

ESTUDIO DE CASO

El Distrito de Colegios Comunitarios del Condado de San Mateo refuerza su resiliencia y seguridad con Infoblox



RESUMEN

El Distrito de Colegios Comunitarios del Condado de San Mateo (SMCCD), fundado en 1922, está compuesto por tres instituciones: Cañada College, College of San Mateo y Skyline College.

Ubicados entre San Francisco y Silicon Valley, los colegios atienden a cerca de 40 000 estudiantes al año, ofreciendo los dos primeros años de educación universitaria a través de una amplia variedad de programas de transferencia y formación técnico-profesional. El alumnado puede obtener un título de asociado en artes o ciencias, o bien un certificado de competencia en el área de su elección. Además, el distrito ofrece servicios sólidos para las escuelas secundarias universitarias en cada campus, así como programas de inscripción dual y simultánea para estudiantes de secundaria.

LA SITUACIÓN

Infraestructura diversa para servir a campus diversos

Una de las principales misiones del distrito es ofrecer una educación secundaria accesible a una población estudiantil diversa a través de sus tres instituciones, así como mediante sus cursos y programas en línea. Para SMCCD, una prioridad fundamental es brindar apoyo a cada estudiante, independientemente de dónde realice sus actividades académicas. «Nos estamos centrando realmente en asegurarnos de que cuenten con todo lo que necesitan cuando no están en clase», afirma Daman Grewal, CIO del distrito. Para apoyar esta iniciativa, el alumnado tiene acceso gratuito a cuentas de Microsoft, Google Workspaces, plataformas de gestión del aprendizaje en línea y aplicaciones en la nube como Salesforce y LinkedIn.

Desde el punto de vista de TI, cada institución es independiente. «No somos un distrito con tres campus; somos uno con tres universidades», señala Adam West, responsable de Seguridad de la Información de SMCCD. Cada universidad cuenta con su propio departamento de TI y su propio presupuesto. «Son entidades completamente separadas, y procuramos respetar esa autonomía y tratarlas de la misma manera», añade West.

“Infoblox es nuestra primera línea de defensa. Forma parte del conjunto de herramientas que permiten que los servicios que alojamos sean más seguros y sólidos que nunca».

Adam West
Oficial de Seguridad de la Información,
Distrito de Colegios Comunitarios
del Condado de San Mateo

Durante las últimas décadas, la infraestructura de red del distrito se apoyó en Microsoft DNS para la resolución interna de nombres y en Linux para la externa, junto con Microsoft para los servicios de DHCP. Esta configuración coexistía con despliegues en múltiples nubes, entre ellas Microsoft Azure y Oracle Cloud Infrastructure (OCI). En cuanto a seguridad, SMCCD utilizaba cortafuegos, filtros de puertas de enlace web y distintas soluciones de detección y respuesta extendida (XDR).

EL DESAFÍO

Falta de resiliencia y agilidad

Con el tiempo, las limitaciones de la solución de gestión de red DNS del distrito, basada en Microsoft y Linux, se hicieron más evidentes. Los estudiantes universitarios esperan acceso inmediato a Internet y a servicios en la nube. Sin embargo, las implementaciones existentes del distrito no estaban a la altura. Tanto estudiantes como docentes se enfrentaban a problemas de conectividad y bajo rendimiento, provocados por errores en los registros DNS o por configuraciones incorrectas de red. Determinar el origen del fallo exigía un esfuerzo manual considerable y el uso de herramientas de gestión avanzadas.

La falta de visibilidad y control centralizado se agravó a medida que el número de dispositivos aumentaba considerablemente. Por ejemplo, muchos de los 5000 empleados y 40 000 estudiantes del SMCCD utilizan varios dispositivos a lo largo del día, incluidos ordenadores portátiles, tabletas y relojes inteligentes, cada uno con su propia dirección IP. Mantener una conectividad rápida entre dispositivos y cargas de trabajo en entornos multinube se volvió cada vez más difícil. La solución basada en Microsoft no ofrecía la agilidad necesaria para responder a las exigencias de un entorno educativo cada vez más orientado a la nube.

