zpe

CASE STUDY

BANKING

Investing in out-of-band management to reduce risks and secure peace of mind

Integrating network management infrastructure helps a global bank provide reliable and secure services across the globe

Customers demand high levels of security for even the smallest banking transactions. For a 130-year-old financial institution with branches across the globe, this requirement is no different. Dealing in private banking, asset & real estate management, investing, and other areas, the company relies on reliable and secure networking to protect their patrons. This includes having a sturdy foundation of out-of-band management solutions to ensure critical IT infrastructure remains up-to-date and operational.

For the bank, it's crucial to invest in today to secure a better tomorrow. Their IT team embodied this principle and turned their attention to their aging out-of-band infrastructure. As this disjointed solution began to jeopardize the peace of mind they delivered every day, it was time to invest in a solution that could overcome access and security issues stemming from outdated operating systems, software client requirements, and EOL devices. They needed a solution that could fully integrate their infrastructure to close the following gaps:

- Reducing months-long maintenance cycles, by reducing their multi-vendor stack of different operating systems and management software
- Reducing resolution times, by enabling remote access without requiring installation of client software
- Curbing fatigue and errors, by fully integrating all out-of-band functions into a centralized management solution
- Avoiding noncompliance penalties, by replacing near-EOL devices with a solution that receives ongoing support
- Reducing attack vectors, by enabling modern security principles such as segmentation and Zero Trust

Continue reading to see how Nodegrid secured the future for the company and their customers.

Background

The financial and wealth management institution is based in Switzerland, and has been serving customers for over 130 years. They have a global presence with 13 locations across Europe, Asia, and the Americas. Their distributed data center and branch networks must be maintained, from the standpoint of both availability and security. This is not only to protect their reputation and sensitive customer data, but to follow the guidelines set forth by different countries and governing bodies, such as the European Banking Authority (EBA).

The EBA and its global counterparts specify guidelines for IT services availability and security, which financial institutions must follow or risk incurring fines and other penalties. These guidelines also focus on response and recovery plans that assist with restoring critical business functions, such as payment systems, in the event of an outage or cyberattack.

For financial institutions, this means having the ability to perform routine maintenance, troubleshooting tasks, and recovery procedures for a variety of distributed infrastructure. The company accomplishes this via out-of-band management that provides remote access capabilities across regions.

Problem and Gaps

Peace of mind is paramount when serving finance and investment customers. This peace of mind relies on one thing: the security of underlying IT systems.

For the bank, a critical part to this is the out-of-band (OOB) management infrastructure that they use to maintain their IT systems. OOB helps their IT teams perform hardware and software maintenance, troubleshooting tasks, and upgrades that directly affect uptime and the customer experience.

However, they faced a problem common among organizations that have been operating for decades. Their OOB system — which connects directly to all management interfaces and therefore must be extra secure — was aging. It was implemented during a time when securing management interfaces was not a priority, and could not support modern security principles such as segmentation or Zero Trust. This was highlighted in their existing management infrastructure, which was comprised of:

1. Two separate models of serial console servers that were soon to be end-of-life (EOL)
2. Automatic Transfer Switches (ATS) for power monitoring
3. A popular management software in a hub-and-spoke setup, with three separate instances dedicated to different regions
4. Dedicated Windows VM to run the management software
5. Dedicated Windows VM to run the monitoring solution

