infoblox

ÉTUDE DE CAS

Sicredi adopte NIOS DDI et BloxOne Threat Defense pour soutenir sa croissance en tant que leader du secteur financier au Brésil

LE RÉSUMÉ

Sicredi est une institution financière coopérative fondée il y a plus de 120 ans. Au cours des deux dernières décennies, l'entreprise a connu une réorganisation interne et a accéléré son expansion. Afin de soutenir cette croissance et de rester à la pointe de l'innovation dans le secteur financier, Sicredi a investi dans la transformation numérique.

Les coopératives de crédit proposent le même portefeuille de produits et services financiers que les établissements financiers traditionnels (comptes courants, cartes, placements), mais se distinguent principalement par leur modèle de gestion. Contrairement aux institutions conventionnelles, dans les coopératives de crédit, les collaborateurs sont les véritables propriétaires de l'entreprise.

Pour mener à bien ce modèle commercial, Sicredi met en œuvre une stratégie de gestion qui repose sur la participation de ses plus de sept millions d'associés, qui jouent le rôle de propriétaires de l'entreprise. Avec plus de 2 500 agences, cette institution financière coopérative est physiquement présente dans tous les États brésiliens et dans le District fédéral, offrant une gamme complète de solutions financières et non financières.

> *"Infoblox a accéléré la livraison de nos produits à nos partenaires et utilisateurs finaux. La configuration d'une machine prenait auparavant en moyenne cinq jours. Aujourd'hui, nous pouvons la réaliser en 15 minutes de manière plus flexible et plus agile."*
>
> **Juliano Luz,**
> **Analyste infrastructure, Sicredi**

LA SITUATION

L'expansion géographique et la numérisation stimulent l'activité des coopératives de crédit

Sicredi a connu une croissance significative en termes de nombre d'agences et de collaborateurs, devenant ainsi l'un des principaux acteurs du secteur financier brésilien ces dernières années. Elle propose actuellement plus de 300 produits et services financiers, allant des comptes courants et des cartes bancaires aux investissements, en passant par les assurances, les consortiums, les terminaux de paiement et les comptes 100 % numériques, destinés aux particuliers, aux personnes morales et aux producteurs ruraux.

Sicredi

Pour accompagner cette évolution, Sicredi a entamé en 2017 un processus de transformation numérique visant à remplacer progressivement ses anciens systèmes de traitement des produits et services, appelés « core banking », par une plateforme plus moderne. Cette adoption de technologie de pointe était cruciale pour offrir une meilleure expérience aux collaborateurs et maintenir la compétitivité sur le marché financier dynamique du Brésil.

Pendant de nombreuses années, Sicredi a fonctionné avec une infrastructure technologique et des machines virtuelles utilisant des outils DHCP et Linux « open source ». Juliano Luz, analyste en infrastructure, qui a rejoint Sicredi en 2008, se souvient d'un environnement obsolète : « Le manque d'évolutivité et d'agilité constituait un véritable défi. L'entreprise avait besoin d'une nouvelle application, d'un nouvel environnement », explique-t-il.

Comme elle utilisait des solutions open source, l'ancien environnement ne bénéficiait d'aucun support externe et tous les problèmes devaient être résolus en interne, ce qui exigeait une implication intense du service informatique. Une autre préoccupation de Sicredi était de renforcer la sécurité contre les cyberattaques.

Sicredi avait déjà mis en place une solution Infoblox en 2013, mais en 2021, elle a décidé de moderniser son environnement technologique. « La mise en œuvre initiale de DDI a été effectuée par l'équipe interne. NTT s'est joint à nous en tant que partenaire lorsque nous avons élargi et mis à jour Infoblox NIOS DDI », a déclaré J. Luz.

LES DÉFIS

Une infrastructure technologique obsolète ralentit les processus manuels

Le nombre croissant de projets, services et produits financiers Sicredi nécessitait un environnement offrant une plus grande flexibilité et une meilleure évolutivité. Une technologie dépassée a limité les projets de croissance. « Notre ancien système a fini par être un goulot d'étranglement. L'attribution des adresses IP et la création d'enregistrements dans un gestionnaire d'adresses IP sous le nom DNS ont été lentes », a déclaré J. Luz. « Il était compliqué de réserver l'adresse IP et d'enregistrer le nom, ce qui a entraîné un manque de contrôle de l'adressage et des problèmes d'infrastructure. »

L'infrastructure nécessitait une plus grande disponibilité des serveurs DNS, par exemple, afin de pouvoir répliquer des fichiers sur une autre machine de manière automatique et non manuelle. L'équipe informatique souhaitait également simplifier et accélérer le processus d'activation des projets afin de soulager les équipes chargées de l'infrastructure et du réseau de ce type de tâches. « Je contactais l'équipe chargée des réseaux pour obtenir une adresse IP et un nom, puis je passais à la dernière étape pour fournir certaines règles. Une machine virtuelle était créée et installée sur le système d'exploitation. C'était très lent », a déclaré J. Luz.

La nouvelle solution devait également garantir la protection des employés et des collaborateurs en raison de la menace de plus en plus sérieuse et fréquente des cyberattaques et de la fraude numérique. Le cadre réglementaire se durcissait également, la Banque centrale du Brésil exigeant des contrôles et systèmes de cybersécurité renforcés au sein des institutions financières.

