ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

DR – Cloud: Multi- Cloud Based Disaster Recovery Service

Greeshma Radhakrishnan[1], Chenni Kumaran[2]

PG Scholar, Dept. of CSE, Indira Institute of Engg and Tech, Thiruvallur, India [1]

Associate Professor, Dept. of CSE, Indira Institute of Engg and Tech, Thiruvallur, India [2]

ABSTRACT: With the rapid popularity of cloud computing paradigm, disaster recovery using cloud resources becomes an attractive approach. This paper presents a practical multi-cloud based disaster recovery service model: DR-Cloud. With DR-Cloud, resources of multiple cloud service providers can be utilized cooperatively by the disaster recovery service provider. A simple and unified interface is exposed to the customers of DR-Cloud to adapt the heterogeneity of cloud service providers involved in the disaster recovery service, and the internal processes between clouds are invisible to the customers. DR-Cloud proposes multiple optimization scheduling strategies to balance the disaster recovery objectives, such as high data reliability, low backup cost, and short recovery time, which are also transparent to the customers. Different data scheduling strategies based on DR-Cloud are suitable for different kinds of data disaster recovery scenarios.Experimental results show that the DR-Cloud model can cooperate with cloud service providers with various parameters effectively, while its data scheduling strategies can achieve their optimization objectives efficiently and are widely applicable.

I. INTRODUCTION

Cloud storage means "the storage of data online in the cloud," wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection for data backup, archival and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware. However, cloud storage does have the potential for security and compliance concerns.There are four main types of cloud storage:

1. PERSONAL CLOUD STORAGE

Also known as mobile cloud storage, personal cloud storage is a subset of public cloud storage that applies to storing an individual's data in the cloud and providing the individual with access to the data from anywhere. It also provides data syncing and sharing capabilities across multiple devices. Apple's iCloud is an example of personal cloud storage.

2. PUBLIC CLOUD STORAGE

Public cloud storage is where the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data center. The cloud storage provider fully manages the enterprise's public cloud storage.

3. PRIVATE CLOUD STORAGE

It is a form of cloud storage where the enterprise and cloud storage provider are integrated in the enterprise's data center. In private cloud storage, the storage provider has infrastructure in the enterprise's data center that is typically managed by the storage provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

4. HYBRID CLOUD STORAGE

Hybrid cloud storage is a combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

BENEFITS OF CLOUD:

1. Internal Resource Efficiency

With cloud backup, organizations can maintain control over their data, but have the actual storage drives off-site at a cloud services provider. By using a cloud vendor that offers agentless technology, organizations can encrypt and compress data before it is transferred off-site. There are significant cost, space and energy savings in taking this approach.Another significant advantage to cloud backup is the ability to centrally manage backup for all of your remote sites and branch offices, which solves a number of complex challenges for IT, including bandwidth allocation, security and disaster recovery.

2. Enhance Security

security should be a number one priority, so you want to make sure your cloud backup vendor offers important security features such as advanced encryption, digital signatures, configurable password management, adaptive protection features and agentless backup architecture. The idea is to have proactive and adaptive protection against privacy and security breaches with continuous data protection.

3. Ease of Scalability

With data storage requirements growing so rapidly, scalability has become a critical concern for businesses. The idea of adding new disks or even tapes for backup no longer makes sense in an environment where space consolidation is critical and costs need to be managed. By using a cloud backup solution, businesses are able to eliminate hardware, software and maintenance costs and can grow their backup in a cost-efficient manner based on what is actually needed. Another important benefit, depending upon the cloud vendor, is the opportunity to manage data throughout its lifecycle.

II. CLOUD DISASTER RECOVERY

More and more services rely on IT systems at present, and some of them, such as financial service and health care service, are critical to their customers and society. Even a very short period of downtime or very small amount of data loss could result in huge economic losses or social problems. Therefore, many important business and public services use disaster recovery mechanism to protect critical data and minimize the downtime caused by catastrophic system faults. Different kinds of technologies are adopted in disaster recovery systems, such as periodically backup or continuous synchronization of data and preparing standby system in geographically separated places.