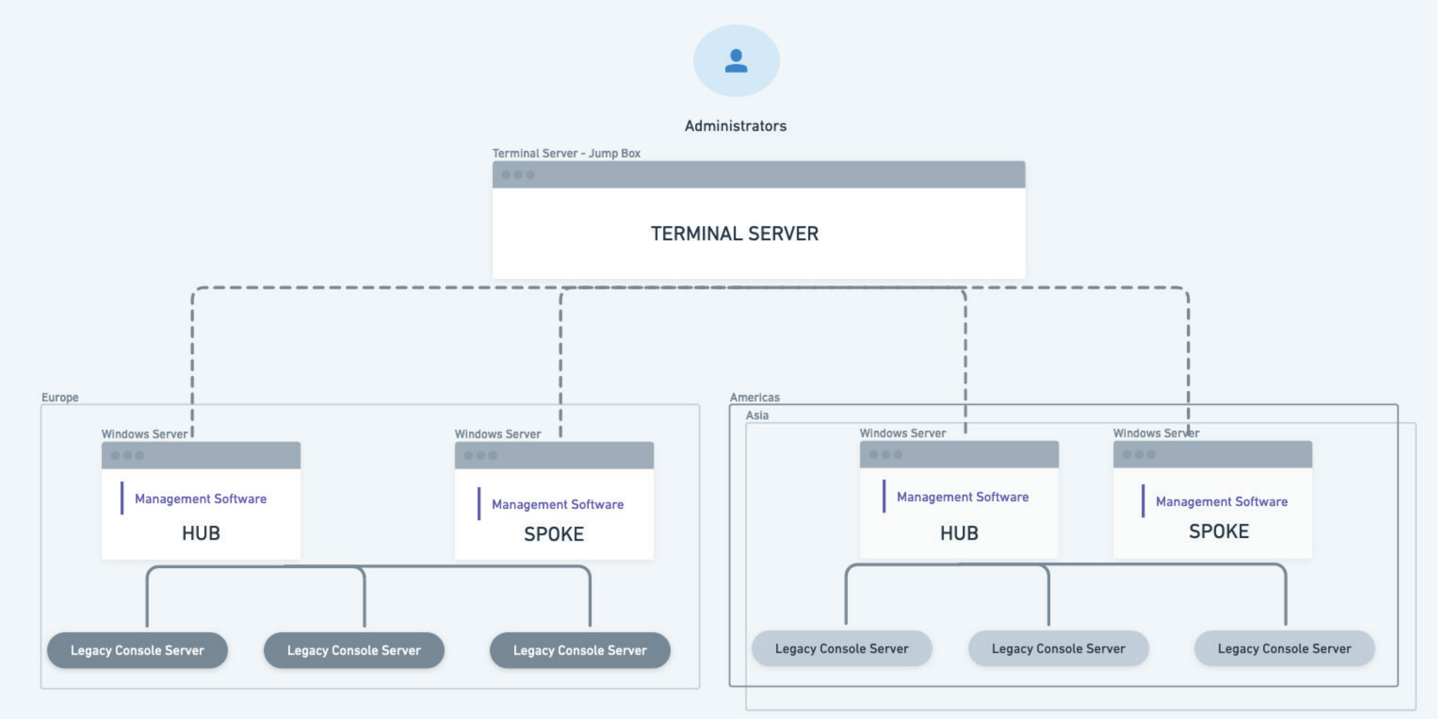


Image: Diagram showing the bank's existing hub-and-spoke architecture, with legacy management devices that were difficult to maintain and nearing EOL.

Without a refresh, their IT infrastructure's security would continue to dissolve. It would only be a matter of time before a critical outage or vulnerability exploit would affect the peace of mind that they delivered to their customers every day.

But the company lives by one conviction: How we invest today is how we live tomorrow. They're dedicated to improving their quality of life and their ability to deliver services, which is why they turned their attention to the following gaps:

- Their existing software stack was complex. It required six Windows Server licenses, six VMs to run Windows Server, and six installations of their chosen management software. Because of this, bug fixes, patching, and security updates typically required a months-long cycle from reporting to resolution.

- Their existing solution required specific software to be installed on all clients. If this client software did not match the existing version, users couldn't gain access to start a session to a device. This slowed support and extended outage times.

- Their existing solution consisted of outdated devices that forced them to separate server and power management — with a dedicated solution for monitoring rack PDUs — and their software did not support monitoring of their ATS devices. This inflated their workload across the board and increased their potential for error-induced outages.

- Because their devices were nearing EOL and no longer received support, their lack of up-to-date patching increased their vulnerability to attack. They also needed to maintain compliance, which states that institutions cannot rely on EOL hardware.

- Their existing setup lacked hardware and software features to support modern security approaches such as segmentation and Zero Trust. This posed a major risk, as attackers could exploit vulnerable management ports and then access any infrastructure they wanted.

