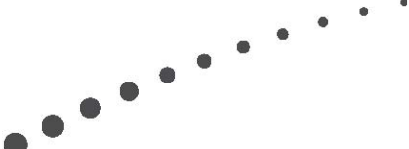




Citrix Cloud Solution for Disaster Recovery





Contents

- Introduction..... 3
- Fitting Disaster Recovery to the Cloud 3
- Considerations for Disaster Recovery in the Cloud 3
- Citrix Cloud Solution for Disaster Recovery 6
- Summary 10

INTRODUCTION

Interruption of application and data availability can cost enterprises significant lost business. While clustering and RAID can protect applications and data within a datacenter, they do not prevent events (e.g., fire, flood, power failure, or cable cuts) that make an entire datacenter inaccessible. Businesses need disaster recovery (DR) solutions that enable business continuity.

FITTING DISASTER RECOVERY TO THE CLOUD

Cloud-based delivery of DR services provides a powerful alternative to the cost and complexity of dedicated “hot-site” standby facilities, flexibly addressing the recovery-time and recovery-point requirements of diverse applications to keep enterprises running cost-effectively in event of site failure.

Lower cost. In the cloud, the coupling of virtualization with flexible replication and backup/recovery technologies can achieve more cost-effective scenarios without sacrificing business priority. By delivering disaster recovery in the shared infrastructure of the cloud, costs of multiple technologies can be applied across a range of organizations and applications, bringing economies of scale.

Increased Flexibility. Cloud flexibility enables DR solutions to be implemented in traditional active-active configurations, but also enables IT organizations to take advantage of multiple live sites, whether internal or external, to provide cross-cloud protection for distributed processing, and to provide “Cloud Burst” capacity for dynamic resource requirements.

Moreover, the same technologies that provide disaster recovery services between enterprise and cloud data centers also apply within the cloud provider’s domain, keeping customers protected in the face of failures affecting the cloud provider’s datacenter.

CONSIDERATIONS FOR DISASTER RECOVERY IN THE CLOUD

Leveraging the power and flexibility of the cloud to provide disaster recovery requires the coordination of virtualization, networking, storage, data protection, replication, and orchestration. To secure business continuity across a range of organizations and their applications, the process of implementing a cloud-based disaster recovery solution must involve:

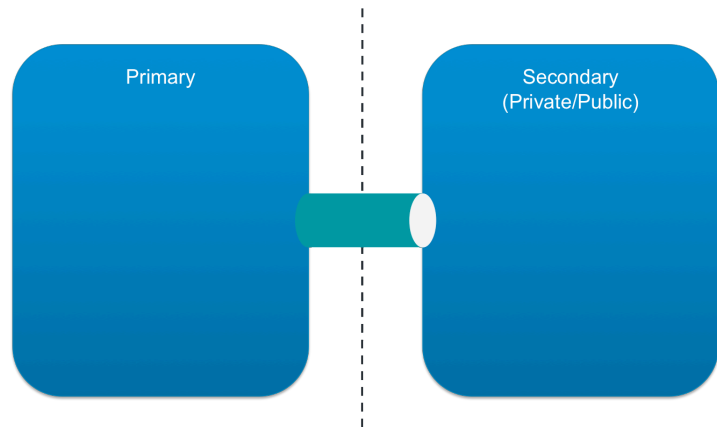
1. Define RTO and RPO

Each protected application or team of applications has characteristics that determine location, bandwidth, and protection requirements for the DR configuration associated with it: the recovery time objective (RTO), which identifies how long it takes for processing to come online and be available at the secondary site after a failure occurs, and the recovery point objective (RPO), how up-to-date the data copy at the secondary site must be for business processes to operate. Before

sites, storage, and network connections can be configured, users must be able to enter the RTO and RPO requirements into the process.

2. Select DR sites

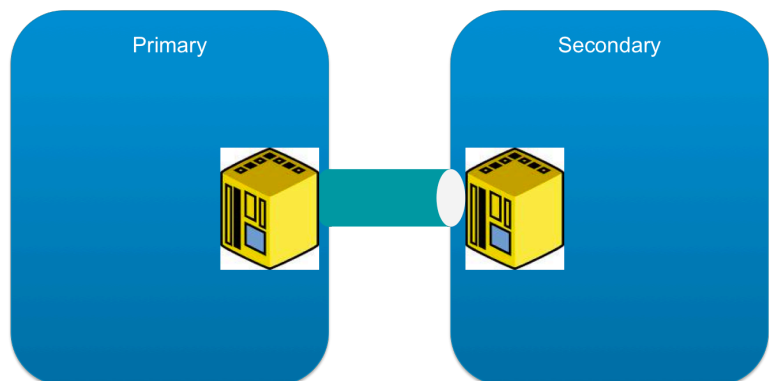
The selection of the DR site must include consideration of both geographic and network-topological location. Optimal distance to both the primary site and to the user base accessing the applications at the secondary site must be achieved, in order to guarantee acceptable latency and bandwidth, both for user access and for replication capabilities sufficient to achieve desired RTO and RPO. For active-active configurations, these requirements must be met bi-directionally, and should also be capable of delivering performance for bursting scenarios.



