datagardens

# SAFEHAVEN® 3.1 DATA SHEET

Disaster Recovery in the Cloud

## BUSINESS NEEED

Traditional disaster recovery systems require a dedicated recovery data center. This "stand-by" data center is expensive to provision and difficult to manage. So many companies are turning to the cloud for disaster recovery protection. DataGardens SafeHaven® is an ideal solution.

## THE DATAGARDENS SOLUTION

*Flexible, comprehensive, & scalable . . .*

SafeHaven provides the most flexible, comprehensive, and scalable IT disaster recovery on the market today. With SafeHaven, any organization can spin up a replica of its production data center in the cloud in just a few minutes and with little or no data loss. SafeHaven supports:

- Full data center disaster recovery orchestration,
- Full run book automation for multi-tiered applications,
- Protection for both physical and virtual IT systems,
- Multiple hypervisors and cloud platforms, and
- Private, public, community, and hybrid cloud deployments.

*Easy to configure & manage …*

SafeHaven includes a simple-to-use interface for self-managed disaster recovery. Administrators can perform point-and-click recovery operations upon individual virtual machines, groups of servers and data drives, or entire data centers. Recovery operations include:

- Lossless migration,
- Failover,
- Failback,
- Continuous Data Protection (CDP), and
- Automatic detection and reporting of data center outages.

*Monitor, test,& report …*

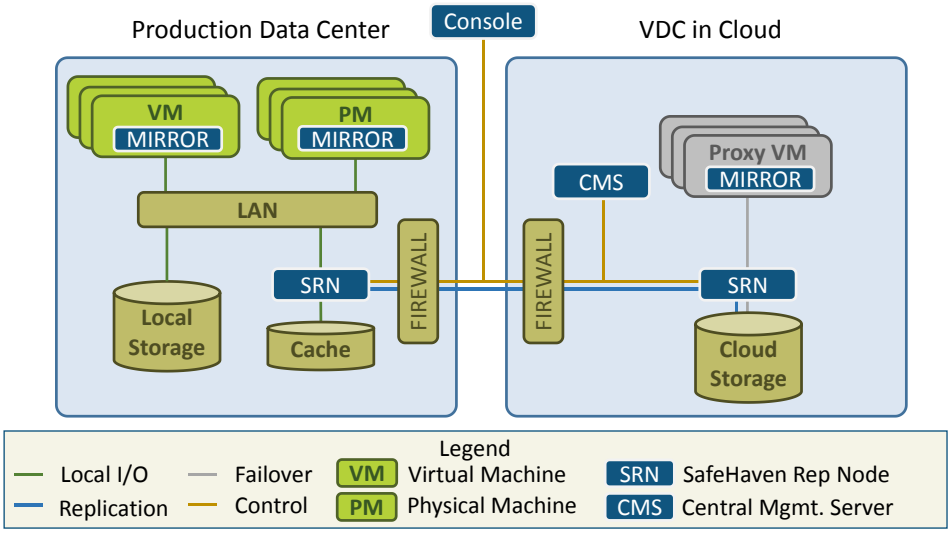
Almost as important as having a disaster recovery system is knowing that the system is healthy and will provide expected levels of protection when disasters actually occur. SafeHaven offers:

- **Continuous monitoring:** SafeHaven continuously monitors and displays through its console the amount of data that remains to synchronize between production and recovery sites
- **Non-disruptive testing:** As a point-and-click operation, administrators can test their group and data center recovery plans without affecting their production operations. SafeHaven spins up fully functional clones of production systems in the cloud according to a prescribed recovery plan. Administrators can validate recovery right up to the application level while receiving a full report on achieved RPOs and RTOs.
- **Reporting:** SafeHaven provides automatic weekly status reports on the health of the disaster protection environment. If, for instance, bandwidth to the cloud is inadequate and the protected company is at risk of not meeting its target RPO, SafeHaven flags the problem.

