RecoverGuard software will ensure DR readiness by automatically detecting hidden recoverability risks in your IT environment.

And we can prove it.

Recently, a leading US electric company conducted an assessment to test the effectiveness of Continuity Software's RecoverGuard. The software ran for 48 hours, automatically testing and monitoring the critical business services hosted in the firm's primary and DR data centers.

What RecoverGuard detected surprised the utility's IT staff and senior managers. But it didn't surprise us.

Results Inside. →

Customer Profile

This electric company serves one of the most demanding power grids in the United States, providing millions of residential and business customers with a reliable and efficient source of electrical power.

Situation Analysis

The utility's IT organization was concerned about managing the volume of changes occurring within its datacenter and the complex provisioning processes being implemented by cross functional teams within IT. The firm hoped an automated discovery and monitoring tool would help minimize potential risks by proactively uncovering and resolving any configuration irregularities before operations could be affected. The utility engaged Continuity Software to perform a Pilot Scan of its environment utilizing Continuity's RecoverGuard™ software. RecoverGuard is an innovative solution that automatically detects hidden data configuration errors which could impact recoverability.

Results

During the Pilot Scan, RecoverGuard analyzed the configuration status and Disaster Recovery (DR) readiness of the critical business services hosted in the electric company's primary and DR data centers. The software identified a number of previously undetected gaps that had the potential to result in data loss, extended downtime and performance degradation.

The risks were created by the constant configuration changes required in this dynamic environment. In any complex infrastructure, it is impossible for an IT organization to eliminate gaps caused by human error, and impossible to perform a full DR test after each change is made within the datacenter. Without RecoverGuard, these gaps would have remained undetected, exposing the utility to serious risk.

This firm has since implemented RecoverGuard in its datacenters and uses the software to automatically test and monitor its environment on a regular basis for configuration inconsistencies.

RecoverGuard discovered **36 hidden configuration gaps** for this leading electric company, some of which posed serious risks to the firm's ability to recover in the event of a disaster. These errors had either gone undetected in the last full DR test, or had occurred after the test was completed

The following pages are excerpted from the firm's full report to illustrate the detail and insight that RecoverGuard can provide.

Note: All identifiable customer data has been removed.

Identified Risks to Business Services

Figure 1 outlines the Threat Landscape identified by RecoverGuard, and displays business services and their threat level weighted in terms of technical severity and business impact. Technical Severity is ranked in order of potential impact to Recovery Point Objectives, Recovery Time Objectives, and best practices. Business Impact is ranked in order of importance to the business service.

- Storage Utility: Subject to data loss. Critical business data is not being replicated in a consistent manner.
- Human Resources System: Subject to possible data loss & prolonged downtime in a disaster event.
- Payroll: Subject to extended recovery time.

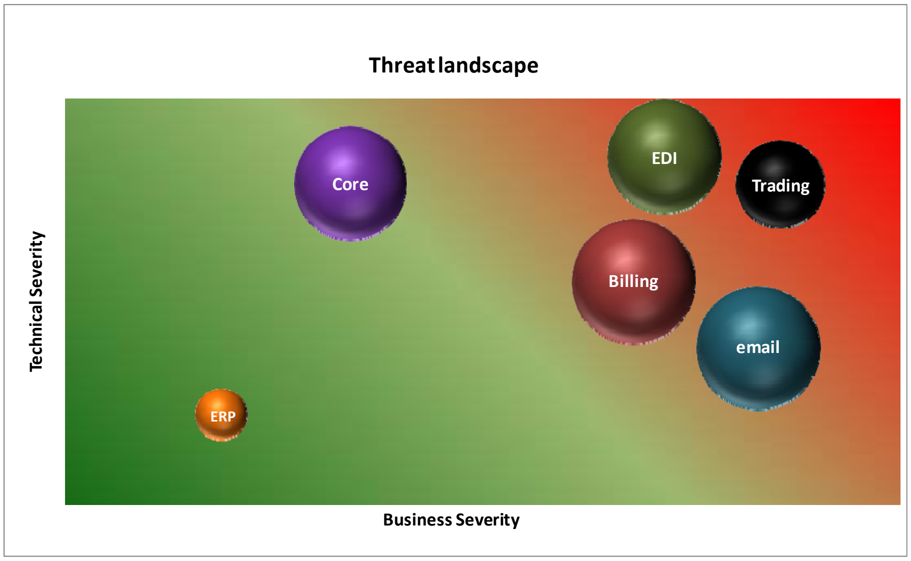


Figure 1

RecoverGuard ranks each identified gap from Informational to Critical. Figure 2 displays the percentage of all the protection gaps discovered in the firm's analysis, categorized by severity.

