AvailabilityGuard/Cluster™

CONTINUITY SOFTWARE

Ensuring High Availability across Your IT Infrastructure

Cross-domain High Availability Management

Used by leading enterprises worldwide, AvailabilityGuard/Cluster enables organizations to manage high availability and business continuity readiness across their entire IT infrastructure.

Hidden risks are inevitable in any cluster environment

As clusters grow in size and complexity, it is practically impossible to ensure 100% adherence to vendor best-practices at all times. In addition, ongoing and frequent configuration changes inevitably result in configuration discrepancies and risks that often remain hidden until disaster strikes.

Manual testing is not the solution

Periodic failover tests are risky and require considerable investment in time and manpower. Most importantly, they still leave your organization vulnerable to configuration errors during long intervals between tests.

Correct availability risks before they impact the business

The AvailabilityGuard Risk Discovery Engine™ automatically scans your cluster environment in a non-intrusive mode, pinpointing any gaps and misconfigurations that could jeopardize cluster failover and lead to downtime or data loss.

Automated notifications and alerts are sent to the appropriate resources when availability or data loss risks are uncovered, allowing your IT teams to proactively address issues before they impact business operations.

Ensure compliance with high availability policies

AvailabilityGuard/Cluster allows you to validate redundancy and reserve capacity for each application tier against your organization's goals and policies, generating daily compliance reports and issuing notifications when compliance is at risk.

> *"We were able to identify the possible risks in our current DR/HA strategy, making it easier for us to anticipate them and establish proactive measures prior to contingency tests and simulations."*
>
> ***Antonio Castillo, Manager, DR/HA Europe, BBVA***

Product Highlights

- Automated daily validation of cluster configuration (local, metro, geo) as well as interconnected resources and application
- Automatic detection of downtime risks and data loss vulnerabilities using a knowledgebase of over 5,000 risk signatures
- Analysis and presentation of potential impact on business services
- Automated daily documentation of your cluster configuration and last known good configuration
- Agentless, non-intrusive data collection using standard communication protocols (SSH, WMI, WinRM, Storage APIs, JDBC, Sudo) with zero impact on the scanned environment
- Integration with leading configuration management databases (CMDBs), ticket management systems, and enterprise consoles.

Key Benefits

- Eliminate 90%+ of cluster downtime and data loss incidents by automatically detecting configuration risks
- Ensure high availability by validating that your cluster configurations are always valid and in sync
- Ensure compliance with high availability redundancy and reserve capacity policies
- Continuously audit and improve high availability and data protection practices
- Reduce the need for risky HA failover tests

AvailabilityGuard Key Features

AvailabilityGuard delivers a robust feature set and cross-vendor/cross-domain/cross-platform support that allow IT teams to proactively identify and eliminate downtime and data loss risks across the entire IT infrastructure.

Best-Practice Violation Detection

Risk Detection Engine automatically uncovers deviations from vendor best-practices that could cause downtime or data loss risks.

Configuration Gap Monitoring

Continuous monitoring and verification of IT changes ensures proactive detection of configuration gaps between the production and DR/HA environments that create data protection, availability, or disaster recovery risks.

The Power of the Community

Community-driven Risk Knowledgebase contains thousands of configuration risk signatures and is constantly updated.

Comprehensive SLA Management

Policy-driven SLA Management monitors established SLA policies and alerts the appropriate teams when violations are detected.

Automated Alerts & Notifications

Instant notification of a potential problem to the proper team in your organization ensures timely response to any issue before it impacts the business.

Risk Assessment Dashboard

Provide non-IT executives with insight into the company's readiness and risk levels.

Live Data Center Documentation

Gain insight with an interactive, graphical topology of all data center entities, dependencies, and relationships.

Data Center Change Audit Trail

Ensure the entire data center team stays informed of all changes.

Identification of Optimization Opportunities

Discover unutilized storage space or other opportunities to reduce costs and improve overall system performance.

Comprehensive Reporting

Get the information you need, on-demand, to monitor and analyze your service availability risks.

