SNIA

Education

How to: Eliminate Configuration Drift Risk

Gil Hecht, CEO
Continuity Software

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

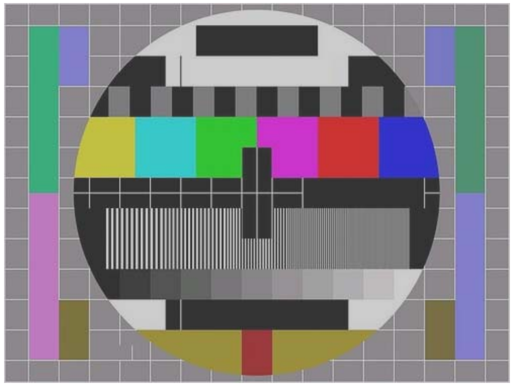
Abstract

- How to Eliminate Configuration Drift Risk
  - This session will appeal to:
    - Chief Information Officers
    - IT Management: System(Unix/Win/Cluster/VM) & Storage Managers
    - Business Continuity Managers
    - Those seeking a fundamental understanding of HA/DR Risks
  - Topics covered
    - Downtime & Data Loss – Major Business Risk
    - Configuration Drift – Leading Cause of Downtime & Data Loss
    - Understanding Configuration Drift
    - Eliminating Configuration Drift with HA/DR Configuration Analytics
    - HA/DR Configuration Analytics – How it works