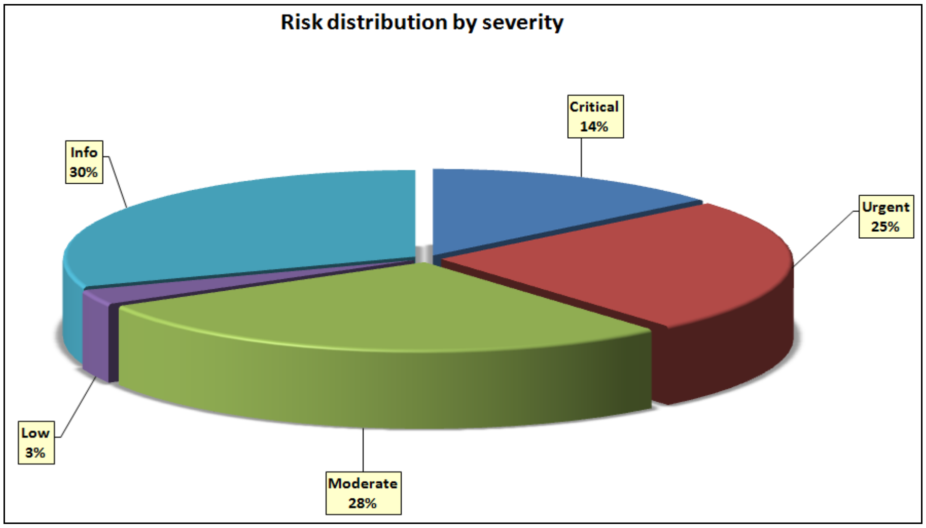


Figure 2

DR Readiness Gaps Identified

RecoverGuard isolated **36 separate protection gaps**, which were divided into 12 threat categories with associated technical impact and technical priority. The firm was able to evaluate the business impact of each gap and correct those that presented a business risk. The following table provides the technical priority risk ranking.

Category	Technical Impact	Technical Priority	Ticket Count
Mixture of SAN and DAS with replication	Data loss in a DR event Bad practice	1	2
Incomplete Replication	Data loss in a DR event	1	4
Replica Symmetrix Device Group Inconsistency	Data loss in a DR event	2	1
Replicas not accessed by DR host	Extended recovery time	2	1
Suspended remote DR replicas	Data loss	3	2
Un-replicated data on replicated hosts	Data loss	3	5
DR host missing mounts/shares	Extended recovery time	4	7
LV with single path to storage	Downtime Performance	4	1
A cluster member missing devices	Downtime	4	1
Storage configuration issues	Data loss upon storage allocation	5	1
RAID level inconsistency	Saving opportunity	6	1
Multiple databases on the same storage volumes	Performance DBMS best practice	7	10

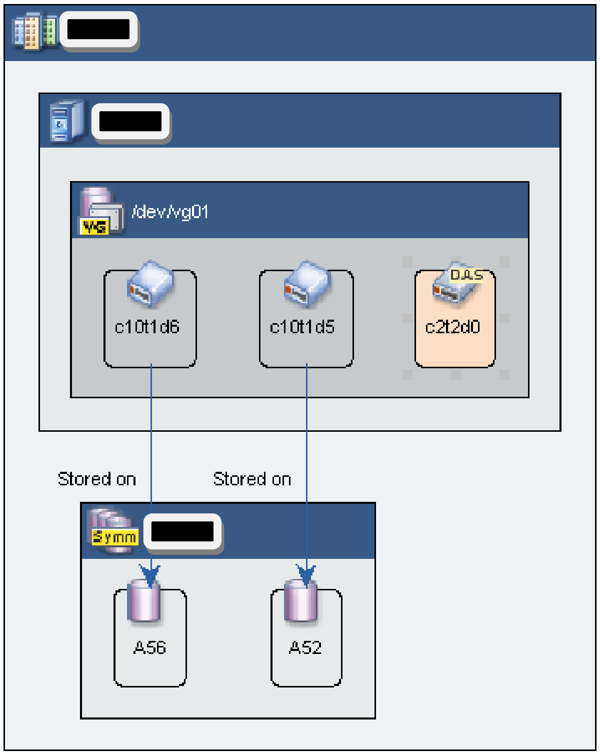
Gap Signature Details

RecoverGuard automatically produces a detailed ticket for every vulnerability gap it detects. These tickets can be used on a daily basis to resolve issues before the business is impacted. The following pages contain three of the tickets produced for the firm during its RecoverGuard test.

