Debunking the Myths: Cloud HA and DR

Common misconceptions about protecting applications and data in cloud environments.

SIOS

Critical applications move to the cloud.

We all know that enterprises are moving more and more applications to the cloud. Gartner predicts that the bulk of new IT spending by 2016 will be for cloud computing platforms and applications and that nearly half of large enterprises will have cloud deployments by the end of 2017.[1]

While the benefits of the cloud may be clear for applications that can tolerate brief periods of downtime, it is not as clear for business critical applications, such as SQL Server, Oracle, and SAP that require high availability and disaster recovery protection.

Separating the facts and myths of HA and DR in cloud deployments can help you save money and reduce risk of downtime and data loss.

The benefits of moving applications to the cloud are summarized in a recent McKinsey report on disruptive technologies:

"Cloud technology has the potential to improve productivity across $3 trillion in global enterprise IT spending, as well as enabling the creation of new online products and services for billions of consumers and millions of businesses alike."[2]

Myth #1: Clouds are HA environments.

The myth: Public cloud deployments – particularly with leading cloud providers – are automatically high availability environments where application downtime is negligible.

The truth. Clouds are not high availability environments unless you add HA protection. In fact, according to a recent study:

“The average unavailability of cloud services is 10 hours per year or more, while the average availability is estimated to be 99.9% (9 hours or more than a day of downtime), far less than the expected availability of business critical applications.”[3]

Cloud Outages in 2013[4]

- Microsoft Windows Azure for 20 hours, a sub-component of the system failed worldwide.
- Google lost all services for five minutes.
- Amazon Web Services: connectivity issues disrupted a notable portion of Internet activity in a single availability zone for under 3 hours.

Redundancy is not enough.

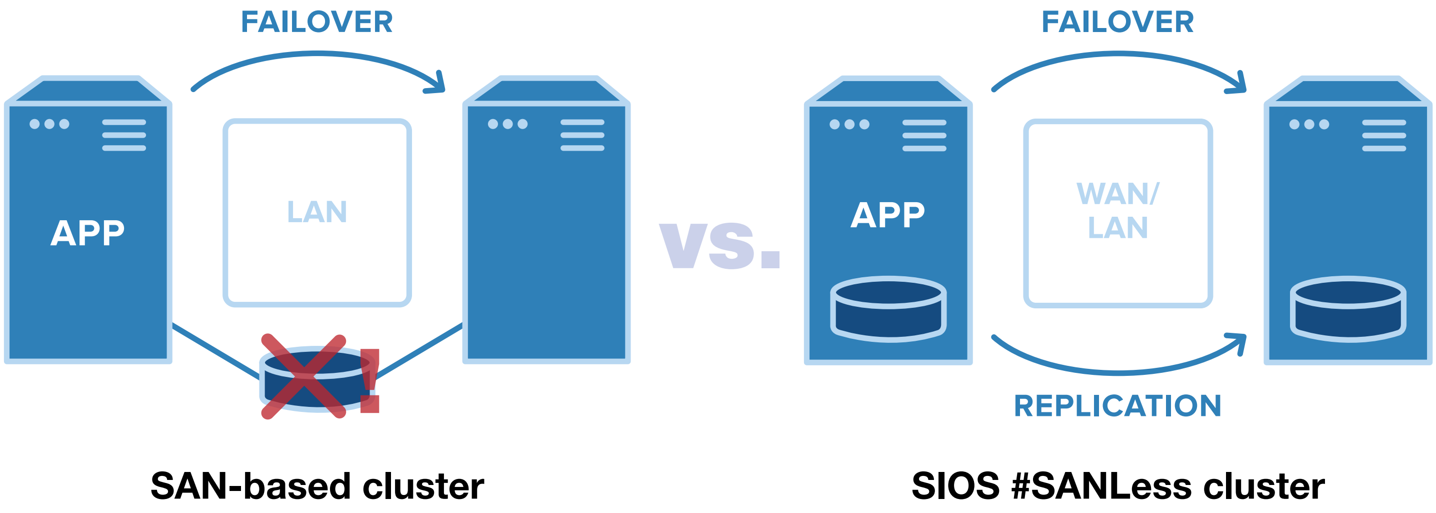
Some cloud solutions such as Windows Azure offer a measure of application protection through some redundancy. You can add some availability protection for web servers such as IIS by putting them in different fault domains and enabling load balancing. However, applications such as SQL Server and File Servers still need additional configuration for high availability and disaster recovery.

SIOS

Myth #2: You can't have cluster protection in a cloud.

The myth: You cannot protect business critical applications in a public or private cloud with a cluster.

The truth. To provide high availability in a physical deployment, you typically use Windows Server Failover Clusters (WSFC) and a shared storage device, such a SAN. But, public clouds, such as Amazon EC2 and Windows Azure have no concept of a cluster-aware shared storage device. You can provide high availability protection for Windows applications in a cloud simply by adding #SANLess cluster software and configuring a WSFC environment. The #SANLess software synchronizes local storage in the cloud through real-time, block level replication, providing applications with immediate access to current data in the event of a failover. #SANLess software is an easy, cost-efficient way to protect SQL, Oracle, SAP or other business critical applications in a Windows environment from downtime and data loss.