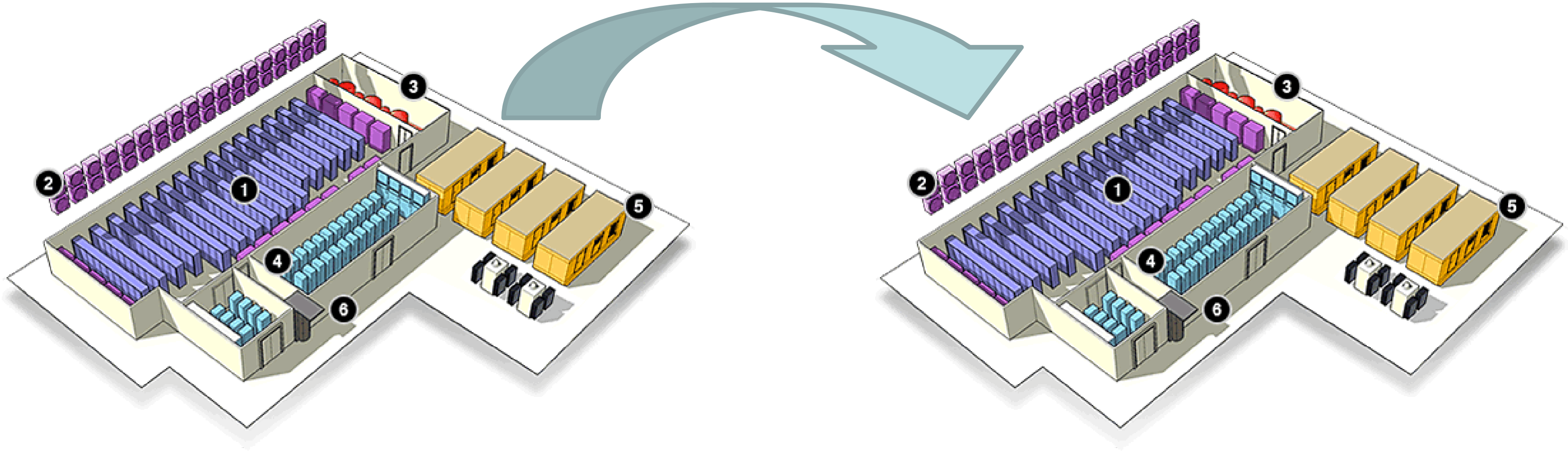
IT’s greatest nightmares

- Critical data loss

- Unplanned (& prolonged…) downtime



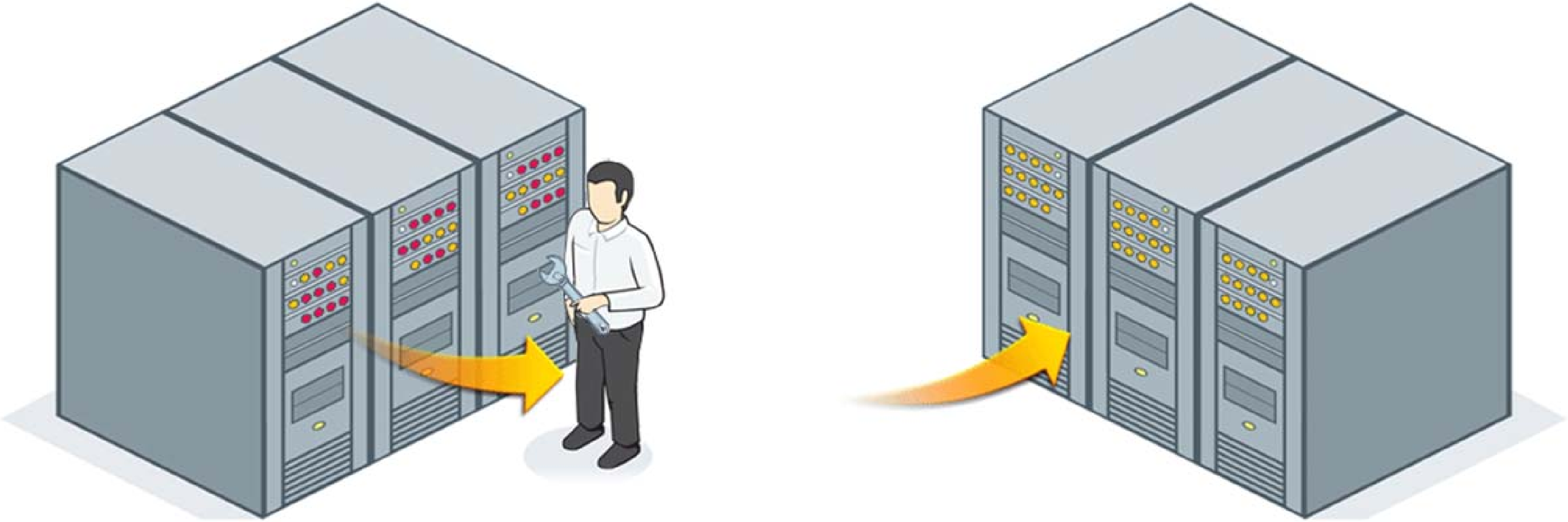
Having the right infrastructure



- Redundant datacenters
- Data replication
- Manual failover configuration / Local and Geo-Cluster

Is simply not enough

The problem: configuration drift



Standby systems get "out of sync"

- Production environment constantly changes
- Changes manually applied to HA and DR systems
- Some changes slip through…

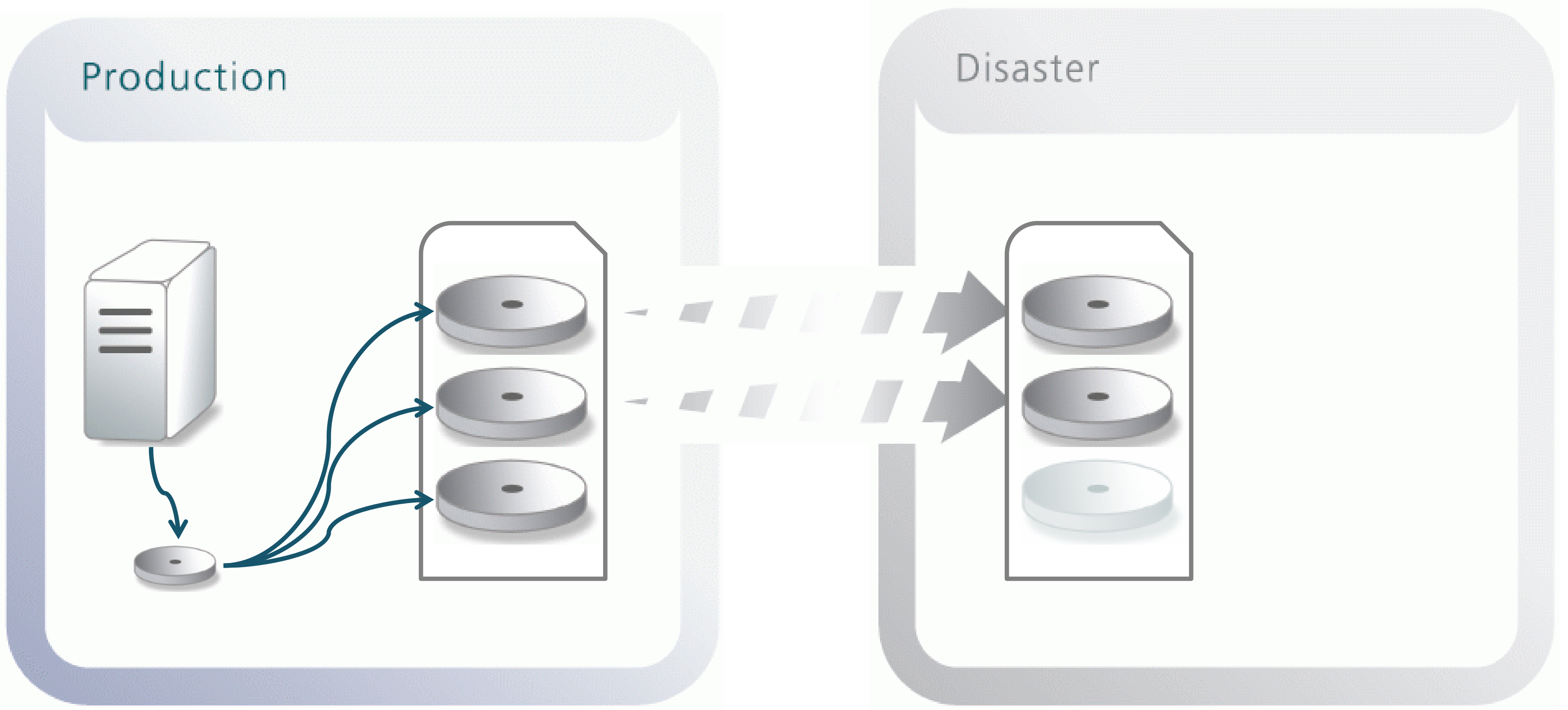
Existing mitigation approach fails

- Annual manual & expensive DR & HA tests
- Testing results: "75% failure rate as recovery configurations are "out of sync" with their production configurations" (*)

Solution: Configuration Analytics

- Automatic Detection & Alerting:
  - HA / Cloud / DR Vulnerabilities & Inefficiencies
  - Cross Vendor Best Practice Violations
- Benefit: Reduced Risks, Effort & Costs

