Top 10 downtime and data-loss risks

Quick Reference Guide

for Private Cloud
Disaster Recovery and High Availability Protection

Table of contents

Enterprises routinely build Disaster Recovery and High Availability measures into their private cloud environments. So why do downtime and data-loss risks still exist?

The reality is that even the most robust Disaster Recovery and High Availability plans are only as good as your ability to test them. IT environments are dynamic in nature. Overtime, changes made to the protected environment may not be identically reflected the recovery environment.

Since manually testing all the risks in an ongoing fashion is virtually impossible, such discrepancies and other issues covered in the examples below often go undetected, leading to an astounding failure rate of disaster recovery environments analyzed using Continuity Software AvailabilityGuard.

How do we know what these risks are?

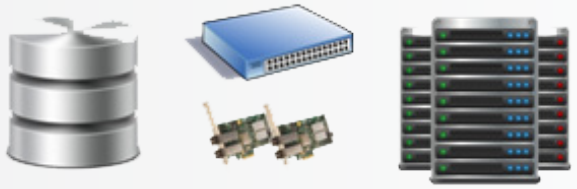
Over the past seven years, we have been working with enterprise customers to ensure their Disaster Recovery and High Availability plans are working as designed. With the help of our customers, we have assembled a community-driven database containing over 4,000 (and growing) known issues that pose downtime and data-loss risks. While we cannot share them all with you, we will review here ten of the top issues in the private cloud environment.

Where do we find these risks?

Risks can be found in each of the three layers of the private cloud environment:

i. The Virtual Infrastructure Layer

- Storage devices
- Virtualization servers
- The networks connecting the two
- Virtualization management



ii. The Virtual Machine Layer

- Storage allocation
- Server image
- High availability provisioning

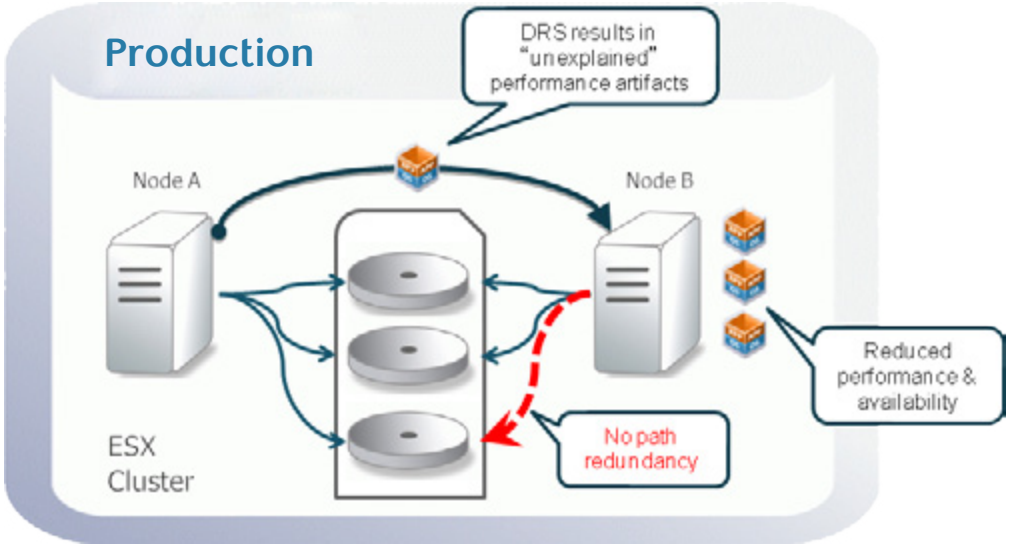
iii. The Disaster Recovery Layer

- Replication settings
- Storage mapping
- Recovery management

1. INFRASTRUCTURE LAYER | STORAGE

The typical ESX cluster spans several nodes. The problem shown in this example is that one of the nodes has no SAN path redundancy like we would expect from all nodes serving the cluster. What it means is that all virtual machines currently running on this particular node have a single point of failure and may suffer reduced performance.

This could also cause certain virtual machines to exhibit intermittent performance degradation as they move to the under-provisioned servers.

