

ÉTUDE DE CAS

Le San Mateo County Community College District gagne en résilience et en sécurité essentielles grâce à Infoblox



LE RÉSUMÉ

Le [San Mateo County Community College District](#) (SMCCD), fondé en 1922, regroupe trois établissements : Cañada College, College of San Mateo et Skyline College.

Situés entre San Francisco et la Silicon Valley, ils accueillent près de 40 000 étudiants chaque année, leur offrant les deux premières années d'enseignement universitaire grâce à une grande variété de programmes de transfert et de programmes de formation professionnelle et technique. Les étudiants peuvent obtenir un diplôme d'associé en arts ou en sciences, ou recevoir un certificat de compétence dans le domaine de leur choix. De plus, le district propose des services de qualité pour les collèges-lycées sur chaque campus, ainsi que des programmes à double inscription et des inscriptions simultanées pour les lycéens.

LA SITUATION

Une infrastructure diversifiée au service de campus diversifiés

L'une des principales missions du district est de fournir un enseignement secondaire accessible à une population étudiante diversifiée dans ses trois établissements, ainsi qu'à ses cours et programmes en ligne. L'une des principales priorités du SMCCD est d'apporter son soutien à chaque étudiant, quel que soit le lieu où il suit ses cours. « Nous nous efforçons vraiment de nous assurer qu'ils aient accès à tout ce dont ils ont besoin lorsqu'ils ne sont pas en classe », déclare Daman Grewal, le DSI du district. Pour soutenir cette initiative, les étudiants bénéficient d'un accès gratuit aux comptes Microsoft, aux Google Workspaces, aux systèmes de gestion de l'apprentissage en ligne et aux applications cloud, telles que Salesforce et LinkedIn.

D'un point de vue informatique, chaque institution est unique. « Nous ne sommes pas un district avec trois campus ; nous sommes un district avec trois universités », note Adam West, responsable de la sécurité de l'information du SMCCD. Chaque université a son propre département informatique et ses propres budgets.

« Les universités sont complètement séparés, et nous essayons de respecter cela et de les traiter de la même manière », déclare Adam.

« Infoblox est notre première ligne de défense. Il fait partie des outils qui rendent nos services plus sûrs et plus robustes. »

Adam West
Responsable de la sécurité de l'information, San Mateo County Community College District

Au cours des dernières décennies, l'infrastructure réseau du district s'est appuyée sur Microsoft DNS pour son DNS interne et sur Linux pour son DNS externe, ainsi que sur Microsoft pour le DHCP. Cette mise en œuvre a coexisté avec des déploiements multi-cloud, y compris Microsoft Azure et Oracle Cloud Infrastructure (OCI). Pour la sécurité, le SMCCD a mis en place des pare-feu, des filtres de passerelle Web et diverses mesures de détection et de réponse étendues (XDR).

LES DÉFIS

Manque de résilience et d'agilité

Au fil du temps, les limitations de la solution de gestion du réseau DNS du district, basée sur Microsoft et Linux, sont devenues plus apparentes. Les étudiants universitaires s'attendent à un accès immédiat à Internet et aux services cloud. Cependant, les implémentations existantes du district n'étaient pas à la hauteur. Les étudiants et le personnel enseignant rencontraient des problèmes de connectivité et des lenteurs en raison d'erreurs dans les enregistrements DNS ou de mauvaises configurations réseau. Identifier la cause première d'un problème était un effort manuel ardu nécessitant l'utilisation de consoles de gestion spécialisées.

Le manque de visibilité et de contrôle centralisés s'est aggravé à mesure que le nombre d'appareils augmentait. Par exemple, parmi les 5 000 employés et 40 000 étudiants du SMCCD, nombreux sont ceux qui utilisent plusieurs appareils au cours d'une journée, notamment des ordinateurs portables, des tablettes et des montres connectées, chacun disposant de sa propre adresse IP. Il est devenu de plus en plus difficile de maintenir une connectivité rapide entre les appareils et les charges de travail multi-cloud. L'implémentation de Microsoft manquait d'agilité pour répondre aux exigences d'un environnement d'apprentissage de plus en plus orienté vers le cloud.

