CenturyLink® Business

WHITE PAPER

Three Pillars of Effective Disaster Recovery

WHITE PAPER

Three Pillars of Effective Disaster Recovery: DRaaS + Networking + Managed Hosting

Disaster Recovery is following the paths of other key IT functions: regular change and constant growth. The chief agents of change for Disaster Recovery ("DR") are virtualization and its constant companion, the cloud. Growth in DR is driven by the reliance on ever-larger bodies of data coupled to the risk of losing the ability to transact business if that data is not accessible. Disaster Recovery is a necessity for almost every IT organization. This white paper reviews the three pillars that constitute an effective and cost-efficient Disaster Recovery solution.

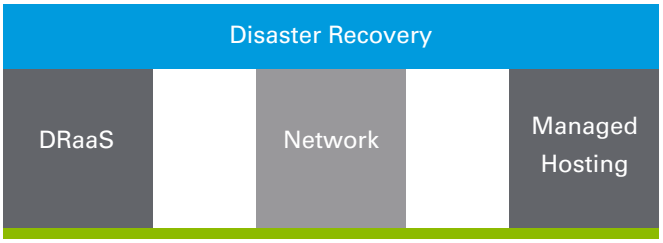
The Pillars

The technology industry overuses architectural metaphors such as "framework," "foundation" and "platform." This white paper adds "pillar" to the list but appropriately so as modern Disaster Recovery does in fact have essential components upon which it must stand.

The first pillar is Disaster Recovery-as-a-Service ("DRaaS"). DRaaS a cloud-based service with computing and storage resources to back-up data, run applications, test/simulate disaster events and manage the migration of services.

The second pillar is Networking. Since DRaaS is a cloud-based service network connectivity is a must-have. In fact, in the context of DRaaS there are two networking choices: robust network connectivity and failure.

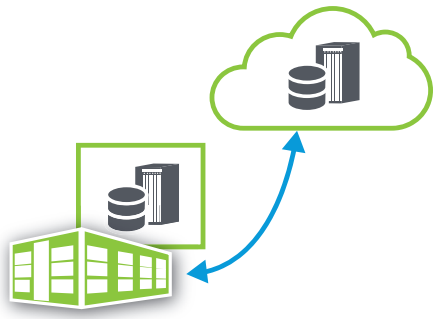
The third pillar is Managed Hosting the server, networking and other infrastructure that is owned and operated by a third party provider in their data center specifically to support your applications and related services. Many organizations used Managed Hosting to reduce CapEx, outsource system management and take advantage of contractual Service Level Agreements. Managed Hosting is a pillar of the Disaster Recovery puzzle because in the event of a catastrophe business continuity may require you to run applications out of an offsite data center in conjunction with replicated data, also stored offsite.



Consider the interactions of DRaaS, Networking and Managed Hosting when defining DR requirements as they collectively form the footing of an effective DR solution.

Pillar #1: DRaaS

Disaster Recovery-as-a-Service uses virtualization technology to deliver economic advantages over dedicated DR. DRaaS complements the computing resources of a Virtual Private Cloud allowing DRaaS to replicate data and run the applications that power an organization. Since many applications run in the cloud today there is natural synergy between Disaster Recovery and the cloud service model.



CenturyLink® Business

DRaaS affords meaningful advantages over other Disaster Recovery options:

- Your data is stored safely off-site
- If your on-premise data center already uses virtualization DR may be managed using existing hypervisor and VM management tools
- The service is an Operating Expense: capital outlay is limited
- You can easily and quickly flex DR capacity upwards or downwards as needed

If after assessing DRaaS you conclude that it meets your needs, probe on the following points when assessing a vendor and their offering to determine they will be a suitable pillar of your DR solution:

1. Can DRaaS management be integrated with your current on-premise IT management tools?
2. How and how well will it back-up my email?
3. Is the vendor stable and certain to be around when I need them? Is the technology proven?
4. Can I choose the specific location where data is stored and the service runs?
5. Do they offer support services or will there be a lot of "DIY" work to do?
6. Does it scale up and down easily to support changing requirements?

Pillar #2: Networking

If you employ DRaaS in conjunction with a virtualized IT environment, on-premise or collocated, a network link is needed to move data to the Disaster Recovery service in the cloud. The link is also used to command & control DRaaS for testing, migrating Virtual Machines in the event of a disaster and to do Failback when the disaster event is resolved.

One option for this link is a public Internet connection. Most organizations can do this without buying new hardware as it utilizes an existing service. But as they say, "There is no such thing as a free lunch." A public Internet connection may or may not be sufficiently reliable for the DR function. Its bandwidth may already be saturated and security is probably insufficient for critical applications. While a public Internet link is inexpensive and can work, relying on one for DR inserts a weak link into the chain.