## ARCHITECTURE

While SafeHaven can protect thousands of companies within one or more clouds, each protected company is provisioned with a distinct, dedicated SafeHaven "Cluster". With this SafeHaven Cluster, a company can protect up to 64 data centers. Some of these may be in-house data centers while others may be virtual data centers that operate on third-party IaaS clouds. The figure below shows a simple SafeHaven Cluster which includes just two data centers: one private and the other in a third-party cloud.

*The SafeHaven architecture provides comprehensive enterprise-class disaster protection . . .*




**Architecture for a SafeHaven Cluster with two data centers**

*Each data center includes at least one SRN*

Each data center protected by SafeHaven must include at least one "SafeHaven Replication Node" (SRN). The SRN is a lightweight virtual appliance responsible for:

- LUN-level asynchronous replication,
- Maintaining scrolling logs of up to 2048 checkpoints for CDP,
- Detecting failure conditions associated with disasters and reporting them to select administrators, and
- Executing commands to perform controlled shut-down and bring-up of individual servers, groups of IT systems, or entire data centers.

Depending on configuration and I/O load, each SRN can protect between ten and twenty servers.

An agent running within each protected server synchronously mirrors writes so that they are transmitted not only to the primary data store, but also to a local SRN. The local SRN can maintain local replica disk images of protected servers and associated data drives along with CDP checkpoints. Alternately, the local SRN can be configured to merely buffer updates in a local disk cache and transmit them asynchronously to one or more SRNs in remote data centers. The recipient SRNs maintain persistent disk images of protected servers and associated data drives along with a scrolling log of checkpoints for CDP.

*A single CMS manages the entire Cluster*

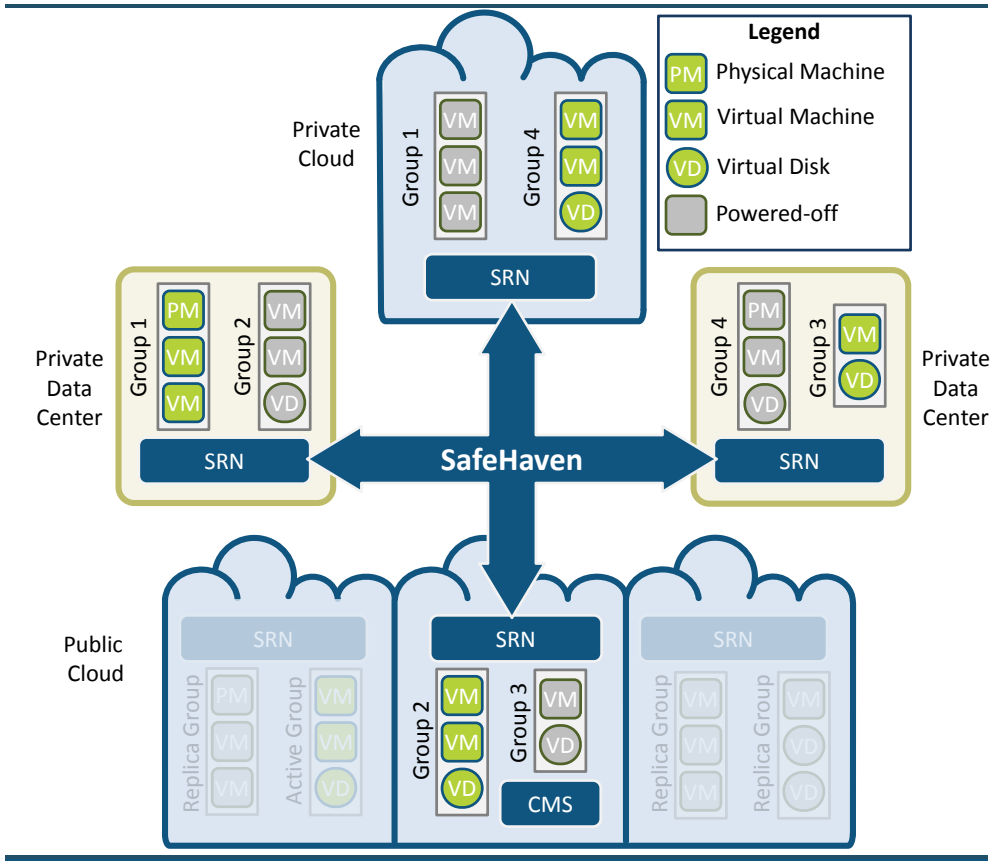
Proxy servers in the recovery sites are kept powered-off under normal conditions. When a disaster condition is declared, the proxy servers boot from the replica images that have been maintained by SRNs.

