everRun® EXTEND

Enabling application fault tolerance across sites connected via a WAN, using asynchronous replication

Whether caused by nature, mechanical or power failure, or human error, disasters can result in the total loss of all computing resources in a facility, potentially leaving your business unable to function for days, or even weeks. With Stratus® everRun® Extend, powered by Arcserve RHA, you can combine system redundancy with wide area network-based disaster recovery to maintain a hot stand-by system located in remote site.

Arcserve RHA software extends the core capabilities of Stratus everRun software to support disaster recovery (DR) capabilities across a wide area network (WAN), in conjunction with system redundancy in either, or both, primary site and remote DR site.

Key benefits

- **Ensure business continuity**: Protect critical applications and data against site-wide disasters
- **Simplify deployment and management**: Use the intuitive Scenario Builder and Control Service to make set up, configuration and management quick and easy
- **Pay for only what you need**: Choose from three different configurations that match your physical and virtual requirements

How it fits with everRun

everRun protects customers from server failures, or other system or network component failures. Arcserve RHA provides disaster recovery in the event of site disasters. The most typical customer configuration includes an everRun system running in a primary site, and a Windows or Linux system running on a single physical machine in a secondary DR site. Arcserve RHA provides DR between the primary and DR site (also called the Master and Replica). Some customers also maintain everRun systems at their DR site, to ensure high availability after a disaster recovery scenario is executed.

The Arcserve DR software is installed in the Windows or Linux system to protect the applications running on that system. It is a complementary and layered product for the everRun product suite. The Windows/Linux system can run on a physical machine, on a virtual machine (e.g. on VMware) or a Windows/Linux system running in an everRun Protected Virtual Machine (PVM).

Arcserve RHA also is installed in a Windows/Linux system at the remote DR site. This can also be a Windows/Linux system running on a physical machine, on a virtual machine (e.g. on VMware) or a Windows/Linux system running in an everRun Protected Virtual Machine (PVM).

Three configurations are possible:

1. **V2P**: The primary site has the application running in an everRun PVM and the DR site has the application running on a non-everRun system.
2. **V2V**: Both sites have the application running in an everRun PVM.
3. **P2P**: Both sites have the application running in a Windows/Linux system running on a physical machine or non-everRun system.

The same software is used to enable and deliver all three configurations. But, the licensing costs for these three configurations vary. There is no difference in the capabilities and functions for these three configurations, aside from the differences outlined above.

How it is set up

A system is set up in the primary site to run the application to be protected. Another system is set up in the DR site to run the application. Either system can be an everRun or non-everRun VM or physical Windows/Linux system. The application is loaded on both sides and the Arcserve engine is loaded in the operating system on both sides. A WAN connection is set up for Arcserve to use for the purposes explained below.

During normal processing, the Arcserve software performs real-time and immediate asynchronous replication of all application data, between the primary site and the DR site. The primary site runs the active application. The DR site does not run the application and is simply being kept up to date in order to be able to take over from the primary site when needed.

When the primary site has a complete failure, the Arcserve software will execute a DR scenario, which brings the DR site up on the network with the identity of the primary site, and restarts applications using up-to-date copies of data.

A separate component, the Control Service module, is installed on a standalone machine (physical or virtual). The Control Service can be replicated for high availability. The fail-over scenario, which drives the fail-over from a primary server to the DR server and back (when needed), is executed from the Control Service.

The Control Service is the central controlling system and users/system managers can use a Manager interface, which is browser based, to connect to the Control Service, and have visibility and control over their entire configuration.

During setup, an Arcserve Scenario Builder is used to set up the following aspects of the Disaster Recovery system environment. This information is encoded in the Site Disaster Fail-Over Scenario:

1. Identifies the files, databases, folders, and disks to be protected. Once the system is started, Arcserve will forward every update made to these identified files, databases, folders, and disks to the DR site, where this information is used to update copies of these files, databases, folders, and disks.
2. Identifies what is used by network clients, to address and connect to the primary server: DNS name, IP address, host name. Arcserve RHA will maintain this information, in order to be able to make the DR system appear like the primary system did on the network before the disaster.
3. All application data is copied over to the DR site. This initial synchronization should be done during off-peak hours.
4. The application can now start. The resulting fail-over scenario is maintained at the Control Service.