The alternative is a dedicated DRaaS link, called "Direct Connect" by some vendors. A dedicated connection is a discrete communications service that must be ordered and provisioned, but in doing so provides the latitude to choose a service that meets your specific needs.

Four common network service options for Direct Connect are:

MultiProtocol Label Switching ("MPLS")

- An IP-based virtual private routed network
- Has a flexible topology with any-to-any VPN connectivity
- Uses the networking vendor's router hardware

Virtual Private LAN Service ("VPLS")

- An Ethernet-based multipoint virtual private network
- Has a flexible topology with dedicated links
- Uses your router hardware

Metro Ethernet ("Metro-E")

- A point-to-point Metro distance virtual circuit
- Employs a cost-effective dedicated link in Metro areas
- Uses your router hardware

Ethernet Virtual Private LAN ("EVPL")

- A point-to-point virtual circuit
- Employs a cost-effective dedicated link that can span long distances
- Uses your router hardware

Relative to an Internet connection, a dedicated connection offers more reliable packet delivery, better security and lower latency at an extra cost. The flexibility of MPLS makes it a popular choice for enterprise network services although DRaaS can also work successfully with VPL, Metro-Ethernet or EVPL. A full service networking provider can offer you all these choices, and possibly others.

The final aspect of the networking pillar is access to major or "Tier 1" network backbone. If your network/DRaaS provider has direct access to a Tier 1 backbone they will be better able to manage throughput and correct network problems quickly. When assessing a networking vendor ask if they have this.

Pillar #3: Managed Hosting

While all computing appears to be migrating to the cloud, Managed Hosting remains a mature and important service. A well-managed Hosting facility is an excellent choice for hosting:

- Enterprise applications (email, HR, ERP, finance, etc.)
- Data storage
- Websites and web-related services
- Databases

One advantage of Managed Hosting is that it you outsource the management tasks for hardware, operating systems and software. Hosting vendors can also help you scale computing, storage, space, power and cooling to meet changing needs. Hosting vendors are "in the business" of providing redundancy and security to industry standards, relieving you of yet another burden. Finally, Hosting vendors operate data centers in a variety of locations letting you choose the optimum spot to host your infrastructure.

If DRaaS is used in conjunction with Managed Hosting the production compute resources, applications and data can reside in the same facility as DRaaS. The link between production resources and DRaaS will be a fast and low cost LAN connection, called a "Cross Connect" by some vendors. This connection does not use wide area network services and does not affect your public Internet access.

To assess Managed Hosting as a pillar of your DR solution you should investigate these points with prospective vendors:

- How many data center sites do you have? Where are they? Location is more than a convenience. A nearby location reduces network latency which in turn improves data replication. These are key to DRaaS.

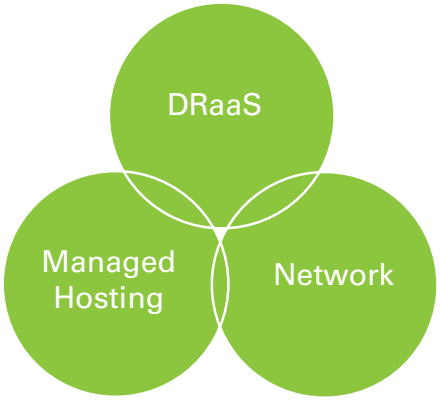
- What network connectivity services do you offer? A range of networking services improves access to the Hosting sites. If the vendor owns and operates its own network it can offer more choices and better manage the connectivity.
- How is security ensured? This encompasses network security (DDoS protection, threat detection, etc.) as well as physical security.
- What support is available? Beyond space and power a vendor should offer Service Level Agreements that spell out all metrics related to support, security, power, cooling, availability and facility management.
- Do you offer and support DRaaS?

Summary

A comprehensive Disaster Recovery strategy is essential for many if not all organizations. The now-infamous "Sony Hack" of November, 2014 drove this point home further because not only were there serious security breaches, data was permanently erased.

Several DR options exist, and Disaster Recovery-as-a-Service is a sound and cost-effective choice.

Coupling DRaaS with Networking and Managed Hosting services create a "golden age" for Disaster Recovery where ease-of-use, economics and speed are derived from these three pillars of technology.



About CenturyLink Business

CenturyLink Business delivers innovative managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in cloud infrastructure and hosted IT solutions for enterprise customers. Parent company CenturyLink, Inc. is the third largest telecommunications company in the United States, and empowers CenturyLink Business with its high-quality advanced fiber optic network. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations.

For more information visit www.centurylink.com/technology.

Global Headquarters
Monroe, LA
(800) 728-8471

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6591 8824

601011315 - WP150387

CenturyLink® Business