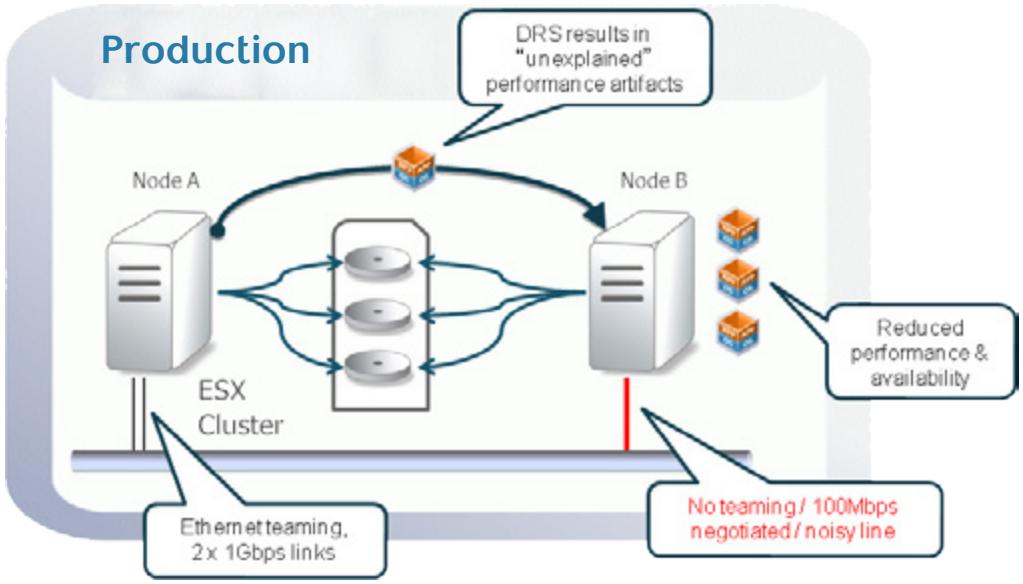


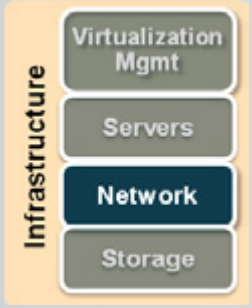
Additional storage-related risks include

- LUN re-signature
- Unmapped RDM
- Different multi-path configurations
- ...and dozens of other risks

2. INFRASTRUCTURE LAYER | NETWORK

What we see here is that one of the cluster nodes has only a single network connection to the shared or public network. The result is a single-point-of-failure and most likely poor performance for all the machines that are currently running on top of that particular server. Like in the previous example, the fact that virtual machines continually change locations makes it very difficult to pinpoint such performance fluctuation.





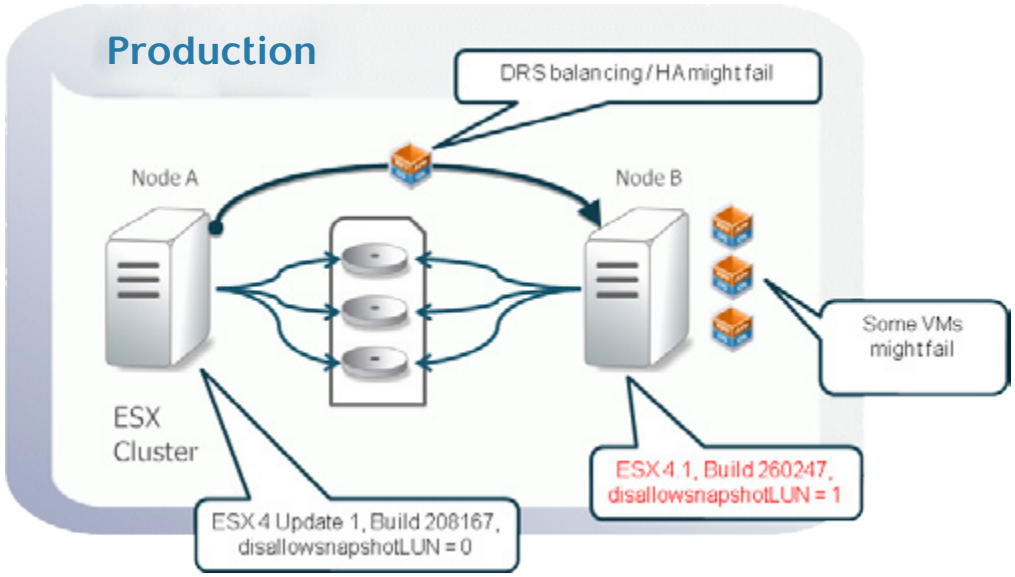
Additional network-related risks include