Storage Volume Type Inconsistency

RecoverGuard will automatically generate a ticket when a Volume group is detected that is composed of several storage devices of different type, such as a DMX box and direct attached storage, as shown here. In the event of a disaster, if the direct attached storage is corrupted, there is no way to restore the data. In addition, mixed storage types usually indicate performance impact, and lower data protection. The system overall performance would be the slowest of the types involved. This is also true for mean time between failure (MTF) and data protection.

Ticket Topology



Ticket Summary

Storage volumes type inconsistency was detected for volume group (VG) /dev/vg01 on host ****** at site ******.

Technical Impact

Volume group /dev/vg01 on host ****** is stored on storage devices. Those storage devices are of mixed storage types (DAS and Symmetrix). Since the DAS portion is not replicated, the copy at the DR site is incomplete, leading to the entire VG or database element being unusable and to data loss. In addition, depending on the drive technology, DAS devices will be inherently far less reliable and slower than SAN devices. The source data itself is vulnerable to corruption and low performance.

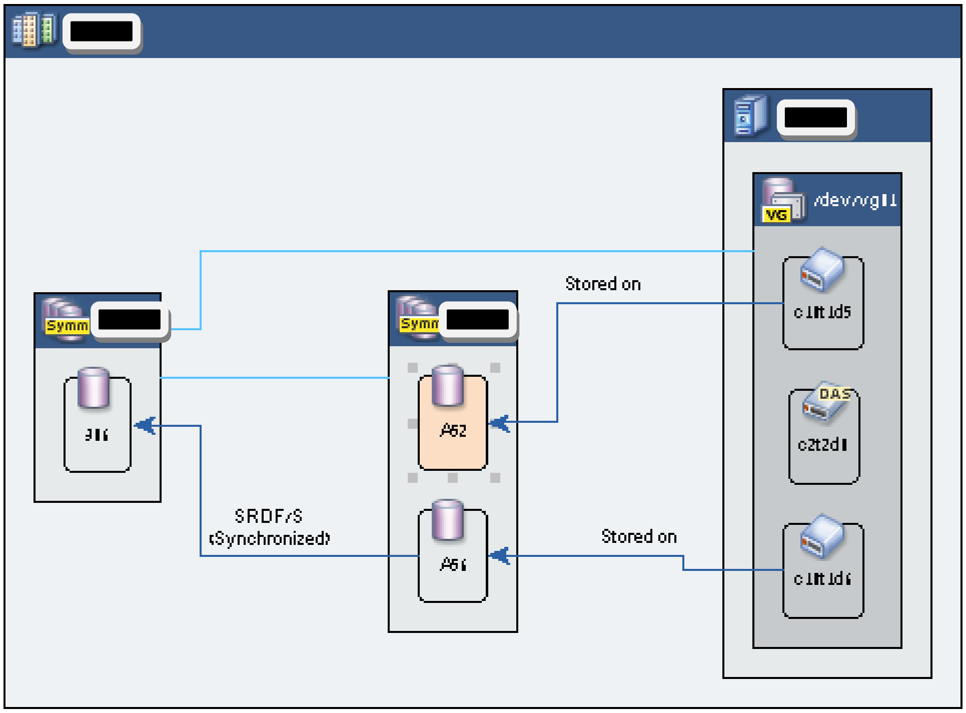
Business Impact

This configuration will lead to data loss and DR failure in a failover event.

Replica [Tree Structure] Inconsistency Ticket

RecoverGuard will generate a ticket when the analysis encounters a database or a file system stored on SAN volumes which does not have the same number of replicas. In case of a disaster event this can lead to data loss.

Ticket Topology



Ticket Summary

Replication tree structure inconsistency was detected on volume group (VG) /dev/vg01 on host ****** at site ******.

Technical Impact

Two gap signatures are detected for this ticket. The first is the replication tree structure gap. All the data storage elements for a volume group must have the same replication structure, meaning each storage device must all be replicated if one or more are. If the volume group is partially replicated it would render the entire volume group useless in the event of a disaster. The other gap is a Mixed Storage Type signature. The volume group contains a mix of both SAN and DAS data storing entities. A volume group should contain the same type of storage devices, whether SAN or DAS, RAID type, or from the same array, unless multi-array consistency technology is used. A variety of adverse affects can occur including data loss if a volume group contains different storage devices.

