Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

DNS based Intelligent Disaster Recovery for Virtual Servers: Failover and failback

Sangeeta
Department of Computer Science
South Point Institute of Technology & Management
Sonipat, Haryana, India

Maneela
Department of Computer Science
South Point Institute of Technology & Management
Sonipat, Haryana, India

Abstract— IT Service Continuity Management is a process that deals with disasters impacting IT services. ITSCM allows an organization to understand the Disaster recovery weaknesses within their IT services and take measures to ensure that services are recovered as efficiently as possible when required. Every organization prepares ITSC plan which is the collection of policies, standards, procedures and tools through which organisations not only improve their ability to respond when Disaster occurs, but also improve their resilience to major disasters, ensuring that critical servers along with their applications and databases do not fail. In case of total failure, mission critical and business critical servers must be recovered within their defined RTO and RPO.
This research paper is based virtual environment which is highly cost effective and easier to recover in case of failure. The trend of virtualization is changing the disaster recovery (DR) process, making it easier and more cost effective with minimal human intervention.
A traditional DR approach having physical servers at both primary and recovery sites is very expensive and resource dependent. It sometimes takes months to recover all servers in case of natural disaster leading to customer dissatisfaction or unrecoverable business loss. Server virtualisation approach helps make disaster recovery easier by representing everything in logical terms. A virtualised environment combined with intelligent DNS enables dynamic routing of traffic at time of disaster keeping same host name as at the primary site by implementing the concept of Doman cname.

Keywords— ITSC(IT Service Continuity), RTO(Recovery Time Objective), RPO(Recovery Point Objective), DR(Disaster Recovery), iDNS(Intelligent DND), url(uniform resource locator)

I. INTRODUCTION

IT Service Continuity is concerned with preventing any unexpected serious interruptions to IT services as a result of a natural disasters or other forms of force majeure having a catastrophic impact on the business. Several parameters have to be looked at by ITSCM when analyzing IT services:

- Loss of profits.
- Loss of market share.
- Damage to brand image.
- Other side effects.
- How long you can wait before restoring service without having an impact on business processes.

IT Service Continuity Management's (ITSCM) strategy needs to judiciously balance procedures that are:
Proactive: which seek to minimize the consequences of a serious interruption to service.
Reactive: Resume service as quickly as possible after the disaster.

Strategies

There are two approaches to IT service continuity:
preventive measures, which avoid interruptions to service, and **reactive** measures, which restore acceptable levels of service in the shortest time possible.
IT Service Continuity Management is responsible for designing prevention and recovery activities offering the necessary guarantees at reasonable expense.

Preventive Activities

Preventive measures require a detailed prior analysis of risks and vulnerabilities. Some of these will be general in nature: fires, natural disasters, etc. whereas others will be strictly IT related: storage system failures, hackers, viruses, etc.
Preventing general risks adequately depends on close collaboration with Business Continuity Management (BCM) and requires measures involving the organisation's "physical" infrastructure. ITSCM needs to pay special attention to preventing risks and vulnerabilities to the IT systems. The close collaboration of Security Management is essential in this regard. The customary protection systems are those that aim to build a fortress around the IT infrastructure by protecting its perimeter.

II. LITERATURE SURVEY

Some preliminary works on ITSC and DR in banking and manufacturing units have been made through using data analysis. This literature review was also conducted to help put the research methodology in a better conceptual framework.

The concept of business continuity has evolved almost with the begging of computer and communication industry since 1950's (Business Resilience). Unfortunately, it was not a major concern for organizations until 2002(Mick Savage, 2002). Michael and Sonia (2004) and also Nijaz (2006) agreed that business continuity is mostly focused on IT systems in a given organization. Business continuity has two major components: Business Continuity Management (BCM) and Business Continuity Planning (BCP).