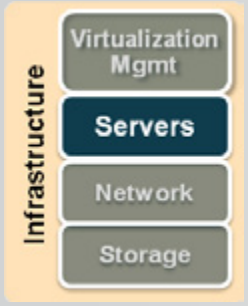
- DNS discrepancies
- Incorrect routing configuration on some nodes
- Time out of sync between nodes
- Different default gateway
- Inconsistent ESX network options
- ... and dozens of other risks

3. INFRASTRUCTURE LAYER | SERVERS

Certain discrepancies in the configuration of virtualized infrastructure cluster nodes present risks to the data residing on the virtual machines running on the cluster.

For example, when running multiple ESX versions, some nodes might be using advanced VMFS options unsupported by earlier versions, leading to potential data loss or extended downtime.





Additional server-related risks include

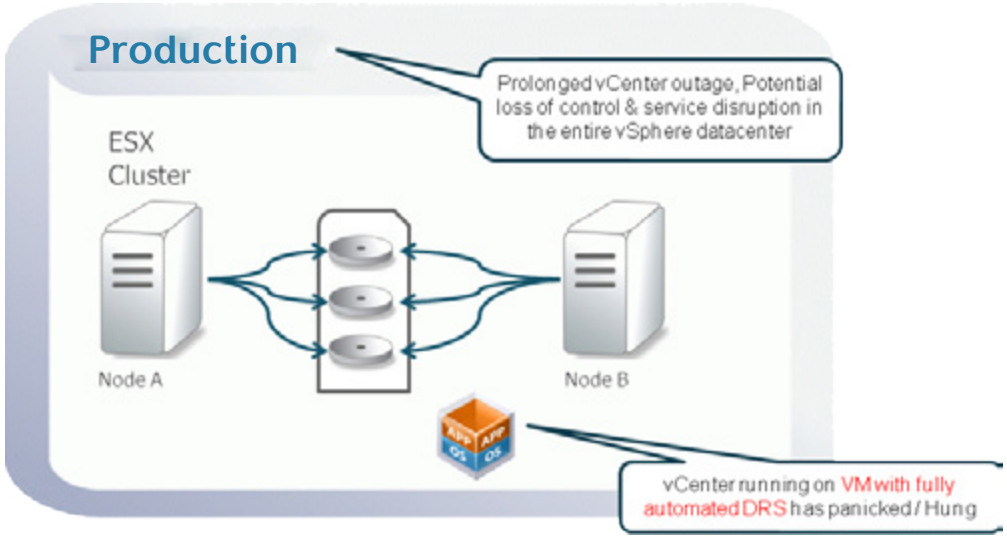
- Hardware discrepancies
- Different firmware versions
- Inconsistent configuration options
- ... and dozens of other risks

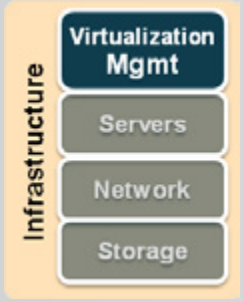
4. INFRASTRUCTURE LAYER | VIRTUALIZATION MANAGEMENT

A recommended best practice is to run the virtualization management application (e.g. vCenter) inside a virtual machine.

A common mistake is configuring this virtual machine with fully automated Distributed Resource Scheduling (DRS), which means that we can't tell in advance on which particular physical node vCenter will run at any given time.

If vCenter stops functioning or exhibits any performance issues, we would not know where to go in order to restart it. In a very large virtualized environment, it can take an unpleasantly long time to figure out how to revive the application.





