the *Availability Digest*

Fault Tolerance with everRun from Stratus
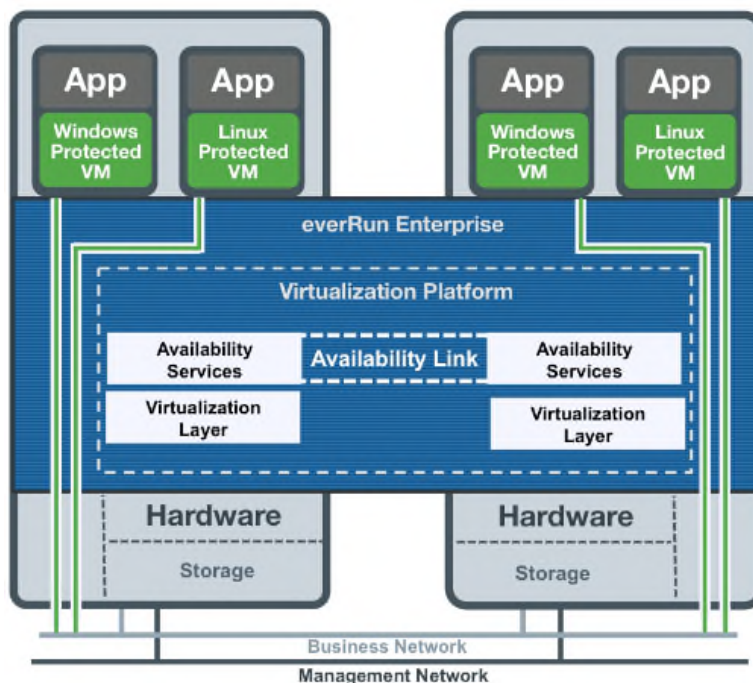
December 2015

everRun from Stratus Technologies (http://www.stratus.com/) provides a platform for running virtualized applications in a fault-tolerant or high-availability environment. Stratus' everRun *prevents* downtime rather than *recovering* from it and protects against data loss in the process.

everRun Overview

The everRun Architecture

everRun is tightly integrated with the open-source KVM hypervisor and runs on two industry-standard x86 host servers. Applications run in virtualized machine (VM) guest operating systems supported by everRun. Each VM has an identical instance running on each host server. The everRun Availability Services synchronize the applications running in each host server via an Availability Link so that if a physical server fails, the applications in the surviving server carry on without interruption or data loss.

Neither the application nor the user is exposed to the redundant computing resources on the two host servers. The application sees only one hostname. If a fault or failure occurs, everRun software

1

automatically redirects I/O to the paired host server for continuous operation. Though redundancy is lost until the failure is repaired, the client experiences no interruption in connectivity and no loss of data. The application continues to execute as if nothing happened. Repair of the failed host server is equally transparent and automatic. When a failed host server is repaired, everRun software automatically incorporates it into the protected environment and restores redundancy without interrupting the application.

Why KVM?

The open-source community has implemented a virtualization solution for Linux on x86 hardware – the Kernel-based Virtual Machine. KVM is different from other hypervisors because it is an integral part of the Linux operating environment. Thus, KVM can take advantage of core features already hardened within Linux. It also is designed to take advantage of the hardware-assisted virtualization features that Intel and AMD have built into their processors. KVM can run unmodified Windows and Linux images in virtual machines.

As an active contributor to KVM, Stratus has integrated KVM into its everRun availability software to enable the virtualization capabilities that allow everRun to provide its fault-tolerant and high-availability services.

Availability Modes

everRun has two availability modes – everRun Enterprise, which supplies full fault tolerance, and everRun Express, which provides disaster recovery.

everRun Enterprise Fault Tolerance

everRun Enterprise furnishes fault-tolerance for applications running in its environment. In fault-tolerant mode, an application continues to run without downtime during a fault. everRun Enterprise is used for applications that need the highest levels of availability.

In fault-tolerant operation, the everRun software transparently protects an application by creating a redundant environment for a VM running across two host servers. With an identical instance of the selected VM on a second host, everRun Enterprise:

- Eliminates downtime due to any CPU, memory, I/O, or other host-system failure.
- Handles failures without IT intervention.
- Ensures no data loss.
- Provides continuous, active validation of all components.
- Ensures complete redundancy and recovery at all times.

everRun Express High Availability

everRun Express provides high availability for applications running in its environment. In high-availability mode, everRun automatically detects, isolates, and handles most hardware faults, thereby keeping applications running.