3. Deploy storage resources

Secondary sites must have available enough storage capacity to host synchronized copies of applications and their data for deployment during recovery. In an active-active configuration, these instances will be in service providing additional live capacity for bandwidth and latency optimization, or scaling up capacity in Cloud Burst scenarios. Many organizations choose to optimize the performance and capabilities of their storage configurations by choosing homogeneous storage systems between sites, or choosing providers with storage that is compatible with their own; with most multi-tenant configurations, whether internally between organizations within the same enterprise or externally at public cloud providers, heterogeneous deployments may be desirable.

To be broadly applicable, a solution must support a wide range of synchronization/replication and data protection technologies, including homogeneous-storage solutions from storage system vendors as well as software-based offerings from software suppliers.

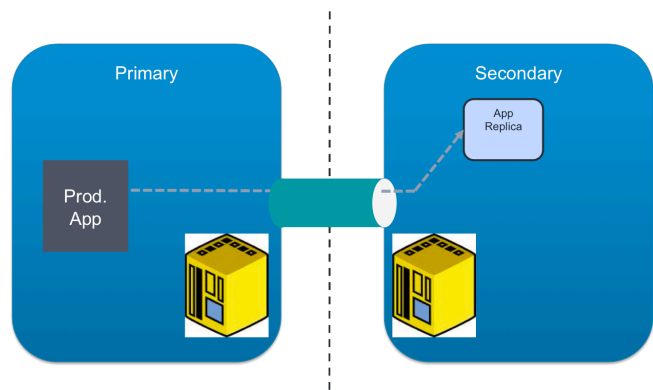


4. Configure seamless access across multiple sites

For applications to be deployed across multiple sites – some of which, in the case of external cloud DR protection, may be partly under the control of other business entities – network access and security must be extended across the bridge between sites, making access secure and seamless. Since an outage of the primary site will result in inability to access directories and other infrastructure information, the authentication and authorization infrastructure must be replicated at the secondary site and (if an active-passive configuration) enabled during failover.

5. Onboard applications and data

The customer’s applications and data must be initially synchronized to the cloud provider’s resources, using a combination of tools including virtual format conversion, backup, and storage replication. In fact, this is often accomplished, especially with higher data volumes, by shipping tapes or disk drives to the secondary site, then synchronizing recent updates. Because the virtualization platform in use on-premise may differ from that deployed by the provider, migration tools with multi-format support are required to establish the recovery site.



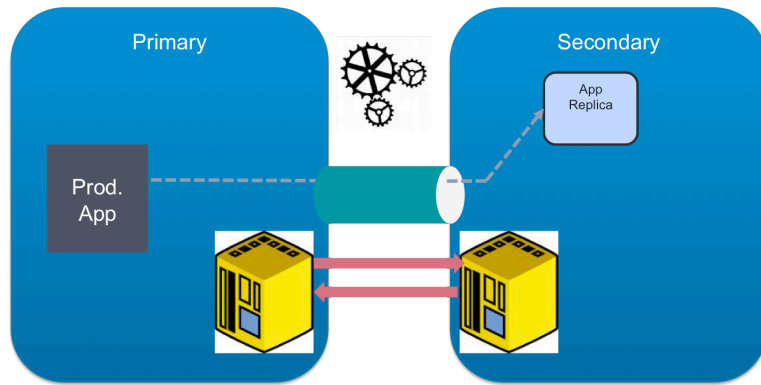
6. Configure replication and synchronization for RTO/RPO optimization

Depending on the RTO and RPO for each application, the proper choice of synchronous or asynchronous replication or backup/restore tools must be made.

Ongoing synchronization of data, as well as application updates, must be performed to meet the recovery objectives of each protected application. In homogeneous environments, this capability is likely to be delivered efficiently by the storage systems; in heterogeneous configurations, additional replication and synchronization software is likely to be required.

7. Develop and test orchestration of recovery scenarios

It must be possible to build the orchestration of the steps required to bring applications online at the secondary site, including application, data, and network configuration, as well as accessibility of the applications at the secondary site as required (whether from internal access points or from the Internet). It must be possible to test steps separately and incrementally, then with full orchestration, non-destructively. (Orchestration and testing of failback scenarios must be possible as well.)