Additional related risks include

- Cluster nodes missing access to NFS datastores
- Virtual datacenters not aligned with physical server storage location
- Missing / expired / incompatible licenses
- … and dozens of other risks

5. VM LAYER | STORAGE ALLOCATION

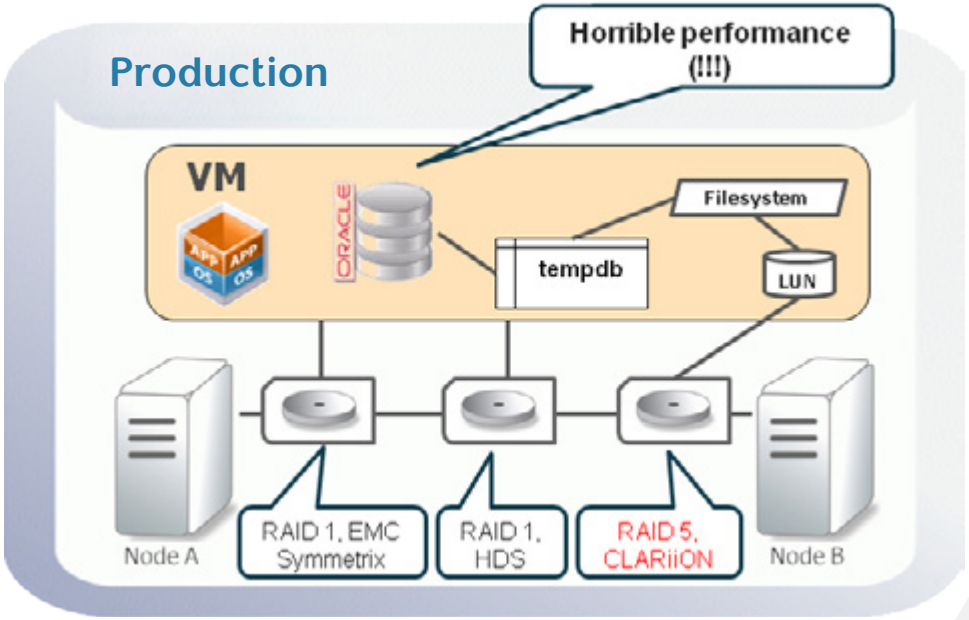
To prevent slowing down the entire database, all vendors recommend that temporary database files are placed on the highest performance storage. However, the abstraction layer added by virtualization makes it difficult for the database administrator to know what physical storage tier is allocated to the database at any given time.

In this example we see a virtual machine running an Oracle database on an ESX cluster with multi-tier RAID storage comprising high performance RAID 1 and lower performance RAID 5 datastores.

Additional related risks include

- Mixing RDM and non-RDM devices
- VM data configured with different persistence modes
- Mapping remote storage to VMs
- RDS on clusters with nodes of significantly different performance
- ... and dozens of other risks

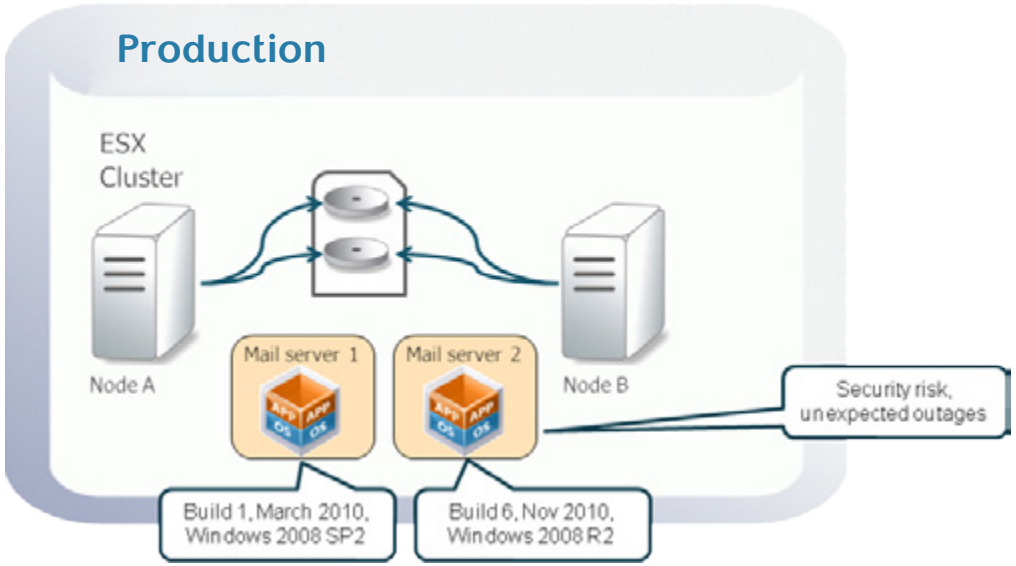
While the intention was for the low-cost, low-performance RAID 5 to be used for archiving and staging, the DBA has no clear way to know to which storage tier supports each VM file system. As a result, the temporary files of a particular database may end up on the lower performance datastore, leading to significant performance degradation.



