

ÉTUDE DE CAS

L'Université de Birmingham économise 125 jours de travail grâce à l'automatisation réseau d'Infoblox



LE RÉSUMÉ

Depuis plus d'un siècle, [l'Université de Birmingham](#) (UoB) poursuit et transmet le savoir à travers un enseignement d'excellence et une recherche de renommée mondiale.

Première des prestigieuses universités « redbrick » du Royaume-Uni, l'institution accueille plus de 40 000 étudiants sur ses campus de Birmingham et Dubaï. Son personnel et ses anciens élèves comptent 10 lauréats du prix Nobel, ayant contribué à des découvertes scientifiques majeures, comme le boson de Higgs ou les ondes gravitationnelles.



Infoblox ne crée pas de problèmes, il les résout."

Renyk de'Vandre,
Ingénieur réseau principal,
Équipe des services cloud,
Université de Birmingham

LA SITUATION

Systèmes DNS multiples et disjoints

Pour atteindre son ambition de rester une institution de recherche publique de premier plan, l'université a besoin d'un réseau rapide, fiable, simple à gérer et hautement sécurisé.

La réalisation de cette vision impliquait une modernisation des services réseau critiques tels que le DNS, le DHCP et la gestion des adresses IP (DDI). L'exploitation de ces services s'est développée de façon organique avec l'évolution du réseau. Et avec le temps, l'université a fini par adopter différents systèmes pour gérer les différents aspects du DDI, notamment le DNS.

La majorité des workloads DNS était traitée via le DNS d'Active Directory (AD) Microsoft, une petite portion par Infoblox NIOS DDI, et d'autres zones par des solutions héritées, dont un logiciel développé en interne il y a 20 ans et un service BIND exécuté sur du matériel ayant dépassé sa fin de vie.



LES DÉFIS

Dysfonctionnements et frustrations liés à la gestion du DNS

Cette cohabitation de systèmes DNS disparates nuisait au bon fonctionnement de l'université : elle freinait les opérations, générait une charge administrative inutile et bloquait les projets en cours. Chaque système fonctionnait de manière indépendante, sans intégration entre les outils. Aucune cohérence dans la configuration DNS pour chaque solution, aucun système de gestion, de reporting ou d'alerte unifié et consolidé. Résultat : un comportement DNS imprévisible et l'impossibilité pour les outils existants de prendre en charge les normes modernes.

Ce manque de cohésion a créé des obstacles même pour les tâches de base, telles que la simple mise à jour des enregistrements DNS. « Lorsqu'on ajoutait un enregistrement DNS dans un système, il fallait vérifier qu'il avait bien été saisi dans les autres », se souvient Renyk de Vandre, ingénieur réseau principal de l'équipe des services cloud de l'Université de Birmingham. Cette situation entraînait inévitablement des erreurs de mise à jour de ces enregistrements DNS sur l'ensemble des systèmes. Des enregistrements DNS devenus obsolètes s'accumulaient, sans moyen de vérifier leur validité, entraînant de plus en plus d'incohérences dans les zones DNS.

La gestion des adresses IP (IPAM) représentait un autre obstacle de taille. Au quotidien, les équipes réseau devaient gérer 400 000 adresses IP statiques. Et chaque fois que des modifications étaient apportées, ce qui était fréquent en raison de la nature évolutive du campus, elles devaient être saisies manuellement.

Parmi les autres obstacles, citons les informations dupliquées, mal formatées ou les enregistrements DNS obsolètes, de même que les conflits fréquents entre l'IPAM et le DHCP (Dynamic Host Configuration Protocol). De plus, chaque système DNS utilisait ses propres API pour étendre les fonctionnalités à d'autres outils et tâches réseau, augmentant la surcharge de gestion.

Avec tous ces problèmes persistants, M. de Vandre et son équipe devaient également composer avec une architecture DDI fondamentalement défaillante en raison de son évolution. Dans une architecture fluide, les systèmes DNS qui gèrent les requêtes DNS sont correctement délégués pour fournir des réponses rapides aux requêtes qu'ils sont autorisés à traiter dans leurs zones DNS respectives. Cependant, en raison de l'évolution hétéroclite des solutions DDI de l'Université de Birmingham, l'autorité DNS déléguée faisait défaut dans des parties clés du réseau. Des problèmes liés à une délégation incorrecte de Microsoft AD, en particulier, entraînaient des retards dans la résolution DNS, voire des échecs, ce qui dégradait les performances du réseau et sa fiabilité. Les délégations incorrectes dans AD affectaient également la visibilité depuis Infoblox, car les clients étaient dirigés vers AD au lieu du résolveur primaire préféré.

