

Technology Brief

Implementing the Right High Availability and Disaster Recovery Plan for Your Business

Date: August 2010 Author: Mark Peters, Senior Analyst

Abstract: IT budgets remain flat, yet businesses demand higher service levels for application availability in a 24/7 global economy. For this reason, organizations require a cost-effective high availability and disaster recovery (HA/DR) business continuity plan that is suitably fast, flexible, adaptable, and automated. Pressures for economic efficiencies are causing managers to rethink expense redundancy in their HA/DR plans.

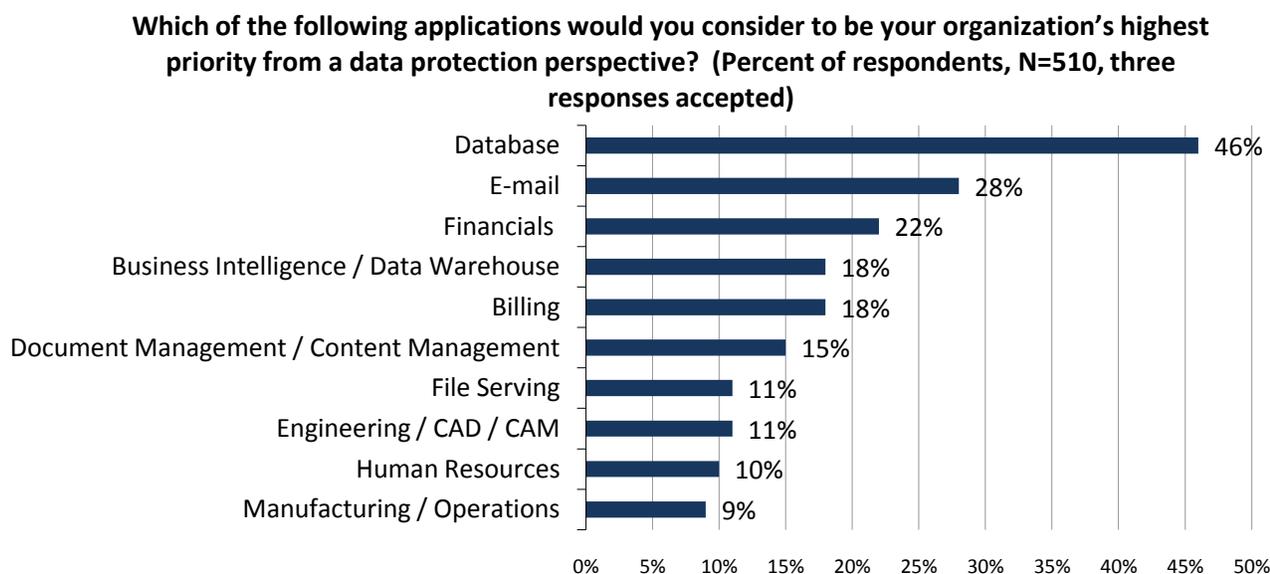
Is Data Replication Enough?

When asked about HA/DR planning, many IT managers immediately think about data replication tactics such as tape backup, off-site vaulting, and remote data replication. However, as important as an organization's data is, it is only a part of the broader requirement for business continuity. Even if the data is recovered, it is virtually useless if the appropriate application is not up and running. Similarly, applications need to be protected from system failures, human error, and natural or man-made disasters. This paper examines strategies that help organizations measure the importance of applications (or the impact of their lack of availability) to their business, followed by a discussion of common HA/DR configuration options.

Business Needs

Successfully aligning an IT infrastructure to business needs in the context of HA/DR planning requires far more than executive-level oversight. Business metrics for success and failure must be specifically linked with the details of both an infrastructure's current and desired states. It's the archetypal "do more with less" dilemma, only now with the added challenge to "do it better" as well. Looking for economic and operational advantage must be balanced with the need to adequately protect data and applications. The highest priority applications to be protected are shown in Figure 1 and can clearly be seen to be at the very heart of any organization.

Figure 1. Top Ten Applications for Data Protection



Source: Enterprise Strategy Group, 2010.