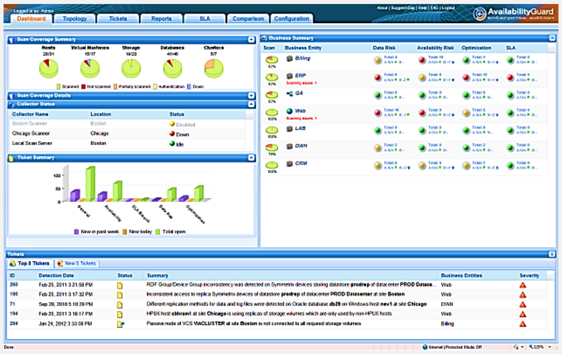
Integration with CMDBs and Tickets Management Systems*

AvailabilityGuard can be integrated with CMDBs and ticket management systems from leading vendors (IBM Tivoli, HP OpenView, BMC Remedy, and others), allowing you to consolidate system management across the enterprise.

** Integration with Ticket Management Systems requires AvailabilityGuard/Enterprise+ Edition*

The AvailabilityGuard Dashboard

The AvailabilityGuard dashboard provides an immediate snapshot of service availability risks throughout your IT infrastructure and the ability to drill down to the details of any issue.

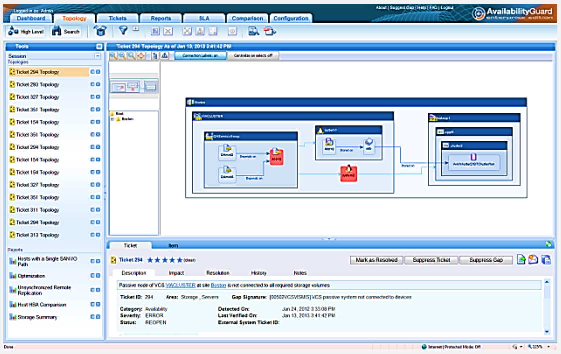


Collector Name	Location	Status
Boston Scanner	Boston	Disabled
Chicago Scanner	Chicago	Down
Local Scan Server	Boston	Idle

ID	Detection Date	Status	Summary	Business Entities	Severity
260	Feb 25, 2011 3:21:58 PM		RDF Group/Device Group inconsistency was detected on Symmetrix devices storing datastore **prodrep** of datacenter **PROD Datace...**	Web	⚠
190	Feb 25, 2011 3:17:32 PM		Inconsistent access to replica Symmetrix devices of datastore **prodrep** of datacenter **PROD Datacenter** at site **Boston**	Web	⚠
71	Sep 28, 2010 5:10:29 PM		Different replication methods for data and log files were detected on Oracle database **db28** on Windows host **nev1** at site **Chicago**	DWH	⚠
194	Feb 25, 2011 3:18:17 PM		HPUX host **ebhram1** at site **Chicago** is using replicas of storage volumes which are only used by non-HPUX hosts	Web	⚠
294	Jan 24, 2012 3:33:08 PM		Passive node of VCS **VIACLUSTER** at site **Boston** is not connected to all required storage volumes	Billing	⚠

The AvailabilityGuard Trouble Ticket

AvailabilityGuard trouble tickets include detailed problem description, the potential business impact, and a suggested remediation action. Each ticket serves as consolidated view to facilitate collaboration among the IT resources tasked with solving the issue.



Ticket 294 ★★★★★

Passive node of VCS VIACLUSTER at site Boston is not connected to all required storage volumes

Ticket ID: 294 Area: Storage , Servers Gap Signature: [00502VCSMSMS] VCS passive system not connected to devices

Category: Availability
Severity: ERROR
Status: REOPEN
Detected On: Jan 24, 2012 3:33:08 PM
Last Verified On: Jan 13, 2013 3:41:42 PM
External System Ticket ID:

Supported Platforms

Operating Systems

- Solaris 8+
- HPUX 11.0+
- AIX 4+
- Linux RedHat AS 3+, SuSE 8+
- Windows 2000+
- ESX / ESXi 3.5+

Virtualization

- VMware vSphere
- All major Unix virtualization environments

Databases

- Oracle 8.1.7+
- MS SQL Server 2000 SP3+
- Sybase 12.5+
- DB2 UDB 8.1+

Storage

- EMC Symmetrix / VNX/ RecoverPoint
- NetApp Filers – All
- HDS AMS, USP, VSP
- IBM DS 6K, 8K, XIV, SVC
- HP XP

Clusters

All major cluster environments

Volume Management

All major LVMs and file systems

Replication

All native local replication engines

PRODUCTS OF THE YEAR 2007 SILVER

Products of the Year '09 Storage magazine/SearchStorage.com