Solution Design Overview

Cisco offers the Disaster Recovery as a Service (DRaaS) Solution architecture. This architecture enables Cloud Service Providers (CSPs) to offer Disaster Recovery (DR) services to workloads outside of the service provider's management domain that are in customer premise environments or in colocated environments. Service providers can also offer data protection and data survivability services to workloads within the cloud provider's Virtual Port Cloud (VPC) environment and management domain.

This chapter includes the following major topics:

Previous releases and white papers for the DRaaS Solution validated DR solutions from Cisco partners (InMage and Zerto) overlaid on Virtual Multiservice Data Center (VMDC) Version 2.3. This allowed VMDC-enabled CSPs to enhance their addressable market, improve financial performance, and differentiate from commodity/public cloud solutions.

Release 2.0 of the DRaaS Solution architecture, which is described in this document, is designed to provide a new set of DR-related capabilities by leveraging new features of the recently released Cisco VMDC Virtual Services Architecture (VSA) Version 1.0 system. This release of the DRaaS solution increases VMDC-enabled CSP differentiation by adding new, advanced network and operations features to the solution, including the following:

- Secure WAN connectivity.
- Layer 2 domain extension via Overlay Transport Virtualization (OTV) with Cisco Cloud Services Router (CSR) 1000V.
- IP mobility and path optimization via OTV and Locator/ID Separation Protocol (LISP) with Cisco CSR 1000V.
- Partial failover capabilities utilizing OTV and LISP.
- Provider multi-tenant services infrastructure based on VMDC VSA 1.0.
- Make use of the stateless computing capability of Cisco Unified Communication System (UCS) servers for dynamic addition of compute resources at the DR target, using UCS service profiles and UCS Director.

What is Disaster Recovery as a Service?

For CSPs, the traditional DR system constitutes a substantial portion of expenses annually. A cloud-based DR system uses a "pay as you go" model and minimizes the impact of downtime through continuous data replication to the CSP cloud. Protected machines can be recovered in the CSP cloud in a matter of minutes rather than hours, enabling business continuity when a disaster event is identified. See Figure 1-1.

The most important end user consumable service being enabled by this system architecture is enabling service providers to offer disaster recovery for both physical and virtual servers from a customer data center to a service provider VPC. The key requirements for DRaaS are Recovery Point Objective (RPO), Recovery Time Objective (RTO), performance, consistency, and geographic separation. RPO is the maximum amount of data loss tolerated during disaster recovery and RTO is the maximum amount of time that can be used to restore services.

CSPs that deploy the DRaaS Solution architecture detailed in this guide can offer the following end user-consumable services for both physical and virtual servers on an aaS (as-a-Service) basis:

- **DRaaS to the Cloud**—Disaster recovery for both physical and virtual servers from a customer data center to a service provider VPC. Targeted at mid-market end-customers with 250-1000 employees. See Figure 1-1.
- **In-Cloud Disaster Recovery (ICDR)**—Disaster recovery of selected virtual machines (VM) hosted in a CSP VPC environment to a remote CSP VPC environment. See Figure 1-2.