6. VM LAYER | SERVER IMAGE

Over time, as the virtual environment grows larger and larger, it becomes more of a challenge to make sure that all of the virtual machines running the same application are consistently provisioned based on the same base image.

For example, a new virtual machine may be provisioned with a different version of the operating system, which may result in security risks, performance issues, and other unexpected behavior.



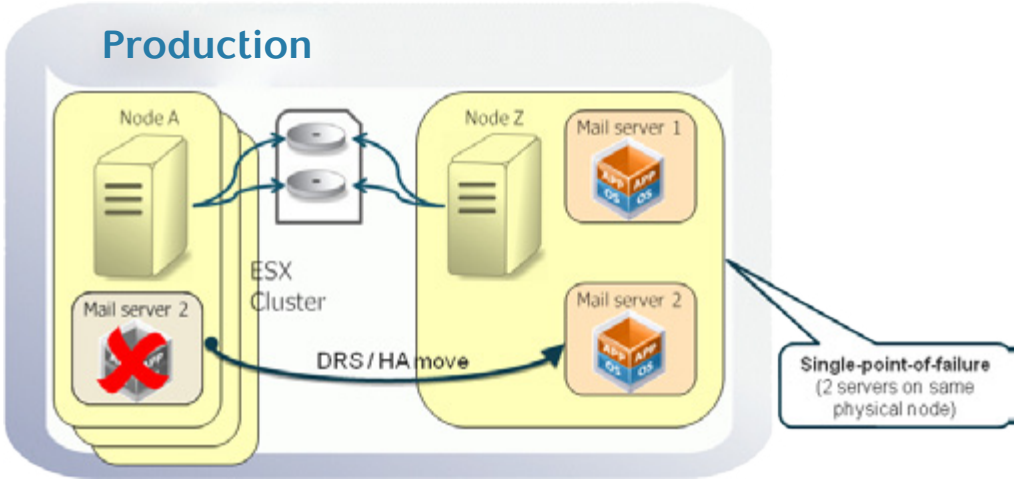
Additional related risks include

- Inconsistent patches applied to virtual machines
- Different startup options selected
- Different locale configurations applied
- Virtual Machines not synced on time
- ... and dozens of other risks

7. VM LAYER | HIGH AVAILABILITY

To achieve higher availability and performance than offered by ESX HA and DRS, it is common to use more than one virtual machines located on separate physical nodes.

As a result of routine maintenance or unplanned outage, one of the virtual machines might fail over or relocate to a different node, which could end up being the same one running the second virtual machine for our application. With the two virtual application servers running on a single physical node, we now have a single point of failure.