In keeping with their conviction, the company identified several key requirements. Their ideal solution would:

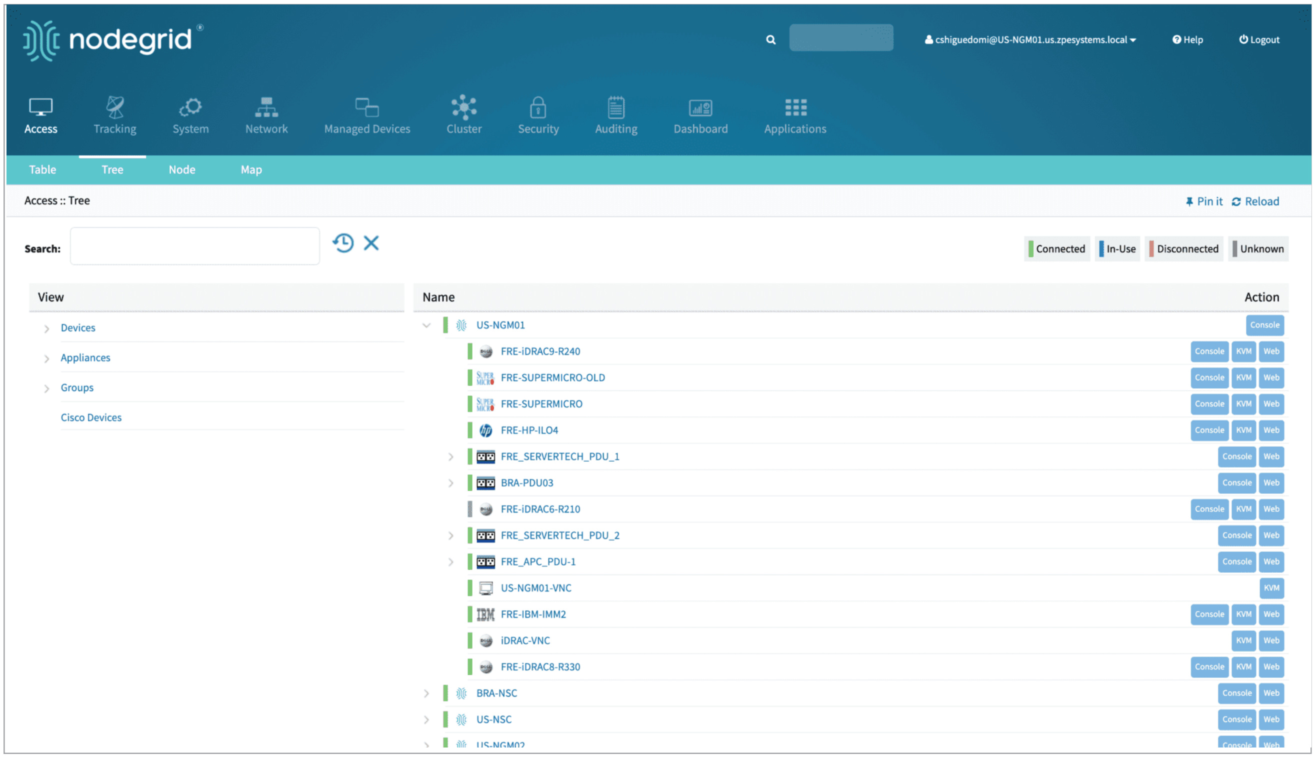
- Shorten maintenance timelines, by reducing their stack's multi-vendor complexities into a cohesive solution
- Reduce outage resolution times and access limitations, by eliminating the need for client software
- Curb fatigue and the risk of errors, by combining management and monitoring capabilities
- Eliminate compliance worries, by receiving frequent patching and ongoing support
- Fulfill their most stringent security requirements, by enabling modern approaches such as segmentation and Zero Trust

The caveat was that although they needed to rapidly adopt a new setup, they would need to do so by taking a gradual, step-by-step approach. This would help them prevent major disruptions and minimize implementation risks while continuing to meet business needs.

Solution

The company deployed a two-part Nodegrid solution in each region to address their challenges.

At the core of their solution was Nodegrid Manager. This management software installed easily from a non-dependent ISO image, and allowed them to gain centralized control of their entire system. They deployed two instances of Nodegrid Manager in a high-availability configuration, to ensure constant access in case either system experienced a failure.