8. Implement security and audit of secondary site operations

Business continuity solutions do not obviate the other requirements on an organization’s applications. Considerations such as access control and audit apply at the secondary site as much as at the primary datacenter – in fact, become even more important when running in the cloud provider’s shared infrastructure – and these processes must be extended to the secondary site.

CITRIX CLOUD SOLUTION FOR DISASTER RECOVERY

The Citrix Cloud Solution for Disaster Recovery leverages virtualization, networking, storage, data protection, replication, and orchestration technologies to provide cloud-based DR capabilities that can be configured to address the recovery requirements of a wide range of organizations and applications.

Based upon the Citrix Cloud Solution for Disaster Recovery reference architecture, Citrix Cloud Partners use a combination of their own internally developed technology and processes coupled with infrastructure from Citrix and partners to meet these requirements.

Requirement	Citrix Cloud Solution Capability
Automate the complex workflows for restoration of application availability, and support non-destructive testing of failover and failback	Recovery Orchestration and Testing
Assure ongoing data and application consistency to satisfy RTO and RPO requirements	Data Synchronization/Replication
Implement backup/recovery and related tools for data protection at	Integrated Data Protection

secondary site	
Deliver updates of applications and data cost-effectively to secondary site datacenter	Data Optimization
Provide high performance and high availability for a wide array of host-based and networked storage configurations	Heterogeneous Storage Support
Make user-facing applications and interfaces accessible from any location using a wide range of endpoint devices	Hosted App Delivery
Leverage identity management infrastructure within the enterprise, and replicate it to the secondary site for authentication and authorization during primary site failure	Cloud Access Services
Seamlessly connect the enterprise datacenter and the cloud datacenter with full security, performance and network transparency	Cloud Bridging Services
Provide transparent optimized external and internal access to applications and data, delivering global access and Cloud Burst support	Edge Networking Services
Implement flexible, scalable platform for deploying and managing applications at secondary site, scaling compute resources as required to satisfy SLAs	Platform Virtualization Services

Recovery Orchestration and Testing

Workflow-driven automation of operation sequences bringing data and applications online in satisfaction of service level agreements (including RPO and RTO objectives as well as runtime availability and performance SLAs) at the secondary site, as well as failback to the primary site.

Effective solutions must be testable without interruption to primary sites, must be deployable in both active-active and active-passive configurations, and must orchestrate the reconfiguration of compute and storage resources as well as infrastructure network access.

To learn more about how StorageLink Site Recovery Services, a feature of the Platinum Editions of XenServer and Citrix Essentials for Microsoft Hyper-V, provides these functions [click here](#).

Data Synchronization/Replication

Depending on RTO/RPO requirements, the ability to assure that data at the secondary site reflects appropriate changes from the primary site, whether based on hardware tools for homogeneous



storage, software tools for heterogeneous storage, or even on guest-level tools to align closely to the protection and recovery requirements of individual applications.

Data synchronization/replication services are supported between homogeneous storage hardware by Citrix Ready Open Storage system suppliers, and between heterogeneous storage environments by Citrix Ready Open Storage software partners, integrated with the StorageLink services in Citrix XenServer and Citrix Essentials for Hyper-V. *For more information please [click here](#).*

Integrated Data Protection

These tools offer ongoing protection at the secondary site. In addition, for less stringent RTO and/or RPO, use of backup/recovery tools instead of live synchronization is more cost effective. As with synchronization/replication technologies, Citrix StorageLink Open Storage partners and Citrix Ready partners provide best-of-breed tools integrated with the Citrix Cloud Solution for Disaster Recovery.

Data Optimization

Compression and encryption techniques can reduce the requirements for storage and for network bandwidth needed for synchronization. These capabilities can be delivered by networking technologies (Citrix NetScaler and Citrix Branch Repeater), by storage systems, or by the two technologies working together.

Heterogeneous Storage Services

Different storage architectures (DAS, NAS, SAN) may be used in different organizations and across premises, as well as variation in storage network infrastructure (iSCSI, Fibre Channel). The flexible DR solution requires the ability to mix storage architectures and storage networks between sites.

Hosted App Delivery

Citrix XenApp™ incorporates built-in redundancy capabilities that can enhance a disaster delivery solution and enable secure access to applications at the secondary site. *For more information on how Citrix XenApp enables on-demand delivery of applications to any device over any network, [click here](#).*

Citrix Open Cloud Framework

Cloud framework services provide the foundational logic for rapidly provisioning, managing and controlling workloads deployed into multi-tenant, shared infrastructure clouds. The cloud framework ensures policy enforcement and security, and provides for integration with existing services such as billing, metering and self-service portals. Interoperability with other popular Cloud interfaces, and extensibility of the framework itself, provide the flexibility to leverage existing investments when migrating between clouds.