Otra preocupación importante era que la solución de DNS en Linux no contaba con una arquitectura distribuida. El distrito necesitaba una forma segura de trasladar los servicios DNS entre sedes, pero esto implicaba riesgos si uno de los servidores fallaba durante una copia de seguridad. «No está diseñada para permitir cambios cuando uno de los nodos deja de funcionar», explica West. Además, un solo fallo podía dejar sin conexión a todo el distrito.

Además de los problemas de conectividad, la seguridad fue siempre una preocupación constante para West, quien lo resume de forma muy clara: «La gente hace clic donde no debería».

LA SOLUCIÓN

Eliminar puntos de fallo mientras se refuerza la seguridad

En el ámbito de las redes, SMCCD sabía que necesitaba una solución que ofreciera una disponibilidad inquebrantable y, al mismo tiempo, simplificara la gestión de tareas complejas. Para Grewal, la elección de Infoblox era evidente: ya había visto en acción su solución para la gestión unificada de DNS, DHCP y direcciones IP (DDI). Al comienzo de su carrera, Grewal implementó con éxito el sistema de Infoblox en un barco autónomo en medio del océano, donde proporcionaba acceso estable a Internet y servicios DHCP para estudiantes y tripulaciones marítimas. «Infoblox fue un salvavidas para la gente del barco», afirma. Grewal confiaba en que, si Infoblox podía garantizar velocidad y fiabilidad de red en medio del océano, también podría hacerlo para el alumnado, el profesorado y el personal del distrito.

Para la gestión de redes, la solución de Infoblox se basa en Infoblox Grid, que, gracias a su tecnología de base de datos distribuida, elimina el problema del punto único de fallo que SMCCD enfrentaba con Linux. Para reforzar aún más la fiabilidad, el distrito se beneficia de una opción primaria con arquitectura multi-red. La solución también incluye dos servidores físicos configurados como un par de alta disponibilidad (HA) y dos servidores virtuales en cada una de las tres sedes del campus. «Quería que cada sede tuviera su propia redundancia», comenta West. La infraestructura se completa con un servidor de informes y otro de detección.

Cliente: Distrito de Colegios
Comunitarios del Condado
de San Mateo
Sector: Educación
Ubicación: San Mateo, California

OBJETIVOS:

- Dotar de seguridad, resiliencia y redundancia a la infraestructura de red de los tres campus del distrito
- Simplifique la gestión de la red para los administradores de sistemas mientras garantiza el acceso ininterrumpido a las aplicaciones y recursos en la nube desde cualquier dispositivo
- Refuerce la seguridad para los estudiantes y el personal

RESULTADOS:

- Disponibilidad de red rápida y continua mediante la eliminación de puntos únicos de fallo gracias a las capacidades de Infoblox Multi-Grid Manager
- Gestión simplificada de redes multinube con capacidades DDI consolidadas accesibles desde cualquier interfaz web
- Seguridad mejorada para todos los usuarios del distrito con una defensa proactiva en profundidad

PRODUCTOS:

- NIOS DDI
- BloxOne Threat Defense

Para garantizar la seguridad, el distrito protege a todos los usuarios de sus tres campus con BloxOne Threat Defense. Esta solución ayuda a detectar y bloquear ataques de ransomware y otros tipos de malware, el 92 % de los cuales dependen del DNS. Además, esta herramienta complementa las soluciones de seguridad de Palo Alto Networks en las que confía el distrito, ya que es capaz de interceptar las amenazas en el plano de control del DNS antes de que sean visibles para los cortafuegos, los endpoints u otras herramientas. Esto permite reducir considerablemente la cantidad de alertas generadas por esos sistemas.

