DATASHEET

superna®

Superna® DR Edition for Dell Isilon/PowerScale

Superna® DR Edition enhances disaster recovery in Dell Isilon/PowerScale environments with a solution based on the “cluster witness” concept.

OVERVIEW

File-based storage is growing faster than any other data type in the enterprise. This means that your business-critical data needs to be protected with a comprehensive, high-availability disaster recovery solution. Dell’s Isilon/PowerScale SyncIQ enables the flexible management and automation of data replication. It allows data from one cluster to be replicated to one or more target clusters to protect the data. Of course, replicating data is only part of a DR solution required to achieve your RTO and RPO targets. Superna® plus SyncIQ combine to enhance DR for Dell Isilon/PowerScale infrastructure. It protects configuration and real data (share, NFS, quota, snapshots), and provides for simulated DR testing and reporting.

Superna DR Edition continually monitors the Isilon/ PowerScale cluster for DR readiness through auditing and SyncIQ configuration, as well as several other cluster metrics.

HIGHLIGHTS

- Superna® DR provides continous DR Readiness Monitoring; more than 30 different validations are monitored between clusters
- Automated, one button failover for NFS and SMB
- Failover whole or partial clusters
- Automatically monitors required cluster settings (data, configuration, active directory) to ensure failover availabilit; sends near-real-time alerts upon detection of conditions that block failover
- Global DR Readiness Dashboard for Isilon/PowerScale file services
- Based on best practices established by the National Institute of Standards and Technology (NIST)

In networking, “clustering” is the use of multiple servers to form what appears to users as a single, highly-available system. A web page request is sent to a “manager” server, which then determines to which of several other servers it should forward the request for handling. Cluster computing load-balances the traffic on high-traffic websites. Load balancing is basically dividing the work among multiple servers to accelerate processing so that users see results more quickly. Superna extends the cluster witness concept further by not only monitoring the cluster’s data replication, but also synchronizing and detecting changes in the configuration data outside the cluster to coordinate share, export, quotas and replication policies between arrays that are acting in Hot/Cold or Hot/Hot configurations. What’s more, many SyncIQ failover and failback functions can be easily automated with additional features found in Superna DR Edition.

QUICK, EFFICIENT REPLICATION

Disaster recovery requires quick and efficient replication of critical business data to a secondary site. Dell's SyncIQ delivers high-performance, asynchronous replication of data, providing protection from both local site and regional disasters, to satisfy a range of recovery objectives. SyncIQ's robust policy-driven engine allows customization of replication datasets to minimize system impact while still meeting data protection requirements.

Superna's DR Edition supports PowerScale SyncIQ by automating the failover process. Without Superna the failover process requires manual administrator intervention which is labor-intensive and can introduce risk through user error. With Superna DR Edition, complexity is minimized with one-button failover, along with updates to Active Directory, DNS, and client data access.

KEY FEATURES

VMware virtual appliance with web user interface for a simplified DR Dashboard View of all SyncIQ policies and related configuration synchronization across managed clusters.

Supports multiple Isilon clusters (both Hot/Cold and Hot/Hot cluster configurations).

DR Readiness Dashboard provides instant snapshot of data and configuration synchronization status between production and DR Isilon clusters.

Automatic Inventory/Discovery of Isilon cluster configuration shares/exports, permissions, quotas and SyncIQ policies.

Intelligent replication (only changes are replicated) of shares/exports required to access the data protected by each SyncIQ policy.

Custom configuration replication jobs allow non-SyncIQ shares/exports/quota configuration to be replicated to the DR cluster.

Automatic sync of share configuration properties including share permissions (SMB AD/LDAP, NFS).

Automatic audit of target DR cluster configuration data for DR readiness raises alarms if source and destination DR configurations are not in sync.

Change Management Support. Interactive GUI of configuration changes for clusters under management with daily email reports on add, modify or delete of cluster configuration.

Visual alarms and events – both display and email – for real-time notification of synchronization failures.

USE CASES

Use Case 1: Standby Cluster at DR Site (Hot/Cold). Cluster data is replicated with SyncIQ between production cluster and DR cluster. Cluster configuration (SMB shares, NFS exports, and their properties) is synced to the failover cluster to support end-to-end DR failover that includes data and configuration. No active shares or exports are present at DR site.

Use Case 2: Active Cluster at DR Site (Hot/Hot). Cluster data is replicated with SyncIQ between two clusters that both serve active clients and replicate independent data sets to each other. Cluster configuration (SMB shares, NFS exports, and their properties) is synced to the failover cluster to support an end-to-end DR failover. Active shares and exports are present at DR site.

ENABLES COMPLIANCE WITH NIST CYBERSECURITY FRAMEWORK

Created through collaboration between industry and government, the framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to better manage their cybersecurity-related risk.

Attribute	How Ransomware Defender Enables Compliance	Compliance
Identify	Threat identified by User Name and IP Address	✓
Protect	Stops the threat in real time with user lockout	✓
Detect	User behavior based, tripwire, and well-known extension detection	✓
Respond	Alerting email, syslog, and auto-matic snapshot creation	✓
Recover	File-level tracking and snapshot data recovery	✓

SUMMARY

Superna DR Edition helps enhance Disaster Recovery for Dell Isilon/PowerScale infrastructure with a solution based on the “cluster witness” concept that is a foundation of many highly-available systems. Superna helps to protect configuration data and real data (shares, NFS, quota, snapshots). It provides reporting in SyncIQ and enables simulated Disaster Recovery testing.

WANT TO LEARN MORE?

Interested in learning more about how Superna allows you to secure and protect your structured and unstructured data regardless of where it resides: on-prem, in the cloud, or in a hybrid environment? Contact us to speak to one of our data protection experts or to schedule a personalized demo.

For more insight into how Superna® can help solve your organization’s unstructured data security challenges, visit us at superna.io.

superna
Securing unstructured data, wherever it resides

superna.io
letschat@superna.io

20230731