Protection Balanced Against Business Value

As the saying goes, you cannot manage what you cannot measure, so two things are important before anything else. The first is for a user to know the hardware and software required to manage and deliver IT services; and the second is to know the requirements to protect the business. Both require financial linkage through measurable objectives to serve the business optimally. *One measure serves to enumerate the value that an application returns to the business when it is running and the other enumerates the expense to the business when it is not.* Their values aren't the same. Generally, the cost of application downtime over time is far greater than the potential revenue the application can create when running. Therefore, the technologies used for business continuity can be thought of as "protection architectures."

The first objective in setting the goals of an investment strategy for these protection architectures is to develop a cost justification model for the expenses required to protect each application. If the expense to protect the application is greater than the value the application provides to the business, plus the cost to recover it, then optimizing the protection architecture to reduce the expense associated with protection is in order.

From Value to Architecture

To build appropriate protection architectures, IT managers must know the business value of the applications they are trying to protect and align that with technologies that results in a cost justified level of protection. It is important to make an implicit point explicit here: not every application deserves the highest level of protection money can buy. That seems reasonable, even obvious. However, in countless data centers, there is a desire to deploy a HA/DR plan with a "best that money can buy" mentality, even though that can exceed the practical needs of many applications. Often—whether because of a lack of personnel or simply too many demands placed on the personnel that exist—there just isn't enough time to think sufficiently about efficiency, which results in many data centers adopting a "one size fits all" strategy. And not that many vendors are going to complain about users buying more than they could, or should, have! So, if you wanted to get it right, where would you start?

Pragmatic Analysis and Planning

Step one, without a doubt, is to have a scheme to characterize and balance the value of the applications to be protected against the cost required to protect them. Different applications will have different values, but as they are analyzed, trends will begin to emerge. That is the time to assign applications a "protection class of service" justifying the protection cost, linked to a reference architecture that contains cost to a known technological approach. Think of it as a blueprint.

The best way to put some structure around the blueprint is to set some parameters for how you intend to protect each application; setting recovery objectives can do that. Recovery objectives include two major measurements that are used as the foundation for building protection architectures:

1. The **Recovery Time Objective (RTO)** is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) to avoid unacceptable consequences associated with a break in business continuity. For example, the RTO for a payroll function may be two days, whereas the RTO for sales order processing may be two hours.
2. The **Recovery Point Objective (RPO)** is the place in time (relative to the disaster) to which you plan to recover your data. Different business functions may have different recovery point objectives. RPO is expressed backward in time from the point of failure. Once defined, it specifies the minimum frequency with which backup copies must be made.

As the data in Table 1 shows, RPO and RTO objectives can be used as a guideline by a system administrator in order to ensure that an organization is employing the appropriate protection tiers to meet the various application objectives. The use of protection architectures defines how HA/DR solutions are used to physically and logically protect the applications to meet service levels defined by the RPOs and RTOs.

Table 1. Typical RTO and RPO Objectives for Various Data Types

| Protection Classifications | Protection Tiers | Availability Objectives | RPO | RTO |
|--|------------------|-------------------------|------------------------|------------------------------|
| <ul style="list-style-type: none"> • Mission Critical Data <ul style="list-style-type: none"> ○ Most valuable to an enterprise, high access ○ High performance, high availability, near zero downtime, highest cost | 1-2-3-4 | 99.999% | Continuous to 1 Minute | Instantaneous to 1.5 Minutes |
| <ul style="list-style-type: none"> • Business Critical Data <ul style="list-style-type: none"> ○ Important to the enterprise, average cost ○ Reasonable performance, good availability, less than eight-hour recovery | 2-3-4 | 99.999% | 1 to 10 Minutes | 2 to 15 Minutes |
| <ul style="list-style-type: none"> • Archive Online Data <ul style="list-style-type: none"> ○ Cost sensitive, low access, large volumes ○ Online performance, high availability, less than eight hours of recovery | 3-4 | 99.99% | 10 minutes to 2 Hours | 15 minutes to 2 Hours |
| <ul style="list-style-type: none"> • Archive Nearline Data <ul style="list-style-type: none"> ○ Cost sensitive, low access, large volumes ○ Less than one-hour access time, automated retrieval | 3-4 | 99.9% | 2 hours to 1 Day | 2 Hours to 1 Day |
| <ul style="list-style-type: none"> • Offline Data <ul style="list-style-type: none"> ○ Backup or compliance related ○ Very cost sensitive, limited access, ○ ~72-hour retrieval time | 3-4 | Offline | 1 Day to 1 Week | 1 Day to 1 Week |