High-availability operation offers basic failover and recovery, with some faults requiring an automatic VM reboot for recovery and return to high-availability operation. This availability mode:

- Eliminates downtime for many, but not all, CPU, memory, I/O, or other host-system failure.
- Handles failures without IT intervention.
- Provides continuous, active validation of all components.
- Ensures redundancy and recovery at all times.

everRun Express is suitable for applications that can tolerate occasional interruptions of a few minutes.

everRun Availability Services

The everRun Availability Services depend upon the redundant Availability Link communication channel connecting the everRun environments running in each host server. The Availability Services monitor the state of each of the VM instances and perform recovery of an instance should it fail. If the failed instance is the currently active instance, Availability Services manages the failover to the backup VM instance.

In fault-tolerant mode, if one host server should fail, the application will continue to run on the other host server without any interruption or data loss. In high-availability mode, one host server is active; and the other is a standby. If the active host server fails, the application is restarted on the standby host server with minimal interruption or data loss.

All input/output operations and state changes are automatically mirrored to the redundant host server via the Availability Link. This "statepointing" ensures that all in-flight transactions as well as data in memory and cache are preserved.

The everRun operating environment is first built on one server with KVM. The Stratus Availability Extensions then are used to create the fault-tolerant or high-availability environment. At this point, the Availability Link is activated to communicate continuously with the second host server.

Supported Guest Operating Systems

everRun supports the following operating systems as guest virtual machines:

Windows Server 2012	Windows 7
Windows Server 2011	Red Hat Enterprise Linux 7
Windows Server 2008	Red Hat Enterprise Linux 6
Windows Server 2003	CentOS 7
Windows 8.1	CentOS 6
Windows 8	Ubuntu

Networks

Private Network

Every everRun system requires one private network. The private network connects the two everRun host servers and is used only for discovery. The simplest private network consists of a single Ethernet cable that directly connects the two systems.

Availability Links

The Availability Link (A-Link) allows everRun to synchronize disks, to shunt networks, to migrate VMs between host servers, to perform heartbeat checks, and to synchronize fault-tolerant memory. The A-link should be redundant and should be directly connected.

The private network can serve as the A-Link if its speed is at least 10 Gps.

Management Network

Every everRun installation must have a management network. It provides connectivity to the everRun Availability Console and handles miscellaneous management tasks. It also provides the connectivity to the quorum server(s) described later.

Business Networks

All other Ethernet ports – aside from the A-Link and management networks – are considered business network ports. The guest operating systems use these ports to connect to external networks.
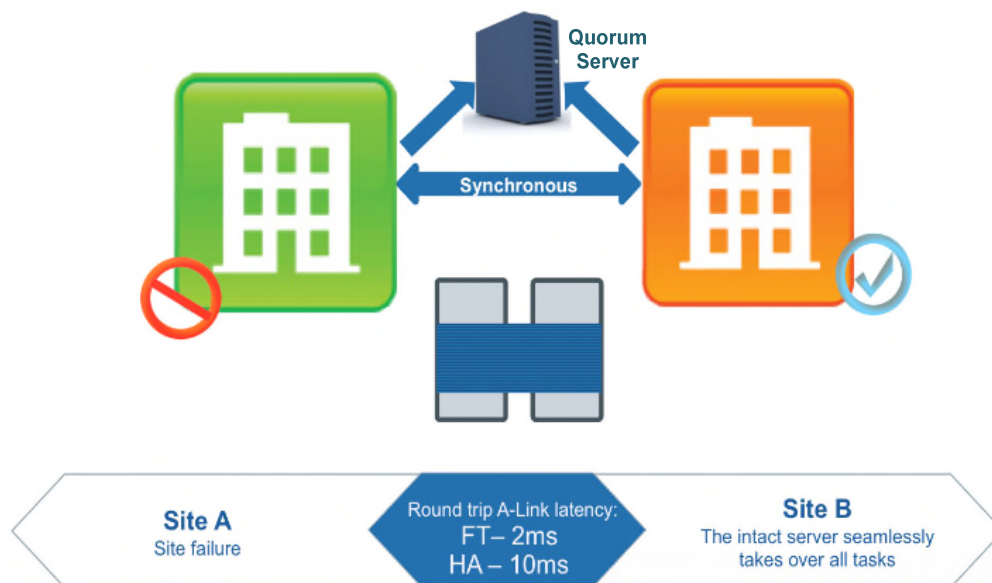
SplitSite Configurations

A *SplitSite configuration* connects two physical machines in two separate sites. It is a disaster-tolerant deployment that maintains hardware redundancy as well as redundancy of physical computer rooms and the buildings containing them. Because of the geographic separation, a SplitSite configuration requires careful planning of component placement and more complex networking topologies.