Mick Savage (2002) sees that since IT is being important component in an organization, then BCP should include detailed specification about IT systems. Such specifications should contain IT systems documentation and preferably in graphical representation. In addition, business functions should be linked to IT systems using either business impact analysis (BIA) or business modeling which will be covered shortly in this chapter. The challenge of having a close-to-perfect and valid-always BCP for IT is due to the fact that IT systems are dynamic in nature in terms of upgrades and re -configuration. (Mick Savage, 2002).

The research in (Michael Pit & Sonia Goyal, 2004) aims at addressing the issues with respect to the service orientation in the IT management industry. The developed approach aims to build a repository of all information needed that is required for business-oriented service management. None of the previously mentioned however makes use of BCP concept to deal with the service oriented fault correlation and service impact analysis as we do in this work.

The dramatic changes of information technology in organizations have resulted in the increased use of IT services expression rather than systems as in traditional perspective to more accurately capture the interactive, aggregated, and highly diversified nature of contemporary IT usage in organizations (Mathiassen & Sørensen, 2008). The services perspective focuses mainly on the use of IT artefacts, whereas the systems perspective focuses mainly on IT Artefacts (Kaitovaara, 2004; Mathiassen & Sørensen, 2008) . In this paper, IT services refers to the use of hardware, software, and supporting infrastructure to manage and deliver information or organization's operations, functions and services to the user. IT services offer responses to specific information processing requirements and are configured into heterogeneous portfolios of information processing capabilities (Mathiassen & Sørensen, 2008).

Violino (2009) not only emphasizes the importance of virtualization and disaster recovery as independent concepts, but also establishes a link between them. Violino (2009) says "Hordes of organizations have embraced server virtualization as they look to consolidate servers, reduce energy consumption in the data center, increase business agility and reduce costs. But there's life for virtualization beyond the server: The future of this technology likely will focus on client devices, and there's also great potential in areas such as business continuity, disaster recovery and capacity planning." (p. 01). Violino (2009) continues to establish the linkage and shared benefit, "Another likely trend is the use of virtualization for business continuity and disaster recovery. Efforts to provide adequate backup in the event of systems disruptions have become a high priority for many organizations, and some believe that virtualization is a natural fit for business continuity and disaster recovery" (p. 01).

Marko Niemimaa, Jonna Jarvelainen, in his publication "IT Service Continuity: Achieving Embeddedness through Planning," has described how IT service continuity planning embeds continuity by reviewing continuity planning methods. As per their findings, Business customers and regulations as well as different IT service management frameworks expect that IT services are continuously operating. A service interruption might have severe impact on customer relationships, business, sales or image of the company. Therefore, organisations spend enormous amounts of time in continuity and recovery planning for IT services, and several continuity planning methodologies have been introduced. However, the connection between continuity planning and continuity management is somewhat unclear, and embedding the continuity practices into organisations have not been discussed in detail in planning methodologies. The continuity planning practices that influence achieving embeddedness are analysed from qualitative and quantitative data from large organisations operating in Finland. The findings suggest that a number of planning practices support the transition from planning to embedded ness, such as creating awareness, increasing commitment, integrating the continuity practices into organisational processes and learning from incidents.

The management of IT services is done by the Information Technology Department (IT Department) in every government agency (MAMPU, 2000, 2009; Haron, Sahibuddin, Harun, Taib, & Botok, 2014). The function of the IT Department is to enhance the services of an organization through the use of Information Technology (Haron et al., 2014)

III. INTELLIGENT DNS BASED DR IMPLEMENTATION

Trends in virtualization are always changing. As the technology matures and advances are made, there are more options open and more cost saving virtualization projects that can be implemented. The purpose of this paper is to look at virtualization from the perspective of DR solutions, that addresses the high cost of physical servers and rack space and can be implemented with ease.

In order to implement a DR solution based on virtualization concept, we assume that we already have virtual servers at the primary site that we need to replicate at the recovery site. Here replication approach is combination of two approaches:

3.1 Intelligent DNS

3.2 VMWare Replication

iDNS enablement can be carried for applications, database connections and ftp/sftp connections that uses virtual host names to connect to their respective applications, databases and ftp connections.