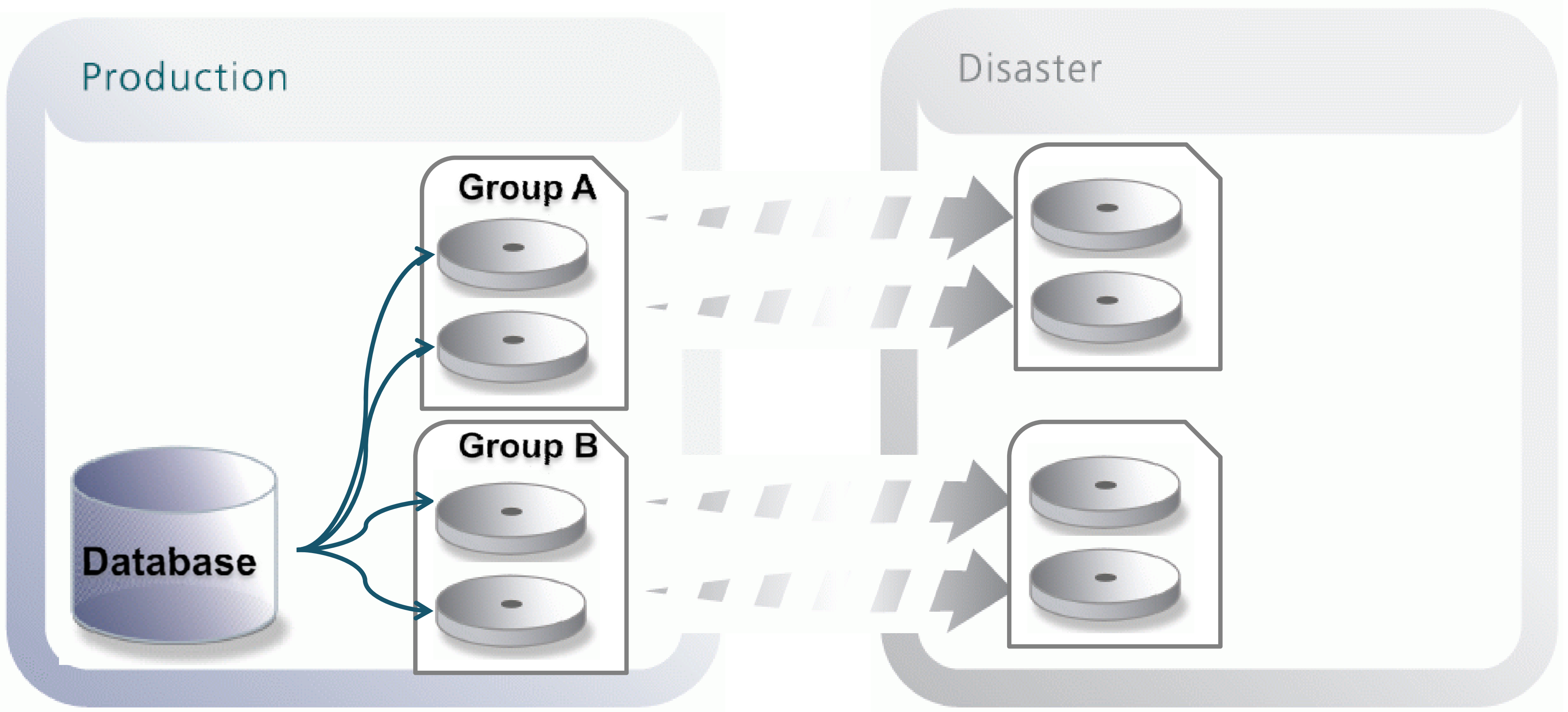
Sample Gap – Partial Replication



Result: Data Loss

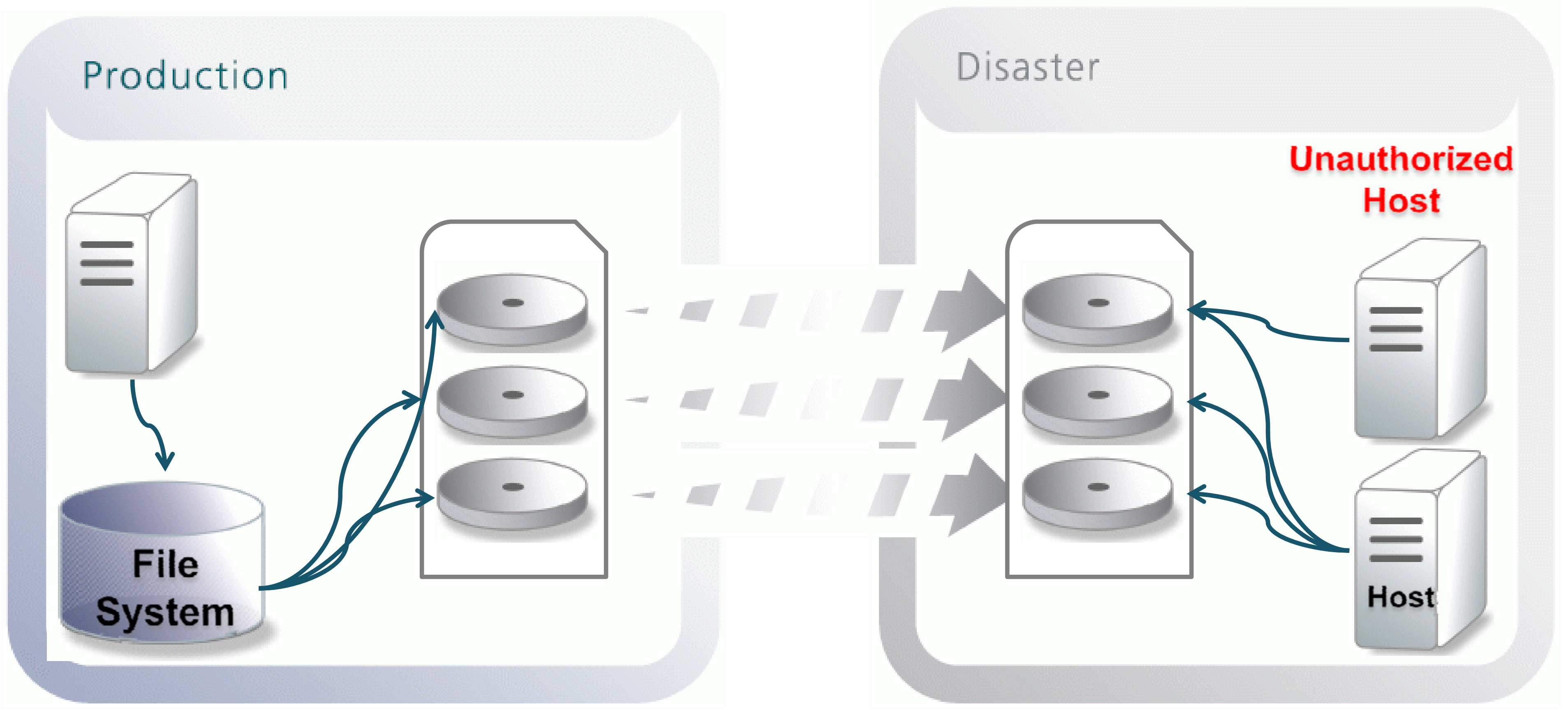