For more information on how Citrix CloudController provides an extensible, full-featured policy engine for controlling a heterogeneous, multi-tenant environment, [click here](#).

Cloud Access Services

Users must be able to authenticate to applications whether they are running at the primary or secondary sites. In active-passive configurations, this requires replication of directories; in active-



active configurations, bidirectional replication can be used to increase performance as well as availability.

Citrix CloudAccess™ is a pragmatic solution to the cross-domain authentication problem that leverages existing enterprise infrastructure and works to extend the policy framework that has already been put in place. Features include: Unified Password Management for SaaS, SSO to Cloud/SaaS applications, Password Workflow Automation, support for all major SaaS providers, and integrates into the with full transparency. Benefits include: Improve security across all applications, no end user training required standardizes password policy across both internal and external applications, automatically removes access to applications for users removed from the enterprise authentication framework, and simplifies password reset for end users.

For more information on Citrix CloudAccess, [click here](#).

Cloud Bridging Services

When services are running at the secondary site, it is desirable that no reconfiguration be required in client software or other applications, making failover and failback as transparent as possible. While this “bridge” does incorporate VPN services for security, the bridge is much more than a VPN tunnel. Strategically, the key role of the bridge is to provide an overlay network across physical and virtual topologies, making the cloud a seamless extension of the enterprise network. With the cloud a transparent extension of the enterprise network, migrating application workloads becomes far easier since the applications network-specific configurations won’t need to be overhauled.

For more information on Citrix CloudBridge, which leverages key capabilities within Citrix NetScaler, Citrix XenServer and Citrix Branch Repeater, please [click here](#).

Edge Networking Services

Edge networking services are critical to ensuring the reliability, security and performance of any cloud-based offering. Properly deployed, these services are largely transparent to the cloud consumers, yet are fundamental to ensuring the cloud remains available in the face of natural and man-made disasters, hacker attacks, planned and unplanned network and server outages and unanticipated surges in traffic.

Citrix NetScaler is an integrated Web application delivery controller that provides advanced traffic management through Layer 4-7 load balancing and content switching. Global server load balancing provides critical business continuity and disaster recovery support during site-level disruptions and outages. NetScaler also includes application security via a web application firewall and SSL VPN. *For more information on Citrix NetScaler, [click here](#).*

Citrix Branch Repeater, available as a physical or virtual appliance, is a WAN optimization solution that provides a high definition desktop and application experience to branch and mobile users while dramatically reducing WAN bandwidth costs and simplifying branch infrastructure. Branch Repeater accelerates desktop and application delivery, decreases WAN bandwidth consumption, and enables server consolidation. *For more information on Citrix Branch Repeater, [click here](#).*



Platform Virtualization Services

Server, storage and network virtualization are linchpins of the flexibility, affordability and scalability of any cloud-based offering. By simultaneously optimizing resource utilization through consolidation while still maintaining full isolation, virtualization supports the cost effectiveness of cloud offerings. By abstracting workloads from the underlying physical resources that run them, virtualization enables the elasticity needed for cloud services to be made available on-demand and self-service.

Citrix XenServer™ is the only enterprise-class, cloud-proven server virtualization platform that delivers the critical features of live migration and centralized multi-server management at no cost. XenServer is an open and powerful server virtualization solution powered by the industry-standard Xen® hypervisor, and created by the inventors of Xen. *For more information on XenServer, [click here](#).*

Citrix NetScaler VPX provides complete NetScaler functionality in a simple, easy to install virtual appliance. With NetScaler VPX, load balancing and web application acceleration, security and offload are available as virtualized services anywhere within the cloud. *For more information on Citrix NetScaler VPX, [click here](#).*

SUMMARY

The Citrix Cloud Solution for Disaster Recovery combines the cost-effectiveness and scalability of virtual infrastructure and pay-as-you-go cloud-based capacity with the capabilities of intelligent storage hardware, software capabilities, and networking to:

Reduce the CapEx and OpEx costs associated with maintaining dedicated standby capacity at enterprise-owned secondary sites or dedicated DR provider datacenters

- Leverage economies of scale in storage and networking resources
- Enable flexible configuration of protection and recovery scenarios to satisfy varying RTO/RPO and service level objectives, as well as gaining extra savings from active-active configurations and Cloud Burst capacity
- Benefit from repeatable expertise in defining robust scalable infrastructure as well as in recovering multiple applications and storage technologies
- Design and iterate recovery and failback scenarios and test them non-destructively



About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was \$1.6 billion.

©2010 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, HDX™, XenServer™, XenApp™, XenDesktop™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.