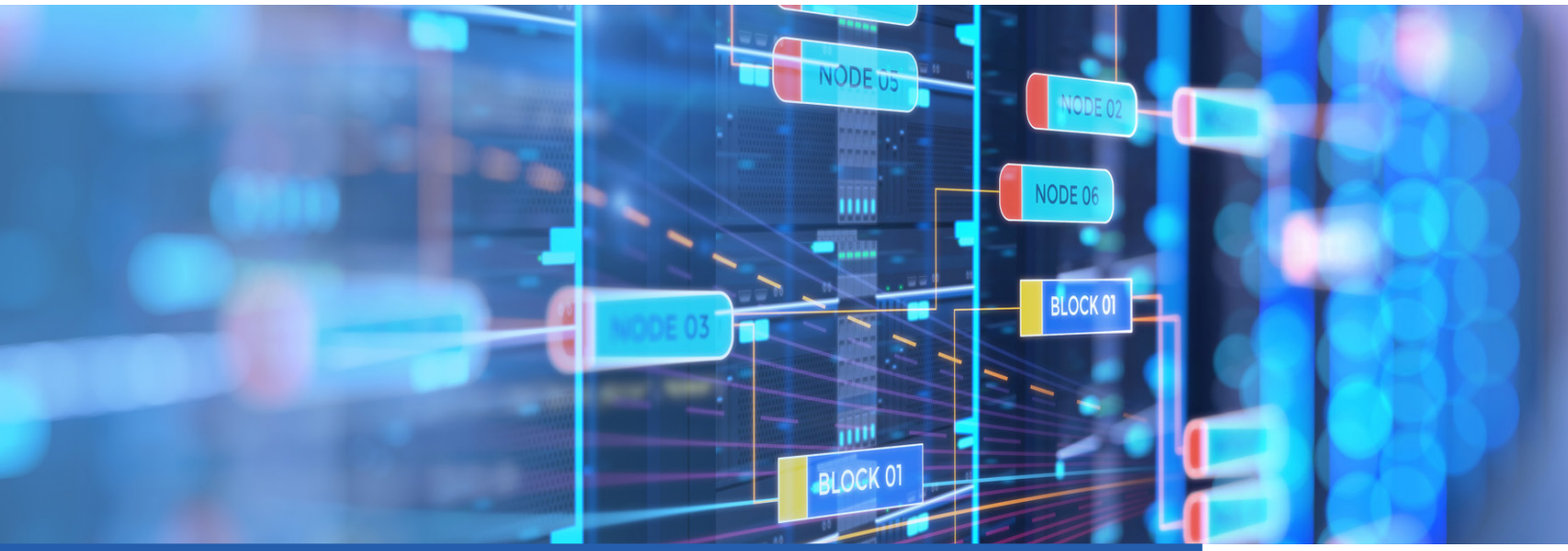
SIOS

SIOS WHITE PAPER

Providing High Availability and Disaster Recovery for SQL Server 2008 Applications in the Azure Cloud



us.sios.com

Extended Support for SQL Server versions 2008 and 2008 R2 ended on 09 July 2019. Extended Support for Windows Server 2008 and 2008 R2 will end six months later on 14 January 2020. Without continued support for critical patches and security updates, organizations will need to take on greater risk for continuing to run these legacy applications, potentially becoming out of compliance for some.

Microsoft is offering three options for all applications affected, details of which are available at Prepare for SQL Server 2008 end of support:

1. Upgrade to a later version of SQL Server that still has full support
2. Purchase Extended Security Update support for those applications remaining on-premises
3. Migrate the application(s) to Azure or the Azure Stack to get an additional three years of free Extended Security Update support for both SQL Server 2008/R2 and/or Windows Server 2008/R2

Upgrading to a later version of SQL Server may not be a viable option for some, for practical and/or financial reasons. Indeed, for those applications that are running well, migrating them to Azure Virtual Machines eliminates the need to “fix something that ain’t broke” for another three years.

Purchasing Extended Security Updates will cost 75 percent of the full license fee annually, and this cost is in addition to active software assurance, which is typically 25 percent of the annual license fee, along with the capital and operational expenditures of running the applications in the enterprise datacenter. Because these costs make migrating to Azure or the Azure Stack attractive if not compelling (including for its other advantages, not the least of which is gaining experience in the cloud), the focus of this white paper is on the third option for migrating to Azure.