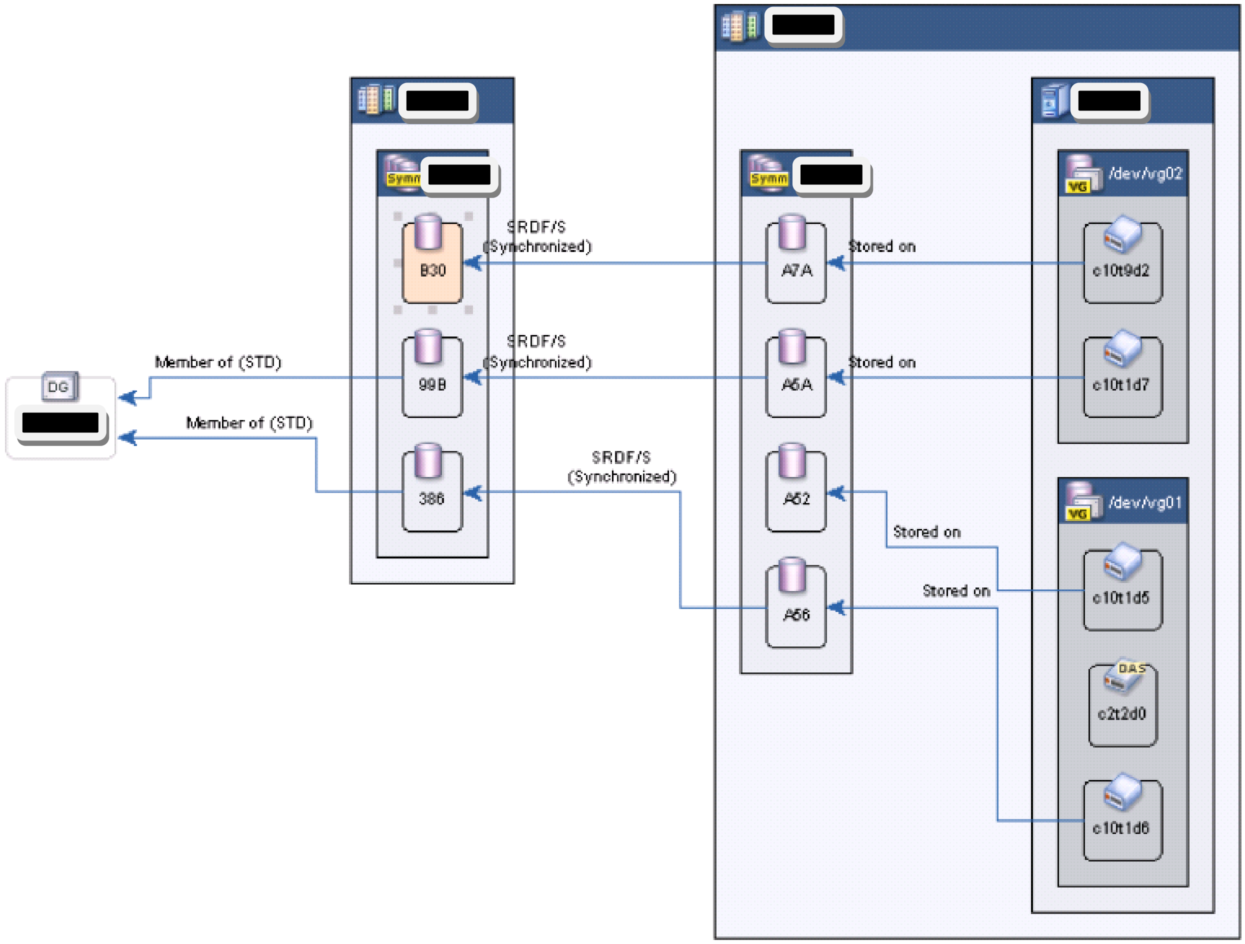
Business Impact

The SRDF replica set on the remote site is incomplete. In the event of a disaster, data will be lost.

Device Group Inconsistency Ticket

RecoverGuard will generate a ticket when a database, volume group or file system are stored on SAN volumes that are not members of the same device groups or consistency groups. In case of a disaster, data might be in an inconsistent state, making it unrecoverable.

Ticket Topology



Ticket Summary

Symmetrix Device Group inconsistency detected for replicas of volume group (VG) /dev/vg02 on host *** at site *****.

Technical Impact

The volume group /dev/vg02 on host ****** is stored on Symmetrix devices. These Symmetrix devices have remote SRDF replicas. Some of the R2 replicas are members of Symmetrix DG ******-data while others are not When operations on the Symmetrix DG are performed, only some of the devices in the DG will be affected.