Sample Gap - Sync Replication

RDF Group Replication Inconsistency



Result: Data loss, increased time to recover

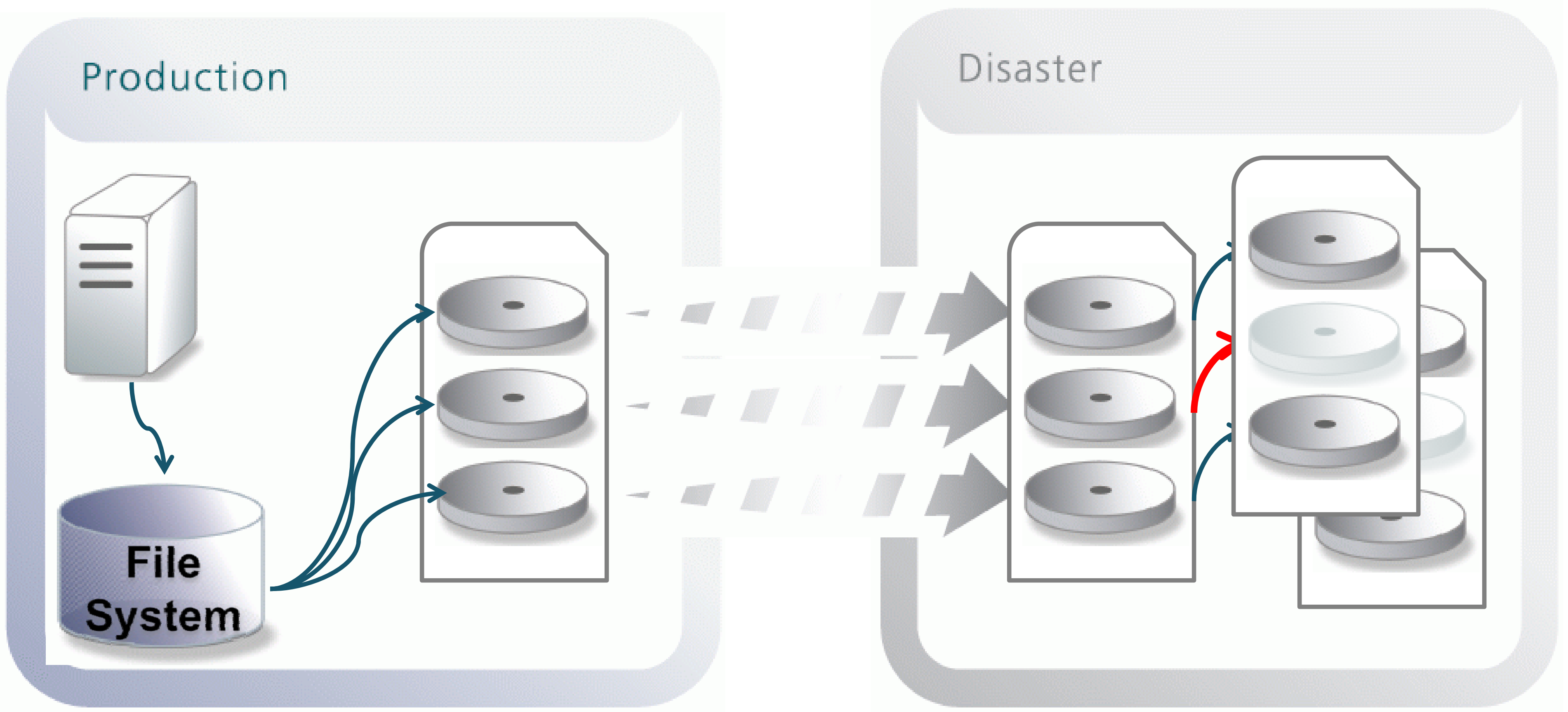