According to Microsoft: “Customers who migrate workloads to Azure virtual machines will have access to Extended Security Updates for both SQL Server and Windows Server 2008 and 2008 R2 for three years after the End of Support deadlines, included at no additional charge over the standard VM pricing. Eligible customers can also use the Azure Hybrid Benefit to leverage existing on-premises license investments for Windows Server and SQL Server to save on Azure Virtual Machines (IaaS) or Azure SQL Database Managed Instance (PaaS).” To assist with the migration, Microsoft permits existing on-premises licenses to be transferred to Azure, and also offers a 180-day transition period during which a single license applies concurrently on-premises and in the cloud.

The purpose of this paper is to help Database and System Administrators assess the options available for providing satisfactory high availability (HA) and disaster recovery (DR) protections for mission-critical SQL Server 2008/R2 applications being migrated to Azure. The content is organized into three sections, followed by a summary conclusion. The first section covers the HA and DR provisions offered in Azure. The second section introduces SIOS DataKeeper as a third-party HA/DR solution for failover clustering in private, public and hybrid clouds. The third section highlights two of the most popular HA/DR configurations in Azure.

It is important to note that the HA and DR provisions discussed here also support other applications, including those using later versions of SQL Server and Windows Server. Any differences among the different versions of software will be noted.

HA and DR Services within the Azure Cloud

The Azure cloud offers redundancy within a datacenter, between Availability Zones and across multiple Regions. Redundancy within a datacenter is provided by distributing servers within an Availability Set across different Fault Domains, with each Fault Domain being a single rack of servers. Placing servers within the same Availability Set protects against failures at the server and rack levels, enabling Microsoft to offer a 99.95% uptime guarantee. The Service Level Agreement (SLA) ensures that if two or more servers are deployed in an Availability Set, at least one will have external connectivity. It does not, however, guarantee availability at the application level and does nothing to protect against site-wide failures, like the one that occurred in Azure's South Central US Region in September 2018.

For protection from single site-wide failures, Azure is rolling out Availability Zones (AZs). Each Region that supports AZs has at least three datacenters that are inter-connected via high-bandwidth, low-latency networking capable of supporting synchronous data replication. When two or more servers are deployed in different AZs, Microsoft offers a 99.99% SLA, guaranteeing that at least one of those will have external connectivity. But caveat emptor: downtime excludes many common causes of failures, including customer and third-party software, and what might be called "operator error"—those inevitable mistakes made occasionally by all administrators. (See Sidebar on "Azure Uptime Exclusions")

For even greater resiliency, Azure offers Region Pairs. Every region is paired with another within the same geography (such as US, Europe or Asia) separated by at least 300 miles. The pairing is strategically chosen to protect against widespread power or network outages, or major natural disasters. Microsoft also takes advantage of the arrangement to minimize the risks associated with infrastructure updates, as well as to accelerate recovery times in the event of a widespread outage impacting multiple Regions. As with AZs, Microsoft's SLA effectively guarantees "dial tone" for the servers and nothing more. (See Sidebar on "Azure Uptime Exclusions") It is up to the customer, therefore, to ensure uptime at the application level.

With so many common causes of downtime excluded from service level assurances in the Azure cloud, achieving satisfactory HA protection for mission-critical applications will require a third-party failover clustering solution like SIOS DataKeeper. The need for third-party solutions derives from the fact that traditional HA failover clustering is not possible in the Azure cloud owing to the lack of a storage area network (SAN) or other shared storage in both the LAN and WAN. Microsoft addressed this limitation when it introduced Storage Spaces Direct (S2D), a virtual shared storage solution. But S2D

Azure Uptime Exclusions

Administrators should be fully informed about some major limitations cited in the Azure Service Level Agreement (SLA), which explicitly excludes these common causes of performance- and availability-related problems:

- "Factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center) ..."
- "The use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services ..."
- "Your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices ..."
- "Faulty input, instructions, or arguments (for example, requests to access files that do not exist) ..."

support began with Windows Server 2016 and only supports SQL Server 2016 and later, and is, therefore, not an option for SQL Server 2008/R2. Even then, S2D is not supported where nodes reside in different Fault Domains or Regions, so the more robust HA/DR options are not available when using S2D. Similarly, the Always On Availability Groups feature that was introduced with SQL Server 2012 is also not an option for the 2008/R2 versions.