Figure 1-1 DRaaS to the Cloud

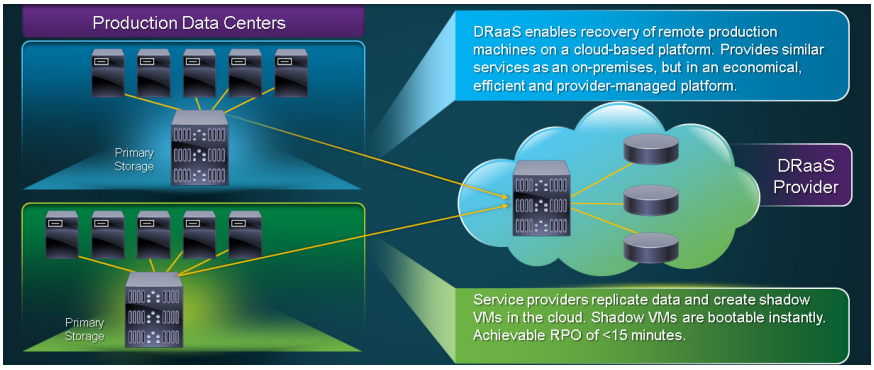
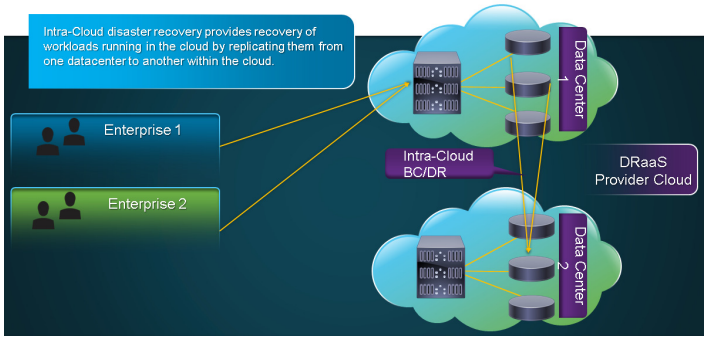
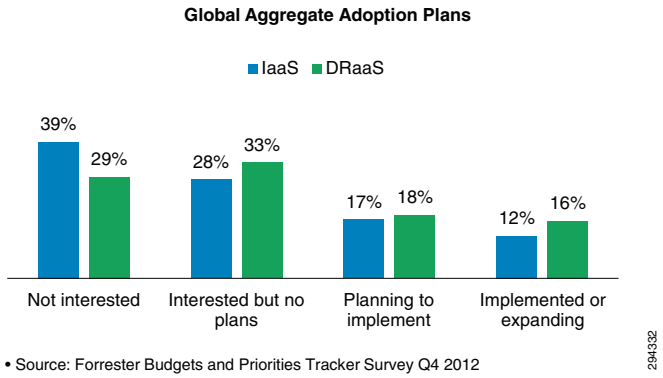


Figure 1-2 In-Cloud Disaster Recovery (ICDR)



The global DRaaS and cloud-based business continuity market is expected to grow from $640.84 million in 2013 to $5.77 billion by 2018, at a CAGR of 55.20%. The market presents a strong opportunity for the CSPs to take advantage of the demand for DRaaS services, as illustrated by Figure 1-3.

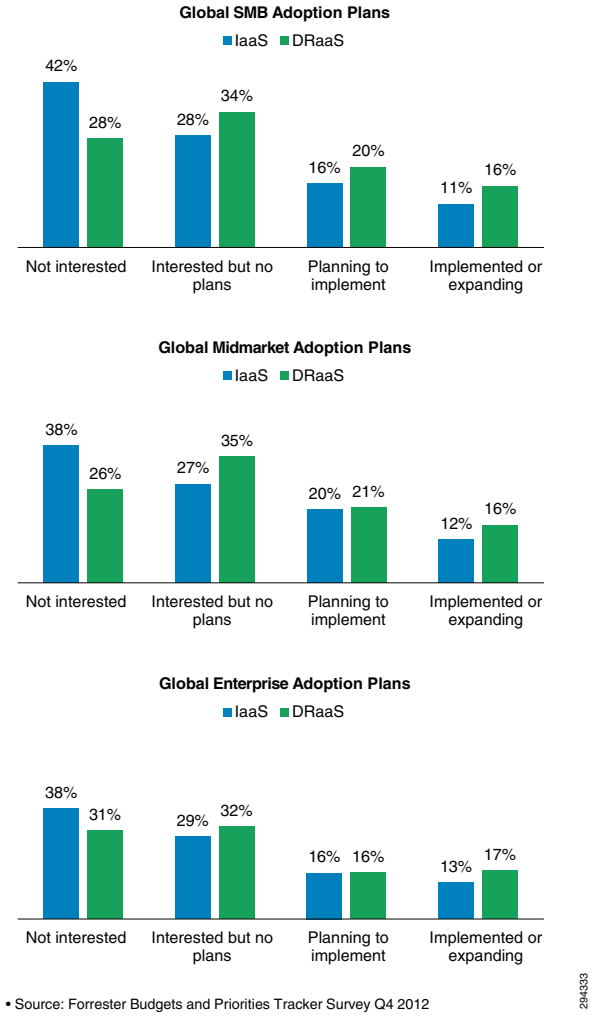
Figure 1-3 Strong Market Demand for DRaaS