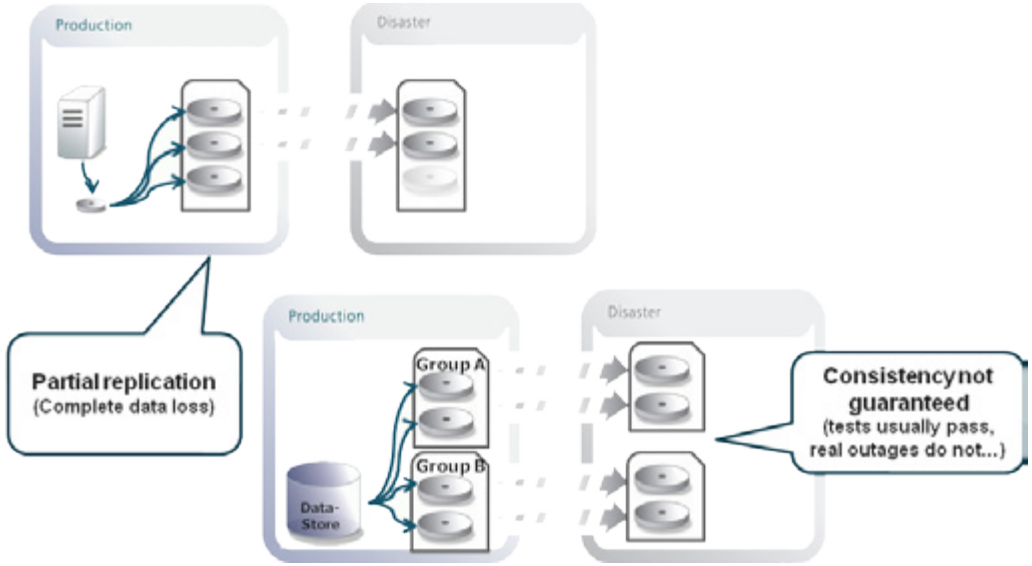
Additional related risks include

- Virtual machines not configured with HA
- VM team definitions not aligned with the supported business applications
- VM configuration allows failover to ESX nodes that do not have access to all required resources (storage, network, etc.)
- … and dozens of other risks

8. DISASTER RECOVERY LAYER | REPLICATION

Incorrect replication settings are a common occurrence. In a simple case, a data store may not be fully replicated. Obviously, all the virtual machines that are dependent on that data store will not be able to recover.

A more complex scenario could be one in which everything is replicated, but not using the same storage consistency group for all the devices on the data store. While the copy is now complete, it may very likely be corrupted, a problem which is more difficult to detect.



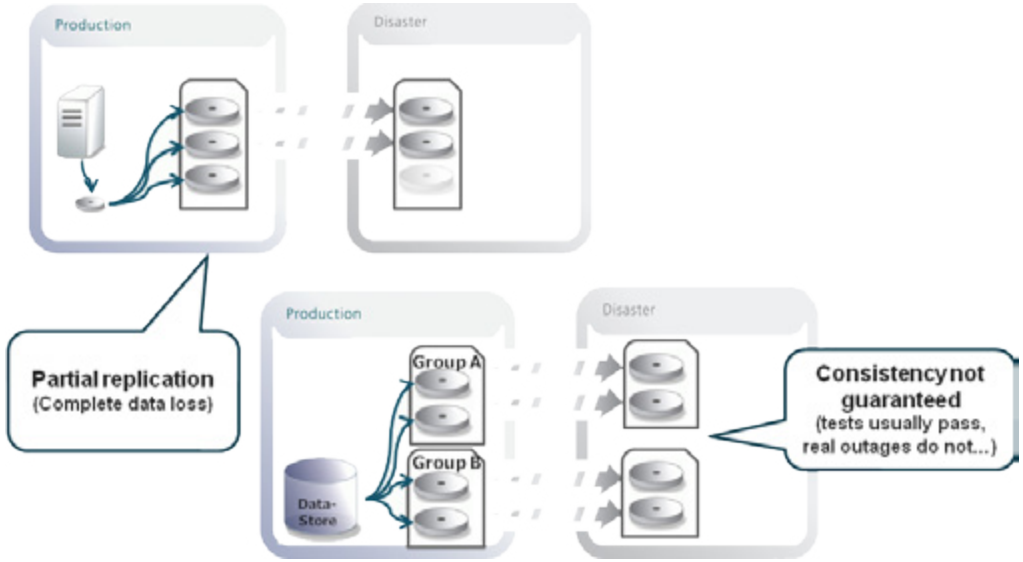
Additional related risks include

- Replication failure
- Data store using more than one array
- Misaligned VM storage
- ...and dozens of other risks

9. DISASTER RECOVERY LAYER | STORAGE MAPPING

Even when data is correctly replicated to the disaster recovery environment, it is still not guaranteed to be accessible in case a failover is attempted.

