SIOS WHITEPAPER

High Availability Protection for Financial Services

Protecting Essential Systems from Downtime & Disasters

us.sios.com

The financial services sector has always been at the forefront of technology innovation – from the first transatlantic telex lines used to communicate financial data to today's online banking, and high-speed stock transaction systems. To stay competitive and deliver excellent customer service, companies in the financial sector, such as commercial banking, credit unions, brokerage firms, and wealth management all rely on a wide range of applications and databases for their online banking systems, ATMs, payment systems and other essential operations.

Even a few minutes of downtime for these essential applications and databases can be devastating for a financial service company, resulting in loss of customer satisfaction and loyalty, costly drains on IT resources, and negative media coverage that threatens revenue as well as reputation. In these high-stakes environments, flexible, application-aware high availability and disaster recovery protection are essential requirements.

Historically, financial services organizations ran critical applications on mainframes. However, today's financial institutions may have critical workloads in a variety of configurations, from all on-premises, hybrid, and all in-cloud infrastructures depending on the server types and bandwidth available to accommodate these configurations. With so many options, careful planning is required to ensure applications and other related resources in HA/DR environments meet the organization's needs for scalability, reliability, and configuration flexibility.

Four Common Downtime Threats to Financial Services Organizations

IT teams should be aware of four common threats to financial services organizations when evaluating their business continuity plans: cyberattacks, system failures, cloud outages, and natural disasters. In the face of these threats, consider which applications and databases would incur the greatest cost to their organization if they were to go offline? Understanding the criticality of applications within the organization is key to defining the most cost-efficient mitigation and protection strategy.

Cyberattacks

Headline news has put cyberattack preparedness at the top of every IT list. Banks and credit unions may face the challenge of protecting vital applications and data without full-time, dedicated cyber-security experts on staff. There are some important steps every organization can take to improve cyber security, regardless of size or IT resources.

Security Audits and Testing

The cost of ransomware and other cyber threats justifies the investment in an expert audit of regulated data and any means of accessing it – including firewall weaknesses, routers, network access points, and servers and recommended countermeasures specific to each weakness.

Document and Inform Staff of Acceptable Use

Document and communicate policies about the acceptable use of the company's computer equipment and network – both in-office and at-home. Include clear restrictions for accessing and downloading sensitive data to local laptops and PCs; use of network access points, wireless security, and best practices to avoid email-borne threats.

Software Protection

Apply software solutions for protection ranging from workstation/laptop antispam software to automated security systems that hunt, detect and manage defenses against threats throughout the system. Evaluate the costs and complexity of these systems as part of a holistic cyber security solution. Consider using HA clustering to perform “rolling” updates/upgrades on essential servers, such as SQL Server, Oracle, SAP or HANA with little to no application downtime.

Hardware System Failures

Component failure within your IT infrastructure – servers, storage, network routers, etc is inevitable. To mitigate the cost of failure, quantify the answers to three questions:

- How much data can you afford to lose? This is your recovery point objective (RPO).
- How quickly do you need to restore operations? This is your recovery time objective (RTO).
- What level of application availability do you need? For example, 99% uptime equates to about 3.6 days of downtime per year. This is known as your “nines” of availability.

Your most critical applications – those that require an RPO of zero, an RTO of just 1-2 minutes, and true high availability (HA) of at least 99.99% annual application uptime – can be protected against hardware failure through failover clustering. For less critical applications and data, a simple backup or archiving plan may suffice.

Failover clustering provides redundancy for potential sources of system failure. Critical applications are run on a primary node or cloud VM (virtual machine). Clustering software monitors application availability. If a threat is detected, this software moves the application operations to a standby server where operation continues with minimal downtime and near zero data loss. It is important to ensure that the clustering software will failover automatically and in accordance with application-specific best practices – and that it will monitor the application at the network, storage, OS, application, and server layers, not just the server layer.

Cloud Outages

Cloud infrastructures do not automatically provide application-level HA or DR protection. Cloud availability service level agreements apply only to the hardware, which may not ensure that an application or database remains accessible. Like any computing system, clouds are vulnerable to human error, software compatibility issues, disasters, and other downtime threats. HA clustering for applications in the cloud should be capable of failing over across both cloud regions and availability zones. Traditional shared storage clustering in the cloud is costly and complex to configure, and in some clouds is simply not available. Instead, most companies use so-called SANless clusters. That is, they configure redundant servers in the cloud, each with its own local storage. They use efficient block-level replication to synchronize the local storage of all cluster nodes. In the event of a failover, this enables a standby node to access an identical copy of the primary node storage for an RTO of a few minutes, an RPO of zero, and an availability of 99.99% or less than an hour of downtime per year.