• Source: Forrester Budgets and Priorities Tracker Survey Q4 2012

Further investigation of the global demand patterns for DRaaS indicates that the market opportunity and interest is equally spread across the enterprise, mid-market, and SMB segments, as summarized in Figure 1-4.

Figure 1-4 Global DRaaS Demand by Segment



• Source: Forrester Budgets and Priorities Tracker Survey Q4 2012

Cisco DRaaS Solution Changes Traditional Capability

The Forrester studies indicate that barriers exist that need to be addressed to achieve wide-scale adoption of disaster recovery at the enterprise level and from a service provider level.

Disparate Hardware Increases Costs

Traditional DR solutions require matching hardware at both the source side and the target side with the replication being performed by a hardware device, usually the storage array. This created a capital cost barrier for the equipment purchased and significantly increased the administrative overhead to the point that the Forrester survey shows the majority of the respondents had no plan of implementing disaster recovery.

From a service provider perspective, the lack of similar equipment at each customer site made offering a DRaaS solution so expensive that it was not pursued as a feasible service offering.

Complexity

Even if the hardware cost barrier can be overcome, traditional DR solutions require large administrative efforts to implement. Implementation usually has an extended professional services engagement and a significant learning curve for the administrators. For the service provider, building the core DR infrastructure is only part of the challenge. Creating a multi-tenant capable service offering has traditionally required a significant application development and programming effort.

Standardization of the Service Provider Infrastructure

Cisco's Disaster Recovery as a Service (DRaaS) solution architecture is based on Virtualized Multiservice Data Center (VMDC) and Cisco Unified Computing System (UCS). VMDC is a reference architecture for building a fabric-based infrastructure providing design guidelines that demonstrate how customers can integrate key Cisco and partner technologies, such as networking, computing, integrated compute stacks, security, load balancing, and system management. Cisco UCS is a next-generation data center platform that unites compute, network, storage access, and virtualization into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility.

Reduced Costs

Cisco VMDC and UCS reduce infrastructure expenditures (CAPEX) and operational expenses (OPEX) to increase profitability by reducing the number of devices that must be purchased, cabled, configured, powered, cooled, and secured. The unified architecture uses industry-standard technologies to provide interoperability and investment protection.

Business Agility

Cisco VMDC and UCS help businesses adapt rapidly and cost efficiently in response to changes in the business environment by enabling the fast provisioning of IT infrastructure and delivery of IT as a service. Deployment time and cost is more predictable using an end-to-end, validated, scalable and modular architecture. The unified architecture supports multiple applications, services, and tenants.

Simplification

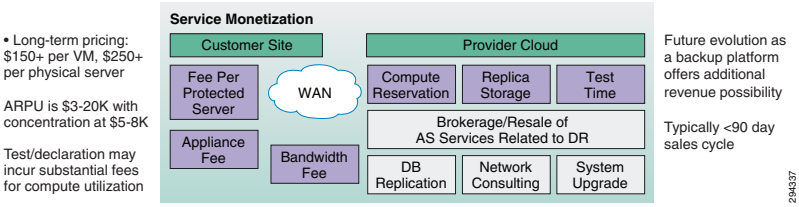
Cisco VMDC and UCS simplify IT management to support scalability, further control costs, and facilitate automation—key to delivering IT as a service and cloud applications. The architecture enhances the portability of both physical and virtual machines with server identity, LAN and SAN addressing, I/O configurations, firmware, and network connectivity profiles that dynamically provision and integrate server and network resources.