Adequate business continuity or DR protections for some applications are, however, possible with either Azure Backup or Azure Site Recovery, Microsoft's DR-as-a-Service (DRaaS) offering. It is important to note the Azure Backup agent does not support SQL Server 2008/2008 R2; it is covered here only as an option for those legacy applications being upgraded to SQL Server 2012 or later. Here is how Microsoft positions these two services in the Overview of the features in Azure Backup:

> *"Azure Backup and Azure Site Recovery are related in that both services backup data and can restore that data. However, these services serve different purposes in providing business continuity and disaster recovery in your business. Use Azure Backup to protect and restore data at a more granular level. For example, if a presentation on a laptop became corrupted, you would use Azure Backup to restore the presentation. If you wanted to replicate the configuration and data on a VM across another datacenter, use Azure Site Recovery. Azure Backup protects data on-premises and in the cloud. Azure Site Recovery coordinates virtual-machine and physical-server replication, failover, and failback. Both services are important because your disaster recovery solution needs to keep your data safe and recoverable (Backup) and keep your workloads available (Site Recovery) when outages occur.*
>
> *Azure Backup supports Recovery Point Objectives (RPOs) ranging from 15 minutes for databases to as long as a full day for VMs. ASR supports RPOs from a few minutes to a few seconds. The Recovery Time Objective (RTO) may need to be as long as a day, or even longer, to make Azure Backup suitable for BC and/or DR needs. ASR supports RTOs of under one hour, and as low as a few minutes with appropriate arrangements."*

With the many exclusions to common causes of downtime in the Azure cloud, along with the inability to take advantage of the many enhancements and new services introduced since 2008, administrators are finding that the best way to be confident about protecting SQL Server 2008/R2 applications is with the only Microsoft recommended solution, SIOS DataKeeper, that is purpose-built for high availability and disaster recovery.

SQL Server Failover Clustering with SIOS DataKeeper

The biggest challenge involved in implementing HA and/or DR provisions for SQL Server 2008/R2 in Azure derives from the need for Failover Cluster Instances (FCIs) to use some form of shared storage, normally in the form of a SAN. SIOS DataKeeper addresses this challenge head-on by creating a SANless failover cluster that is fully compatible with virtually all applications, including both legacy and current versions of SQL Server and Windows Server.

SIOS DataKeeper for Windows Server is available in both a Standard Edition and a more robust Cluster Edition. The Standard Edition provides real-time data replication for disaster recovery protection in a Windows Server environment. The Cluster Edition seamlessly integrates with Windows Server Failover Clustering (WSFC), enabling both high availability and disaster recovery configurations.

SIOS DataKeeper is a complete HA/DR solution that integrates data replication with continuous application-level monitoring and configurable policies for failover/failback, and offers these value-added capabilities:

- Implementation entirely in software delivers virtually unlimited scalability across private, public and hybrid cloud infrastructures
- Automatic and manual failover/failback recovery policies that are easy to configure and enable planned maintenance to be performed with minimal downtime
- Support for physical, virtual and cloud-based Windows Servers
- A storage-agnostic design that supports any direct-attached storage
- High performance, low-overhead, block-level synchronous or asynchronous volume replication
- Simple wizard-driven implementation and an intuitive graphical user interface with "single pane of glass" monitoring and management

SIOS DataKeeper works by building a failover cluster instance using locally-attached storage in a way that makes the storage appear to be shared among the cluster nodes. SIOS DataKeeper registers a third-party storage class resource called a SIOS DataKeeper Volume Resource that takes the place of a physical disk resource. Rather than control disk locking, as would be the case with physical disk, SIOS DataKeeper instead controls the mirror direction among two or more servers. This approach ensures that writes occur on the primary or active cluster node and are synchronously or asynchronously replicated to all other secondary or standby nodes in the failover cluster. The block-level volume replication occurs synchronously between nodes in the same Azure region (Availability Set or Zone) and asynchronously across Regions. The resulting shared-nothing SANless failover cluster eliminates all potential single points of failure, thereby ensuring dependable HA and/or DR protection.