Une préoccupation plus importante concernait la solution DNS Linux, qui n'était pas distribuée. Le district avait besoin d'un moyen de migrer les services DNS entre les sites, une opération risquée si l'un des serveurs Linux tombait en panne pendant qu'une sauvegarde était en cours. « Le système n'est pas conçu pour permettre d'apporter des modifications si l'un des nœuds tombe en panne », explique M. West. En outre, une défaillance de ce genre pourrait potentiellement mettre le district hors ligne.

Outre les problèmes de connectivité, la sécurité n'a jamais quitté l'esprit de M. West, des préoccupations qu'il résume par une inquiétude majeure : « Les gens qui cliquent sur quelque chose qu'ils ne devraient pas. »

LA SOLUTION

Éliminer les points de défaillance tout en renforçant la sécurité

Du côté de la mise en réseau, le SMCCD savait qu'il lui fallait une solution qui offrirait une disponibilité infaillible tout en simplifiant les tâches de gestion complexes. Pour M. Grewal, le choix d'Infoblox était évident : il avait déjà vu à l'œuvre sa solution de gestion consolidée des DNS, DHCP, et de la Gestion des adresses IP (DDI). Au début de sa carrière, M. Grewal a mis en œuvre avec succès le système Infoblox sur un navire autonome au milieu de l'océan, fournissant un accès Internet stable et le DHCP pour les étudiants et les équipages maritimes. « Infoblox a sauvé les personnes à bord du navire », clame-t-il. Il était convaincu que si Infoblox pouvait offrir la vitesse et la fiabilité du réseau au milieu de l'océan, il pourrait faire de même pour les étudiants, le corps enseignant et le personnel du district.

Pour la gestion du réseau, la solution Infoblox se compose de l'Infoblox Grid, qui, grâce à sa technologie de base de données distribuée, élimine le problème du point de défaillance unique que le SMCCD rencontrait avec Linux. Pour renforcer davantage la fiabilité, le district utilise une option primaire multi-grille. La solution comprend également deux serveurs physiques fonctionnant en tant que paire à plus grande disponibilité (HA) et deux serveurs virtuels pour chacun des trois sites du campus. « Je souhaitais que chacun soit indépendant et redondant », explique M. West. Un serveur de reporting et un serveur de découverte viennent compléter la solution.

Client : San Mateo County
Community College District
Secteur : Éducation
Lieu : San Mateo, Californie

LES OBJECTIFS :

- Assurer la redondance, la résilience et la sécurité du réseau pour les trois campus indépendants du district
- Simplifier la gestion du réseau pour les administrateurs système tout en garantissant un accès ininterrompu aux appareils qui se connectent aux applications et ressources basées sur le cloud
- Renforcer la sécurité pour les étudiants et le personnel

LES RÉSULTATS :

- Disponibilité réseau rapide et continue grâce à la suppression des points de défaillance uniques grâce aux fonctionnalités d'Infoblox Multi-Grid Manager
- Gestion simplifiée des réseaux multi-cloud avec des capacités DDI consolidées accessibles depuis n'importe quelle interface web
- Sécurité renforcée pour tous les utilisateurs du district avec une défense en profondeur proactive

LES PRODUITS :

- NIOS DDI
- BloxOne Threat Defense

Pour des raisons de sécurité, le district protège tous les utilisateurs de ses trois campus avec BloxOne Threat Defense. La solution aide à détecter et à bloquer les attaques de ransomwares et autres malware, dont 92 % reposent sur le DNS. De plus, elle complète les produits de sécurité de Palo Alto Networks sur lesquels le district mise. Pour ce faire, elle détecte les menaces au niveau du plan de contrôle DNS avant qu'elles ne soient visibles par les pare-feu, les endpoints ou d'autres solutions, réduisant ainsi le nombre d'alertes de sécurité générées par ces autres outils.