Le fait qu'une si grande partie du réseau repose sur Microsoft AD causait également d'autres problèmes, le plus sérieux étant le manque de visibilité sur la sécurité. Les données DNS offrent une visibilité sans précédent sur les appareils clients : où ils vont et à quoi ils se connectent. « Si vous ne pouvez pas voir ce client, vous ne pouvez pas le contrôler. Vous ne pouvez pas le corriger », déclare M. de Vandre. Il pouvait voir clairement tous les clients se connectant via Infoblox NIOS, mais aucun de ceux passant par Microsoft AD. Et étant donné que Microsoft AD représentait 90 % de tous les clients, les implications en matière de sécurité étaient énormes.

Client : University of Birmingham
Secteur : Éducation
Lieu : Birmingham, Angleterre

LES OBJECTIFS :

- Surmonter les défis réseau liés à l'utilisation d'outils DDI fragmentés
- Réduire la surcharge réseau et l'effort administratif
- Améliorer la visibilité de la sécurité sur l'ensemble du réseau
- Fournir une plateforme pour l'automatisation de DDI

LES RÉSULTATS :

- Passer de six solutions indépendantes à une solution unifiée de gestion réseau et de sécurité
- Protection complète pour tous les utilisateurs du réseau, y compris les 90 % associés à Microsoft AD
- Automatiser la gestion des adresses IP pour 1 000 imprimantes et économiser 125 jours de travail par an
- La capacité de déployer une solution unique dans le cloud et sur les campus distants

LES PRODUITS :

- [NIOS DDI](#)
- [Infoblox Threat Defense](#)

LA SOLUTION

Migration de Microsoft AD vers Infoblox

L'université a compris que la manière de résoudre ses nombreux problèmes architecturaux et opérationnels liés au DDI était de s'appuyer sur un fournisseur unique pour ses services réseau critiques. Pour atteindre cet objectif, l'équipe informatique a d'abord envisagé de se détourner d'Infoblox NIOS et d'exécuter tous les services DDI via le DNS Microsoft AD, où résidait déjà la majorité de la charge de travail DDI. Cette hypothèse a été formulée avant que l'équipe comprenne l'étendue des fonctionnalités offertes par NIOS DDI. En conséquence, l'équipe IT de l'université a suivi une formation dispensée par Infoblox sur les avantages d'une solution DDI consolidée et agile. Une fois la formation terminée, il est devenu clair que AD DNS n'était pas une solution DDI complète capable d'offrir l'éventail de gestion, de visibilité, de reporting et d'API unique nécessaire à l'automatisation robuste dont Birmingham avait désespérément besoin, ni les capacités de sécurité DNS intégrées recherchées.

La [formation Infoblox](#) a été déterminante dans la décision de l'université de renouveler Infoblox NIOS ainsi que l'ensemble du Grid Infoblox physique, d'en étendre les fonctionnalités, et de renouveler son contrat de support sur cinq ans, incluant un abonnement de formation sur cette même durée. Les membres de l'équipe sont désormais certifiés sur l'ensemble des produits Infoblox.

Parmi toutes les solutions initialement en place pour la gestion réseau critique de l'université, Infoblox NIOS DDI était la seule à regrouper DNS, DHCP et IPAM sur une plateforme unique. Combiné au Grid Infoblox, il représentait un atout puissant pour l'équipe informatique, mais celle-ci n'utilisait qu'une infime partie de ses capacités. « C'était comme avoir une Porsche qu'on conduit jusqu'au fond du jardin avant d'en descendre », dit M. de Vandre avec du recul. Il a également découvert que NIOS DDI n'avait jamais été correctement configuré. « Il ne faisait pas ce qu'il était censé faire. » Grâce à la formation Infoblox, M. de Vandre a corrigé les problèmes de configuration, ce qui a permis de résoudre de nombreux problèmes persistants.

L'établissement avait une liste étendue d'exigences pour sa plateforme DDI et de sécurité. Tout d'abord, toute solution DNS devait coexister avec AD DNS, et non le remplacer totalement, car celui-ci représentait une part majeure du réseau. D'un point de vue réseau, l'architecture devait également être évolutive et résiliente. De plus, elle devait permettre à l'équipe réseau d'accéder facilement à la gestion de manière sécurisée, et réduire la complexité et la charge administrative en rationalisant les services DDI à travers les différents systèmes. Pour réaliser cet objectif, la migration de tous les services DNS Microsoft vers la plateforme NIOS DDI était essentielle.

