DESIGNING "ARCHITECTURE BASED BACKUP SITE PROJECT" WITH A SMALL SET OF INFORMATION AND DETAILS

Daniel de Souza Carvalho [1], Samuel de Barros Moraes[2]

Abstract *— When information technology became closer or an important part of the company main business, it requires a non stop infrastructure to guarantee clients/partners attendance and preserve the company image to the market place in case of a disaster. In recent years small and medium companies are concerned about their disaster recovery plans, and they are looking for high availability environment to attend business continuity. To address those issues, one role of system architect is to design an effective project with a small set of information and details about the company systems. This paper presents an approach for system architecture design that succeeds, and a hypothetical scenario based in real cases.*

Index Terms — data center, infrastructure, disaster recovery plan, business continuity, business impact analysis, system architecture.

CONCEPTS

Disasters such as: flood, fire, earthquake, complete machine failure, human error or just an unplanned application (APP)/software outage can result in downtime or data loss. To ensure resilience and afford system operation and availability for unexpected events, that cans unable business to run totally or partially, it is fundamental to prepare a DRP (Disaster Recovery Plan) [30, 5]. A DRP usually require a remote data center to take over mission critical operation when a disaster occurs at the main data center [17, 37].

Does not matter the institution size, it is not **IF** a disaster will occur but **WHEN** it will happen [25]. Even small companies require IT (Information Technology) to support business and to guarantee services and systems continuity in a failure/disaster. Sometimes a disaster and recovery project should be designed by the system architect without a BIA (Business Impact Analysis) and details about the organization modus operandi [10, 28]. Some small companies or enterprise's business unity do not want to provide all details about their operation for partners or suppliers/providers. Moreover for security reasons, or because business and IT are very close, understand the infrastructure that supports business means understand some particular strategies.

This paper presents an approach to create a backup (BKP) site based in infrastructure architecture, with a small set of details, but is important to notes that it is not the intent to replace a DRP and BIA, but the "**Architecture Based Backup Site Project**" presented at this article is a different approach to work with a lack of information about a company.

There are documents and references about many industry standard technical terms and acronyms used along this text. Some of them require a description:

Domino Server: This is the IBM collaboration software, with build in e-mail and workflow systems named "IBM Lotus Domino", the client application is called "Lotus Notes". It helps companies to manage information and no structured data (text documents). The HC has 2 of them.

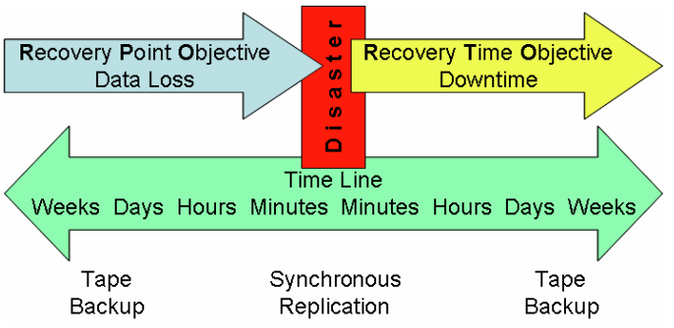
Terminal Server: It is a component of Microsoft Windows OS, which provide a thin-client solution, in with users can run a remote application installed at the server instead of their own workstation (client). The HC has three of them.

Web Farm: A set of WEB server that work together to attend the amount of Internet requests.

METRICS

Without a DRP, BCP (Business Continuity Plan) and BIA in place, it is possible to define for guide lines some metrics to understand the infrastructure criticality and design a backup site project centred in the architecture, such as RPO (Return Point Object) and RTO (Return Time Objective). The RTO is related with the downtime, it is the total amount of time acceptable for the business to wait the system start running again, after a disaster event. The RPO is related with data loss, it is the time between the last backup and the disaster moment, it is the business tolerance to data loose [17, 26, 29], such as illustrated at figure 1.