Access :: Tree

View
- Devices
- Appliances
- Groups
- Cisco Devices

Name	Action
US-NGM01	Console
FRE-iDRAC9-R240	Console KVM Web
FRE-SUPERMICRO-OLD	Console KVM Web
FRE-SUPERMICRO	Console KVM Web
FRE-HP-ILO4	Console KVM Web
FRE_SERVERTECH_PDU_1	Console Web
BRA-PDU03	Console Web
FRE-iDRAC6-R210	Console KVM Web
FRE_SERVERTECH_PDU_2	Console Web
FRE_APC_PDU-1	Console Web
US-NGM01-VNC	KVM
FRE-IBM-IMM2	Console KVM Web
iDRAC-VNC	KVM Web
FRE-iDRAC8-R330	Console KVM Web
BRA-NSC	Console Web
US-NSC	Console Web
US-NGM02	Console Web

Image: Nodegrid Manager provides one UI and normalized commands for managing all connected infrastructure, regardless of vendor.

Making their solution seamless and easy to use was the Nodegrid Serial Console (NSC). The company replaced their out-of-band devices with the NSC, which features high port counts and a powerful Intel® processor. This enabled them to connect every device in their stack to a single box — from routers and switches, to PDUs and UPS devices. The NSC was able to efficiently process every connection while serving as a secure, unified access gateway. On top of this, the onboard Nodegrid OS directly hosts Nodegrid Manager to make implementation simple.

Image: The Nodegrid Serial Console features serial, ethernet, and USB ports, with an Intel processor and Linux-based OS that enable direct hosting of management software such as Nodegrid Manager.

Results and Benefits

Deploying Nodegrid allowed the bank to streamline and fortify their distributed networks — all the while taking the phased approach that they desired.

The NSC allowed them to eliminate many out-of-band devices, and instead unify control of their stack with a cohesive, single-vendor solution. They were able to gradually implement each NSC at the rack level and set up a system that allows for secure remote access to their stack. Hosting Nodegrid Manager centralized server and power management, and allowed them to implement a power monitoring solution that was unsupported by their legacy configuration.

Prior to Nodegrid, the company needed to maintain a multi-vendor solution consisting of:

- 6x VMs (to run Windows Server)
- 6x Windows Server licenses
- 6x management software

Nodegrid reduced this software stack by eliminating the Windows Server licenses and the legacy management software. Now, the company easily maintains a single-vendor solution consisting of:

- 6x VMs (to run Nodegrid Manager)
- 6x Nodegrid Manager

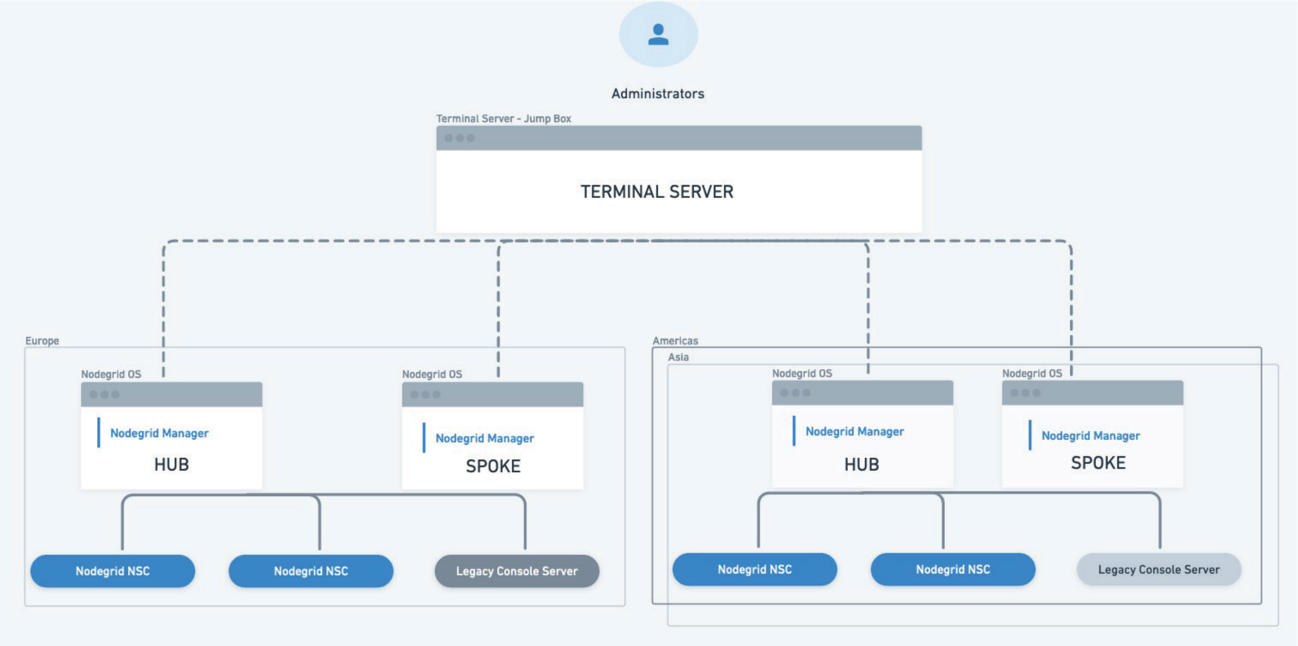


Image: Diagram showing the bank's new hub-and-spoke architecture, with Nodegrid devices in a high-availability configuration.

Their Nodegrid solution brought the following results:

- **High availability** - Each region operates two instances, with management software that doesn't require manual version control
- **Reliable access** - Nodegrid eliminates the need for additional client software and allows access via HTML5 browser or SSH client
- **Ease of use** - Nodegrid Manager removed the need for a dedicated monitoring solution for PDUs, and provides one UI for centralized control of all out-of-band functions
- **Easy compliance** - Nodegrid receives continuous patching and has a long product lifecycle, which eliminate hardware and software compliance issues
- **Modern security** - Nodegrid supports micro-segmentation and includes features such as SAML and MFA, which allow management ports to be secured through modern security approaches such as Zero Trust

The company's concerns centered on having a secure infrastructure. By modernizing their existing network, they were able to implement a high-availability configuration that eliminated weak points, helped avoid failures, and kept their infrastructure compliance out of the danger zone. This unified infrastructure and management solution brought benefits including:

- Cost savings, as they eliminated six Windows Server licenses
- Reduced maintenance and response times, as their IT team now had a cohesive, single-vendor solution that was easy to maintain
- Fast resolution times, with always-ready user access via web browser or SSH session
- Less work and risk of errors, with full integration of management solutions and normalized commands
- Ongoing peace of mind due to up-to-date security and compliance
- Less risk of attack with a platform that supports modern security approaches

Using traditional solutions would have significantly prolonged a gradual implementation, or forced the company to opt for an all-at-once approach. But with Nodegrid, the company phased in their new solution even for their global deployment. This led to simpler implementation and savings on resources, while allowing them to find and fix issues as they gradually presented themselves. They avoided running two different solutions side by side and the potentially catastrophic problems that accompany such an approach.

They also achieved a unified, easy-to-use management platform that gave them control of all systems — including their ATS devices and rack PDU monitoring. Nodegrid Manager provided secure remote access to every level of their infrastructure, and gave them normalized commands across vendor solutions. This allowed their network staff to reduce response times and maintain secure connectivity, so their global customers could remain online and protected. Because they could now monitor and control their ATS systems, they could defend against downtime and ensure the appropriate switches would be used in the event of a power failure.

Finally, they no longer needed to worry about growing weak points in security or falling out of compliance by letting their legacy devices go into EOL. Nodegrid delivered built-in protection and customizable features, with ZPE Systems' engineering team providing semi-annual releases, 24-hour CVE patching, and fast feature request turnaround times. Built-in hardware and software security features such as encrypted disk, signed OS, SAML, MFA, and role-based access control provide a foundation for segmentation and Zero Trust Network Access to protect against evolving threats. ZPE Systems also continues to provide support and updates to even the oldest Nodegrid products, which means the company implemented a solution that will remain compliant and secure for many years to come.

If you need to modernize your network infrastructure and management capabilities, ZPE Systems is the solution. As traditional configurations continue to fall short at many levels — from management, to security and compliance — financial institutions now realize that only flexible networking will withstand tomorrow's challenges. Nodegrid provides extensible hardware and software to help you evolve with changing requirements.

Call or visit our website for a free demo.

www.zpesystems.com