Application (URL/DNS): we will need to enable iDNS so that users and connecting systems do NOT need to change their url. iDNS will direct traffic to the appropriate ip address accordingly.

3.1.1 **Application iDNS probing method options**

There are two options available to applications:

3.1.1.1 **Web page probing:**

Web page probing is the ITSC preferred method, if a web server is in the application's architecture. The only requirement is that a web page must be running on the production server that is going to be replicated.

Requirements to define for iDNS setup for web page probing

1. Identify which web page will be used for probing.
2. Identify a search string – word or phrase – that iDNS will search for to determine if application is active.
3. Define frequency of iDNS probing the webpage. This is the frequency in which iDNS checks which location is the active location based which location meets requirements defined.

How iDNS web page probing works:

1. iDNS device will probe the page at the frequency indicated in the TTL configuration.
2. If the web application is accessible and the search string identified is found then that is determine to be the active location.

3.1.1.2 Server Port probing:

In this case, the server port must exist on both the production and failover servers.There must be a service running on that port in order to answer/respond to the iDNS probe.

How iDNSport probing works:

1. iDNS device will probe the port at the frequency indicated in the TTL configuration.
2. If the port is accessible/up then that is determine to be the active location.

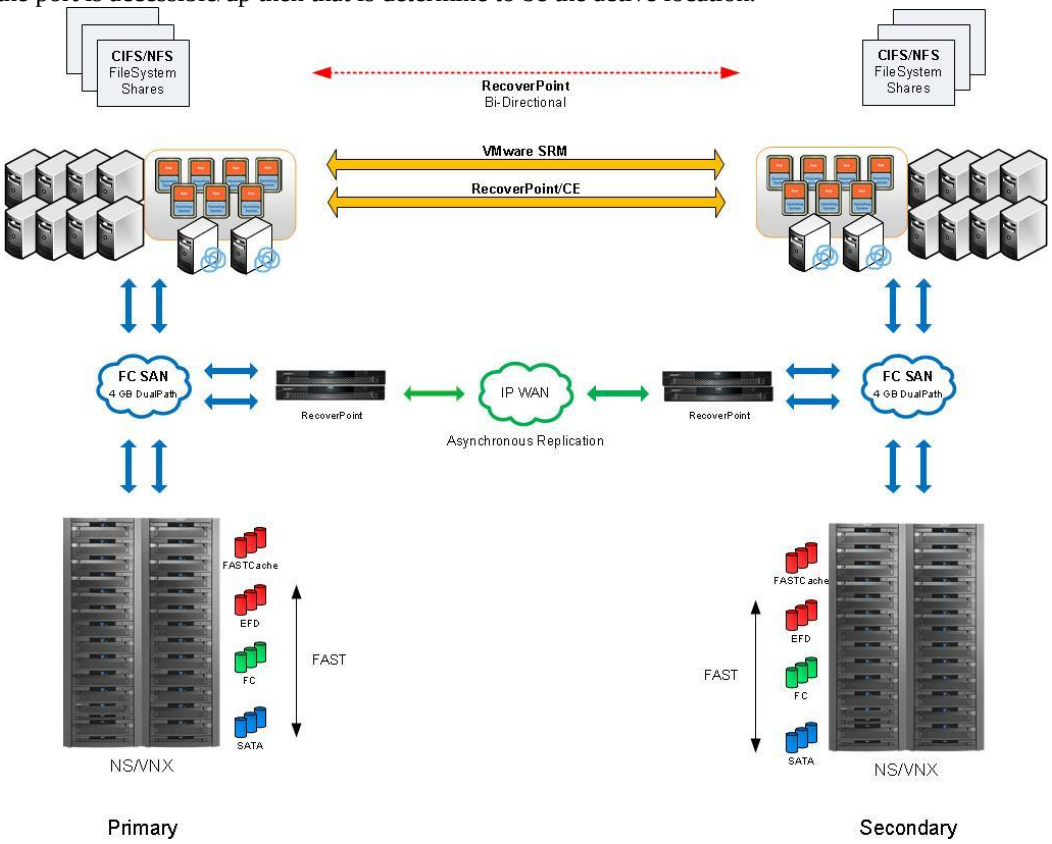

Fig. 1 IP Change in application iDNS Probing method

3.1.2 Database connections: iDNS will enable clients and other databases to connect to the active database location. This will require changes to the TNSNames / HostFiles / Hardcoded IP addresses within your application and INTERFACING clients / databases. Your connection strings to the database will need to be changed to the iDNS hostname. This is because the hostname of the database servers (prod and DR) are different.

3.1.2.1 Database iDNS probing method:

There are two options for DB Query configurations:

1. Connect to the database – do not run any query
2. Connect to the database and run a query.

Table for option 1- Connect to the database – do not run any query

Primary Database	Recovery Database at DR site
Type: Oracle	Type: Oracle
Import Settings: oracle	Import Settings: oracle
Interval (seconds): 30 seconds	Interval: 30 seconds
Timeout (seconds): 60 seconds	Timeout: 60 seconds
Probe Timeout (seconds): 10 seconds	Probe Timeout: 10 seconds
Ignore Down Response: No	Ignore Down Response: No
Send String: (empty)	Send String: (empty)
Receive String: (empty)	Receive String: (empty)
User Name:	User Name:
Password:	Password:
Database:	Database:
Receive Row: (empty)	Receive Row: (empty)
