The prerequisite for high availability is redundancy for both data processing nodes and data storage nodes in a system. In addition, the system must contain mechanisms to automatically transfer work from faulty nodes to redundant nodes, and also to automatically recover faulty nodes (and their data for storage nodes) once they have been repaired. Building a system with redundant processing nodes is relatively easy, and businesses have been doing this for decades using load balanced web server farms.

The most challenging redundancy is that of the data stored by a system. Keeping multiple copies of data on different storage nodes synchronized with each other continuously and reliably can be very difficult to achieve in practice. When the storage nodes are hosted in geographically separate locations it becomes even more difficult. This capability, along with horizontal data storage scalability (shards) is what differentiates a distributed grid from an ordinary distributed system.

Requirements

1. Omnidirectional merge replication (DGP replication or SQL Server Availability Groups)

What: *An innovative asynchronous merge replication based on immutable append-only storage of database records; similar to CRDT or copy-on-write mechanisms.*

Why: *One of the most important characteristics of distributed grid computing platforms is their fault-tolerance and reliability. This is only made possible by their distribution of data to multiple locations and the constant real-time synchronization of data between those locations.*

Testing: *Data replication can be tested manually using the test harness application, and also automatically using the automated data verification processes run constantly in the background by the AutoWork subsystem..*

2. 100% system availability / uptime: depends on DGP replication and redundant servers

What: *A system should always be available for use, with no maintenance windows and no downtime (planned or unplanned).*

Why: *Large Internet-scale companies provide software products and services that have 100% uptime with extremely good performance and scalability. One of the main purposes of DGP is to provide those same capabilities to companies in the SMB market at a very low cost.*

Testing: *Overall uptime metrics can be monitored and measured to see the amount of downtime that occurred during a particular time period.*

3. Automated failover and recovery between redundant processing nodes

What: *A distributed grid system must have mechanisms that detect processing node problems and fail over to other redundant processing nodes. The system should also be able to automatically recover failed processing nodes when those problems have been resolved..*

Why: *A distributed grid is a reliable system built using unreliable parts. Individual parts of the system are expected to fail periodically, while the system as a whole continues to function unimpeded. Processing nodes are stateless identical copies of each other, which makes failover an recovery of individual nodes fairly easy.*

Automated failover is intended to cover for unplanned node or location downtime, while the manual failover is used for periodic node maintenance.

Testing: *Manual and automated failovers between redundant nodes can be tested in Test and QA environments for both processing nodes and storage nodes.*

4. Automated failover and recovery between redundant storage nodes

What: *A distributed grid system must have mechanisms that detect resource problems and fail over to other redundant resources. The system should also be able to automatically recover failed storage nodes when their issues have been resolved..*

Why: *A distributed grid is a reliable system built using unreliable parts. Individual parts of the system are expected to fail periodically, while the system as a whole continues to function unimpeded. Failover and recovery for storage nodes is much more complex than for processing nodes because of the need to insure that the data remains synchronized between active nodes at all times.*

Automated failover is intended to cover for unplanned node or location downtime, while the manual failover is used for periodic node maintenance. Within a single location, traditional clusters can be used for fault-tolerant redundancy. Between locations, DGP replication can be used for fault-tolerant redundancy, and can also be used within locations in some configurations as well.

Testing: *Manual and automated failovers between redundant nodes can be tested in Test and QA environments for both processing nodes and storage nodes.*

5. Maintenance during system use: depends on DGP replication

What: *A mechanism to incrementally patch and maintain locations, or individual processing and storage nodes within each location is necessary. The overall system must remain online and in use during the maintenance work.*

Why: *Maintenance of processing and storage nodes must be performed while the overall system remains in use. There are two options. The first option does maintenance work on an entire location at a time. For this option, one location is designated as the primary for all users, while another location is designated as the backup. In this configuration, each location is taken offline for maintenance while all users continue their work in the other location.*

A second option keeps all locations online, and requires individual nodes be sequentially removed from the cluster or farm, patched and maintained, and then merged back into the subsystem, while all locations remain in use.

Testing: *The maintenance processes can be tested and verified in the Testing and QA environments prior to using them in production environments.*