DRaaS: Business Drivers

Increased regulatory pressure drives the need for DR and business continuity plans and presents a hierarchy of requirements for the implementation of these solutions (geographic restrictions, regulatory compliance, etc.). Enterprises are constantly faced with budget constraints that prevent infrastructure duplication. Building disaster recovery infrastructure is a contextual business activity that requires a

degree of specialization with IT skillsets or resources that are significantly harder to build without sufficient scale. Under these circumstances, a growing desire exists to consume DR as a service, allowing incremental deployment and growth as budget becomes available. See Figure 1-5.

Figure 1-5 Cisco's DRaaS Blueprint Solution



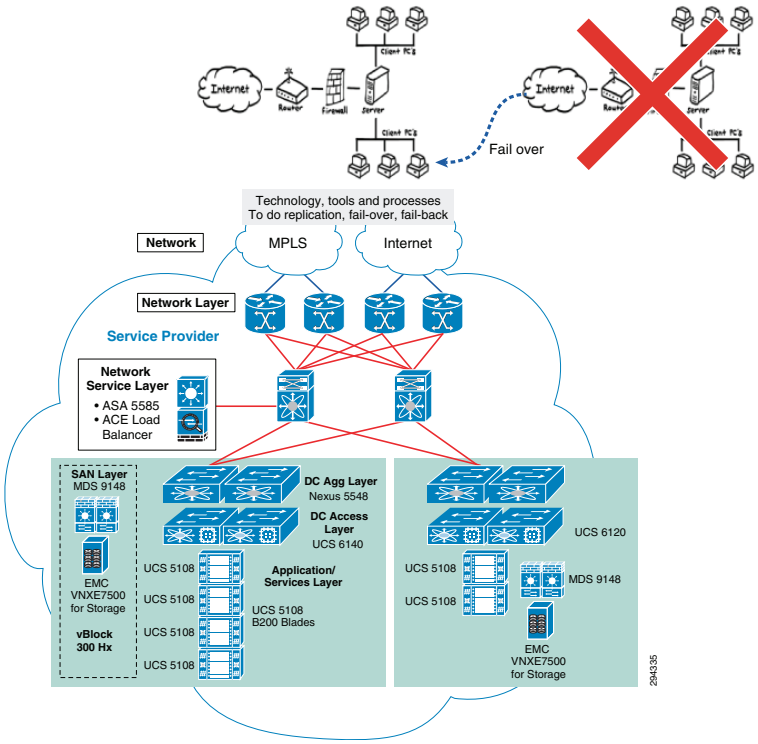
DRaaS: Technical Challenges

The selection of a specific technology and implementation for the implementation of DRaaS is a highly complex decision with technology challenges that need to be adequately explored and analyzed. See Figure 1-6 on page 1-7.

The following questions arise in the choice of the DRaaS implementation:

- How do we replicate data, databases, and virtual machines?
- What replication technology do we use?
- What are our RTO/RPO requirements for the various applications requiring Disaster Recovery?
- How should we monitor what is being done during the testing and recovery events?
- How should we perform failover either during a test or a during an actual disaster?
- How should the virtual machines and databases be rebuilt?
- How can we ensure the consistency of databases and applications?
- How can we redirect traffic, reconfigure the Domain Name Services, etc.?
- How should we perform failback after a recovery event?
- How should our organization staff for Disaster Recovery and testing?
- How can our organization afford Disaster Recovery (which is a cost and not a revenue generating activity)?