EXISTING SYSTEM

In existing system, it uses only one cloud to maintain one backup, and focuses on the mechanism in local file system, not the cloud platform.They created a disaster recovery cloud model for web site applications which illustrated that data backup built on top of cloud resources can greatly reduce the cost of data disaster recovery for corporations. However, they didn't study on how to further improve the service quality using multiple clouds.

Problem Statement

Data disaster recovery is a kind of service with highest data reliability requirements. To perform data disaster recovery service using cloud computing paradigm to maximize the data reliability with reduced cost is still a challenge. No difference with other computer systems, cloud computing system can also encounter certain risks such as software bug, hardware fault, network intrusion, human-caused damage, natural disasters, etc. Because of the diversity of requests parameters, i.e., data size and store duration, it is a typical multi-objective combinatorial optimization problem to make excellent scheduling decision.All of these risks may lead to cloud service interruption, even loss of data in some cases. Popular distributed storage systems used in cloud platforms currently, such as Amazon S3[5], Google GFS[6], and Apache HDFS[7], have adopted 3-replicas data redundant mechanism by default. However, with an entire data center failure, data may still be lost.

In proposed system, we are about to utilize multiple data centers from different cloud service providers. In this pattern, one cloud service provider who provides data disaster recovery service to the public can lease resources from

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

other cloud service providers in the pay-as-you-go mode. Thus, data disaster recovery is no longer limited to the data centers of one cloud service provider. A disaster recovery service provider can selectively backup data to its own data centers or other cloud service provider's data centers. By using an appropriate backup data scheduling strategy, the disaster recovery service provider can achieve better effect, which is to minimize the cost while promoting the service quality.DR-Cloud proposes multiple optimization scheduling strategies to balance the disaster recovery objectives, such as high data reliability, low backup cost, and short recovery time, which are also transparent to the customers.We propose a practical system model for multi-cloud based disaster recovery service, which we call DR-Cloud (DR for disaster recovery). DR-Cloud utilizes resources of multiple cloud service providers cooperatively. Customers only need to deal with the DR-Cloud, using very common and unified service interface.

III. SYSTEM ANALYSIS

Many cloud service provider provide storage as a service. They take the data from the user and stored on the large data centers, henceproviding a user means of storage. Althoughthese service provider says that data stored in a cloud is safe but there have been some cases where data is been modified or lost due to security holes. Variouscloud providers adopt various technologies to resolve the problem of cloud data storage. Thevirtualized nature of cloud make the traditional mechanism unstable for handling the securityrisks so these service provider use different encryptingtechnique to overcome these problems. Another major issue that is mostly neglected is of data remanences.It refers to the data left out during transfer.It cause minimal security threat in private cloud computing offerings, howeverserver security issues may emerge in case of public cloud
offerings as a result of data remanence.

Virtualizationincreasesthe securityof cloud environment.Withvirtualization a single machine can be divided into multiple virtualmachine, thusprovide better dataisolation. Thevms provide thesecurity test bed for executingof untested code fromentrusteduser.Anhierarchicalreputation system have been proposed in a paper[9]formanagingtrust I n the cloudenvironment.

Application level security refers to the usage of software andhardware resources to provide the security to application suchas attackers are not make any changes in the application format. Nowadaysattackerlaunchedthem as a trusted userand system consider them astrusteduser and allow full accessto attackingparty. Thereason behind this issuing outdatednetwork policies. With the technological advancementthesesecuritypolicies becomeobsoleteas there have been instances whensystem security have beenbreached, but with the recent technologyadvancements it is quit possible to imitate a trusteduser. Thethreatto application level security include sql injection attack, dos attack,captchabreaking ,xss attack. Hence, it is necessary to install high level security check to minimize these risks.These traditional method to deal with increased securityissue have been to develop a task oriented asic device which canhandle the specific task and provide high level of security[10].Butwith application level threat being dynamic and adaptable to thesecurity check inplace, theseclosed system have to observed to be
slow in compare to the open ended system.