Disaster Recovery

Some applications may need protection from disasters that damage the local IT infrastructure. Disasters can occur for many reasons; For applications needing HA, the primary and standby cluster nodes should be geographically separated but connected by efficient replication that can synchronize storage between locations.

By assessing the criticality of the applications, databases, and ERP systems required to operate efficiently and calculating the real cost of downtime for these systems, financial service organizations can invest time and resources wisely to mitigate those threats cost efficiently.

Protect Financial Systems from Downtime and Data Loss

After defining the criticality of applications and the potential threats that are most costly to the financial services organization, IT teams can begin to choose the application protection technology that provides the best balance of cost and risk mitigation.

Fault-tolerant (FT)

Fault-tolerant (FT). FT approaches promise that the servers running the applications and/or database will be available 99.999% of the time (also known as "five nines" of availability) or less than 5.5 minutes of unscheduled downtime per year. But FT solutions can be extremely expensive to purchase and complex to configure and manage. They effectively become bespoke solutions that require companies to "lock in" to a single vendor.

High availability (HA)

An alternative to the FT approach is an HA approach—where HA stands for "high availability." HA solutions, which can be configured using Linux or Microsoft Windows Server, guarantee that protected infrastructure will be available at least 99.99% of the time ("four nines" of availability).
Four nines of availability translate to no more than 53 minutes of unscheduled downtime per year—and it can translate into a dramatically lower total cost of ownership (TCO) for a still powerful financial service solution.

In an HA cluster, essential applications are run on a primary server and connected to a secondary server to eliminate single points of failure. Clustering software monitors the health of the application environment and, in the event of a failure, moves application operation to the secondary node.

High availability in the Cloud

Banks have historically put applications on mainframes, but more and more are running important apps on servers and in the cloud where they need each.

There are two common scenarios for financial services businesses. First, customers with applications on Windows OS are using Windows server failover cluster on-prem, and want to move to the cloud without changing their configurations or processes; and second, customers running applications on Linux OS are concerned about the complexity of configuring and managing a clustering environment, particularly in the cloud. Now with the shift from on-prem to cloud, there is still a business requirement, and often a service level agreement(SLA) to be met in the cloud for HA/DR for Oracle, SAP, SQL, MaxDB, file shares, and generic applications.

Now, there is a misconception that if a business' resources reside in the cloud, they are protected from downtime and disasters. Clouds only protect applications from hardware issues, they do not provide application HA/DR. While most large financial institutions have on-premises to on-premises, on-prem-to-cloud (hybrid), and/or an all-in-cloud infrastructure as their bandwidth allows. All cloud providers offer HA infrastructure solutions with hardware SLAs that guarantee 99.99% uptime, but they do not guarantee *application* availability.

SIOS Solution

SIOS provides cost-effective high availability and disaster recovery solutions that protect transaction processing, administrative applications, and other essential financial services systems without adding IT complexity. A SIOS solution adds the flexibility, reliability, and scalability to meet all of the financial services company's needs. Here are some of the reasons why we think so:

Reliable disaster protection

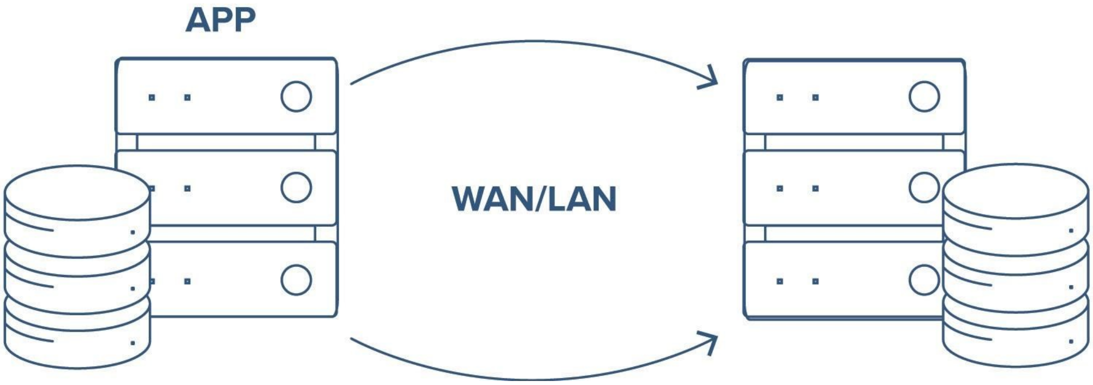
Critical systems in financial services organizations today may be running in on-premises, cloud, or hybrid cloud environments. SIOS high availability and disaster recovery solutions ensure availability and eliminate data loss for critical Windows and Linux applications operating in any environment.