L'université avait également besoin d'une plateforme permettant l'automatisation des processus statiques, comme l'IPAM, avec la prise en charge d'une API unique, et des capacités d'intégration étendues avec des outils d'automatisation comme Aruba ClearPass.

Pour la sécurité, Birmingham exigeait une solution capable de fournir de la threat intelligence, d'automatiser la remédiation des menaces et de protéger l'ensemble des clients. Il a fallu plus d'un an à l'université pour achever la migration de Microsoft AD vers Infoblox, principalement en raison de son ampleur : 38 000 machines fixes et des problèmes accumulés en 30 ans de gestion DDI disparate. La migration s'est déroulée sans interruption majeure de service. Aujourd'hui, M. de Vandre et ses collègues ont une visibilité et un contrôle complets sur le DNS, le DHCP et l'IPAM à travers leurs différentes solutions réseau. « Tout est géré depuis un seul endroit », déclare M. de Vandre. Cela inclut également Infoblox Threat Defense™, qui protège de manière proactive l'ensemble des 40 000 étudiants et membres du personnel de l'université contre la plus vaste gamme de menaces : malwares, ransomwares et exfiltrations de données.

LES RÉSULTATS

Simplicité réseau, économies et sécurité réunies dans une seule solution

Avec Infoblox, l'université a éliminé la complexité réseau et les conflits de données qui nuisaient aux performances et faisaient grimper les coûts de gestion. La résolution DNS est plus rapide et plus réactive qu'auparavant. Les équipes réseau et sécurité disposent désormais d'une source unique de vérité pour le DDI et d'une vue consolidée de l'ensemble des actifs réseau, y compris ceux associés à Microsoft AD. Contrairement à Microsoft AD, NIOS DDI offre l'ensemble des fonctionnalités DNS, DHCP et IPAM. « AD est une solution DNS », déclare M. de Vandre, « mais elle est loin d'égaler Infoblox en matière de DHCP ou d'IPAM. »

D'un point de vue réseau et sécurité, la solution est synonyme d'autonomie pour M. de Vandre et ses collègues. « Infoblox me fournit les outils pour concrétiser les projets qui sont essentiels à la réalisation de la vision stratégique de l'université », explique-t-il. Combiné au Grid Infoblox, NIOS DDI offre l'évolutivité et la résilience nécessaires, sur site comme dans les environnements hybrides et multicloud, permettant aux administrateurs de gérer de manière centralisée le DDI sur les campus du Royaume-Uni et des Émirats arabes unis.

Outre le temps gagné grâce à l'automatisation des enregistrements auparavant statiques et à la réduction des incidents et du temps moyen de résolution (MTTR), la résolution des problèmes DDI a été grandement simplifiée grâce à des fonctions de reporting et d'alerte de niveau entreprise, ainsi qu'à la visibilité accrue offerte par Infoblox.

Standardiser le DDI sur une solution unique signifie que les déploiements hors site, dans le cloud ou sur le nouveau campus de plusieurs millions de dollars à Dubaï, ne nécessitent désormais plus qu'une seule solution (et non plus jusqu'à trois comme auparavant), réduisant considérablement la complexité et les coûts pour l'établissement.

Un avantage central d'Infoblox ressort aux yeux de M. de Vandre : « Infoblox apporte une visibilité et un reporting sur tout l'espace DDI qui n'existaient tout simplement pas auparavant. » Avec Infoblox, ce qui était autrefois incontrôlable et complexe est désormais simple et presque sans risque en cas de modifications. Par exemple, avant la migration AD, la gestion DNS nécessitait des saisies distinctes dans jusqu'à six systèmes différents. « Lorsqu'un problème apparaît aujourd'hui, nous avons un seul endroit où chercher, et nous pouvons voir exactement comment un client est configuré », dit-il.

Centraliser le DDI sur une plateforme unique Infoblox a permis des économies substantielles. Avec Infoblox, l'université n'a plus besoin d'un service DDNS séparé pour maintenir les enregistrements DNS à jour. Elle a également pu se débarrasser de BIND et des anciens logiciels maison. En outre, avant la migration d'AD vers Infoblox, l'université devait attribuer manuellement des adresses IP statiques à plus de 1 000 imprimantes, ainsi qu'à des milliers de machines situées dans des salles de classe, laboratoires et amphithéâtres. La solution DHCP d'Infoblox, à la fois riche en fonctionnalités et résiliente, a rendu la migration de ces IP simple et fluide. L'intégration étroite entre l'IPAM et le DHCP dans Infoblox a également permis d'identifier facilement les enregistrements dupliqués, d'automatiser les données DHCP dans l'IPAM et le DNS, d'introduire de nouvelles capacités et de réduire la charge administrative pesant sur les équipes opérationnelles. Grâce à l'attribution automatisée des adresses IP dans NIOS DDI, l'université économise désormais plus de 125 jours de travail par an, et les déplacements d'imprimantes se font désormais en plug-and-play.