Its application-agnostic design enables SIOS DataKeeper to support virtually all application software, including all versions of SQL Server, making it a universal, general-purpose HA/DR solution. This same design also makes it possible for SIOS DataKeeper to support FCIs in the Standard or Enterprise Edition of all versions of SQL Server, from SQL Server 2008 through SQL Server 2019.

It is worth noting that for legacy applications being upgraded, SIOS also offers the SIOS Protection Suite for Linux. Microsoft began supporting Linux with SQL Server 2017, and the SIOS Protection Suite provides both HA and DR protections that are comparable to SIOS DataKeeper for Windows Server.

As a universal solution purpose-built for high availability and disaster recovery, the combination of SIOS DataKeeper and WSFC is capable of immediately detecting failures at the application level regardless of the cause and without the exceptions cited in the Azure SLA. This capability is what enables SIOS DataKeeper to accommodate far more stringent Recovery Time and Recovery Point Objectives (RTOs/RPOs) compared to standard Azure HA/DR provisions, making it suitable for even the most mission-critical of applications.

Popular HA/DR Configurations for SQL Server 2008/R2 in the Azure Cloud

With HA provisions for legacy SQL Server 2008/2008 R2 being problematic in the Azure cloud, the only viable option is a third-party solution that enables SQL Server Failover Cluster Instances to be built on top of replicated storage rather than shared storage. For DR by contrast, administrators have a choice of using Azure Site Recovery or SIOS DataKeeper for both HA and DR. This section describes both of these popular configurations: A "Basic" one using SIOS DataKeeper for HA and Azure Site Recovery for DR; and an "Advanced" one using SIOS DataKeeper for unified HA/DR protection.

Important Note: For running SQL Server applications on failover clusters in Azure on Windows Server 2008 R2 or Windows Server 2012, Microsoft offers this hotfix to enable the listener to be used by both FCIs and Availability Groups: https://support.microsoft.com/en-us/help/2854082/update-enables-sql-server-availability-group-listeners-on-windows-serv. Depending on the configuration, additional hotfixes may be needed. If possible, using Windows Server 2012 R2 or later eliminates the need for any hotfix.

"Basic" Configuration: SIOS DataKeeper for HA and ASR for DR

The combination of SIOS DataKeeper for HA and Azure Site Recovery (ASR) for DR provides a cost-effective solution that would be extraordinarily difficult and potentially cost-prohibitive to deploy in a private cloud with SAN replication across two or more enterprise datacenters. The shared storage required by FCIs is provided by the SIOS DataKeeper Volume Resources in the SANless HA failover cluster, and ASR replicates the pair of VM images in the cluster (both the active and standby) to another region in a Region Pair to protect against widespread disasters.

"Lifting and Shifting" an existing SQL Server 2008/2008 R2 failover cluster from the premises to the Azure cloud is quite straightforward, and involves replacing physical disk resources with SIOS DataKeeper Volume Resources, and replacing the drive witness with a File Share Witness. During the migration, ASR can be used to replicate the existing servers on premises to Azure. The last step involves configuring the Azure Internal Load Balancer (ILB) for client redirection and running a PowerShell script on the local nodes to update the SQL Server cluster IP resource to listen for the ILB probe. Because the IP addresses and subnet of the cluster instances will likely change as part of this migration, this step may also require other changes to related IP addresses and job endpoints.

An alternative approach is to simply build a new SANless cluster in Azure first, then either backup and restore the production databases to this new instance, or replicate just the data volumes using DataKeeper from on-premises to the cloud and attach the replicated databases to the SANless cluster in Azure.