Receive Column: (empty)	Receive Column: (empty)
Count: 0	Count: 0
Alias Address (ip)	Alias Address (ip)
Alias Service Port: 1580	Alias Service Port: 1580
Debug: No	Debug: No

iDNS Database Server Port Probing:

In order to implement port probing, The server port must exist on both the production and failover server(s).There must be a service running on that port in order to answer/respond to the iDNS probe. Once iDNS is configured we will need to map the iDNS hostname to a DNS entry as an Alias/CNAME.

Requirements to define for iDNS setup

1. Determine if there is an existing service running on a port to use or if a new service has to be setup/configured.
2. Define the service and port that iDNS will use to probe.
3. Define frequency of iDNS probing the port. This is the frequency in which iDNS checks which location is the active location based which location meets requirements defined.

How iDNSport probing works

1. iDNS device will probe the port at the frequency indicated in the TTL configuration.
2. If the port is accessible/up then that is determine to be the active location.

3.2 VMWare Replication

Here we use storage replication, where an "image" of the system (including all local filesystems, applications, patches, user accounts, etc.) is replicated to the secondary site. As changes are made to the primary site, those changes are automatically replicated to the secondary site. As such, we always have an image of the machine at the secondary site, minutes to hours behind the primary copy. All virtual machines associated with a given application will be replicated consistently, so that they will all be available from the same point in time.

The Site Recovery Manager Process will automate the failover to the recovery site, as well as changing the IP address of the machine when it starts so that it can communicate on the recovery site network. It is important to note that the virtual machine will be issued a new IP address at the recovery site.

3.2.1 VM Build and Failover Procedure:

i. Build a VM machine with standard OS Boot LUN configuration/remediation.
ii. configure EMC RPA replication between both LUNs and specify the production to recovery site direction.
iii. Shutdown Production site server.
iv. Start the recovery server, it will boot the OS from the replicated LUN.
v. Perform Data integrity test – Validate OS/data, access the OS files, log files, verify file/dir size, time stamp etc.
vi. Create new files to the recovery server. Note down the files/dir time stamp, size, checksum in order to validate it upon failback.

3.2.2 VM Build and Failover Procedure:

i. Reverse the replication direction Recovery to Production site.
ii. Once replication is complete, break the RPA
iii. Start the primary server
iv. Perform Data integrity test – Validate OS/data, access the OS files, log files, verify file/dir size, time stamp etc.