Administrators issue commands through the SafeHaven Console, a rich JAVA client that runs on one or more administrative desktop computer. The commands are transmitted to another virtual appliance, the SafeHven Central Management Server (CMS), which is responsible for forwarding them to the appropriate SRNs in the appropriate data centers and reporting state information back to the SafeHaven Console.

## DEPLOYING SAFEHAVEN PROTECTION

*SafeHaven supports private, public, community, and hybrid cloud deployments . . .*

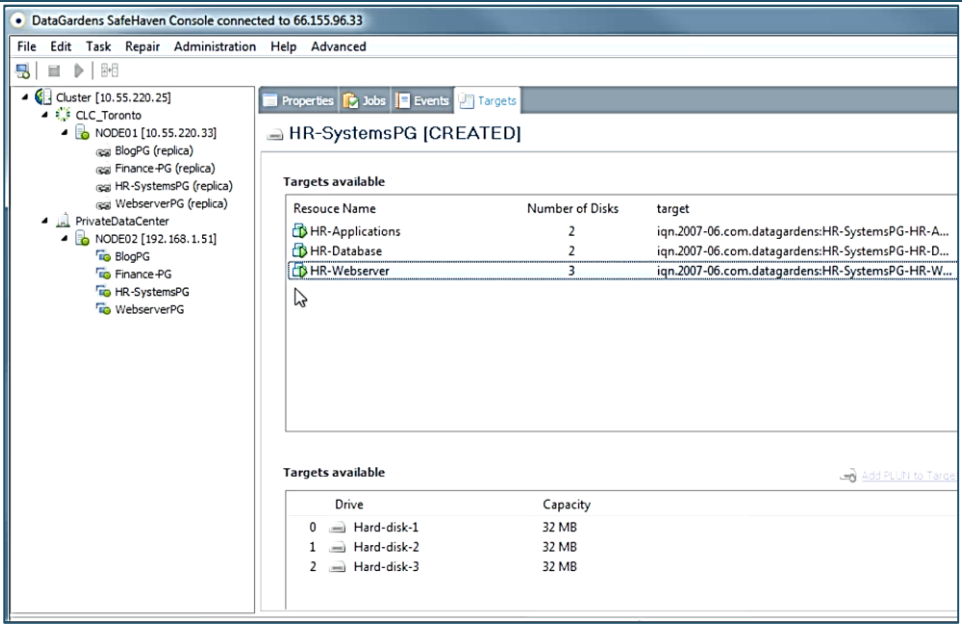
The administrator deploys a new SafeHaven Cluster using an automated installer. The installer downloads an SRN virtual appliance in production and recovery data centers along with a CMS virtual appliance to control the Cluster. Data centers within the cluster may be private data centers managed through VMware vCenter Server or third-party clouds managed through vCloud Director, Nebula OpenStack, or other SafeHaven supported cloud platforms (see figure below).




**SafeHaven® Console**

The administrator then installs the SafeHaven Console on any client desktop. Finally, the administrator uses a wizard launched through the SafeHaven Console to onboard servers and data drives for disaster recovery protection.

*Right-click on the protected system & select from the drop-down menu*




**SafeHaven® Console**

To perform a recovery operation the administrator simply right-clicks on a VM, a group, or a data center within the SafeHaven Console and selects the desired operation from the drop-down menu.

## SYSTEM REQUIREMENTS

- CMS: 1 virtual CPU, 2 GB RAM, 5 GB disk
- SRN: 2 virtual CPU, 4 GB RAM, 5 GB disk
- VMware vSphere 4.0+ for private data centers
- VMWare vCloud Director 1.5+, Nebula OpenStack
- Storage in recovery site to protect disk images for production servers
- Additional storage for CDP checkpoints.

## SALES ENQUIRIES: sales@datagardens.com