What to Look for in Optimum HA and DR Implementations

Once a business impact analysis has been completed, it will be apparent that not all applications are equal and that different applications should be mapped to different protection tiers. Of course, if resources were fully abundant and/or free, then everything could have the best possible protection: since that is never the case, the intent of all the planning is to ensure that the available resources are allocated in an optimum fashion to the various applications (from the invariably revenue-impacting “tier-1” through to less vital materials on tiers 3 and 4). The constraints that limit the world from being perfect range from the pragmatic (such as cost, number of sites, and data growth) to the more prosaic (such as process errors, virtualization, and the need for testing).

Even when the business impact analysis has been done well and the resources allocated optimally, there is unfortunately still plenty of room for things to go wrong and throw a spanner in the works of all the apparently wonderful RTO and RPO planning. And users know that there’s not a lot of room for error. ESG research shows the very tight parameters that businesses are working with—53% of the respondents to a recent ESG survey said their organization would suffer *significant revenue loss or other adverse business impact if their Tier 1 applications were unavailable for anything from no time up to one hour*.¹ And even a slight deterioration in that RTO objective would rapidly make things worse; some small issue that took downtime over one hour (but still less than three) would cause the “significant negative impact” to apply to an additional 21% of tier-1 applications. Not to mention that, by this stage,

¹ Source: ESG Research Report, [2010 Data Protection Trends](#), April 2010.

nearly half (47%) of *tier-2* applications would also produce significant adverse impacts for their organizations. And what might the “small issues” be that could cause deterioration in the recovery time? The range covers awareness of the issue; not having some mix of the right people, configurations, or patches available; and actual error diagnosis.

All of this leads to the realization that effective HA/DR needs to be supported by solutions that can help avoid the negative impacts of small things destroying a plan that was based on good diagnosis and looked great on the whiteboard! Such solutions which can dramatically enhance and protect application availability should do the following:

- **Automate the process:** while most users will want to be notified that the system is being recovered per whatever plan is in place, automation is a good way to ensure that pressure and mistakes don't become a cocktail that causes errors to creep in to the HA/DR execution; automation reduces errors and will usually speed the process as well as reducing the reliance on specific individuals and teams.
- **Accelerate the recovery:** anything that can improve the speed of failover is invariably going to be a good thing. This will, of course, involve automation, but should also include solutions that mean failover is less of a *move* to something else and more of a *switch over* to something else that's already there—this, if you will, is like having the spare tire already fitted rather than having to pull over, jack up the car, and fit it (even though it could be argued that having an available and suitable spare at all is at least some level of DR!). Put another way, the best form of reconnection to a new application and storage is no actual reconnection at all; merely a switch to another available connection.
- **Ensure advance and regular testing:** both of the readiness and appropriateness of the response; readiness is testing that the system is functional, while appropriateness is testing that the system is fit for purpose. The above solutions—in combination with a thorough business impact analysis—will provide an overall “best practice” approach to HA/DR ... and help many an IT manager sleep better!

Symantec Offerings

While the purpose of this paper is mainly to inform users of what to look for with HA and DR, [Symantec](#) does have an impressive set of solutions to address the needs that have been outlined. While the key components are briefly summarized here, there is considerably more explanation of how they all function in the appendix to this paper:

- **Veritas Cluster Server (VCS):** this solution adds useful functionality to the basic automated failover requirements—it can move applications to the node that is most able to accept the new workload and can do that at local, synchronous (up to 100km) or asynchronous distances, utilizing either a spare node approach or rebalancing across all available nodes. Because Symantec tends to agnosticism whenever it can, the actual data can be replicated using just about any tool the user wants.
- **Veritas Cluster File System:** this is what provides the accelerated recovery; the clustering of file systems avoids many of the recovery steps involved in “classic” recovery processes (such as unmounting a file system, deporting and importing disk groups, and remounting the new file system) by, to continue the analogy, having the virtual “spare tire” already mounted.
- **Fire Drill (this is in VCS) / Disaster Recovery Advisor:** these are the testing solutions. The former can simulate a disaster to ensure that the clustering and failovers will work properly when needed; the latter supports VCS, but is separate and is all about whether the HA/DR configurations are fit for purpose. To use an analogy, rather than testing whether all the fire extinguishers and escape routes work (that's Fire Drill), it calculates whether the available extinguishers and escape routes are sufficient to cope with a potential fire and the number of people to evacuate.
- **Veritas Volume Replicator (VVR):** which provides application and storage hardware independent long distance data replication. Volume Replicator offers flexibility to choose any mix of SAN based storage architectures and replicate data over existing IP networks; this enables the implementation of lower cost storage at the DR location, which can result in significant savings.