Sample Gap - Tampering Risk



Result: DR failure and data corruption

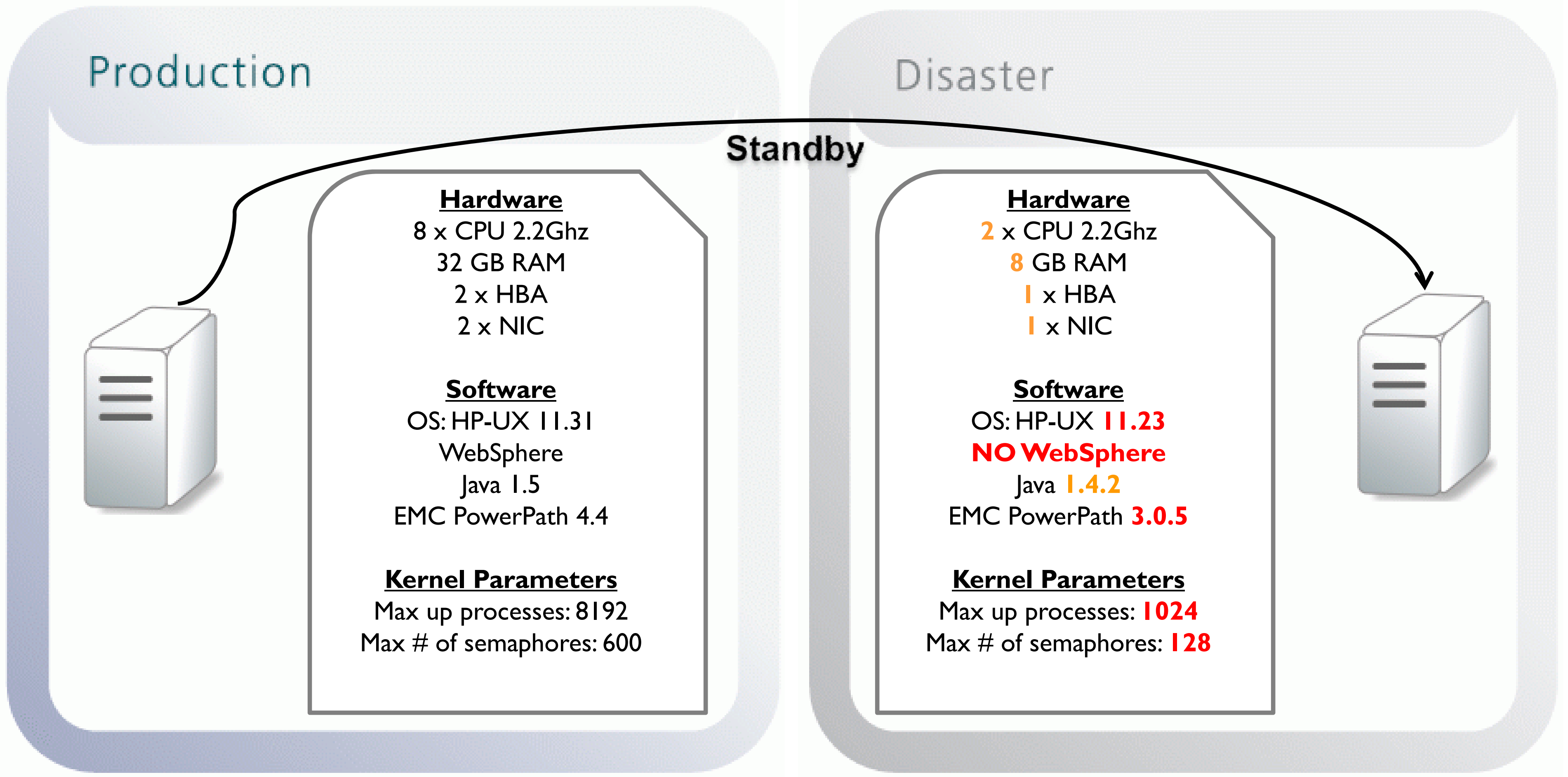
Sample Gap - Local Replication with BCVs