SAN-based cluster

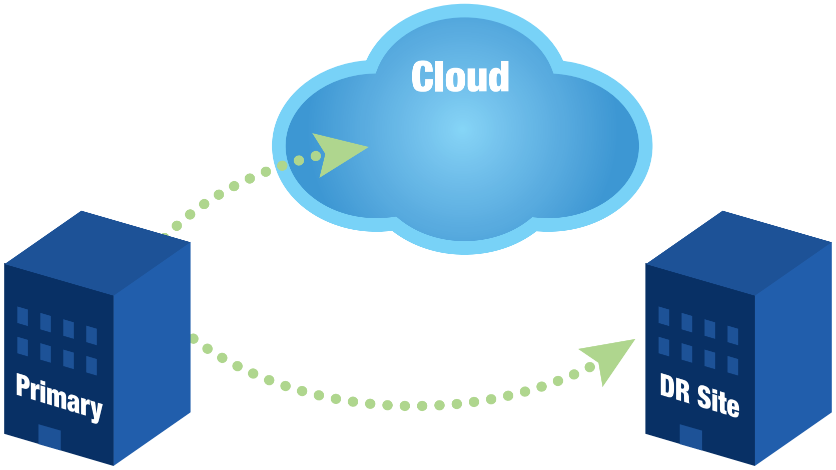
SIOS #SANLess cluster

Myth #3: You don't need remote replication for DR.

The myth: Applications and data are protected from disasters in the cloud without additional configuration.

The truth: Cloud providers experience downtime and regional disasters like any other large organization. While providing high availability within the cloud will protect you from normal hardware failures and other unexpected outages within an availability zone (Amazon) or fault domain (Azure), you still need to protect against regional disasters.

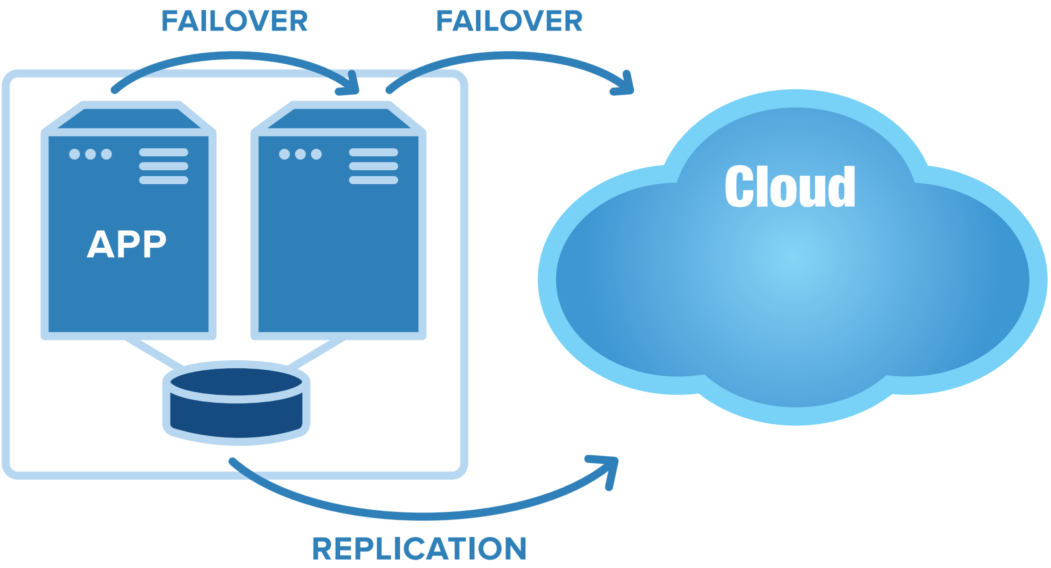
The easiest solution is to configure a multisite (geographically separated) cluster. You can build a #SANLess cluster within a cloud and extend it by adding an additional node(s) in an alternate datacenter or different geographic region. Simply adding a third, geographically separated node to your #SANLess cluster can give you a recovery point objective (RPO) of near zero data loss and a recovery time objective (RTO) of just about one minute.



Myth #4: Using the cloud is an “all or nothing” decision.

The myth: You either run your application in the cloud or in your on-premises data center.

The truth: You can use your on-premise data center as your primary datacenter and the cloud as your hot standby DR site. This is a very cost effective alternative to building out your own DR site, or renting rack space in a business continuity facility. In this case, the on-premise servers can be traditional SAN-based clusters, #SANLess clusters or even single servers not currently participating in a cluster.



Myth #5: HA in a cloud is costly and complicated.

The myth: Creating a high availability environment in a cloud environment requires complex scripting, specialized skills, or added complexity.

The truth: You can create a cluster for high availability in a cloud in **three easy steps** using #SANLess cluster software. The software provides an intuitive configuration interface that lets you create a standard WSFC in a cloud in minutes without specialized skills.

You can also use this software to eliminate the need to buy costly enterprise edition versions of Windows applications to get high availability and added disaster protection or as described in Myth 4, to eliminate the need to build out a remote recovery site.

You can also use SQL Server Standard Edition (instead of more costly Enterprise Edition) with DataKeeper Cluster Edition to replicate to a third node outside of the cloud for cost-efficient disaster protection.

Notes

[1] "Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016."
http://www.gartner.com/newsroom/id/2613015

[2] Manyika, James and Michael Chui, et al, "Disruptive technologies: Advances that will transform life, business, and the global economy," McKinsey Global Institute (May 2013) http://www.mckinsey.com/insights/business_technology/disruptive_technologies

[3] Whittaker, Josh, "Amazon Web Services Suffers Outage, Takes Out Vine, Instagram, Others with it," ZDNet, (August 26, 2013) http://www.zdnet.com/amazon-web-services-suffers-outage-takes-down-vine-instagram-flipboard-with-it-7000019842/

[4] Mackay, Martin, "Downtime Report: Top Ten Outages in 2013," Business2Community.com, (December 2013) http://www.business2community.com/tech-gadgets/downtime-report-top-ten-outages-2013-0720582#Z2xCkBHqs5SrECkO.99

Ready to Learn More

About protecting your applications with SIOS SAN or #SANLess cluster?

www.clustersyourway.com

SIOS