Incorrect replica mapping is a common issue. For example, one of the designated disaster recovery hosts may not have a path configured correctly to one of the storage replicas. In this case, all the virtual machines that depend on that particular data store will not function properly in a failover attempt.



Additional related risks include

- Locked devices
- Mismatched devices
- SRA misconfiguration
- ...and dozens of other risks

10. DISASTER RECOVERY LAYER | RECOVERY MANAGEMENT

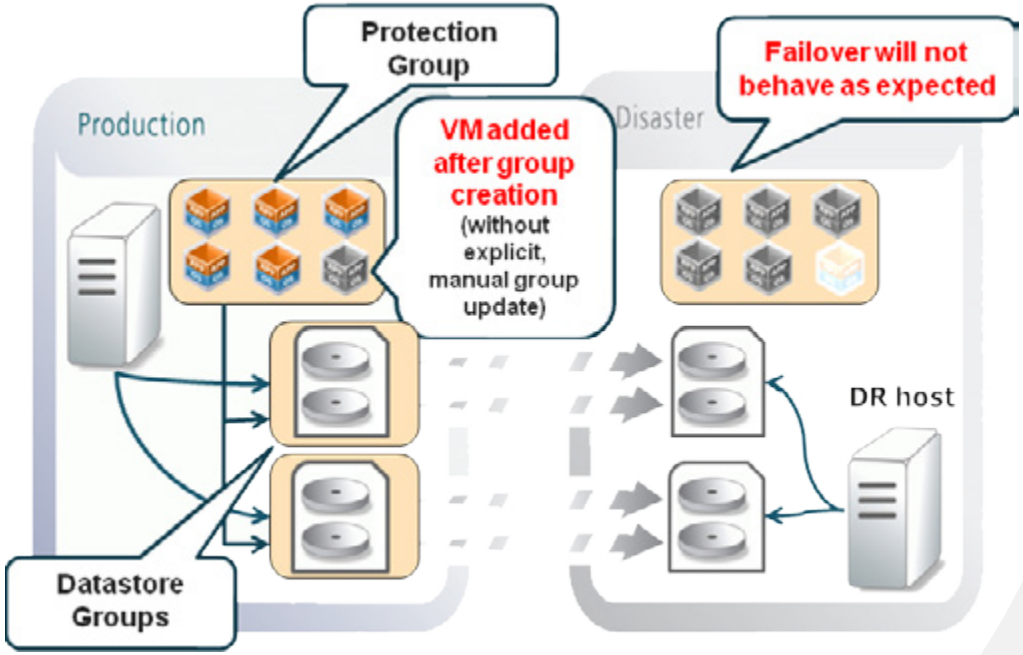
Automated recovery management tools (e.g. VMWare's SRM) help streamline the disaster recovery process and are definitely recommended for any private cloud environment.

With that said, it is important to note that such tools are also vulnerable to configuration changes. Keeping the configuration of the recovery manager aligned with the production configuration is an ongoing challenge.

Additional related risks include

- Misaligned recovery plans
- Missing components
- Unprotected non-virtualized components (e.g., DNS, NAS)
- ...and dozens of other risks

For example, we may have created a Data Store group and a Protection group that contains the VMs on that particular Data Store group. Over time, however, new VMs have been added to the Protection Group. Unless we manually refresh the recovery manager configuration, it will not be aware of these additions. In case of a failover, we may experience a partial or failed recovery.