Client : ***Sicredi Bank***
Secteur : ***Banque***
Pays : ***Brésil***

LES INITIATIVES :

- Mettre en place un environnement plus flexible et évolutif pour répondre aux besoins croissants des projets, services financiers et produits de Sicredi
- Remplacer les produits technologiques obsolètes qui limitaient les plans de croissance
- Augmenter la disponibilité de l'infrastructure, par exemple dans les serveurs DNS, afin de pouvoir répliquer automatiquement les fichiers sur une autre machine, sans intervention manuelle

LES RÉSULTATS :

- Qualité et agilité améliorées pour fournir des ressources à l'entreprise
- Accélération de la livraison des produits aux membres et aux utilisateurs finaux
- Optimisation des délais de provisionnement : auparavant, il fallait en moyenne cinq jours pour configurer une machine ; aujourd'hui, cela ne prend que 15 minutes

LES SOLUTIONS :

- NIOS DDI
- BloxOne® Threat Defense

LA SOLUTION

Une administration DNS simplifiée et sécurité renforcée contre les cyberattaques

Sicredi a commencé à mettre en œuvre Infoblox NIOS DDI, qui alimente les services réseau fondamentaux d'Infoblox, permettant ainsi le fonctionnement continu de l'infrastructure. La mise en œuvre a été effectuée avec le partenaire NTT. Tout d'abord, Sicredi a migré la base DNS vers la nouvelle infrastructure Infoblox. Au fil du temps, les fonctionnalités se sont étendues, tant en interne qu'en externe. Infoblox NIOS a facilité l'intégration et la centralisation des services DNS, DHCP et IPAM (DDI) de Sicredi sur une plateforme unique.

« Parallèlement à VMware, une intégration avec Infoblox a été réalisée, et tout cela a été automatisé. Aujourd'hui, nous pouvons accéder à un portail, commander une machine, enregistrer le nom IP et réserver l'adresse IP ; un système d'exploitation est installé et une machine virtuelle est fournie, prête à être utilisée », a décrit Andrius Lima, analyste d'infrastructure chez Sicredi. Infoblox a également permis la mise en place d'automatisations via des API afin de faciliter l'accès aux applications d'autres équipes. Cette fonctionnalité a été essentielle dans les actions pionnières de Sicredi dans les programmes « Open Banking » et « Open Finance » au Brésil.

Infoblox NIOS a renforcé la sécurité, le contrôle et la visibilité. En 2021, Sicredi a investi dans BloxOne Threat Defense, la solution de sécurité hybride d'Infoblox. Cette mise en œuvre a permis à l'organisation de mieux s'organiser en termes de DNS, d'enregistrements et de contrôles, et de bénéficier d'une stratégie de sécurité améliorée dans l'ensemble. Cet outil complète les fonctionnalités que l'environnement précédent possédait, telles que le pare-feu et la DDR.

« Infoblox nous a permis de faire évoluer notre infrastructure DNS et DHCP et d'organiser notre environnement pour faire face à la croissance de l'entreprise », explique J. Luz

LES RÉSULTATS

Infoblox a réduit les coûts opérationnels et simplifié les activités de Sicredi

La transition vers les solutions Infoblox a représenté un gain considérable pour Sicredi en termes de qualité et de rapidité dans la mise à disposition des ressources pour l'entreprise. La nouvelle infrastructure a réduit les coûts opérationnels, car les tâches d'administration du réseau sont désormais gérées dans une interface unique, automatisant et décentralisant les processus essentiels qui devaient auparavant être effectués manuellement dans le centre de données. Les coopératives peuvent désormais administrer leurs propres ressources grâce à la gestion des files d'attente.

« Infoblox a accéléré la livraison de nos produits aux partenaires et aux utilisateurs finaux. La configuration d'une machine prenait auparavant en moyenne cinq jours. Aujourd'hui, nous y parvenons en 15 minutes. C'est plus flexible et plus agile, » explique J. Luz.

La plus grande disponibilité de l'infrastructure permet de répartir les services entre les deux centres de données et d'effectuer des interventions obligatoires sans interrompre le service.

« Nous exécutons des tests périodiques pour des raisons de conformité et de continuité des activités. Avec Infoblox, nous avons l'esprit tranquille lors de l'exécution de ces tests, sachant qu'il n'y aura aucun impact sur les opérations de Sicredi », explique J. Luz.

En matière de cybersécurité, Sicredi a adopté des mesures pour prévenir les attaques de Malware et de ransomware et a mis en œuvre l'outil de protection contre les attaques par déni de service (DoS) BloxOne Threat Defense. Le responsable affirme qu'il est aujourd'hui difficile d'imaginer Sicredi sans les solutions Infoblox : « Au sein de Sicredi, Infoblox est considéré comme faisant partie intégrante des services de base. La perte du NIOS DDI aurait un impact financier ainsi que des conséquences sur notre réputation. C'est un outil essentiel au fonctionnement de l'entreprise », explique J. Luz.

Prochainement, Sicredi prévoit d'intégrer le DNS cloud d'Infoblox, d'acquérir une licence Threat Analytics et d'étendre ses fonctionnalités de sécurité.

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

+1.408.986.4000
www.infoblox.com

Version : 20230824v1