



The complete guide to high availability in the Azure cloud

The quick-start guide to getting beyond SQL Server 2008 end of support

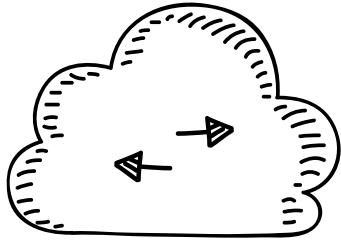


Get the security updates, keep the high-availability

When Microsoft support for SQL Server 2008/2008 R2 ends on July 9, 2019, a lot of organizations will choose to move their SQL Server instances to Azure. This makes some sense, and it also gets them the Azure offer of three years of extended security updates at no additional cost. The problem with this solution is that you may have a SQL Server failover cluster instance (FCI), or use hypervisor-based high availability (HA), or other clustering technology on-premises for HA. In any of those cases, you'll probably need the same in Azure. The trouble is, none of those solutions are natively supported in the cloud.

So, if you need to migrate to Azure at end of support (EOS), and you require HA for SQL Server 2008/2008 R2, there's only one solution recommended by Microsoft: SIOS DataKeeper. SIOS DataKeeper enables clustering in the cloud, including the creation of a SQL Server 2008/2008 R2 FCI, allowing you to achieve your HA goals.

This e-book will give you an overview of a complete, high-availability move to Azure, including an overview of how SANless clusters work and what it takes to deploy Windows Server failover clusters with SIOS DataKeeper.



A choice of ways Azure helps you maintain high availability

With Azure, you have a choice of two service level agreements (SLAs).

Fault domains

The first one has been around for a while. It provides for 99.95% availability with **fault domains**. This involves putting your two instances of SQL into an availability set, which distributes the instances into different fault domains within a single Azure region.

With this option, you'll need SIOS DataKeeper to keep the data in sync between the SQL Server instances. With this SLA, each region has up to three fault domains, and servers in the same availability set get distributed between them. In this option, Microsoft guarantees at least one server in your Availability Set will always be online.

Azure Availability Zones

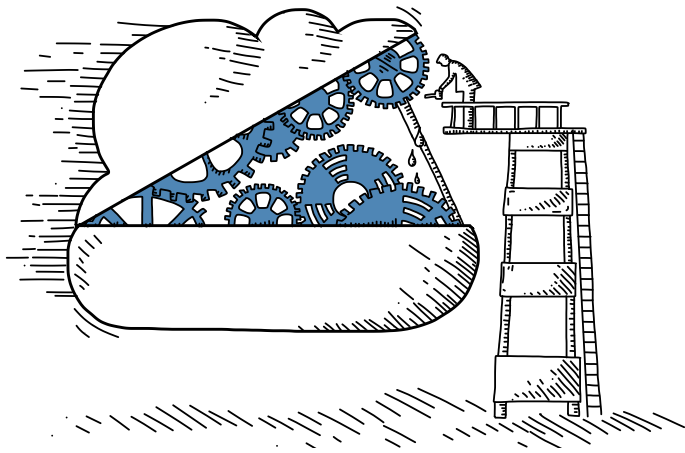
The second option which is new, involves **Azure Availability Zones**. With this arrangement, Microsoft gives you a 99.99% availability SLA.

Availability Zones position multiple datacenters at least 10 miles apart for redundancy in region outages such as the September 4, 2018, multi-day outage in the south-central region of the United States. All of the datacenters are well connected to each other through low-latency cable on a single subnet. To reduce risk, there are at least three Availability Zones in the regions that support Availability Zones.

While the Azure SLA guarantees infrastructure availability, SQL Server 2008/2008 R2 requires the use of SIOS DataKeeper to ensure application availability. This provides you with:

- Geographically dispersed datacenters for disaster recovery
- Cost-effective business continuity
- Azure Site Recovery for simple, cost-effective disaster recovery

It also gives you three-year extended SQL Server 2008/2008 R2 security updates from Microsoft. This works to extend your deadline and allow IT time to plan migration or upgrade, reduce costs, and ensure critical security updates are available. It also allows you to migrate SQL Server workloads to Azure with on-premises licenses with no application code changes.



How SANless clusters work—a 30,000-foot view

As you're planning your best course of action for end of service—whether it's Fault Domains, or Availability Zones—it's important to consider how SANless clusters in the cloud enhance availability over physical datacenters.

In a traditional cluster, you have two or more nodes connected to shared storage. (This is the shared storage that isn't available in Azure.) To make up for the lack of shared storage, the SIOS DataKeeper solution is the Microsoft-recommended replacement. This solution is software that runs on each cluster node. There's no additional infrastructure to buy. You simply run configure SIOS DataKeeper on each cluster node and build the SQL Server FCI as you normally would.

The difference is, instead of using shared storage (represented in the cluster as a physical disk resource) you use a SIOS DataKeeper volume, which is locally attached disk replicated by SIOS DataKeeper. That's what takes the place of the physical disk resource.

Then, when failover clustering detects an outage, it will fail over to the other node, but instead of controlling disk locking, it simply reverses the mirroring direction from one cluster node to the other. Once the failed cluster node returns to service the mirror continues, ensuring your SQL Server instance is protected should another failure occur.

A word about paired regions

If you plan to use Azure Site Recovery to replicate your SQL Server FCI to an entirely different region for disaster recovery, you will want to know about paired regions. The region you choose for your disaster recovery location is a critical consideration. Currently, Azure supports 54 regions worldwide and is available in 140 countries. Once you've picked the region you're operating in, you need to know what region it will be paired with. Microsoft usually pairs regions within the same country but more than 300 miles apart to reduce the risk from any single event or outage.

When Microsoft rolls out an update, they only do one region pair at a time. That way, if there's a problem with the update, you know the paired region is not impacted. And if multiple regions go offline at once, one paired region gets prioritized for recovery. You can find the paired regions in the Azure documentation.



How it works: A summary of the 8 basic steps to completing your configuration

To give you an idea of the scope of a SIOS DataKeeper launch, here's a quick overview of the steps to configure either a two-node SIOS DataKeeper high availability (HA) failover cluster or a single SIOS DataKeeper node for disaster recovery (DR).

For more detail on the process, take a look at the white paper, [Windows Azure IaaS: High Availability and Disaster Recovery with SIOS DataKeeper](#).

1. Provision three virtual machine (SQL1, SQL2, FSW) instances either within an Availability Set or distributed across three Fault Domains
2. Configure each instance to use a static IP address and join the existing Windows Domain
3. Enable both Windows Server Failover Clustering (WSFC) and .NET Framework 3.5 on both cluster nodes (SQL1, SQL2) Create two global domain security groups and add domain user accounts to each group.
4. Run cluster validation and create a two-node cluster consisting of SQL1 and SQL2 and specify FSW as the file share witness in the cluster quorum settings.
5. Install and set up SIOS DataKeeper on SQL1 and SQL2
6. Install SQL Server 2008/2008 R2 on SQL1 and choose "Create New Cluster Instance."
7. Install SQL Server 2008/2008 R2 on SQL2 and choose "Add Node to Existing Cluster."
8. Configure an Azure Load Balancer for client connections to the cluster.



Your link to the high-availability cloud

SIOS is more than a Microsoft Gold Partner. We're an essential piece that ensures SQL Server 2008/2008 R2 high availability while running in the Azure cloud. Our SANless cluster software is a vital part of any cluster solution, providing the flexibility to protect your SQL Server in any configuration of physical, virtual, and cloud, whether it's public, private, or hybrid — all without sacrificing performance or availability.

[Explore more](#)