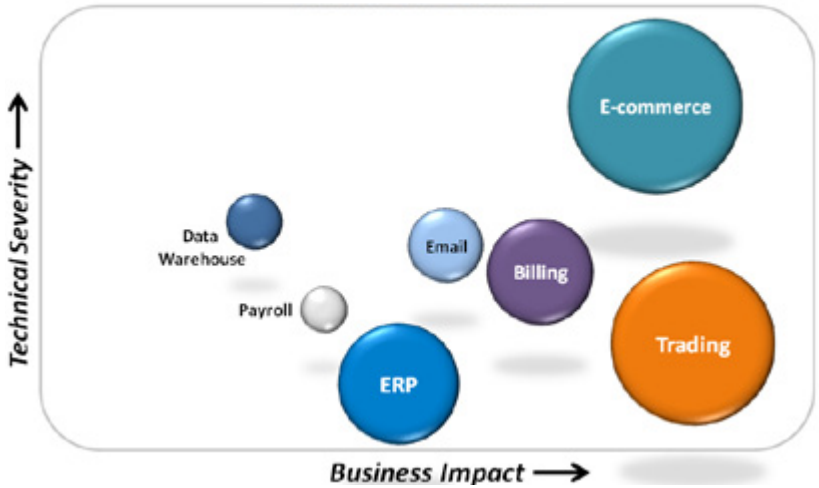
CONTINUITY SOFTWARE

Sign up for your own Private Cloud Vulnerability Audit

- Find out what data-loss and downtime risks exist in your private cloud environment
- Grade your private cloud HA/DR readiness
- Test your environment against a database of 4,000+ documented vulnerabilities

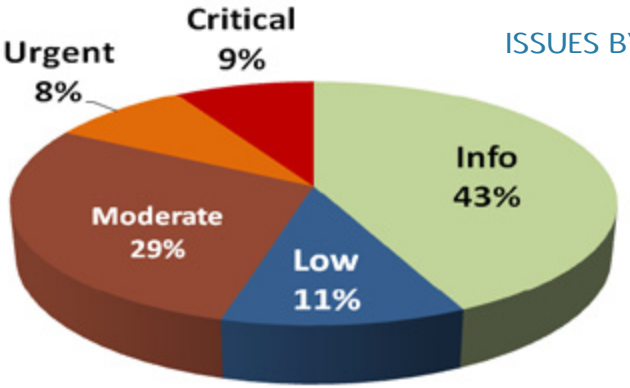
100% of the companies that have performed the audit uncovered vulnerabilities that were previously undetected.

THREAT LANDSCAPE

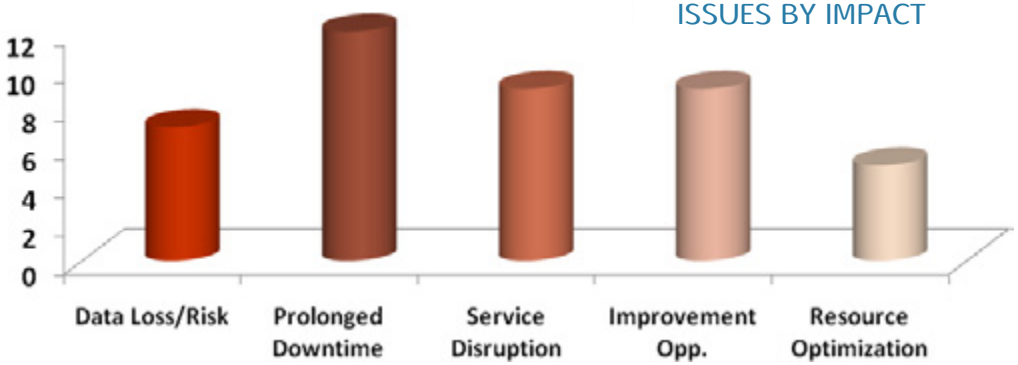


Click here to see if your private cloud environment qualifies for this offer

ISSUES BY SEVERITY



ISSUES BY IMPACT



Your audit report will include:

- Detailed assessment of all the risks and threats to your production and Disaster Recovery (DR) environments
- Resolution guidelines for each risk identified
- Optimization opportunities for your private cloud environment
- Many additional reports, topology maps, navigational models, and more!

About Continuity Software

Continuity Software's solutions are used by leading Global 2000 companies to ensure their Disaster Recovery and High Availability implementations will function as designed at all times.

By continuously and seamlessly monitoring and testing the production, cloud, high availability and disaster recovery configurations in your data center, our AvailabilityGuard software enables you to detect downtime and data loss vulnerabilities and performance risks before they impact your business continuity goals.

Continuity Software
5 Penn Plaza, 23rd Floor
New York, NY 10001
Phone: 646.216.8628
Fax: 646.417.6171
Toll Free: 888.782.8170
www.continuitysoftware.com