Top VMware Storage Configuration Issues That Can Jeopardize Your Data Availability

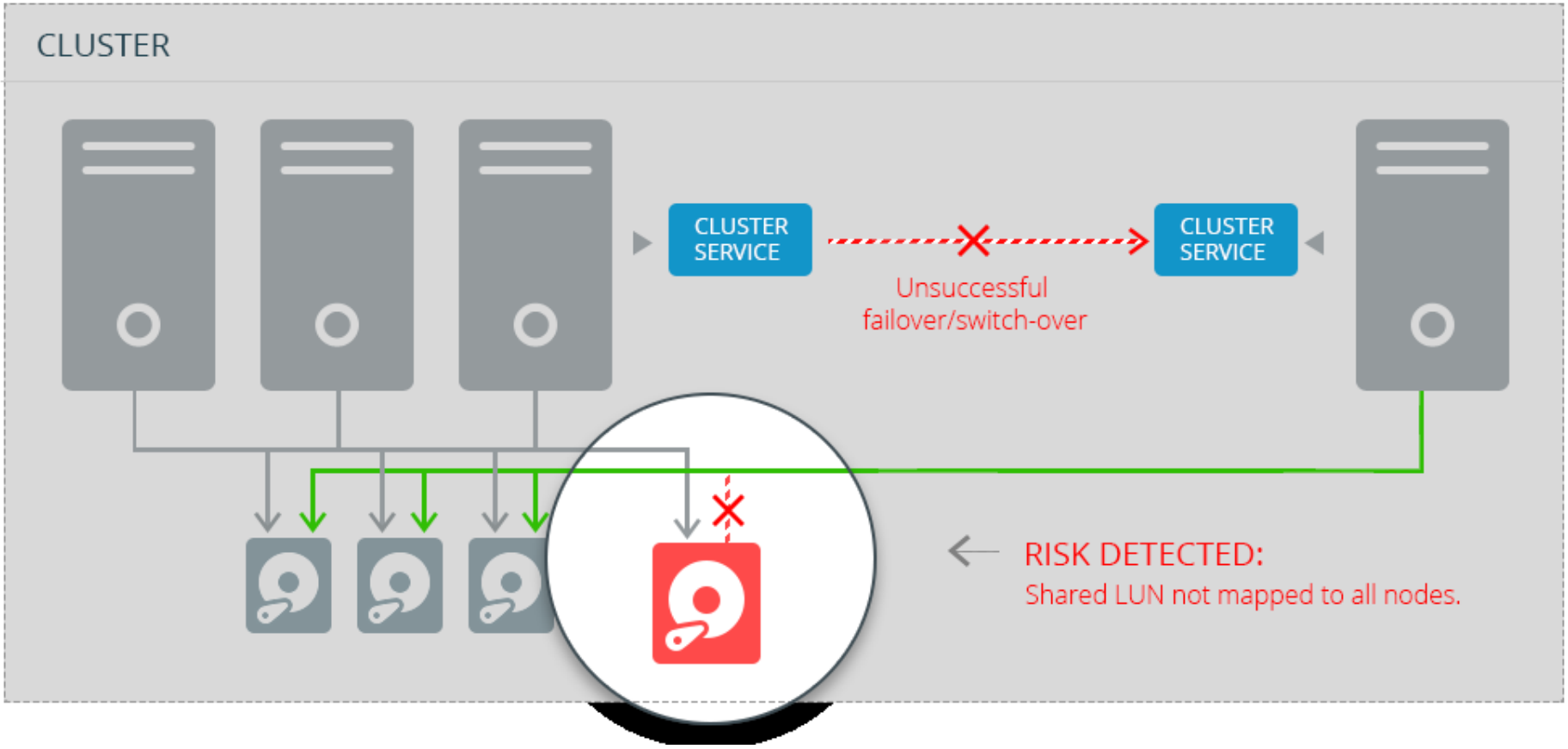
Introduction

As the IT landscape grows in size and complexity, it is practically impossible to manually maintain a configuration that is 100% consistent with vendor best-practices. It is even harder to ensure that changes in other IT layers are aligned with your VMware and vCenter configuration. Unfortunately, even a minor discrepancy between storage, OS, virtualization, cluster and networking can put your entire infrastructure and business applications at risk.