Des économies supplémentaires sont rendues possibles grâce à l'API Infoblox, qui permet aux équipes de se connecter facilement aux outils des fournisseurs de leur choix. L'API Infoblox permet l'automatisation de 99 % des fonctions Infoblox ; encore en phase initiale, c'est une capacité que l'université est déterminée à développer.

D'autres économies sont réalisées grâce aux capacités en libre-service de NIOS DDI. Avant l'adoption complète d'Infoblox, les ingénieurs réseau de l'université étaient submergés par les demandes des utilisateurs finaux pour effectuer des tâches de bas niveau, comme la mise à jour d'enregistrements DNS. Ces allers-retours consommaient un temps précieux et provoquaient des retards inutiles pour d'autres équipes et les « clients » internes de l'université.

Grâce à l'interface web intuitive de NIOS, avec des droits d'accès basés sur les autorisations, les utilisateurs finaux peuvent désormais effectuer eux-mêmes les tâches de base, avec des impacts clairs en termes d'économies. « Imaginez le retour sur investissement que nous obtenons en supprimant toute cette bureaucratie, tous ces délais ? » déclare M. de Vandre. Bonus : la fonction libre-service de NIOS libère les ressources techniques principales pour qu'elles se consacrent à des projets à plus forte valeur ajoutée.

Toute cette visibilité et ce reporting ont également permis à l'université de répondre plus facilement aux exigences de sécurité et d'audit, grâce à des rapports automatisés générant à la demande des preuves d'audit, au lieu de devoir s'y atteler lors d'un exercice annuel fastidieux.

Sur le plan de la sécurité, Infoblox permet à l'Université de Birmingham d'assurer une protection complète sur l'ensemble de son réseau. Le fait de prendre en charge les clients Microsoft Windows directement depuis Infoblox donne aux équipes sécurité une visibilité critique sur 90 % de l'activité réseau, qui leur échappait jusque-là. « Maintenant que tous les clients DNS passent par Infoblox, je peux tous les voir et agir sur chacun individuellement. Je peux tout protéger, partout », déclare M. de'Vandre.

Contrairement à Microsoft, Infoblox est conçu pour offrir les meilleures capacités à tous les clients, pas uniquement aux clients Windows, il n'y a donc aucune inquiétude à avoir concernant les incompatibilités ou les limitations liées aux standards. Tant que le client est basé sur les standards, ça fonctionne, et dans de nombreux cas, la souplesse de la plateforme permet même de prendre en charge des exigences spécifiques.

M. de'Vandre est catégorique sur le mythe selon lequel Active Directory nécessiterait AD DNS pour fonctionner. Il a fallu beaucoup de persuasion pour convaincre les parties prenantes que la mise hors service de AD DNS ne poserait aucun problème, mais à ce jour, aucun incident n'a été causé par l'utilisation d'Infoblox comme seule source d'information DDI pour AD.

Pour M. de'Vandre, l'une des raisons principales du succès rencontré avec Infoblox tient à son engagement en matière de formation et de support. « Je pensais connaître le DNS quand j'ai commencé. Je me trompais », admet-il. « J'ai compris avec la formation Infoblox. » D'un point de vue gestion de compte, la relation qu'il entretient avec l'équipe Infoblox est unique. « En 30 ans de carrière, je n'ai jamais connu cela avec une autre organisation. »

CONCLUSION

Les capacités étendues d'Infoblox sont quelque chose que M. de'Vandre valorise énormément. « C'est un véritable couteau suisse qui nous permet de résoudre les problèmes. » Alors que M. de'Vandre envisage d'ajouter encore plus d'automatisation et de fonctionnalités multicloud à son arsenal, la gestion du réseau n'est plus un obstacle pour lui. « Nous pouvons désormais envisager l'avenir avec confiance, sachant que notre solution DDI est capable de porter la vision de la plateforme et de l'université. »



Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

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

+1.408.986.4000
www.infoblox.com/fr