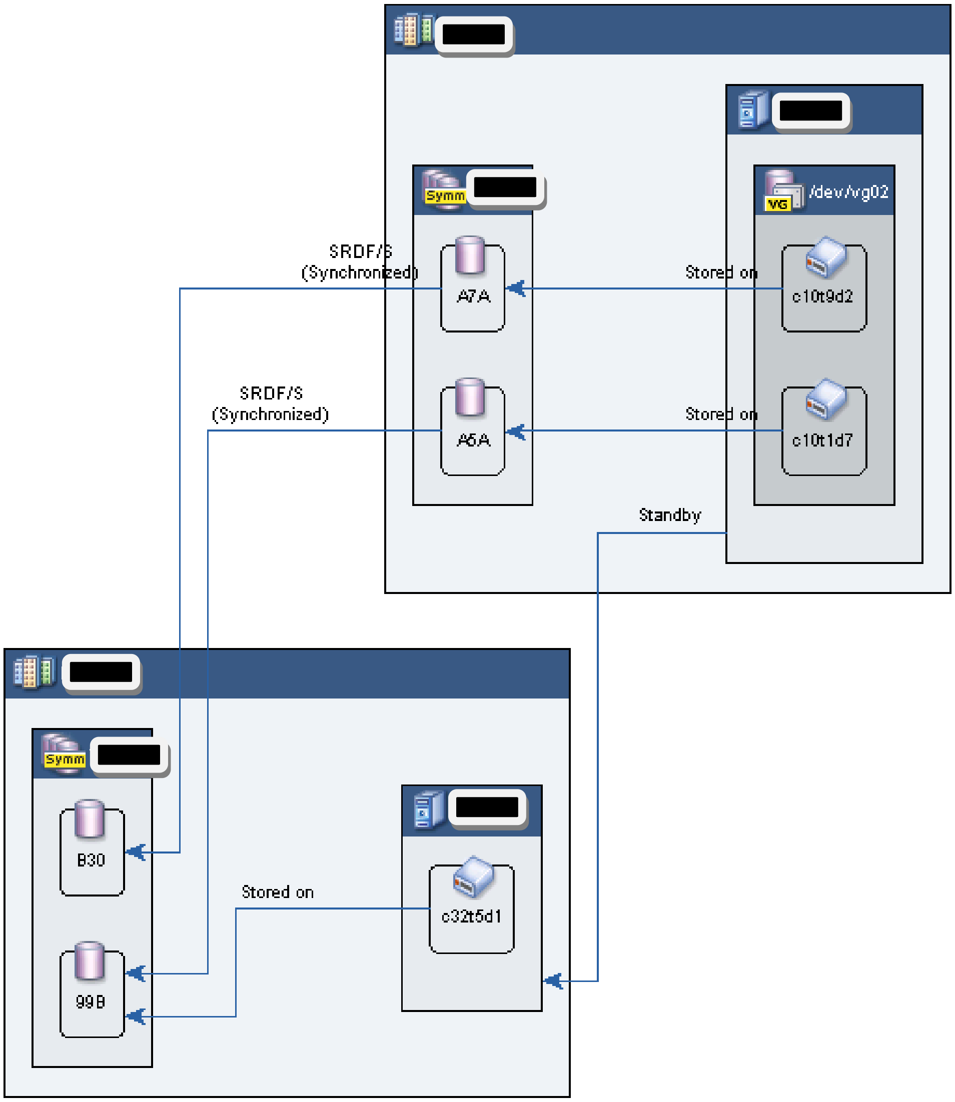
Business Impact

In the event of a disaster, data will be corrupted.

Visible and Invisible Storage Volumes

RecoverGuard will generate a ticket when a host is detected to access / map only a part of the data it needs to access compared to the originating host. In the event of a disaster event, this would impact availability and RTO. In order for the host to function and access all the data of the production environment, the IT team would need to identify the problem and then make the proper amendments.

Ticket Topology



Ticket Summary

Inconsistent access to replicas of volume group (VG) /dev/vg02 on host ****** by host ****** was detected at site ******.

Technical Impact

The volume group /dev/vg02 on host ****** is stored on Symmetrix devices. These Symmetrix devices have remote SRDF replicas. Only one of the SRDF replicas is mapped to host ******.

Business Impact

Data will not be available on the DR host upon disaster. The storage administrator will need to locate the missing devices, map them to the host and configure them in the target volume group. Extended downtime is expected while the missing device is identified, which can be hidden among hundreds of other unmapped replicas. If the missing devices are incorrectly identified, in case of incomplete or missing documentation, data will be lost.

Would you like to have this level of insight into your own environment?

You can take a closer look with our
RecoverGuard Pilot Scan.
Let RecoverGuard monitor
your environment for 48 hours, and
find the hidden risks in your infrastructure.

www.continuitysoftware.com/proof

or email closerlook@continuitysoftware.com

CONTINUITY
SOFTWARE