Replication Age Inconsistency



Result: Data corruption

Config Drift: Production → DR/HA



Hardware
8 x CPU 2.2Ghz
32 GB RAM
2 x HBA
2 x NIC

Software
OS: HP-UX 11.31
WebSphere
Java 1.5
EMC PowerPath 4.4

Kernel Parameters
Max up processes: 8192
Max # of semaphores: 600

Hardware
2 x CPU 2.2Ghz
8 GB RAM
1 x HBA
1 x NIC

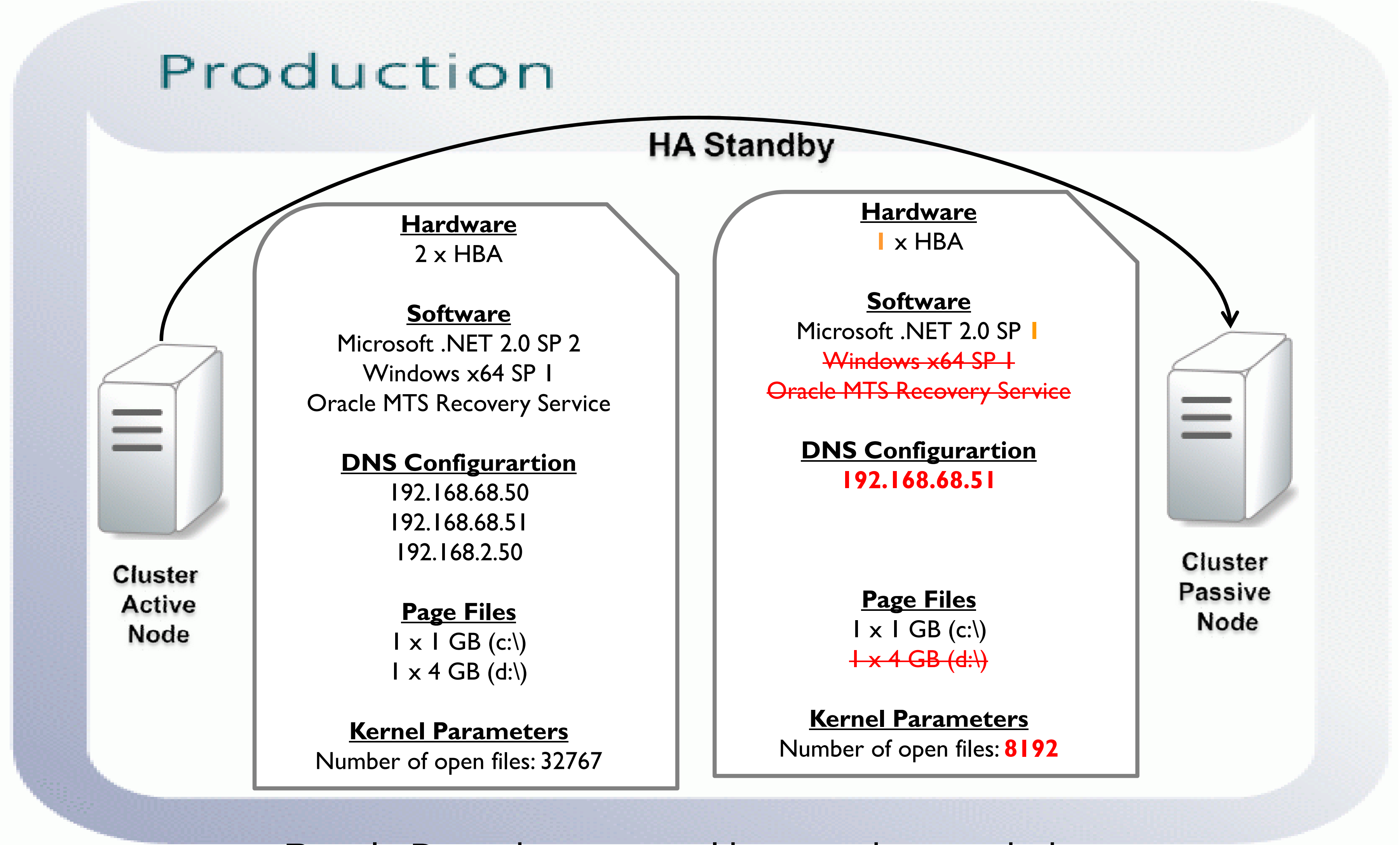
Software
OS: HP-UX **11.23**
NO WebSphere
Java **1.4.2**
EMC PowerPath **3.0.5**

Kernel Parameters
Max up processes: **1024**
Max # of semaphores: **128**

More differences in the areas of DNS, NTP, Page files, Internet services, patches, etc

Result: Increased time to recover

Config Drift 2: Production → DR/HA



Hardware
2 x HBA

Software
Microsoft .NET 2.0 SP 2
Windows x64 SP 1
Oracle MTS Recovery Service

DNS Configurartion
192.168.68.50
192.168.68.51
192.168.2.50

Page Files
1 x 1 GB (c:\)
1 x 4 GB (d:\)

Kernel Parameters
Number of open files: 32767

Hardware
1 x HBA

Software
Microsoft .NET 2.0 SP 1
~~Windows x64 SP 1~~
~~Oracle MTS Recovery Service~~

