Stratus Technologies For an **Always-On** World

Use Cases for everRun MX and CA ARCserve RHA

Introduction

Stratus Technologies is pleased to offer CA ARCserve RHA, a disaster recovery solution, as an add-on to everRun MX®, Stratus's best-in-class software solution, to keep your systems and applications always-on. Stratus utilizes CA ARCserve for disaster recovery and data replication in three specific use cases, as described in this document, when disaster recovery and data replication is required. For use of CA ARCserve outside an everRun Disaster Recovery (DR) solution, please refer to CA's website, http://www.arcserve.com/us/backup.aspx.

Disaster Recovery General Application

Stratus' everRun software and ARCserve RHA 16.5 provide data replication and failover to applications running on Windows from a primary source Windows machine to a target Windows machine. The target can be a virtual machine, protected virtual machine or a physical machine. As data changes in the primary source location, the changes are also sent to the remote target location. By using a fault tolerant configuration in the primary source site, all platform failures are managed and there is no need to fail over to the DR site unless the primary source location fails due to circumstances such as a widespread power failure, water damage or other site disasters. If that should occur, the customers are redirected to the DR target site for continued connectivity. Replication can also occur in the opposite direction once the primary source location is backed up.

CA ARCserve Core Features

Continuous LAN/WAN Replication

- Continuous and scheduled LAN and WAN replication for data protection
- Built-in WAN optimization technologies to help overcome bandwidth challenges
- For Windows, Linux and UNIX on physical and virtual servers
- Scheduled/periodic replication available for Windows servers

Real-time Server and Application Monitoring with Automatic and Push-button Failover

- Gets you up and running quickly after a disaster
- Includes push-button failback after server repair or replacement
- For Windows, Linux and UNIX

CA ARCserve® Assured Recovery™

- Automated, non-disruptive recovery testing in Windows environments

Data Rewind

- Continuous data protection (CDP) that complements any periodic backup solution

Virtual Server Protection

- Protects both physical and virtual servers with a single solution
- For VMware ESX and vSphere, Microsoft Hyper-V and Citrix XenServer

Custom Application Protection

- Wizard-based tool creates replication and failover scenarios
- For Windows-based third-party and custom applications

Multi-stream Replication

- Enables the use of multiple data streams to increase network replication throughput over high-latency WANs

Secure Communication

- 128 bit SSL encryption across the network without the need for a VPN or IPSEC tunnel, reducing cost and complexity

Network Address Translation (NAT) Support

- Enables remote replication and failover in NAT environment without sacrificing security

Windows Server 2012 Support

- Including replication and failover of NTFS dedupe, ReFS, Hyper-V 3.0, and Storage Spaces

4K Sector Drive Support

- Greater flexibility in selecting storage devices

CA ARCserve Key Benefits for Customers

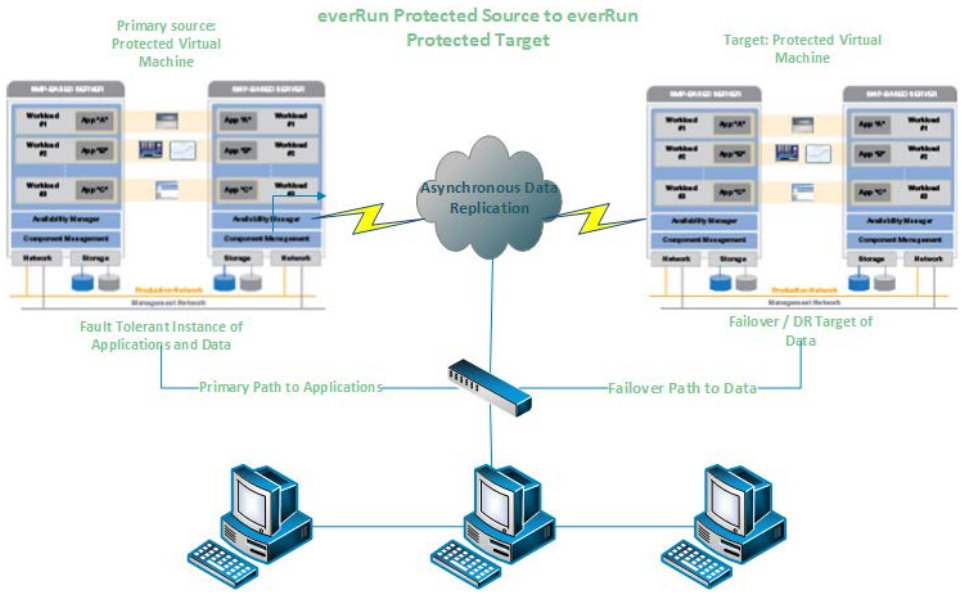
- Minimizes the risk of business downtime during planned and unplanned outages that can result in lost revenue from Sales, Service, Support and worker productivity levels
- Reduces recovery time after data loss or damage
- A key component to any disaster recovery strategy

For additional information visit www.arcserve.com/partnerportal or contact your CA representative.

The illustrations below show the three types of everRun and ARCserve installations.

Use Case 1: Replicating single PVM to PVM and Replicating multiple PVM's to multiple PVM's

A single or multiple primary source virtual machine/s running everRun MX with data replicating asynchronously to a single or multiple target virtual machine/s running everRun MX.