The Bigger Truth

As is so often in IT, laborious work is required to achieve the payoff of an optimum HA and DR strategy. Knowledge of the applications and their business needs and impacts is first and foremost. And then the art of possibility and pragmatism must be applied to the science of the facts. Choices must be made, especially if the resulting plans are to be done in an “economically optimum” manner. The solutions that Symantec offers can certainly help, especially since the company is agnostic in terms of the applications and server/storage hardware with which it has to work. Having essentially one tool that can cover HA and DR across a wide range of applications and scenarios and distances is an advantage that many users would value and do well to investigate.

However, the most important thing for users is to realize that planning and thoughtfulness are key to this process; the title of this paper refers not only to the “right” HA/DR, but also to “implementing” it. Like any insurance policy, it is not always fun to discuss or to pay for, but also like any insurance policy, it is equally important not just to have one, but to ensure that the one you have is adequate for your needs and that it is going to work properly when needed.

ADDITIONAL NOTES: COMMONLY USED HA/DR CONFIGURATIONS

The following information is designed to add additional technical detail and insight to the business aspects covered in the preceding ESG Brief. The material discusses various clustering and data replication architecture options.

Application recovery solutions are designed to protect mission-critical applications running at the primary data center from a disaster that no longer allows those applications to run at that location. This could be a disaster as simple as a backhoe cutting all of the communications cables outside the primary data center or disconnecting external users from the applications. It could also be as severe as a major natural disaster (earthquake, tsunami, hurricane, tornado, pandemic, etc.) or terrorist activity. Application recovery solutions are designed to automate the process of recovering from a disaster and to ensure that not only is the mission-critical data protected by using replication, but also that mission-critical applications using that data are highly available locally and remotely in the event of a disaster.

Supported Application Recovery Configurations

There are basically two types of configurations in the application recovery model: Metro Clusters and Global Clusters. The difference is in how a failover is treated when going from one site to another. Is there a degree of control involved or is it fully automated? Both methods support local failover within the site.

Metro Clusters extend a single cluster between multiple sites and act at all times like a single cluster. The operator can configure failover ordering to always failover between systems located within the primary site before failing over to systems located at the disaster recovery site. However, when an outage affects all servers at one site, a failover to the second site will occur automatically. The single cluster solution is typically deployed in a metropolitan area, with full synchronous mirroring or replication and very reliable communications links between sites. In such cases, the company is essentially expanding the concept of high availability to include more than one data center. Assuming that all the infrastructure components are solid and that a business need exists to have full automated failover to a remote site, this is a very viable solution.

The following sections provide more detailed information on various cluster configurations.

Metro Clusters

Metro Clusters are single clusters that have been extended to more than one site. A Metro Cluster behaves exactly the same way as a cluster in a single site in terms of failover behavior. The underlying data transport mechanism between the sites provides for slightly different configurations in terms of the storage and how data from the primary site is “copied” to the disaster recovery site. The data can be replicated using application-based, host-based, or array-based replication. Metro Clusters can provide metropolitan area disaster recovery.

Metro Cluster with Replication

A Metro Cluster with Replication is a single cluster spread across two physical locations. This configuration eliminates the single point of failure represented by a single data center as it assumes independent power and communications at each facility. The Metro Cluster provides extended area high availability, which gives it the capability to provide disaster recovery automation at metropolitan distances. The extent of separation between the two data centers depends on the risks that the company wants to protect its environment from, but is limited at the margin by the requirement for synchronous replication. This typically is metropolitan in nature—less than 80 kilometers (50 miles). The nodes within each data center share storage at that data center. There is no shared storage between data centers, nor is there an extended SAN between the data centers. A Metro Cluster uses data replication to assure data access to all nodes at each data center. In a Metro Cluster configuration, if an application or a system fails, the application is restarted on another system within the current primary site or zone. If the entire primary site fails, the application is automatically restarted on a system at the remote secondary site (which then becomes the primary). In the event of a storage failure at the primary site, the cluster will detect that there has been a failure and will perform the operations necessary to prepare the storage at the disaster recovery site for production use and then restart the application using that storage.