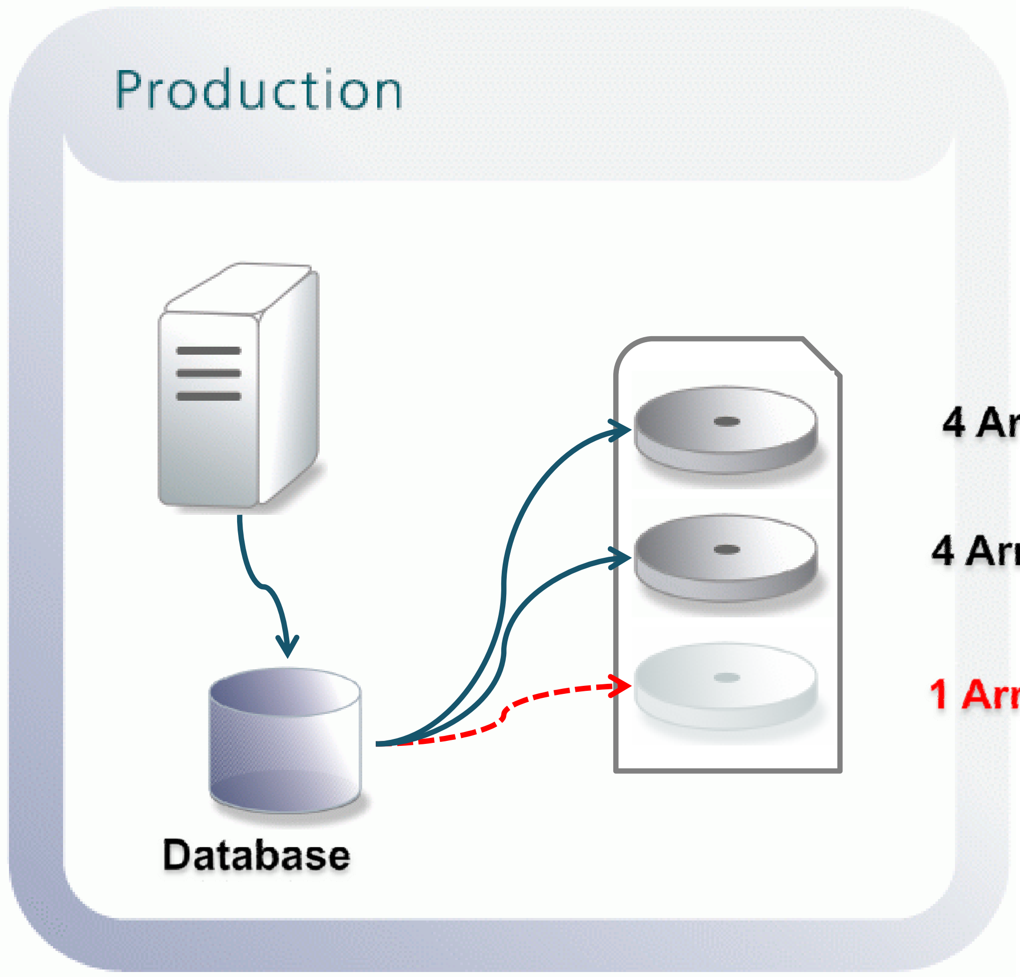
DNS Configurartion
192.168.68.51

Page Files
1 x 1 GB (c:\)
~~1 x 4 GB (d:\)~~

Kernel Parameters
Number of open files: **8192**

Result: Downtime, manual intervention needed to recover

Suspended Replication



4 Array Port Mappings & multiple I/O paths

4 Array Port Mappings & multiple I/O paths

1 Array Port Mappings & single I/O path

Result: Reduced MTBF, Downtime, Sub-optimal performance

Config Drift is Not for Humans

Numerous interconnected systems in the Datacenter

X

Practically unlimited configuration options for each

X

(Daily growth, changes, patches, upgrades +

Inability to instantly validate configuration)

