



RecoverGuard™

Ensuring business continuity and data protection with automated HA/DR testing and monitoring

Configuration Drift: The Greatest Threat to Business Continuity

Configuration drift, an inevitable condition in today's constantly changing data centers, occurs when production or primary infrastructure configurations "drift" or become different in some way from the recovery or secondary infrastructure. This creates serious data protection gaps which can impact your Recovery Point Objectives (RPO) and host configuration gaps which impact your Recovery Time Objectives (RTO).

Manual HA/DR Testing is Not the Solution

Periodic high availability (HA)/disaster recovery (DR) testing requires considerable advance planning, along with a sizable investment in time and manpower. But because it can only be performed several times per year, it still leaves your organization vulnerable to configuration errors over 95% of the time.

RecoverGuard™ - Automatic HA/DR Vulnerability Detection

RecoverGuard software automatically detects all HA/DR risks immediately, as they occur, so you can resolve them before they impact your business.

This innovative software Integrates non-disruptively into your IT

infrastructure and operates in read-only mode. It automatically scans storage, databases, servers, virtual machines, cluster and replication configurations for vulnerabilities such as unprotected databases, erroneous cluster settings, noncompliant replication configurations, data that cannot be recovered to a valid consistency point, and much more. When gaps are uncovered, the software issues an alert which includes detailed descriptions and remediation suggestions.

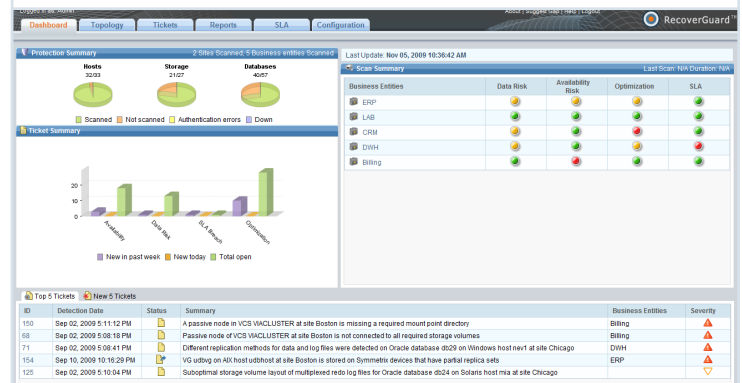
RecoverGuard Offers:

- Automatic detection of availability and data protection vulnerabilities using a knowledgebase of over 3,500 gap signatures
- Analysis and presentation of dependencies between IT assets and business services
- Identification of infrastructure optimization opportunities and best practices recommendations
- Agent-less, non-intrusive data collection using standard communication protocols (SSH, WMI, Storage API, JDBC, Sudo). Zero impact on scanned environment
- Integration with leading configuration management database (CMDB), ticket management and enterprise console products

Key Benefits

- Dramatically reduce business downtime and data loss by automatically detecting HA/DR readiness and data protection vulnerabilities
- Verification and measurement of disaster recovery SLAs (RPO, retention, and more)
- Reduce HA/DR pre-test effort and time, and improve test success rates
- Ensure business continuity by validating that your production and replication/cluster environments are always in sync
- Continuously audit and improve cluster, DR and data protection practices
- Effectively manage capacity of disaster recovery and high availability
- Maximize your cluster, replication and DR investments and identify wasted storage, bandwidth and server resources

RecoverGuard Dashboard



The RecoverGuard dashboard provides a wealth of information about HA/DR risks and highlights optimization opportunities throughout your IT infrastructure.

RecoverGuard delivers a robust feature set and cross-vendor/cross-domain/cross-platform support to ensure business operations can quickly resume in the event of disaster or unexpected downtime.

Business Continuity Vulnerability Detection

- Gap Detection Engine automatically uncovers data protection, availability or disaster recovery risks that exist between the production and DR environments or production and HA servers.
- Community-driven Gap Knowledgebase contains thousands of configuration gaps and is constantly updated. See examples of detected gaps at www.continuitysoftware.com/gaps
- Real-time verification of IT changes enhances HA/DR tests and configuration audits.

Comprehensive SLA Management

- RPO Measurement & Analysis offers a high-level, aggregated, graphical infrastructure overview to identify potential RPO problems. You can also drill down by business unit or host component.
- Policy-driven SLA Management monitors established SLA policies by host, business service or business unit. Notifications are issued when a violation is detected.
- Disaster recovery and high availability capacity tracking helps ensure business continuity.

HA/DR System Configuration Validation

Automatically identify significant differences between production, HA and DR servers to eliminate cluster

gaps and ensure cluster node hardware and software parameters are aligned so there is no single point of failure.

Live Data Center Documentation

Gain insight with an interactive, graphical topology of all data center entities, dependencies and relationships.

Comprehensive Reporting

Get the data you need, on-demand, to assess and analyze your current ability to maintain business continuity.

Data Center Changes Journaling & Search

Ensure that the entire data center team stays informed of all changes.

Risk Assessment Dashboard

Provide non-IT executives with insight into the company's readiness or risk levels.

Automatic Alerting & Management

Direct instant notification of a potential problem to the proper person in your organization.

Identification of Optimization Opportunities

Discover unutilized storage space or other opportunities to reduce costs and improve overall system performance.

Integration with System Management Consoles

Consolidate system management across the enterprise. Integrates with IBM Tivoli, HP OpenView and other leading System Management products.



TECHNICAL REQUIREMENTS

- Dual Intel XEON
- Minimum 4 GB RAM
- 100 GB disk space

SUPPORTED ENVIRONMENTS

Storage:

- EMC Symmetrix
- EMC CLARiiON
- Hitachi AMS, USP
- IBM DS
- NetApp filers
- HP XP

Operating Systems:

- Windows 200X+
- HP-UX 10/11+
- Sun Solaris 9/10+
- Linux RHAS 2.1, SUSE 8+
- IBM AIX 5L+

Databases:

All major databases

Clusters & Virtualization:

All major cluster and virtualization environments

Copyright ©2009, Continuity Software, Inc. All rights reserved. RecoverGuard is a trademark of Continuity Software, Inc.

Data Protection

Replication

- Data completeness
- Data consistency
- Identify replication process failure

Data Protection SLA

- RPO management
- Data retention
- Insure protection of critical assets

SAN Best Practices

- I/O multi-pathing best practices
- Data tampering prevention

Optimization

- Identify reclaimable storage
- Optimize WAN
- Optimize I/O configuration
- SAN best practices

Database Best Practices

- Data corruption
- Performance best practices
- Verify DB vendor recommendations
- Verify Joint DB / storage vendor recommendations

Availability Management

DR Data Access

- Correct access to shared storage (HA) and replicas (DR)
- Redundancy and performance

Host Configuration

- OS version / SPs
- Installed products / versions
- Kernel parameters
- Network services

Root Cause Analysis

- Datacenter change analysis

Clustering Best Practices

- Insure identical / compatible configuration across cluster nodes
- Vendor best practices
- Local / geo clustering

Redundancy

- RAID level
- SAN Multi-pathing
- Network
- Physical (NIC / teaming)
- Logical (DNS, LDAP, AD)
- Database file configuration