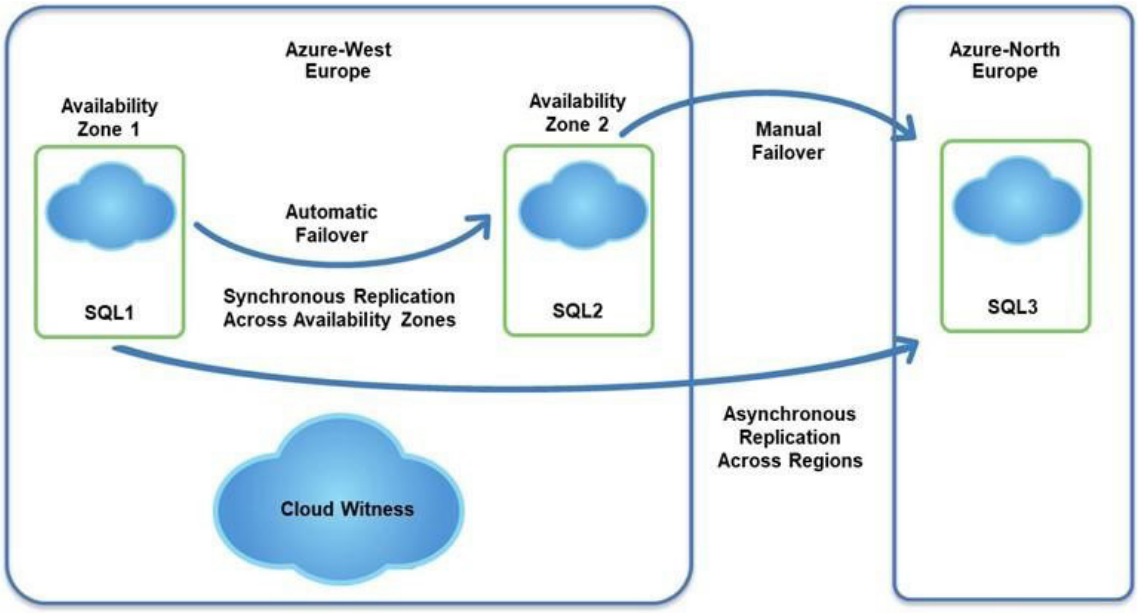
If no on-premises HA failover cluster exists to be lifted and shifted, it will be necessary to create one in the Azure cloud. The steps required to do that are a subset of those included in the following section for configuring SIOS DataKeeper for both HA and DR.

When using ASR to migrate an existing SQL Server FCI it is necessary to first replace the on-premises physical disk resources with SIOS DataKeeper Volume Resources and remove the Disk Witness. Once that is done follow the steps here to migrate the cluster from on-premises into Azure: https://docs.microsoft.com/en-us/azure/site-recovery/migrate-tutorial-on-premises-azure.

"Advanced" Configuration: SIOS DataKeeper for both HA and DR

Like all DRaaS offerings, Azure Site Recovery has some limitations. For example, WAN bandwidth consumption cannot exceed 10 Megabytes per second, and that may be too low for high-demand applications. More serious limitations involve the inability to automatically detect and rapidly failover from many causes of application-level downtime. Of course, this is why the service is characterized as being for disaster recovery and not for high availability.

More robust DR protection is possible with SIOS DataKeeper, normally in a three-node configuration as shown in the diagram. Two of the nodes provide HA protection with rapid, automatic failover based on real-time synchronous data replication across an Availability Set or Zone. The third node, located across the WAN in a different Azure region (preferably as part of a Region Pair), offers DR protection for localized outages that affect an entire datacenter (Availability Set), as well as for more widespread disasters affecting an entire region (Availability Zone).



A two-node SIOS SANless failover cluster consisting of SQL1 and SQL2 is deployed across AZs in the West Europe Region for HA protection. SQL3 is located remotely in the North Europe Region to provide DR protection.

The main advantage of using SIOS DataKeeper for both HA and DR is more effective use of bandwidth because only the application data is being replicated, rather than the entire instance. This enables achieving a much better RPO, as well as a better RTO because the DR node is already provisioned and online.

Highlighted here are the seven basic steps needed to configure a two-node SIOS DataKeeper high availability (HA) failover cluster, along with a single SIOS DataKeeper node for disaster recovery (DR), when running SQL Server 2008 R2 applications in the Azure cloud. Each step involves details that are not covered here, but can be found in Step-by-Step: How to configure a SQL Server 2008 R2 Failover Cluster Instance in Azure.

Note that while this configuration is for SQL Server 2008 R2 running on Windows Server 2008 R2, the same basic steps are similar to those needed to configure SQL Server 2012, 2014, 2016 and 2017 (and the soon to be released 2019) to run on Windows Server 2012 R2, 2016 or 2019.

