infoblox

案例研究

作为巴西金融领域的领导者，Sicredi 采用 NIOS DDI 和 BloxOne Threat Defense 继续发展壮大

概述

Sicredi 是一家成立于 120 多年前的合作性金融机构。在过去的二十年里，该企业经历了内部重组并加速了扩张。为了支持这一增长并引领金融领域的创新，Sicredi 已投资实施数字化转型。

信用合作社拥有与传统金融机构相同的金融产品和服务组合（活期账户、卡、投资），但主要区别在于管理模式。与传统机构不同，在信用合作社中，合作社的合伙人是企业的真正所有者。

为了成功执行这一业务模式，Sicredi 采用一项管理策略，即利用超过 700 万充当企业主角色的合伙人的参与。这家合作性金融机构拥有超过 2,500 家分支机构，业务遍及巴西所有州和联邦区，提供全套金融和非金融解决方案。

> “*Infoblox* 加快了我们产品的交付速度。向合伙人和最终用户交付产品的速度。以前，预配一台计算机平均需要 5 天时间；如今，我们可以在 15 分钟内完成，而且配置过程更加灵活和敏捷。”
>
> **Juliano Luz,**
> **Sicredi 基础架构分析师**

现状

地域扩张和数字化推动信用合作社业务发展

Sicredi 的分支机构和合伙人办事处显著增长，近年来成为巴西金融领域的主要参与者之一。目前提供超过 300 种金融产品和服务，从活期账户和卡到投资、保险、联盟、刷卡机和 100% 数字账户，这些产品和服务适用于个人、法人实体和乡村生产者。

Sicredi

为了配合这一进展，Sicredi 于 2017 年开始了数字化转型过程，他们计划使用更加现代化的平台逐步取代用于处理产品和服务的旧系统（称为“核心银行业务”）。这种尖端技术的采用对于为合伙人提供更好的体验以及在巴西充满活力的金融市场中保持竞争力至关重要。

多年来，Sicredi 一直在“开源”DHCP 和 Linux 工具上使用技术基础架构和虚拟机。基础架构分析师 Juliano Luz 于 2008 年加入 Sicredi，他回忆起过时的环境：“存在缺乏可扩展性和灵活性的挑战。企业需要新的应用程序，新的环境，”他说。

由于使用开源解决方案，旧环境没有任何外部支持，所有问题都必须在内部解决，同时需要 IT 部门的大力参与。Sicredi 的另一个关注点是加强抵御网络攻击的安全性。

Sicredi 已于 2013 年实施 Infoblox 解决方案，但在 2021 年，它决定更新技术环境。“最初的

DDI 实施由内部团队执行。当我们扩展和更新 Infoblox NIOS DDI 时，NTT 作为合作伙伴加入，”Luz 说道。

挑战

过时的技术基础架构导致手动流程缓慢

越来越多的 Sicredi 金融项目、服务和产品需要一个具有更强大的应急性和可扩展性的环境。过时的技术限制了增长计划。“我们的旧系统最终成为了瓶颈。在 IP Address Manager 中以 DNS 名称分配 IP 和创建记录的速度很慢，”Luz 说道，“保留 IP 和注册名称很复杂，导致缺乏寻址控制和基础架构问题。”

例如，基础架构需要 DNS 服务器具有更高的可用性，这样它们才能自动而非手动将文件复制到其他计算机上。IT 团队还希望简化并加速激活项目的过程，以便将基础架构和网络团队从这些类型的任务中解放出来。“我会通过网络团队获取 IP 和名称，然后在最后部分提供一些规则。已在操作系统上创建并安装虚拟机。它非常缓慢，”Luz 说。

由于网络攻击威胁和数字欺诈日益严重和频繁，新的解决方案还需要保证对员工和合伙人提供保护。监管环境也变得愈加严格，巴西中央银行开始要求金融机构采用更加稳健可靠的控制论安全控制和系统。

