CONTINUITY SOFTWARE

AvailabilityGuard/SAN™

Proactive validation of SAN fabric configuration and best practices

AvailabilityGuard/SAN is an add-on for the AvailabilityGuard IT Operations Analytics solution which provides extended visibility and risk detection for your SAN environment.

Ensuring Service Availability in a Challenging SAN Environment

The SAN (Storage Area Network) is at the heart of the modern datacenter. Yet, the SAN environment can be highly complex, presenting a concentrated area of risk and significant management challenges. Frequent configuration changes and the ever-growing volume of vendor recommendations and SAN best practices require complex adjustments at each layer.

In addition, the increasing adoption of virtualization technologies and today's dynamic environment further complicates dependencies. So even the best IT teams are extremely challenged when it comes to keeping pace and ensuring configuration alignment and service availability.

Proactive SAN Risk Detection

The AvailabilityGuard/SAN Risk Detection Engine™ performs non-intrusive scans of your SAN fabric and collects up-to-date configuration data from physical and virtual infrastructure. Using predictive analytics, AvailabilityGuard pinpoints any single-points-of-failure or other misconfigurations that impact your SAN-readiness and can lead to potential downtime and data loss, alerting the relevant IT teams with the suggested resolution.

The addition of AvailabilityGuard/SAN to your AvailabilityGuard deployment, provides an even more complete risk management solution, helping to prevent expensive service disruptions and costly firefighting for your entire IT stack.

- Eliminate up to 90% of SAN-related infrastructure outages
- Achieve higher IT operations stability and configuration quality
- Ensure service availability goals are met with proactive validation of SAN configuration
- Increase cross-domain collaboration and resource productivity
- Maximize your SAN investment and identify wasted storage resources

orange™ · Industrial Bank of Korea · El Corte Inglés · BBVA · Ministry of Government Administration and Home Affairs · amdocs

CONTINUITY SOFTWARE

AvailabilityGuard/SAN™ Key Features

Proactive Single-Points-of-Failure Detection & Impact Analysis

- I/O path as a single-point-of-failure (SPOF)
- HBA port / card as a SPOF
- Storage Array Director port as a SPOF
- Logical SPOF caused by masking/zoning configuration
- SAN switch as a single-point-of-failure
- Fabric single-point-of-failure
- Storage Array Engine/Directory as a SPOF

What-If Scenario Analysis

- Impact prediction of Switch/Array component failure

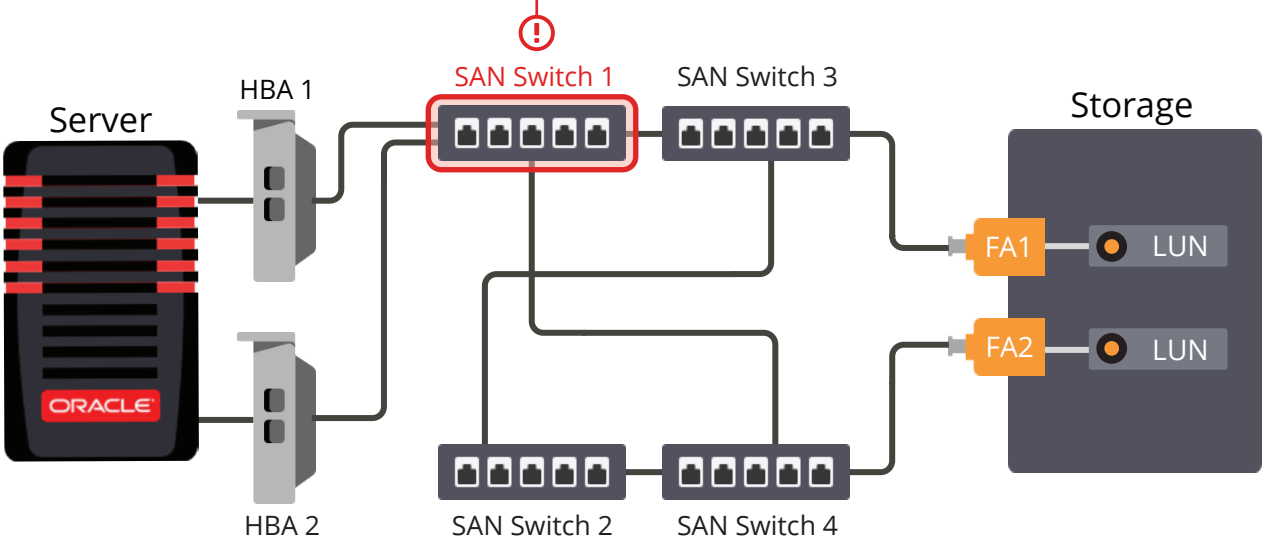
I/O Multi-Pathing Best-Practice Validation

- Load-Balancing Policy
- Configuration consistency of MPIO across cluster nodes
- Path state analysis
- I/O Queue Depth configuration
- HBA firmware/driver alignment

SAN Security & Tampering Prevention

- LUNs presented to unauthorized host WWNs
- Array port flag/option analysis
- LUN Map / Port mapping best practices
- Masking/zoning bets practices

SAN Single Point of Failure Detected



© 2016 ContinuitySoftware **US Headquarters:** 5 Penn Plaza, 23rd Floor, New York, NY 10001
Phone: 646.216.8628 | Email: sales@continuitysoftware.com | Website: www.continuitysoftware.com