1. Provision three virtual machine instances (two HA cluster nodes and one file share witness) in either an Availability Set (within a single datacenter) or across Availability Zones (spanning multiple datacenters in a region). Configure another VM instance as the DR node in a different Azure region, preferably as part of a Region Pair. This step also involves attaching storage, formatted with NTFS, to both HA cluster nodes and the DR node.
2. Configure each instance to use a static IP address, then specify the Domain Name Server of the Active Directory domain and join each VM to the domain. Enable both Windows Server Failover Clustering (WSFC) and .NET Framework 3.5 on both HA cluster nodes and the DR node. Configure any firewalls and/or network security to permit the required ports to be open between the HA cluster nodes, and allocate external connections on the SQL Server and Load Balancer Probe ports.
3. Create two Global Domain Security Groups and add Domain User Accounts to each group. These groups and accounts will need to be referenced later when installing the SQL Server software. Create another Domain User Account and add it to the Local Administrators Group on each of the HA cluster nodes and the DR node. This account will need to be referenced later when installing the SIOS DataKeeper software.
4. Create the cluster between the two HA cluster nodes. Owing to the way Azure handles DHCP, the cluster must be created using PowerShell to specify a static IP address. This step also involves adding the File Share Witness after the cluster is created.
5. Install and setup SIOS DataKeeper on the two HA cluster nodes and the DR node. This step also involves creating the SIOS DataKeeper Volume Resources, choosing the Source and Target instances, and creating new mirrors for data replication. A synchronous mirror will be created between the two HA cluster nodes first and then an asynchronous mirror will be added to the DR node.
6. Install the SQL 2008 R2 software on the first HA cluster node and choose “Create New Cluster Instance.” Then install the SQL Server software on the second HA cluster node and choose “Add Node to Existing Cluster.” Finally, install the SQL Server software on the DR node as a Standalone Instance. For the DR instance, be certain to keep the system databases stored on the C: drive, or some other non-replicated volume.

7. Create the Azure Internal Load Balancer (ILB) or Public Load Balancer if the database is to be exposed on the Internet. This step is necessary because Azure does not support gratuitous ARP, preventing clients from connecting directly to the cluster's IP address. This step also involves running a script on one of the cluster nodes to enable the Load Balancer Probe to detect which node is active.

Once complete, the configuration will provide both automatic and manual failover capabilities between the two local nodes. To activate the third server in the event of a disaster, use the SIOS DataKeeper interface to make the third node the source of the mirror, then attach the replicated databases using SQL Server Management Studio. Finally, it will be necessary to redirect applications to use this new instance, either through a DNS update or by manually reconfiguring connection strings. For more detailed information visit these links for:

- Attaching a database… https://docs.microsoft.com/en-us/sql/relational-databases/databases/attach-a-database?view=sql-server-2017
- Extending a clustered SIOS DataKeeper Volume Resource to a node outside the cluster… http://docs.us.sios.com/dkce/8.6.4/en/topic/extending-a-clustered-datakeeper-volume-to-a-node-outside-the-cluster

Getting Started

A good best practice is to practice with one or more of the affected applications migrated to a non-production environment set up in the Azure cloud. With all HA and/or DR configurations, comprehensive testing is essential to ensuring dependable operation. There are numerous "moving parts" with high availability, making it common for initial configurations to contain at least a few mistakes, and even a seemingly minor mistake can cause failover provisions to fail when needed.

SIOS helps make it easy to get started by offering a Free Trial of SIOS High Availability Clustering Software. The SIOS DataKeeper for Windows Server software works with all versions of SQL Server, as well as with virtually all other Windows Server applications. This same link also offers a free trial version of SIOS Protection Suite for Linux that can be used with any Linux applications, including those running on SQL Server 2017.

SIOS also offers comprehensive documentation, an assortment of templates that automate all or part of application-specific and/or cloud-specific configurations, responsive support, and a variety of other useful resources to help get you started. SIOS even offers a No-Cost Assessment for Moving SQL Server 2008 to Azure or Azure Stack to maintain security updates Sign up for the assessment now!

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

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