Synchronous data replication keeps the copies of data at the two data centers synchronized. Asynchronous replication cannot be used for a Metro Cluster due to the potential for data loss during an automatic failover between sites.

Replication can take place at the application, host, and storage levels. Application-level replication products, such as Oracle Data Guard, maintain consistent copies of data between systems at the SQL or database levels. Host-based replication products, such as Veritas Volume Replicator, maintain consistent storage at the logical volume level. Storage or array-based replication products such as EMC SRDF or Hitachi Data Systems TrueCopy maintain consistent copies of data at the disk or RAID LUN level. Supported distances between data centers for synchronous replication are approximately 80 kilometers (50 miles) or less. The Metro Cluster configuration provides both local high availability and disaster recovery functionality in a single cluster.

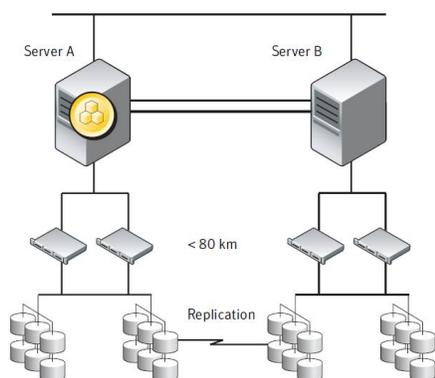


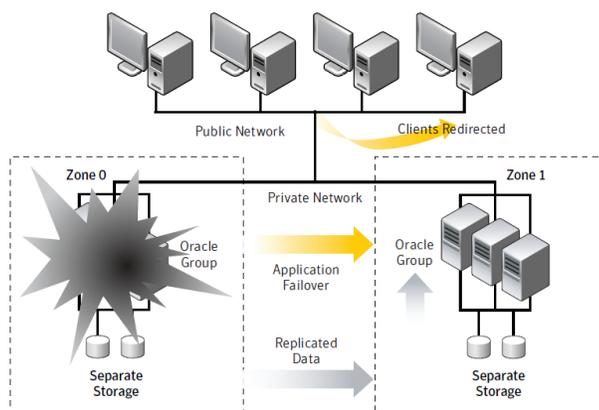
Figure 4. Metro Cluster with Replication

Notes Figure 1: Metro Cluster with Replication

A Metro Cluster configuration is appropriate in situations where dual dedicated cluster interconnects are available between the primary site and the disaster recovery secondary site, but there is no shared storage or SAN interconnect between the primary and secondary data centers. To understand how a Metro Cluster configuration works, consider the example of an Oracle database configured in a Veritas Cluster Server HA/DR Metro Cluster. The configuration has two system zones:

- Primary zone (zone 0) comprising nodes located at the primary site and attached to the primary storage
- Secondary zone (zone 1) comprising nodes located at the secondary site and attached to the secondary storage

Oracle is installed and configured on all nodes in the cluster. Oracle data is located on shared disks within each Metro Cluster zone and is synchronously replicated across Metro Cluster zones to ensure data concurrency. The Oracle service group (a service group within Veritas Cluster Server is the smallest unit of failover—it contains all of the resources that a mission-critical application needs to come online) is online on a system in the current primary zone and is configured to fail over in the cluster.