The Control Service functions as the single point of control of the Arcserve recovery and fail-over operation, and it contains the data of the existing scenario. The Control Service manages all scenario-related tasks, and the Managers that are connected to it enable you to monitor the Arcserve activities. To overcome the danger of losing the Control Service data, or losing the ability to manage and monitor your scenarios, Arcserve RHA offers you replication (redundancy) and fail-over for the Control Service to assure very high availability of the Control Service data and functionality.

The primary site can have Arcserve installed, without having a DR site up and running, in order to run in “assessment mode”. In this mode, the system will track the amount of data being modified over time, in order to allow the customer to set up a WAN connection to the DR site, with the appropriate bandwidth.

How it works

During normal operation, the following happens:

1. All updates made to application data on the primary site are immediately forwarded to the DR site. The data is sent out asynchronously, meaning that the updates are sent in a network message, but the primary site keeps running full speed, not waiting for the DR site to update its copies of the data. This replication is accomplished by real-time capture of byte-level changes in files on the Master server, using a file-system filter-driver. The captured changes are transmitted asynchronously to the Replica servers using the Engine. The replication process does not interfere with write operations. As long as there is enough bandwidth on the network link, to keep up with the updates, the DR site will be kept fully up to date in real time. Once a packet gets on the network, it has left the primary site and latency is not important. It will get to the DR site and be used to keep the copy of the application data up to date.

2. If a network failure or other disruption occurs, then the two servers are automatically resynchronized when the connection is restored. Updates are buffered on the primary site until such point in time.
3. There is an "assured recovery" capability which can be exercised when desired, for automated, non-disruptive recovery testing and data integrity.
4. Solution software also monitors the application, not just the hardware and Windows/Linux OS, and provides automated or push-button fail-over in case of failures.
5. The communication between the two sites is done using 128 bit SSL encryption.

When disaster recovery is initiated, the following happens:

1. Depending on how things were set up at the start, using the scenario builder, the system will detect that the primary site is lost and recovery needs to start, or it will ask the operator to confirm that disaster recovery needs to be initiated. We strongly recommend the second option, since the DR site is at the other end of a WAN and confirmation that the primary site is indeed down and DR is needed, avoids undesirable fail-over's (e.g. when the WAN connection is lost).
2. Arcserve RHA will make sure that the primary system is relegated to being the DR site, if it happens to come back.
3. The DR scenario will update the DNS, if needed, and update the server's IP address and/or host ID, if needed. The actions taken depend on the application being protected and what it uses (e.g. DNS, IP address, etc.) to have clients and devices on the network find it.
4. The server will then reboot and start the application.
5. The server will now appear on the network like the primary server did—indistinguishable from it, with up-to-date application data.

Technical details

1. Maximum distance between the two servers:
   - There is no maximum distance. The two servers are connected via a WAN.
2. Extra hardware requirements for the Windows systems in the primary and the DR site:
   - None. Two systems (Standard Windows/Linux server or everRun based system) properly configured to run the application, can have Arcserve added without any additional hardware.
3. Software requirements for the Windows systems in the primary and the DR site:
   - Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, or Windows 2012/2012 R2
4. Hardware/OS requirements for Control Service system:
   - Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, or Windows 2012/2012 R2.
5. Minimum bandwidth for the WAN connections between the two servers:
   - Adequate to carry the file/database updates sent over from the primary to the DR site. Users can do back-of-the-envelope calculations, based upon their knowledge of the application, or run the assessment mode explained above, to determine the bandwidth needed.
6. Maximum round-trip latency over the A-links between the two servers:
   - Latency is not an issue, as long as a reliable WAN connection exists.
7. Management:
   - The management utility, called the Management Center, is available through a browser to present the status of the system to the user. The browser connects to the Control Service.
   - The system can be set up to execute tasks for every significant event that occurs:
     i. Send a message with a description of the event.
     ii. Execute a user specified script.

To learn more about worry-free computing, visit **www.stratus.com.**