SplitSite provides application availability across geographically separated sites using synchronous replication. Therefore, A-Link round-trip channel communication latency must be limited to 10 milliseconds for high-availability VMs and 2 milliseconds for fault-tolerant VMs. Most deployments can be separated by up to ten kilometers.

For SplitSite configurations, Stratus strongly recommends that a quorum server be used because a SplitSite configuration exposes the A-Link networks to other potential failure scenarios.

Quorum Servers

It is recommended that a *quorum server* be configured for both fault-tolerant and high-availability operation. The quorum server prevents a condition called *split-brain*, where both host servers of a high-availability or fault-tolerant pair have lost communication with each other and are running independently. If split-brain operation is allowed to continue, the databases of the two systems will diverge.

A quorum server is a Windows operating system-based service deployed on a server distinct from the two host servers running high-availability- or fault-tolerant-protected virtual machines. Quorum servers provide data-integrity assurances and automatic restart capabilities for specific failures in an everRun environment. An everRun pair can be configured with 0, 1, or 2 quorum servers.

Quorum servers ensure the integrity of VMs against multiple network failure scenarios, including split-brain, and provide for unattended startup of VMs after specific failures. Quorum-server communication occurs via the management network.

Quorum servers are particularly important in SplitSite configurations. Best practice for SplitSite is to place a preferred quorum server in a third facility and an alternate quorum server in a fourth facility. However, you also can place the alternate quorum server with the preferred quorum server and still obtain satisfactory service.

If only two sites are available (thereby preventing the best practices configuration described above), and if one host server goes down and the surviving host server is unable to communicate with the quorum server (for example, because it is on the same site as the downed host server), the VMs at the surviving site are automatically shut down to avoid a potential split-brain scenario.

Simplex Operation

A simplex everRun system may be used in a disaster-recovery configuration. In such a configuration, fault-tolerant- and/or high-availability-protected virtual machines run on a duplex everRun system at one site; and snapshots of those VMs are replicated to a simplex system at another site.

If a failure occurs on the duplex system such that the VMs on it are not able to operate, VMs can be started from the snapshots on the remote simplex system.

The everRun Availability Console

The everRun Availability Console is a browser-based interface that provides management and monitoring of an everRun system from a remote management computer. Many administrative operations can be performed from the console because it allows access to the system as a whole as well as to physical machines (host servers), virtual machines, and other resources.

Using the everRun Availability Console, you can perform a variety of administrative functions:

- Read system alerts from the Dashboard.

- View VM, CPU, memory, and storage statistics; and reboot or shut down the system.

- Set system preferences, diagnostics, notifications (e-Alerts and SNMP configuration), and remote support (notification and access). System preferences include owner information and configuration values for IP addresses, quorum services, date and time, etc.

- View alerts and audit logs.

- Monitor, manage, and maintain resources:

    - Host server status, storage, disks, network, and sensors.

    - VM status and management tasks such as creating, importing/restoring, managing, and maintaining VMs.

    - Snapshot status and management tasks such as exporting and deleting snapshots.

- Volumes, including their states, sizes, and storage groups.

- Storage groups, including names, sizes used, sizes, and numbers of volumes.

- Networks, including states, physical interfaces, speeds, MAC addresses, and network bandwidths.

- Virtual CDs, including their states, names, sizes, and storage groups.

- Monitor and manage upgrade kits, users, and groups..

Remote Support

With remote-support technology, the everRun software notifies the Stratus support center of various issues, indicating the type of fault and its exact location. This combination of automatic fault detection, isolation, and remote-support technologies ensures speedy access to expert support technicians and rapid problem resolution.

Summary

Stratus everRun is installed at hundreds of sites supporting mission-critical solutions. Coupled with its redundant hardware-based, fault-tolerant ftServer and its continuously available OpenStack Cloud Solutions, Stratus Technologies has been a leader for over thirty years in providing high-availability and fault-tolerant solutions for applications that simply cannot fail or lose data.

I have personally used Stratus systems to implement many mission-critical systems, including world-wide correspondent networks for Time Magazine and McGraw-Hill. I continue to be impressed with the continuous availability that these systems provide.