Meet availability objectives and SLAs

SIOS gives you the flexibility to build SAN and SANless clusters for Windows or Linux environments on physical or virtualized servers and in the cloud, to achieve high availability or disaster tolerance. Set up clusters across availability zones or regions for maximum HA/DR protection or create hybrid clouds to meet your service level agreements and availability RTO/RPOs. Extend a cluster to a third node in the cloud or DR site for maximum protection from local, regional, and sitewide disasters.

High Availability Protection for Every Environment

Unlike traditional clusters that rely on a shared storage area network (SAN), SIOS enables a SANless cluster. Each node in a failover cluster is configured with local storage, and SIOS block level replication synchronizes the local storage among the nodes by replicating data written to the primary system to the secondary node. The replication services are application agnostic, so all the data written to a specified storage system—and not just that associated with a specific application, such as SQL Server—is replicated to secondary storage at very high speeds. This approach enables failover clusters in physical, virtual, cloud, and hybrid cloud environments.



Whether you need an on-premises, cloud, or hybrid solution, SIOS has the expertise and support to assist.

What SIOS Solution is Right for Me?

SIOS DataKeeper

SIOS DataKeeper enables HA and DR in Windows Server Failover Cluster (WSFC) environments without the need for shared storage by keeping real-time copies of data synchronized across multiple servers and data centers. It protects data in physical, virtual, and cloud environments and provides enterprise-class protection for all server workloads at a fraction of the cost of array-based replication.

Add **SIOS DataKeeper** software to a WSFC environment to protect your business-critical Windows applications and the databases they run on, including Microsoft SQL Server, Oracle SQL Server, SAP, and SAP S/4HANA.

- **Configuration flexibility**—Protect all server workloads. Replicate within a single site or across data centers.
- **Cost-savings**—Advanced clustering without costly application upgrades (e.g., SQL Server Enterprise Edition.)
- **Reduced complexity**—Migrate on-premises WSFC to a cloud without disruption.

Learn more about SIOS DataKeeper

SIOS LifeKeeper

SIOS LifeKeeper for Linux provides advanced, application-aware protection for essential applications on-premises or in flexible, scalable, cloud environments, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform.

Powerful Application Recovery Kits included with SIOS LifeKeeper automate manual tasks, monitor the entire application stack, and ensure failovers maintain application-specific best practices. ARKs for leading applications, ERPS, and databases are included with LifeKeeper. Customizable ARKs are also available to specialized applications.

SIOS ARKs provide:

- **Advanced automation**—Auto-validated user input eliminates the need for costly, specialized skills and removes the risk inherent in manual scripting, to configure and manage a cluster in complex financial environments.
- **Deep application monitoring**—Monitor your entire application environment.
- **Application-aware automated failover**—Maintain compliance with application best practices for reliable failovers and no surprises.

Learn more about SIOS LifeKeeper

See how companies around the world are using SIOS to maintain business continuity.
View our case studies.

About SIOS Technology

SIOS Technology Corp. high availability and disaster recovery solutions ensure availability and eliminate data loss for critical Windows and Linux applications operating across physical, virtual, cloud, and hybrid cloud environments. SIOS clustering software is essential for any IT infrastructure with applications requiring a high degree of resilience, ensuring uptime without sacrificing performance or data – protecting businesses from local failures and regional outages, planned and unplanned. Founded in 1999, SIOS Technology Corp. (https://us.sios.com) is headquartered in San Mateo, California, with offices worldwide.

SIOS Technology Corp.
155 Bovet Road, Suite 476
San Mateo, CA 94402
Tel: 650-645-7000

info@us.sios.com
https://us.sios.com