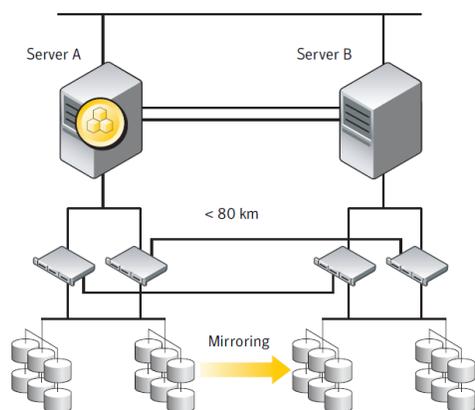


Notes Figure 2: Metro Cluster with Replication Failover Example

In the event of a system or application failure, Veritas Cluster Server HA/DR attempts to fail over the Oracle service group to another system within the same Metro Cluster zone. However, in the event that Veritas Cluster Server HA/DR fails to find a failover target node within the primary Metro Cluster zone, Veritas Cluster Server HA/DR automatically switches the service group to a node in the current secondary Metro Cluster zone (zone 1). Veritas Cluster Server HA/DR also redirects clients by bringing up the application IP address(es) at the zone 1 data center. The Metro Cluster with Replication configuration requires Veritas Cluster Server HA/DR to be installed on each server at each location and supports the use of VCS HA/DR Fire Drill for automated testing.

Metro Cluster with Mirroring

The Metro Cluster with Mirroring is a single cluster that spans two or more physical locations, similar to the Metro Cluster. The storage at one location is mirrored to the other using a data replication technology. Mirroring is a synchronous process. Unlike Metro Cluster with Replication, the storage at both data centers is connected using an extended SAN. Effectively, the user is configuring a RAID 1 mirror between two arrays at different sites. All data is written simultaneously to both mirrors. Reads can be configured to be serviced by the site where the application is currently running. The separation between the data centers has a practical limit in terms of performance of about 80 kilometers (50 miles). A Metro Cluster with Mirroring can also be configured using the concept of zones to set failover ordering to always attempt failover locally first.



Notes Figure 3: Metro Cluster with Mirroring

A Metro Cluster configuration is appropriate in situations where dual dedicated cluster interconnects are available between the primary site and the disaster recovery secondary site and there is an extended SAN connecting the shared storage between the two sites. The storage at one site is configured so that it will be mirrored to the second site.

For failures not involving storage, a Metro Cluster with Mirroring will have the exact same failover behavior as the Metro Cluster with Replication.

Global Clusters link two (or more) independent local clusters to form a global failover relationship for specific applications. Failover between local systems in either cluster is fully automatic. Failover between sites (i.e., clusters) requires operator confirmation. Enabling confirmation gives operators the ability to ask “what should I do?” in the event that local failover protection can no longer protect the mission-critical applications, and a decision has to be made around whether to perform an application recovery at the disaster recovery location. An operator can thus indicate:

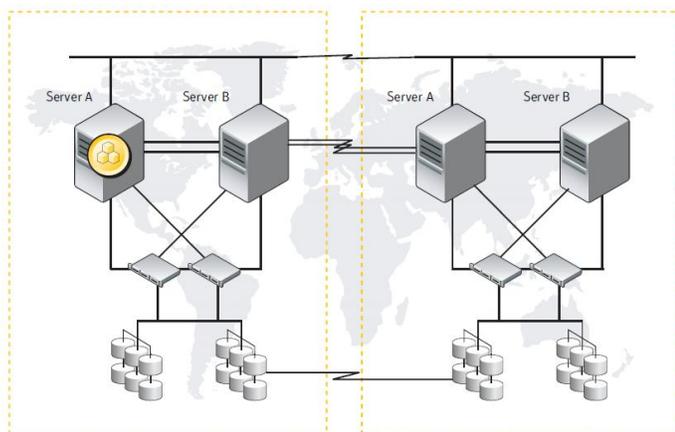
- “Yes,” we will incur a site failover. The local disaster is not expected to be resolved in the near future—or more specifically within our RTO limits—and it makes sense from a business perspective to bring all of the mission-critical applications up as quickly as possible at the disaster recovery site. In cases where an asynchronous replication technology is employed, this decision essentially accepts that the company will be coming up on somewhat out-of-date data.
- “No,” we believe that the disaster will be resolved shortly, within our RTO limits, and therefore we will not incur a site failover. It is less disruptive to stay at the primary site, even though the site is down, than it is to

incur a site failover to the disaster recovery site, and then another one to come back to the primary data center once the disaster has been resolved.

The decision to place an operator in the decision path with global clustering is usually recommended as it allows the business to assess the severity of the disaster with respect to the RTO goals of the mission-critical applications and then act accordingly. Manual disaster recovery failover control also eliminates the risk of faulty communications between sites, triggering an automated response. In many situations, site-to-site communications are provided by an outside vendor and may not always be as reliable as desired.