客户：*Sicredi Bank*
行业：银行
地点：巴西

举措：

- 为不断增长的 Sicredi 项目、金融服务和产品建立一个具有更强大的应急性和可扩展性的环境
- 更换限制增长计划的过时技术产品
- 提高基础架构的可用性，例如，在 DNS 服务器中能够自动而非手动将文件复制到其他计算机

成果：

- 提高向企业提供资源的质量和敏捷性
- 加速向会员和最终用户交付产品
- 缩短预配时间：以前，预配一台计算机平均需要 5 天时间；如今，我们可以在 15 分钟内完成

解决方案：

- NIOS DDI
- BloxOne® Threat Defense

解决方案

简化 DNS 管理并提高抵御网络攻击的安全性

Sicredi 开始实施 Infoblox NIOS DDI，它为 Infoblox 基本网络服务提供支持，从而实现基础架构的持续运行。实施过程由 Sicredi 与合作伙伴 NTT 共同进行。首先，Sicredi 将 DNS 基础迁移到新的 Infoblox 基础架构。随着时间的推移，它在内部和外部进行功能扩展。Infoblox NIOS 促进了 Sicredi 的 DNS、DHCP 和 IPAM (DDI) 服务在单一平台上的集成和集中化。

“除 VMware 外，还与 Infoblox 进行了集成，所有这一切都是自动进行的。如今，我们可以访问门户，订购设备，注册 IP 名称并保留 IP；安装了操作系统并提供虚拟机，且随时可以使用，”Sicredi 基础架构分析师 Andrius Lima 描述道。Infoblox 还通过 API 实现自动化，帮助其他团队的应用程序进行访问。此功能对于 Sicredi 在巴西“开放式银行”和“开放式金融”计划中的开创性行动至关重要。

Infoblox NIOS 加强了安全性、控制力和可视化。2021 年，Sicredi 投资创建 Infoblox 混合安全解决方案 BloxOne Threat Defense。这一实施使该组织在 DNS、记录和控制方面变得更有组织性，并从整体安全状况的改善中获益。此工具对以前环境具有的功能进行了完善，例如防火墙和 DDR。

“Infoblox 使我们能够扩展 DNS、DHCP 基础架构并组织我们的环境，以应对业务的增长，”Luz 说。

结果

Infoblox 降低了 Sicredi 的运营成本并促进了业务发展

就向企业提供资源的质量和敏捷性而言，向 Infoblox 解决方案的过渡为 Sicredi 带来了巨大的益处。新的基础架构降低了运营成本，因为网络管理任务现在通过单一界面进行管理，从而实现了以前必须在数据中心手动执行的基本流程的自动化和分散化。合作社本身现在可以通过队列管理来管理自己的资源。

“Infoblox 加快了我们向合伙人和最终用户交付产品的速度。以前，预配一台计算机平均需要 5 天时间；如今，我们可以在 15 分钟内完成，而且配置过程更加灵活和敏捷，“Luz 说。

基础架构的更高可用性允许在两个数据中心之间分配服务，并在不中断服务的情况下进行强制干预。

“出于合规性和业务连续性的考虑，我们定期运行测试。借助 Infoblox，我们在运行这些测试时可以高枕无忧，因为我们知道这不会对 Sicredi 的运营产生任何影响。”Luz 说道。

在控制论安全方面，Sicredi 采取了相应措施来防范恶意软件和勒索软件攻击，并实施了 BloxOne Threat Defense 拒绝服务 (DoS) 防护工具。这位经理表示，如今，很难想象如果没有 Infoblox 解决方案，Sicredi 该是何种状况：“在 Sicredi 内部，Infoblox被视为基础服务的一部分。如果没有 NIOS DDI，会对财务和品牌形象产生影响。它是企业运作的重要工具，”Luz 说。

在不久的将来，Sicredi 打算集成 Infoblox 云 DNS、获取 Threat Analytics 许可证并扩展安全功能。

公司总部
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

版本： 20230824v1