Hidden availability risks are inevitable in any IT environment.

This eBook highlights the top storage configuration issues often found in VMware environments that can put your data at serious risk and even take down your critical systems. Identifying and fixing these single-points-of-failure ahead of time will surely help you run a more stable IT operation and protect the substantial investment you have already made in sustaining high availability and resiliency in your environment.

#1: Inconsistent Storage Allocation



The Environment:

A VMware Private Cloud environment with an ESX cluster that has multiple nodes. The cluster is connected to shared datastores (could be LUNs or RDM).

The Problem:

Some storage objects (datastores, LUNs, RDM) are not mapped to all nodes in this cluster.

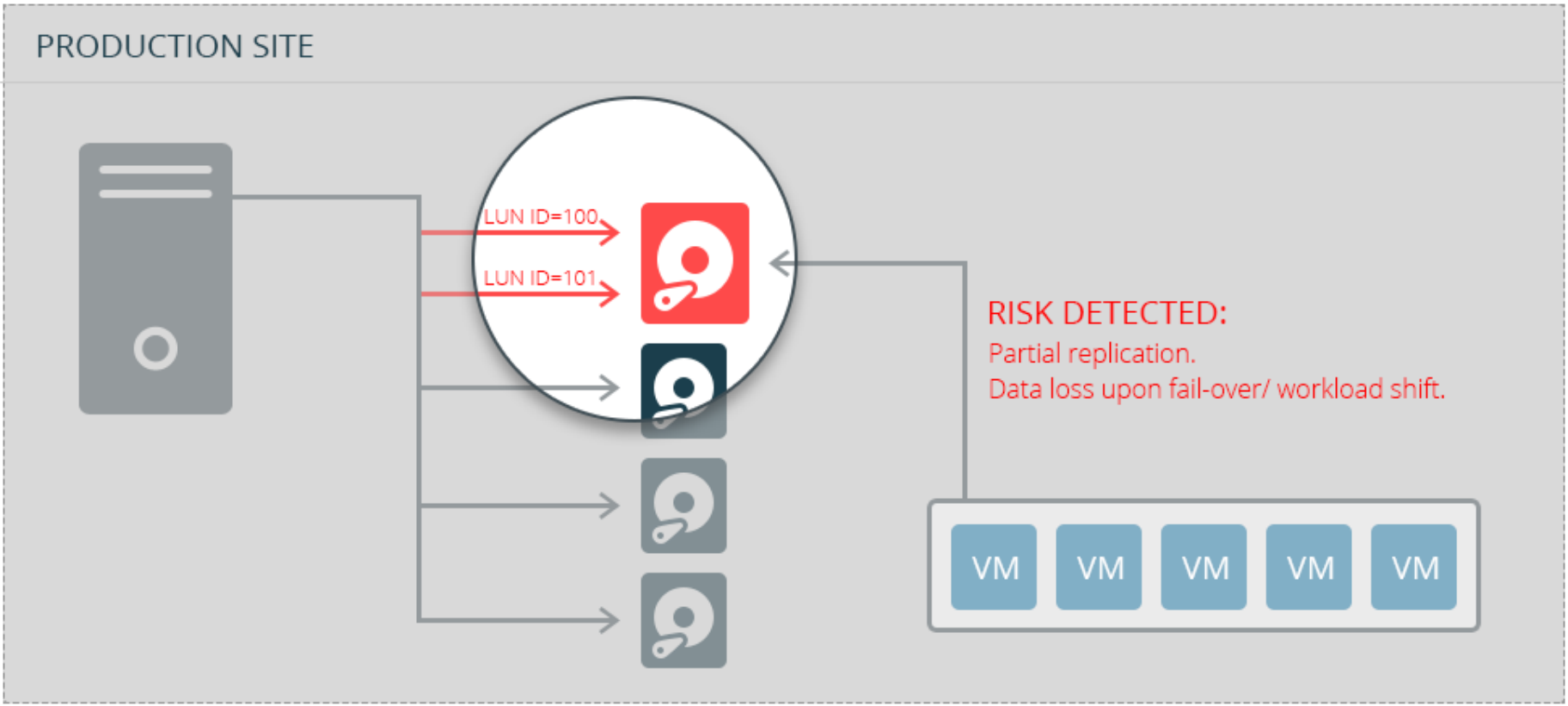
The Reason:

A new storage object was added to the cluster but inadvertently was either not mapped to all the nodes or not configured correctly across all nodes. This can happen for several reasons as a result of a confusion between the storage and the VMware teams, or it can be the outcome of a typo in zoning or masking values in the SAN fabric.

The Impact:

VM HA failure (even with Admission Control is in use).
vMotion will not be able to correctly balance the load.

#2: Inconsistent LUN ID w/Native MPIO



The Environment:

A VMware ESX host connected to multiple LUNs using the ESX native MPIO (multi-pathing I/O).

The Problem:

Paths to the same LUN were configured with different LUN IDs - contrary to the VMware ESX storage best practice.

The Reason:

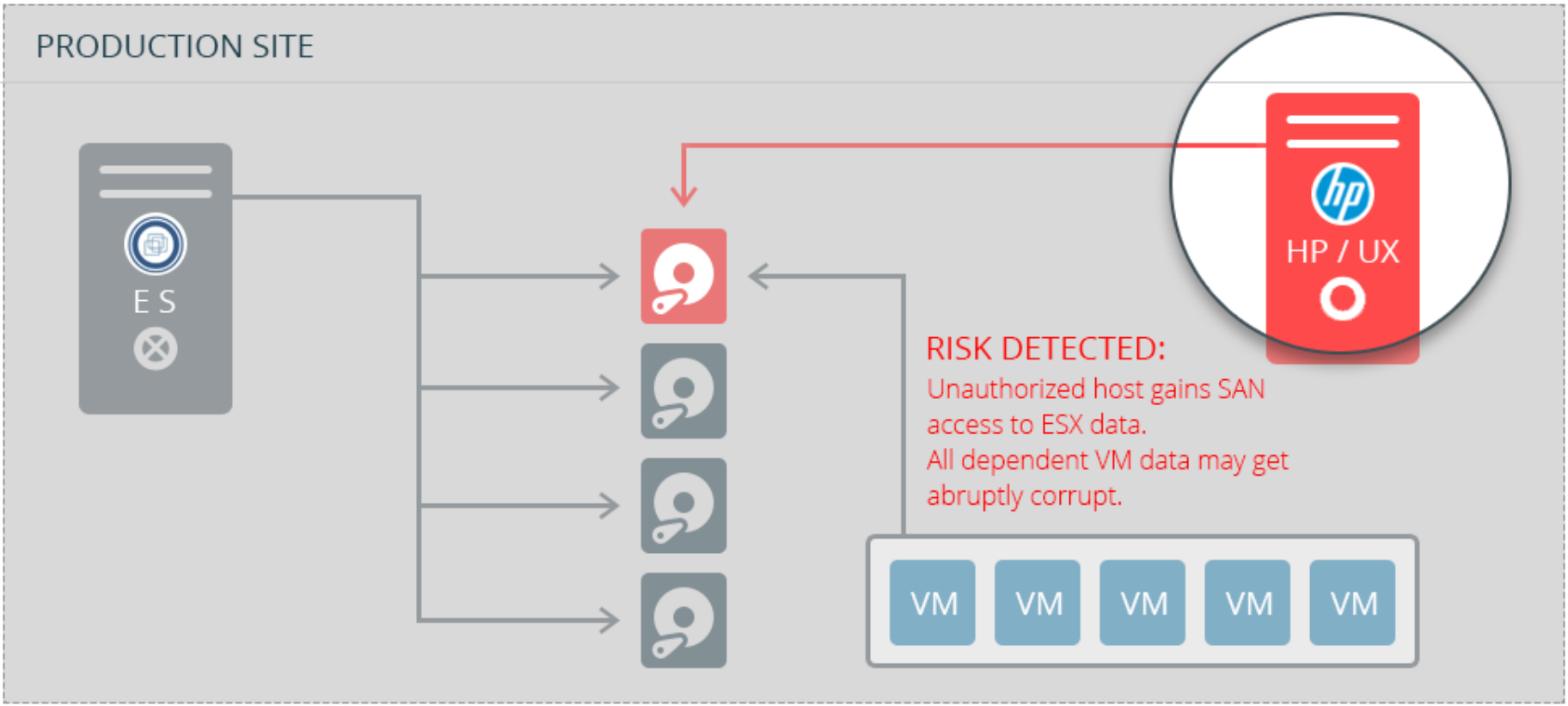
Maintaining path redundancy across multiple layers (hosts, SAN fabric, storage arrays) is complex and challenging. Coordination issues among different teams and human errors may result in various single-points of failure:

- Host HBA and port level.
- SAN fabric switch.
- Storage array front-end director.

The Impact:

All dependent VM data may get abruptly corrupt

#3: Risk of Data Tampering



The Environment:

A VMware ESX host is connected to multiple LUNs.

The Problem:

A non-vSphere host (in this case a HP/UX host) gains access to a vSphere-managed LUN.

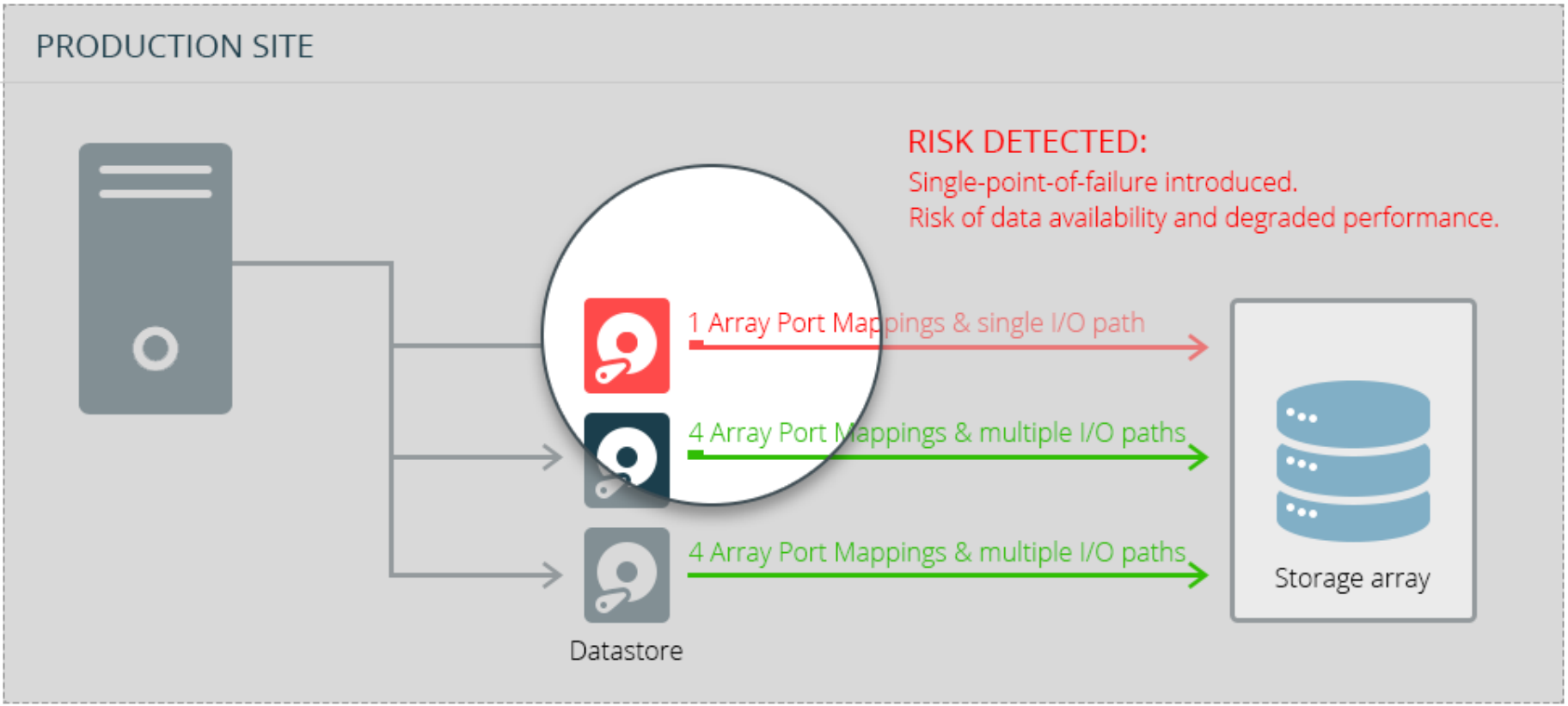
The Reason:

There could be a multiple reasons for this error (e.g., a mistake in zoning or masking - whether manually configured or scripted or an HBA upgrade).

The Impact:

As soon as the HP/UX hosts mounts the LUN, hundreds of VMs will lose their data and many might crash.

#4: SAN I/O Path - Inconsistent Configuration



The Environment:

A datastore managed by a VMware ESX host is connected to SAN volumes with 4 I/O paths on different Host HBAs and ports, SAN fabric switches, and storage array ports to provide full redundancy and high performance.

The Problem:

As more capacity is needed, a new volume is added - but for some reason it is configured with only a single I/O path.

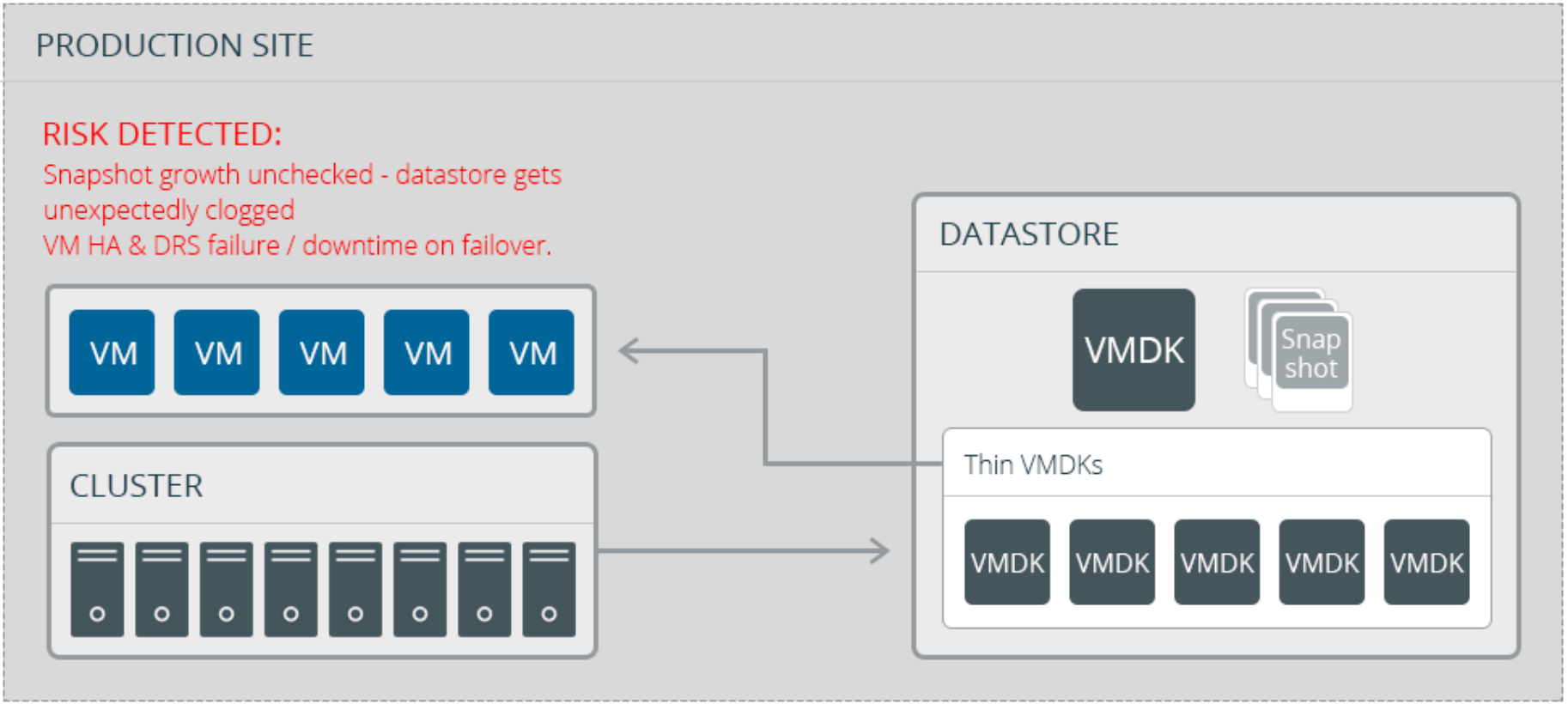
The Reason:

This mistake could result from a human error or confusion, errors in automation and scripting, etc.

The Impact:

A single-point-of-failure introduced to the environment which might lead to multiple VM failure. Another noticeable impact is a steep decrease in performance every time vMotion relocates a VM to the affected host.

#5: Snapshots Growing Too Large



The Environment:

A shared VMFS (Virtual Machine File System) datastore, contains multiple thinly provisioned VMDKs (Virtual Disks). VM-based snapshots are routinely used to safeguard against issues during maintenance and upgrades.

The Problem:

When left unattended - Snapshots can grow out of control and clog the datastore.

The Reason:

Snapshots should be purged periodically. Snapshot monitoring and housekeeping might not have been automated (or implemented incorrectly).

The Impact:

Thin VMDKs claiming new blocks will experience permanent write errors. Multiple VMs will crash - potentially involving data loss. Subsequent HA activities will fail.

CONTINUITY SOFTWARE

Get a Free Demo

Sign up for a Free Demo

See how to prevent your next IT infrastructure outage:

- Find hidden risks that can jeopardize your Cloud infrastructure
- Test your environment against a database of 5,000+ documented availability risks
- Get actionable recommendations that will help you eliminate single-points-of-failure and availability risks before they impact your business

Learn how you can proactively uncover infrastructure issues and single-points-of-failure that were previously undetected!

Sign up Today!

About Continuity Software

Continuity Software is the world's leading provider of IT Operations Analytics solutions for infrastructure outage prevention. Continuity Software's award-winning solution enables IT teams to proactively identify and eliminate single-points-of-failure before they can impact business.

AvailabilityGuard helps many of the world's largest companies, including 3 of the Top 5 banks in the US to stay on top of their IT operations and availability goals.

For more information

Website: www.continuitysoftware.com
Email: info@continuitysoftware.com
Tel: 1-888-782-8170 or +1-646.216.8628