Replicating PVM to PVM

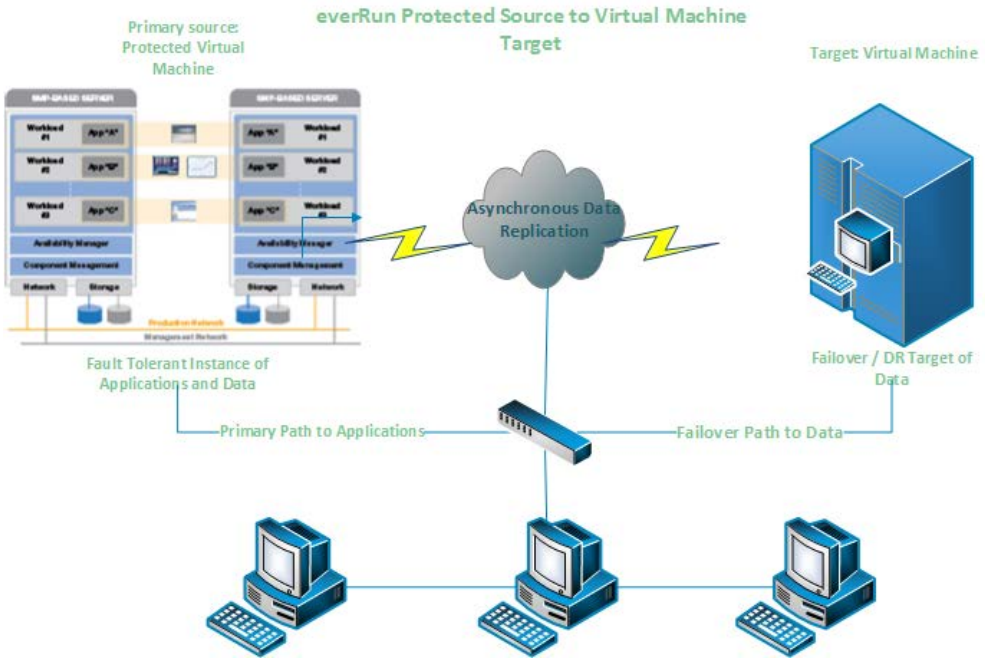
- The application's data sets are replicated to the storage of the target PVM
- Uses DNS failover to redirect network traffic to target PVM
- When the primary site fails, client traffic is redirected to the target PVM in the Secondary site via DNS A-record modification
- The target PVM starts production applications and continues operation using replicated data

Replicating multiple PVMs to multiple PVMs

- Each PVM uses a separate scenario to replicate and restart on respective target PVM
- All scenarios are grouped together so when one PVM fails over, they all do (all PVMs run from the same site)
- All PVMs start applications and services to continue operation using replicated data
- Client network traffic is redirected to each target PVM via DNS failover

Use Case 2: Replicating PVMs to VMs not running everRun MX

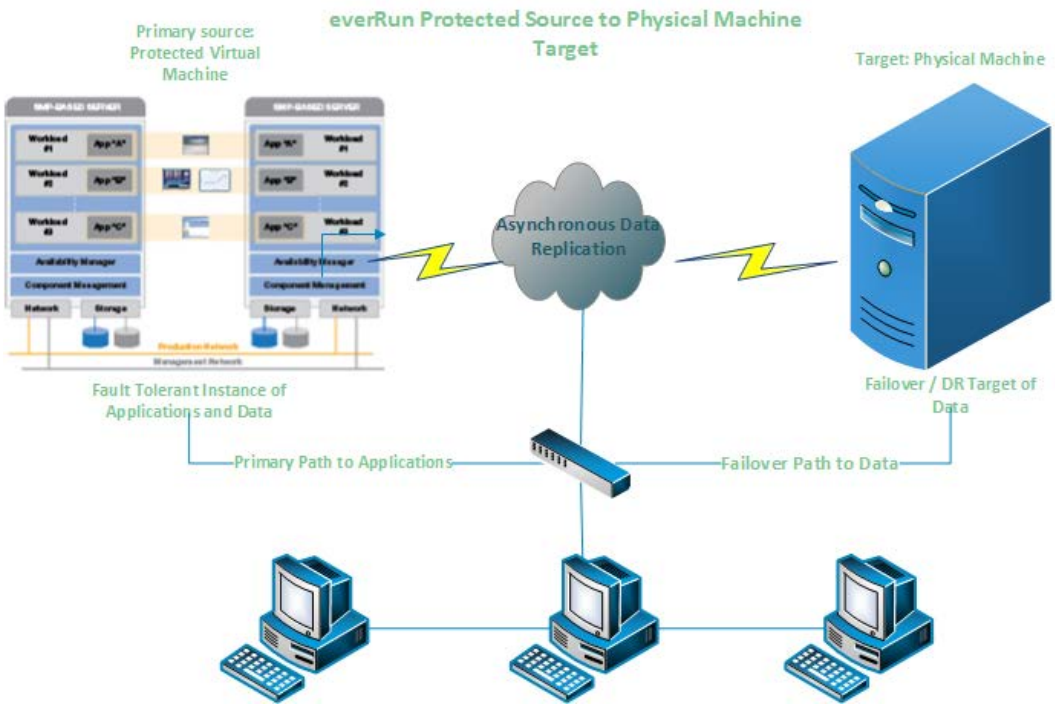
A single or multiple primary source virtual machine(s) running everRun MX with data replicating asynchronously to a single or multiple target virtual machine(s) that's not running everRun MX.



- Each application's dataset is replicated to a specific VM's dataset
- Using MoveIP feature to have Target VM assume Primary Source's IP address on recovery (note that this requires PVMs and VMs to be on the same subnet)
- When Primary site fails, traffic is redirected to VMs in Secondary site. Each VM uses same IP address as its corresponding master PVM
- Applications in the target VM's, attach to replicated data and continue operation

Use Case 3: Replicating a VM to a physical machine

A virtual machine running everRun MX with data replicating asynchronously to a physical machine.



Replicating PVMs to physical servers

- Each primary source PVM must have a separate target physical server
- Data is replicated to storage of each physical server
- When the primary site fails, each physical server will take over application operation of the corresponding master PVM using the replicated data