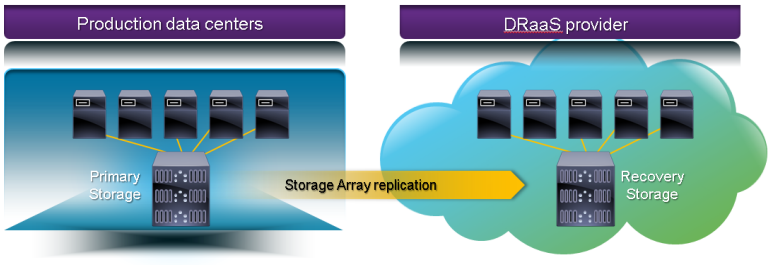
Figure 1-6 DRaaS Technical Challenges



Challenges with Traditional Storage-based Replication

The use of traditional storage-based replication requires an identical storage unit on the disaster recovery site from the same vendor. The storage array-based replication software is not application aware and needs additional intervention at the host level to achieve application consistency. Multiple points of management are required while performing disaster recovery and this introduces complexity in protecting and recovering workloads. The traditional storage-based replication approaches lack granularity and can replicate either all VMs or none that are residing on a logical unit number (LUN). Replication of data happens between LUN pairs that need to be identical and this restricts the ability to failover a single VM residing on the LUN. See Figure 1-7.

Figure 1-7 Storage-based Replication



Traditional storage replication approaches need additional functionality to take snapshots or clones of the target LUN to perform disaster recovery drills without interrupting data replication. Otherwise, replication has to be stopped for disaster recovery drills. Storage array-based replication does not support continuous data protection natively and data cannot be protected from logical failures.

Value of Cisco DRaaS Architecture for Service Providers

DRaaS offers the following value to service providers:

- **Increased Customer Relevance**—Not all of the customers requiring disaster recovery services want an Infrastructure as a Service Offering (IaaS) offering. Offering DRaaS provides better alignment with a typical IT buyer's focus. Leveraging DRaaS offerings by service providers gives them an opportunity to differentiate from commodity and over-the-top IaaS providers.
- **Bigger, More Profitable Deals**—Disaster recovery instances command a premium and provide improved margins due to lack of commoditization. Disaster recovery deals are typically larger compared to IaaS deals for SPs and generate higher margins. DRaaS offerings create reduced capital expenditures on compute resources and lower operating expenses on licensing due to oversubscription opportunities.
- **Strong Services Growth**—DRaaS offerings provide the ability to attach additional services with the offerings and create a pipeline of revenue from new and existing customers through new and improved monetization via services growth. Additional monetization opportunities present themselves through possibilities for hybrid services.

Cisco DRaaS Approach versus Backup-based Disaster Recovery

One commonly encountered question is how the backup-based disaster recovery approaches compare to Cisco's recommendation for DRaaS architecture for SPs. Table 1-1 shows the key considerations and a comparison of the approaches.

Table 1-1 Comparison of Cisco DRaaS with Backup-based Disaster Recovery

	Managed Backup using Cloud Storage	Backup-based Cloud Recovery using Snapshots	Cisco Approach
Use Case	Backup to cloud: Cloud storage for backups	Disaster recovery: SP-managed disaster recovery	Disaster recovery: SP or customer self-managed disaster recovery
Pros	Customers have ability to store data offsite without shipping tapes or having a secondary site to host data	Makes use of existing backup and virtualization tools for recovery	• SP managed or enterprise self managed • Single solution for protecting both physical and virtual environments • Automated recovery

Table 1-1 Comparison of Cisco DRaaS with Backup-based Disaster Recovery

	Managed Backup using Cloud Storage	Backup-based Cloud Recovery using Snapshots	Cisco Approach
Cons	• Does not ensure continuity of operations. • Provides data availability only. • Impacts performance of application during backup window. • No automated recovery	• No P2V capability, protection for only virtual environments • Performance impact on production applications during snapshot creation • No automated recovery	
RPO/RTO	Very high	High	Near Zero
Continuous Data Protection (CDP)	N/A; works based on traditional backups	Near CDP, cannot achieve real CDP. Depends on the frequency of snapshots.	Real CDP, provides multiple point-in-time copies for an extended period of time.

Service Provider Tenant Operating Models

Cisco DRaaS presents a model (see Table 1-2) that clearly delineates the responsibilities of the service providers that provide the DRaaS services and the end customer guidance on the ownership and expectations in the system offering.