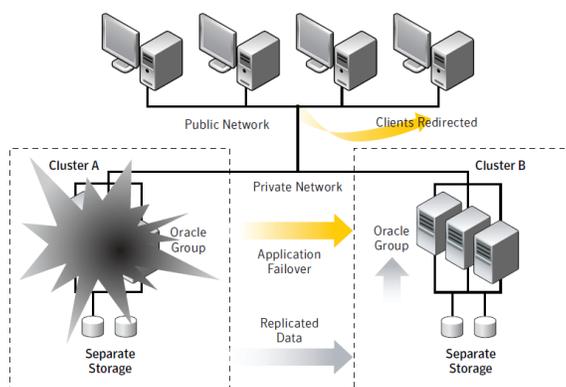
Global Clusters

A Global Cluster is a collection of 2-4 clusters in separate locations linked together to enable intelligent application recovery over any distance, i.e., globally. There is no shared storage between the clusters in a Global Cluster. Each cluster within the Global Cluster is connected to its own shared storage. A Global Cluster has a single primary cluster (i.e., site), and up to three secondary clusters (sites). The storage within the Global Cluster is replicated, either synchronously or asynchronously, from the primary cluster to each of the other secondary clusters. Typically, asynchronous replication over the wide area network (WAN) connecting the data centers is used, but synchronous replication can be used for shorter distances (less than 80 kilometers/50 miles). Local clustering provides local failover for each site or building. Metro Cluster configurations offer protection against disasters affecting very small geographic regions. Large-scale disasters such as major floods, hurricanes, earthquakes, and acts of terrorism can cause outages for an entire city or region. In such situations, a company can ensure global availability by migrating applications to sites located a considerable distance apart. Over the past few years, the best practice regarding the minimum distance separating the primary and disaster recovery data centers has grown from 50 to over 200 miles. In a Global Cluster, if an application or a system fails, the application is migrated to another system within the same cluster. If the entire cluster fails, the enterprise can make a business decision as to whether or not to move operations to one of the alternate disaster recovery sites. If the decision is to move to a specific disaster recovery site, the application is automatically restarted on a system in the cluster at that disaster recovery site(s).



Notes Figure 4: Global Cluster

Now consider the example of an Oracle database configured in a Veritas Cluster Server HA/DR Global Cluster that connects two clusters together. Oracle is installed and configured in both clusters. Oracle data is located on shared disks within each cluster and replicated across clusters to ensure data concurrency. The Oracle service group is online on a system in cluster A and is configured to fail over globally, on clusters A and B. Veritas Cluster Server HA/DR continuously monitors and communicates events between clusters. Inter-cluster communication (ICMP-based) ensures that the Global Cluster is aware of the state of the global service group at all times.



Notes Figure 5: Global Cluster Failover Example

In the event of a system or application failure, Veritas Cluster Server HA/DR fails over the Oracle service group to another system in the same cluster. If the entire cluster fails, Veritas Cluster Server HA/DR alerts the operator and provides an opportunity for action. The operator may declare a “disaster,” which indicates that the primary data center has been lost, (at least as far as the application is concerned—this might perhaps be the result of a localized power outage) in which case operations are migrated to the disaster recovery data center automatically. Or the operator may declare an “outage” and decline to allow failover in cases where local restoration of service will happen in a short (or at least acceptable) period of time. In either case, a business decision must be made regarding whether or not a failover is in the enterprise’s best interests, considering RTO limits and what is known about the particular disaster. The Global Cluster configuration requires Veritas Cluster Server HA/DR installed on each server at each location and supports the use of VCS HA/DR Fire Drill for automated testing.

Replication Support in Metro and Global Clusters

Clustering technologies need to support a wide variety of replication products to completely automate the process of replication management and application startup at the remote site without the need for complicated manual recovery procedures involving storage and application administrators. The clustering solution should provide all the necessary logic to completely control the underlying replication configuration, whether that replication operates:

- At the storage array level (e.g., EMC SRDF)
- At the database level (e.g., Oracle Data Guard)
- Synchronously or asynchronously

Depending on the type of failure, this control may involve reversing the direction of the replication (otherwise known as role reversal, role swap, dynamic swap, or personality swap) or simply moving the data and applications back when the original site comes back online. This solution should also include the capability to select automatic or operator-confirmed site-to-site failover.