= Failure = Downtime

& Data Loss

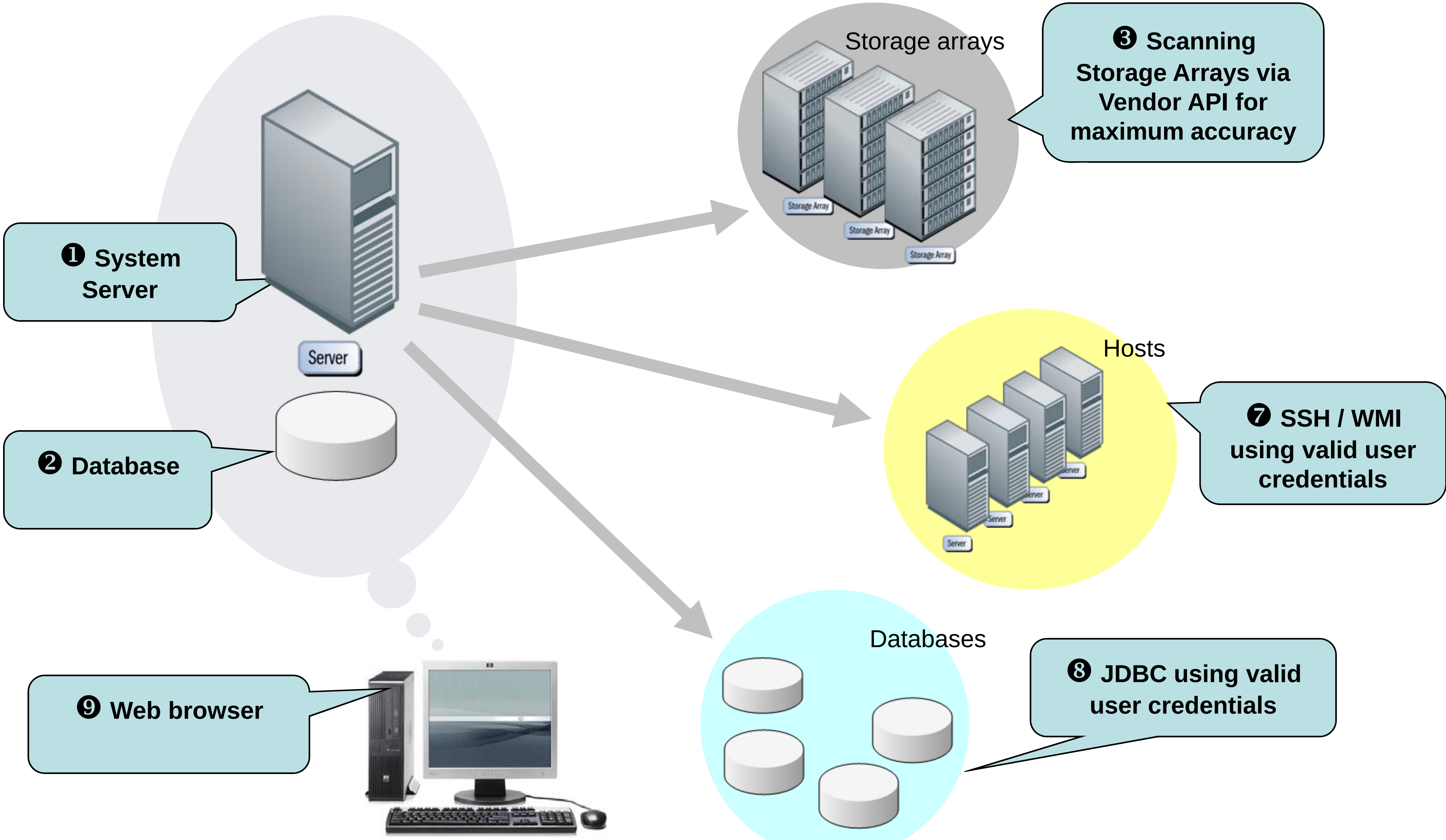
Solution: Configuration Analytics

- Automatic Detection & Alerting:
  - HA / Cloud / DR Vulnerabilities & Inefficiencies
  - Cross Vendor Best Practice Violations
- Benefit: Reduced Risks, Effort & Costs

What’s required

- Discovery
  - Import of IT elements from CMDB / Other Systems
  - Optional: Automatic discovery
- Scanning of entire IT for configuration data:
  - Database-Cluster-Virtualization-Server-Storage-Replication
  - Optional: Use existing CMDB data
  - Recommended: Agent-less, Read-only, Non-intrusive
- Configuration Analytics to discover Risks & Inefficiencies
  - Recommended: Updatable Risks & Inefficiencies databases
- Community driven risk database

How It Works



❶ System Server

❷ Database

❸ Scanning Storage Arrays via Vendor API for maximum accuracy

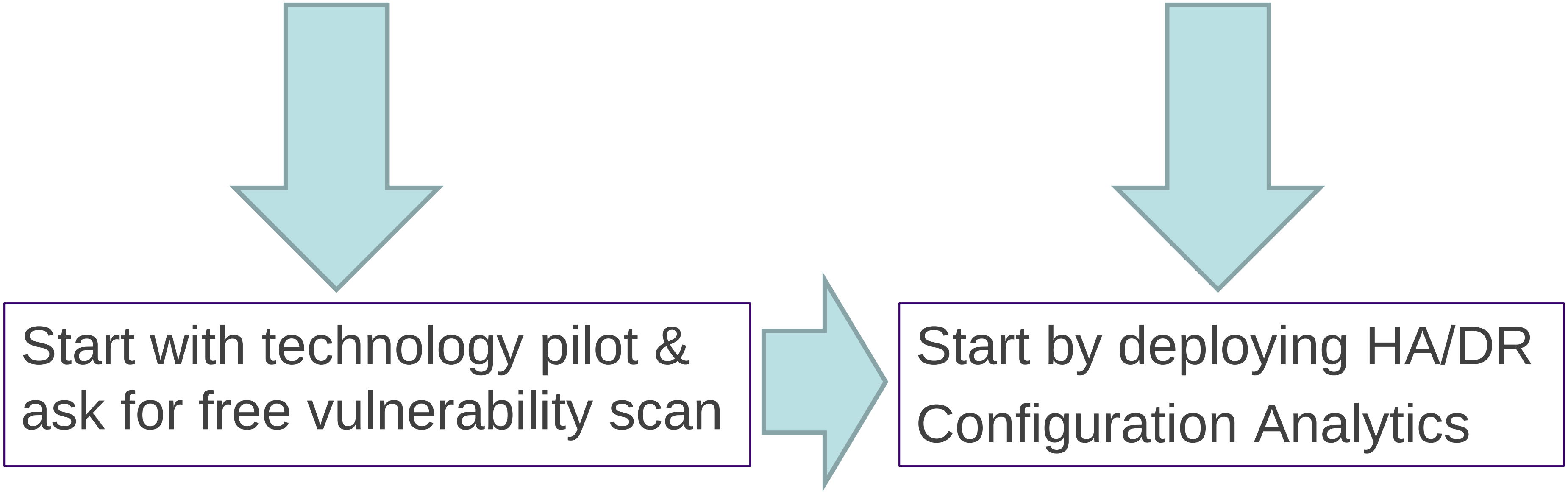
❼ SSH / WMI using valid user credentials

❽ JDBC using valid user credentials

❾ Web browser

How to get started?

- If you want to
  - Get a **one time** accurate assessment of your Downtime & Data Loss Risks
- If you want to
  - **Continuously** monitor for Downtime & Data Loss Risks



Start with technology pilot & ask for free vulnerability scan

Start by deploying HA/DR Configuration Analytics

Starting with Technology Pilot

- Demand the free HA/DR Vulnerability Detection Report from your leading IT Provider / Vendor.

- Report should cover Risks & Improvement opportunities for:
  - Databases, Clusters, Private Cloud / Virtual Machines, Operating Systems, Servers, Storage Arrays, Replication Mechanisms, Etc…

- Typically takes < 3 days from install to report

Starting with Full Deployment

- Key factor for choosing the right system:
  - Breadth & depth of Risk (Signatures) Database
  - Impact on production systems (Should be minimal)
  - Deployment effort (Should be <5 days for large datacenter)

- Expected benefits / results
  - Dramatic reduction in downtime & data loss events
  - HA/DR Testing Results Improvement & reduced effort
  - New Risks expected to be discovered daily for med-large datacenters

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: trackstoragemgmt@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Gil Hecht