LES RÉSULTATS

Réussir le test COVID-19 et aller au-delà — haut la main

En matière de déploiement technologique, le SMCCCD n'aurait pas pu choisir un meilleur moment. Les nouvelles solutions Infoblox ont été mises en œuvre à l'été 2019, quelques mois seulement avant que la pandémie mondiale ne frappe. « COVID-19 a évidemment tout changé », déclare Adam. Avant la pandémie, la possibilité pour les étudiants d'accès à Internet et aux ressources cloud était un luxe. « Ce n'était pas essentiel pour la mission », explique-t-il. « Maintenant, ça l'est. Je ne pense pas qu'un étudiant puisse venir en classe sans un ordinateur portable fonctionnel et être opérationnel. »

Alors que la COVID-19 se répandait et que l'enseignement passait du présentiel au virtuel, la disponibilité des services est devenue une préoccupation primordiale pour M. Grewal. « La solution Infoblox est entrée en jeu car nous nous sommes demandé si nous serions en mesure de traiter les pannes en cas de panne de notre centre de données principal, » se souvient M. Grewal. « Pouvons-nous encore fournir des services de base ? Pouvons-nous toujours accéder à Internet pour les technologies utilisées en classe et continuer à répondre aux besoins de nos étudiants ? Et la réponse était : « Oui. » Nous avons suffisamment de redondance intégrée dans nos systèmes. » Adam approuve. Ces appréhensions initiales le préoccupaient également beaucoup. « Nous n'avons plus à nous en préoccuper. Infoblox se charge de tout. »

La possibilité de créer plusieurs grilles primaires Infoblox a non seulement rendu le réseau du SMCCCD plus résilient, mais aussi plus facile à gérer. « Lorsque nous avons découvert Infoblox et le mode multi-primaire distribué qu'ils utilisent, cela a été l'application révolutionnaire pour nous », déclare Adam. Cela a permis à ses équipes d'accéder au système depuis n'importe quel endroit. « Ajoutez à cela le fait que vous pouvez utiliser une interface web pour effectuer les modifications », note-t-il. Les administrateurs système peuvent utiliser un appareil de leur choix sans avoir à installer de logiciel de bureau à distance. Le déploiement d'Infoblox automatise les tâches courantes, par exemple, en éliminant la nécessité d'éditer manuellement des fichiers texte sur un serveur Linux.

Avec Infoblox, West n'entend plus parler des administrateurs système concernant des sites en panne ou des problèmes de configuration perturbant les performances. « Le nombre de problèmes DNS que nous avions avant Infoblox a énormément, énormément, énormément, énormément diminué. »

En outre, la solution Infoblox a optimisé le réseau du SMCCCD grâce à l'automatisation DDI dans les infrastructures sur site, hybrides et multi-cloud. « Dès que vous branchez cet ordinateur portable, dès que vous vous connectez au Wi-Fi, vous obtenez l'adresse IP, les bonnes informations DNS et vous accédez à Internet », explique M. Grewal. « Vous pouvez donc commencer votre journée de manière optimale. »

BloxOne Threat Defense joue un rôle crucial dans l'amélioration de la stratégie de sécurité globale du district. La solution complète d'autres déploiements de sécurité dans la pile de sécurité du SMCCCD et ajoute la capacité essentielle de renforcer la protection des charges de travail et des données multi-cloud du district. « Le fait que toute notre infrastructure soit équipée d'Infoblox, qui surveille l'ensemble du trafic, nous est très bénéfique », souligne M. Grewal. Pour Adam, Infoblox présente l'avantage supplémentaire d'offrir une sécurité multicouche sans compromettre la confidentialité ni la vie privée. « Il est extrêmement important de pouvoir sécuriser le réseau sans avoir à s'immiscer dans la vie d'autrui. »

Parmi ses nombreuses fonctionnalités, BloxOne Threat Defense associe une expertise DNS de premier plan à une science des données innovante pour identifier l'infrastructure des cybercriminels. Cette approche perturbe les activités des pirates et empêche l'exposition aux attaques émergentes et ciblées. « Infoblox est notre première ligne de défense, » explique Adam. « Cette solution fait partie des outils qui rendent nos services plus sûrs et plus fiables. »



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