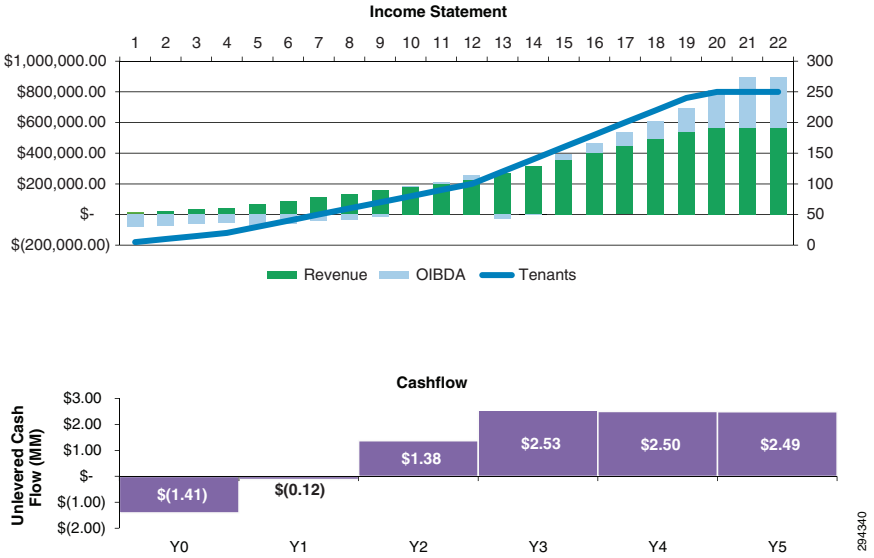
Table 1-2 Well-Defined Tenant/SP Operational Responsibilities Model

Responsibility	Service Provider	Tenant
Provide, manage, and monitor replication software and configuration	X	
Provide standby recovery environment (compute, network)	X	
Configure standby recovery environment with replication/ recovery plans for protected servers and network elements	X	
Recover/ boot protected servers to recovery environment with pre-defined VLAN/ IP address mapping and network topology	X	
Provide recovery to a specific point in time using CDP technology to create a bootable VMDK; boot associated VMs	X	
Ensure reachability of running VMs over pre-defined recovery network	X	
Validate application configuration and functionality		X
Provide notification of changes requiring recovery plan updates - VLANs, IPs, added/ removed volumes, new servers		X
Participate in annual recovery tests/ drills (no production impact)	X	X
Declare disaster		X

SP Monetization of Cisco DRaaS

Figure 1-8 is a financial model that presents the monetization opportunity for service providers associated with the deployment of the Cisco DRaaS solution architecture.

Figure 1-8 Monetization Opportunity for SPs



Value of Cisco DRaaS for Enterprises

DRaaS provides the following value for Enterprises:

- **Recovery Time Is Key**—Enterprises frequently lack the knowledge to select and deploy the optimal DR tools for their needs. Current enterprise tools for low RPO/RTO tend to be cost prohibitive for widespread deployment.
- **Reduced Cost and Impact of Disaster Recovery Testing**—Disaster recovery exercises present a significantly high cost and distract from the normal business operation. The use of DRaaS allows enterprises to focus on application validation without being distracted by rack, stack, and recover activities with their infrastructure and IT services. It also presents a potential opportunity to better leverage the disaster recovery environment.
- **Accelerated Implementation**—DRaaS presents an easier framework for implementation of business continuity plans and test execution and provides end customers with the ability to grow over time from a limited scope. An equivalent DRaaS solution to replace one that is provided and managed through a service provider's robust offerings would be extremely time consuming to build for enterprises on their own as they include self-service, monitoring, and service assurance capabilities as a holistic offer from service providers.
- **Better Odds of Success**—The use of specialized SP offerings eliminates the need for a strong disaster recovery competency and addresses the difficulty associated with hiring and retaining talent for disaster recovery. DRaaS is a niche technology that requires a significantly large scale to gain the required specialized experience. Globalization means many organizations cannot use traditional primary/secondary model of dedicated infrastructures for disaster recovery and business continuity operations.