Single "All-in-one" Server:

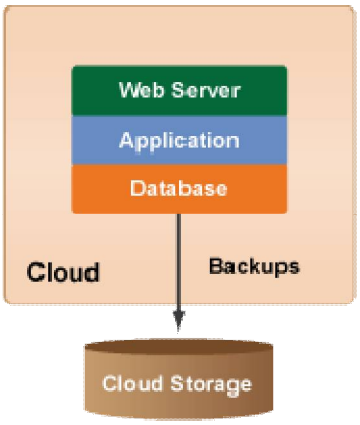
Use one of the All-in-one ServerTemplates, such as the LAMP (Linux, Apache, MySQL, PHP) ServerTemplate to launch a single server that contains a web server (Apache), as well as your application (PHP) and database (MySQL). You'll find a collection of simple All-in-one ServerTemplates in the MultiCloud Marketplace, which are useful for new RightScale users and basic demos.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

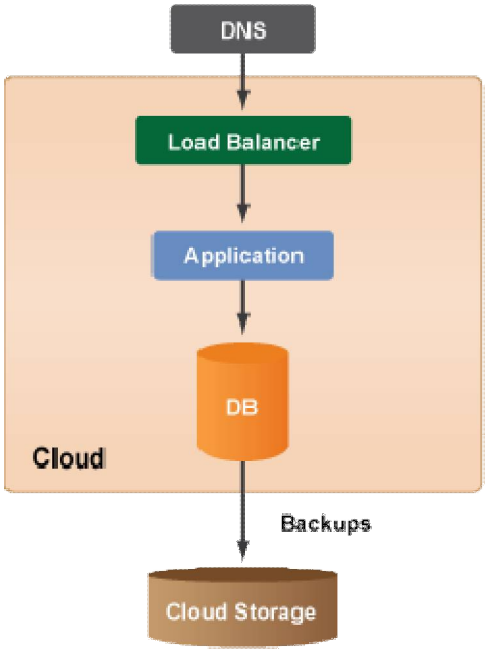


Single Cloud Site Architectures:

In a standard three-tier website architecture, there is at least one dedicated server in each tier of the system architecture. (Load Balancing Server, Application Server, Database Server).

Non-Redundant 3-Tier Architecture:

Non-redundant system architecture it is primarily used for basic test and development purposes. In the example diagram below, there are dedicated servers for each tier of the application/site. A non-redundant architecture is not recommended for production environments.



Redundant 3-Tier Architecture:

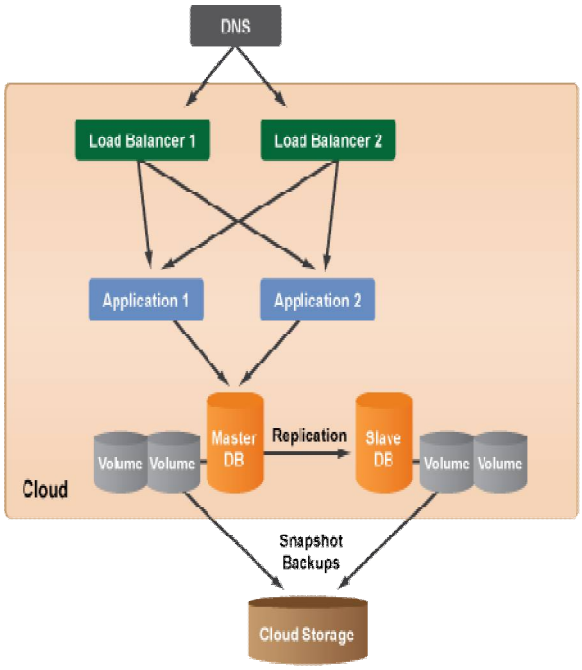
Any production environment that is launched in the cloud should also have a redundant architecture for failover and recovery purposes. Typically, you will use a Server Array for your application tier to take advantage of autoscaling in the cloud, however there may be some scenarios where your application is not designed to autoscale. In such cases, you can still create a redundant multi-tier architecture where you have redundancy at each tier of your reference architecture. In the example below, there aretwo load balancer servers, two application servers, as well as master and slave database servers. A redundant architecture will help protect your site/application from system downtime.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

