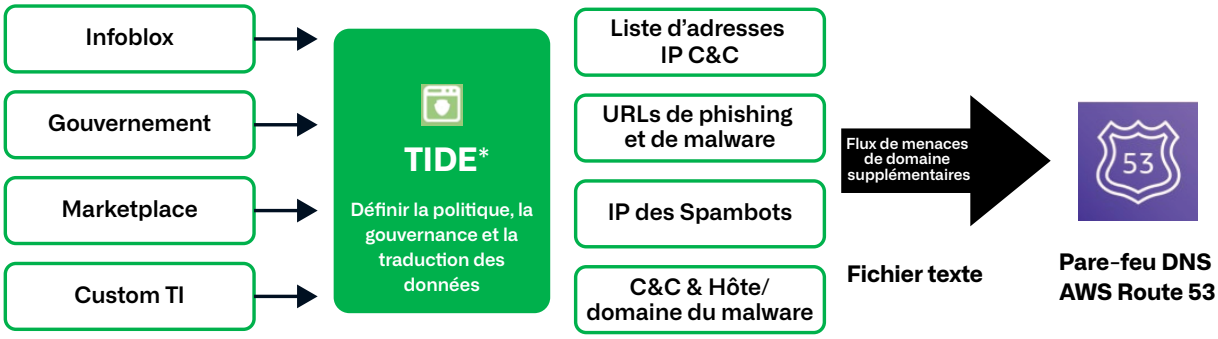
Étendre la sécurité de la couche DNS et la détection des menaces à AWS

Les utilisateurs peuvent également tirer parti d'Infoblox DNS Security, de l'IPAM (Gestion des adresses IP) et de la Threat Intelligence sélectionnée pour obtenir une visibilité sur les VPC AWS et optimiser la détection des menaces pour le pare-feu DNS d'Amazon Route 53. La mise en œuvre de BloxOne® Threat Defense d'Infoblox dans le cadre d'une stratégie globale réduit considérablement le risque d'attaques et d'exploits avancés, ainsi que l'exfiltration de données DNS.

Grâce aux intégrations étendues de l'écosystème, les utilisateurs peuvent automatiser la réponse aux événements détectés et utiliser le contexte réseau pour prioriser la réponse. Les utilisateurs peuvent gérer et minimiser efficacement les menaces dans les VPC AWS en acheminant le trafic DNS des VPC vers BloxOne Threat Defense Cloud, en suivant et en obtenant une visibilité sur les instances cloud, et en réduisant les risques liés aux cybermenaces.



En outre, les organisations peuvent tirer parti de la plateforme Infoblox TIDE (Threat Intel Data Exchange) pour transmettre des indicateurs de compromission (IOC) à la fois à l'appliance DNS AWS d'Infoblox et au pare-feu DNS Amazon Route 53, assurant une sécurité cohérente pour tous les environnements et optimisant la précision grâce à leur choix de flux de renseignements sur les menaces en fonction de leurs besoins spécifiques. L'accès à des dizaines de flux de menaces supplémentaires d'Infoblox TIDE complète ceux fournis par le pare-feu DNS Route 53. La capacité de détecter et de bloquer les menaces actuelles à l'aide d'un « super-feed » personnalisé améliore la pile de sécurité pour renforcer les capacités de défense, d'investigation et de réponse.



CONCLUSION

L'accent isolé d'Amazon Route 53 sur AWS présente des lacunes en matière de gestion et de services réseau de base lors de la gestion d'infrastructures sur site et hybrides multi-cloud, y compris un manque de visibilité, d'incohérence et de sécurité entre les plateformes. Infoblox DDI pour AWS comble ces lacunes en exploitant la plateforme DDI leader du marché et en simplifiant la gestion grâce à une console unique pour administrer les composants DNS sur site, dans le cloud public AWS et les composants DNS critiques. BloxOne Threat Defense offre une sécurité DNS de base pour protéger les environnements hybrides grâce à la détection des menaces, la réponse et les intégrations d'écosystèmes afin d'optimiser les performances de sécurité.

CONTACTEZ-NOUS

Pour plus d'informations ou pour obtenir des réponses sur Infoblox DNS et IPAM et autres services réseau pour Amazon Web Services (AWS), contactez votre équipe Infoblox, consultez nos intégrations réseau critiques ou contactez-nous sur Infoblox.com.

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

+1.408.986.4000
www.infoblox.com

Version : 20240529v2