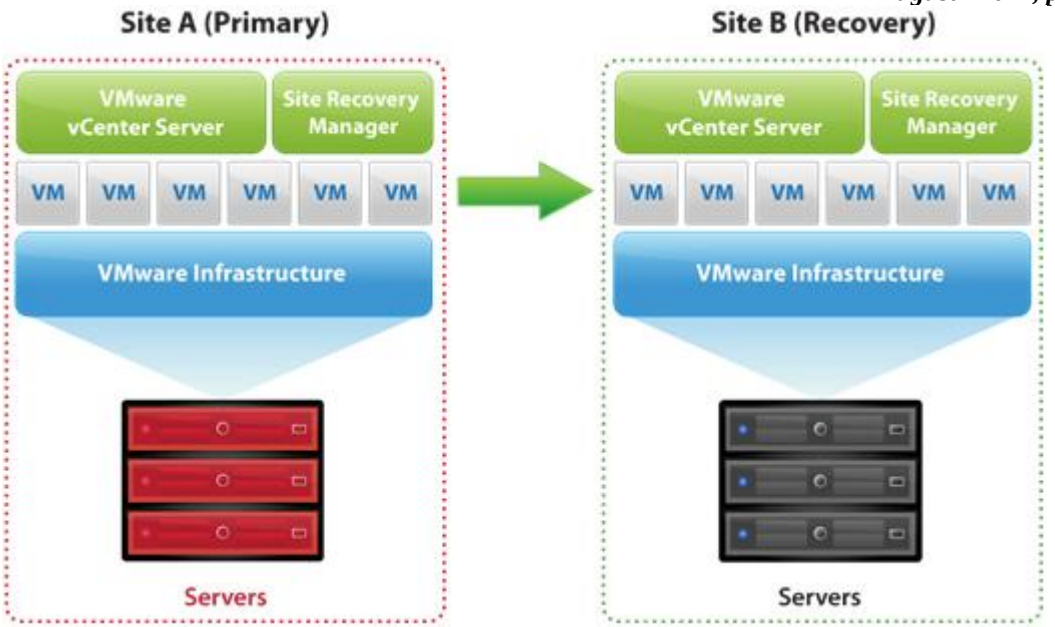

Fig. 2 Diagram showing VMWare Replication

IV. CONCLUSIONS

Disaster recovery (DR) has taken on a new sense of urgency in recent years. Emerging issues like natural disasters, computer software and hardware failures, terrorism, hackers, computer viruses have all led to increase our focus on preparing for disasters. Therefore disaster recovery plan must be integrated with the overall organization ITSC approach and that must be tested through regular yearly drills as well as a test drill whenever an environmental change occurs. The plan should include documented and tested procedures with tested RPO and RTO.

Here are the significance of RP based research on VMWare:

- Improved RTO and RPO
- Enable Alignment with Business Continuity
- Operational improvements
- Faster backup and restore times through data replication
- Data DeDuplication and Replication
- Reduces the dependency on tape technology
- Avoids storage cost / less disk required

REFERENCES

[1] Marko Niemimaa, Jonna Jarvelainen, "IT Service Continuity: Achieving Embeddedness through Planning," ares, pp.333-340, 2013 International Conference on Availability, Reliability and Security, 2013

[2] Virtualize Your IT Infrastructure. (2012). Retrieved October 15, 2012, from http://www.vmware.com/virtualization/

[3] Kontzer, T. (2010). Virtualization as a tool for agile it. CIO Insight, (113), 28-31. Retrieved from http://search.proquest.com/docview/755009140?accountid=27965

[4] Violino, B. (2009). Virtualization's new frontier. CIO Insight, (101), 28-30,32-33. Retrieved from http://search.proquest.com/docview/213016211?accountid=27965

[5] Laura DuBois, "Best practices in Business Continuity and Disaster Recovery", IDC, Feb 2011

[6] EMC, "Improving VMware Disaster Recovery with EMC RecoverPoint", emc.com, August 2012