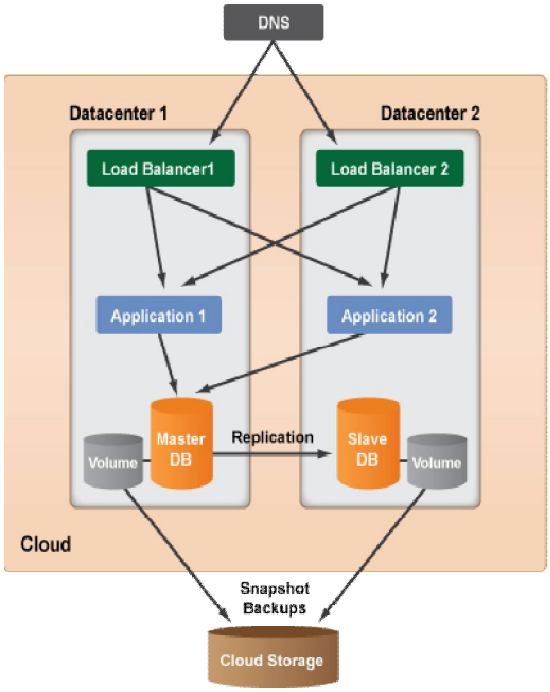
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016



Multi-Datacenter Architecture:

Each datacenter in a cloud is designed to be an isolated segment inside the same geographical cloud. So if a power failure occurs in one datacenter, the other datacenters will be unaffected. For example, within a cloud/region there may be several resource pools called availability zones and datacenters. The benefit of using multiple datacenters is to protect your entire site/application from being negatively affected by some type of network/power failure, lack of available resources, or service outtage that's specific to a particular datacenter.



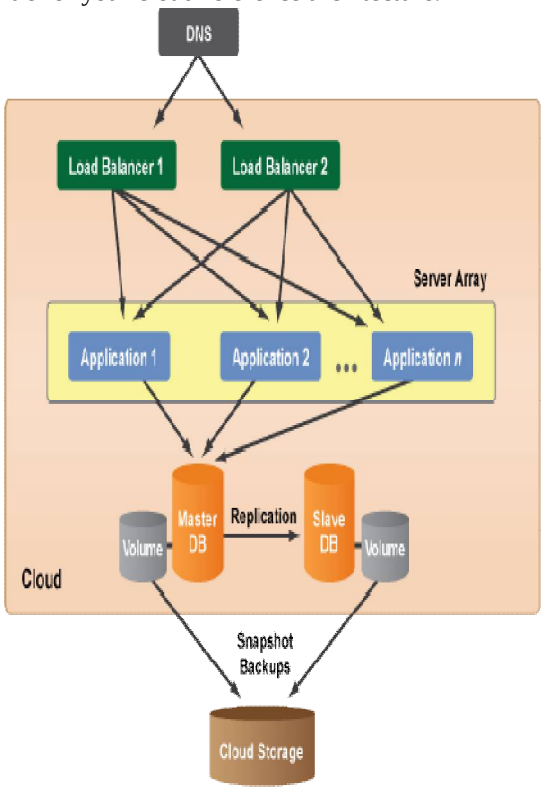
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Autoscaling Architecture:
One of the key benefits of the cloud is the ability to horizontally scale (i.e. grow or shrink the number of running server resources) as the demands of your application/site change over time. With RightScale, you can use Server Arrays to set up a particular tier of your architecture to autoscale based on predefined alert conditions. Autoscaling is most commonly used for the application tier of your cloud reference architecture.



Scalable Architecture with Membase:
Master-Slave MySQL setup, you could also use Membase (Couchbase) nodes for your database tier, which is a distributed NoSQL database, which replicates data across all of the Membase nodes. If you are using the Enterprise edition you can attach volumes to each node (shown below), but the Community Edition doesn't support the use of volumes.

IV. SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

Unit testing:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing:

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional testing:

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.
Invalid Input: identified classes of invalid input must be rejected.
Functions : identified functions must be exercised.
Output : identified classes of application outputs must be exercised.
Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Testing:

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing:

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing:

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

6.1 Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

- No duplicate entries should be allowed
- All links should take the user to the correct page.