EL RESULTADO

Superar con nota la prueba de la COVID-19

En lo que respecta a las implementaciones tecnológicas, el momento elegido por SMCCD no podría haber sido más acertado. Las nuevas soluciones de Infoblox se desplegaron en el verano de 2019, pocos meses antes de que golpeará la pandemia mundial. «Obviamente, la COVID lo cambió todo», afirma West. Antes de la pandemia, que los estudiantes pudieran acceder a Internet y a los recursos en la nube se consideraba un lujo. «No era fundamental para la misión», dice West. «Ahora lo es por completo. No creo que un estudiante pueda asistir a clase sin un portátil funcional y desenvolverse con normalidad».

A medida que la COVID-19 se desarrollaba y la enseñanza pasaba de ser presencial a virtual, la disponibilidad de servicios se convirtió en una preocupación primordial para Grewal. «En ese momento, se preguntaba: «Si nuestro centro de datos principal dejara de funcionar, ¿podríamos seguir procesando las nóminas?». «¿Podríamos seguir prestando servicios básicos? ¿Mantener el acceso a Internet para las tecnologías del aula? ¿Y continuar atendiendo a nuestro alumnado? Y la respuesta fue: «Sí». «Habíamos incorporado suficiente redundancia en nuestros sistemas». West está de acuerdo. Él también tenía muy presentes esas dudas al comienzo. «Ya no tenemos que preocuparnos por eso. Infoblox simplemente funciona».

La posibilidad de crear múltiples servidores primarios en el Infoblox Grid no solo hizo que la red de SMCCD fuera más resiliente, sino también más fácil de gestionar. «Cuando conocimos Infoblox y su modo distribuido con múltiples servidores primarios, supimos que era la solución ideal para nosotros», afirma West. Esto permitió que sus equipos pudieran acceder al sistema desde cualquier ubicación. «Y si a eso le sumamos el hecho de que se pueden hacer los cambios desde una interfaz web...», añade. Los administradores del sistema pueden utilizar el dispositivo que prefieran sin necesidad de instalar software de escritorio remoto. La implementación de Infoblox automatiza tareas comunes y elimina, por ejemplo, la necesidad de editar archivos de texto manualmente en un servidor Linux.

Con Infoblox, West ya no recibe noticias de los administradores del sistema sobre sitios que se caen o problemas de configuración que interrumpen el rendimiento. «El número de problemas de DNS que teníamos antes de Infoblox ha disminuido muchísimo»

Además, la solución de Infoblox hizo que la red de SMCCD fuera más rápida gracias a la automatización de DDI en la infraestructura local, híbrida y multinube. «En cuanto conecta el portátil, en el momento en que se conecta al Wi-Fi, obtiene la dirección IP, la información correcta de DNS y accede a Internet», explica Grewal. «Así que puede comenzar su jornada de inmediato».

BloxOne Threat Defense desempeña un papel vital en mejorar la postura de seguridad general del distrito. La solución complementa otros despliegues de seguridad en la pila de seguridad del SMCCD y añade la capacidad esencial de reforzar la protección para las cargas de trabajo y los datos en entornos multinube del distrito. «Tener Infoblox en toda nuestra infraestructura viendo todo el tráfico realmente nos beneficia», señala Grewal. Desde la perspectiva de West, un beneficio adicional es que Infoblox proporciona seguridad en capas sin comprometer la confidencialidad ni la privacidad. «Poder mantener la red segura sin tener que entrometerse en la vida de las personas es extremadamente importante»

Entre sus múltiples capacidades, BloxOne Threat Defense combina la experiencia líder en el mercado en DNS con ciencia de datos innovadora para identificar la infraestructura de los actores de amenazas. Este enfoque interrumpe las actividades de los atacantes y previene la exposición a ataques emergentes y dirigidos. «Infoblox es nuestra primera línea de defensa», afirma West. «Es parte del conjunto de herramientas que hace que los servicios que ofrecemos sean más seguros y robustos que nunca».



Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

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

+1.408.986.4000
www.infoblox.com