6.2 Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

6.3 Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

V. MODULE DESCRIPTIONS

Multi-cloud:

In this paper, we propose a practical system model for multi-cloud based disaster recovery service, which we call DR-Cloud (DR for disaster recovery).

DR-Cloud utilizes resources of multiple cloud service providers cooperatively. Customers only need to deal with the DR-Cloud, using very common and unified service interface.

The on-demand nature of cloud computing vastly reduces the cost of disaster recovery, whose peak resource demands are much higher than average demands.

However, data disaster recovery is a kind of service with highest data reliability requirements. How to perform data disaster recovery service using cloud computing paradigm to maximizing the data reliability while reducing cost is still a challenge.

Disaster recovery:

With DR-Cloud, resources of multiple cloud service providers can be utilized cooperatively by the disaster recovery service provider. A simple and unified interface is exposed to the customers of DR-Cloud to adapt the heterogeneity of cloud service providers involved in the disaster recovery service, and the internal processes between clouds are invisible to the customers.

DR-Cloud:

We can see the multi-cloud mode is a suitable approach to the data disaster recovery service.

But it also brings in some new challenges to design a practical system model, which are summarized as follows:

- The model should be able to utilize a variety of cloud platforms.
- To reduce service barriers.
- The model should provide enough space for optimization to achieve enough advantage.

To meet all these challenges, we design a multi-cloud based data disaster recovery service model, named DRCloud, from the perspective of the service provider.

VI. CONCLUSION

This paper presents a practical multi-cloud based disaster recovery service model: DR-Cloud. With DRCloud, resources of multiple cloud service providers can be utilized cooperatively by the data disaster recovery service provider. And customers only need to deal with that service provider, using very simple and unified service interface, without concerning the internal processes between heterogeneous clouds. DRCloud can ensure high data reliability, low backup cost, and short recovery time by using intelligent data scheduling strategies. Different scheduling strategies based on DR-Cloud are proposed, which are suitable for different kinds of data disaster recovery scenarios.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

REFERENCES

[1] Aws economics center. http://aws.amazon.com/economics/.
[2] RajkumarBuyya, Rajiv Ranjan, and Rodrigo N. Calheiros.InterCloud:Utility-Oriented Federation of Cloud Computing Environments for Scalingof Application Services. In The 10th International Conference on Algorithmsand Architectures for Parallel Processing, Busan, Korea, 2010.
[3] Emmanuel Cecchet, AnupamChanda, SamehElnikety, Julie Marguerite,and Willy Zwaenepoel.Performance Comparison of Middleware Architecturesfor Generating Dynamic Web Content.In 4th ACM/IFIP/USENIXInternational Middleware Conference, June 2003.
[4] Brendan Cully, Geoffrey Lefebvre, Dutch Meyer, Mike Feeley, NormHutchinson, and Andrew Warfield. Remus: High availability via asynchronousvirtual machine replication. In Proceedings of the Usenix Symposiumon Networked System Design and Implementation, 2008.
[5] Albert Greenberg, James Hamilton, David A. Maltz, and Parveen Patel.Cost of a cloud: Research problems in data center networks. In ACM SIGCOMMComputer Communications Review, Feb 2009.
[6] Kimberley Keeton, Cipriano Santos, Dirk Beyer, Jeffrey Chase, and JohnWilkes. Designing for Disasters. Conference On File And Storage Technologies,2004.
[7] Kimberly Keeton, Dirk Beyer, Ernesto Brau, Arif Merchant, Cipriano Santos,and Alex Zhang. On the road to recovery:restoring data after disasters.European Conference on Computer Systems, 40(4), 2006.
[8] TirthankarLahiri, Amit Ganesh, Ron Weiss, and Ashok Joshi.FastStart:quickfault recovery in oracle. ACM SIGMOD Record, 30(2), 2001.
[9] Vmware high availability. http://www.vmware.com/products/high-availability/.
[10] T. Wood, A. Gerber, K. Ramakrishnan, J. Van der Merwe, and P. Shenoy.The case for enterprise ready virtual private clouds. In Proceedings ofthe Usenix Workshop on Hot Topicsin Cloud Computing (HotCloud), SanDiego, CA, June 2009.