FIGURE. 1
RPO AND RTO [5, 6]



[1] Eng. Daniel de Souza Carvalho, Master studant of Electronic Engineering at Universidade Presbiteriana Mackenzie, São Paulo, Brazil, danielscarvalho@gmail.com
[2] Eng. Samuel de Barros Moraes, Pos graduation professor at FASP – Faculdades Associadas de São Paulo, São Paulo, Brasil, samuel.barros@gmail.com

Those metrics in a normal process should be defined at the BIA time, which is part of BCP or DRP. Different values for RTO and RPO can be defined by each system. It's important the IT team keep in contact with each application sponsor/owner to define appropriate metrics even without a formal BIA process, and elect key users to help build up the disaster strategy. The engagement and evaluation of key users is important to provide quality to the process. With these two metrics defined for each application and the main data center current IT architecture, it is possible to find out the appropriate technology to move data from the main site to the backup site for each application, around the amount of different possibilities.

CURRENT ARCHITECTURE ANALYSIS

The first step to analyse the current IT architecture is to identify applications and their particular criticality, creating a list with the following minimal information:

- Application identification
- Server where the application is hosted in
- RPO and RTO per application

The list can be used as a guide line, to find out the suitable solution to transfer data between two data centers. The list at table 1 describes the hypothetical scenario (HS) for this paper, based in real cases for small and medium companies.

Application Identification	Server Name	RTO Time to Recover	RPO Acceptable Data Loss
WEB Farm	WEB1	1 HOUR	1 DAY
	WEB2	1 HOUR	1 DAY
	WEB3	1 HOUR	1 DAY
	WEB4	1 DAY	1 DAY
	WEB5	1 DAY	1 DAY
	WEB6	1 DAY	1 DAY
Domino – E-Mail	DOM1	4 HOURS	15 MINUTES
Domino – Applications/DB	DOM2	1 DAY	15 MINUTES
Terminal Server – User App	TS1	6 HOURS	1 DAY
	TS2	1 DAY	1 DAY
	TS3	1 DAY	1 DAY
File Server	FS1	8 HOURS	15 MINUTES
	FS2	8 HOURS	15 MINUTES
Application Server – Cluster	APP1	1 HOUR	1 DAY
	APP1	1 DAY	1 DAY
Data Base – (Active-Active)	BD1	1 HOUR	15 MINUTES
	BD2	1 DAY	15 MINUTES
Backup Server	BKP	1 HOUR	15 MINUTES
Development Server	DES1	2 DAYS	12 HOURS
Quality Server	QOS1	2 DAYS	12 HOURS
Application Test Server	TEST1	2 DAYS	12 HOURS

TABLE. 1
APPLICATION CRITICISMS LIST

At this HC, the data is concentrated at the data base (DB), file and Domino servers, and the acceptable data loss is less than one our, this is the most critical point, moreover those servers are in cluster or parallel processing (active-active) at the main data center, figure 3. Some server does not keep data in their internal disks (hard drives), just logs, executable and configurations files, which should be saved by the backup process, such as: WEB Farm; Terminal Server (TS); Application Server; Backup Server.

The Development, Quality and Test servers keep the source code of applications, this is a critical component too, but there is not data in local storage.

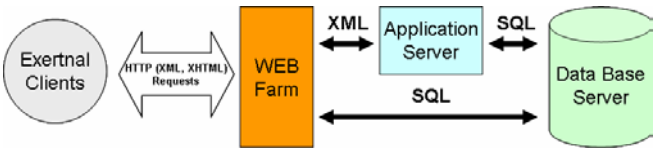


FIGURE. 2
WEB APPLICATION COMPONENTS

The critical application path, figure 2, requires 1 Hour RTO to attend external requests from clients and partners; this is the first system to be restored in a disaster. The WEB application is composed of WEB Farm, Application and Data Base Servers.

There is a bigger RTO tolerance, medium priority, for systems that provide services for internal clients (users) such as Domino Application, File and Terminal servers. In another hand, the E-Mail Domino system that keeps the communication with clients and employees has a different priority.

At last, the low priority systems are the development, test and quality environment. Many practical scenarios, do not support it at the backup site, this decision can be defined by the IT team in accordance with key users.

The HC requires hybrid solution as follow:

WEB Farm, Terminal Server and Application Server – Manual (procedure) approach can be adopted, when a new configuration, system or file is installed by the administrator/operator, the same procedure should be executed at the backup site. On another hand, deployment systems such as CVS (Concurrent Version System) can be configured to install new files in booth servers (main site and backup site).

Domino Servers – It can use the native replication capability and synchronize data at booth sites, at Application and E-Mail servers, it can guarantee the required RTO and RPO.

File Server (FS) – The build in replication capability of the operation system (OS) can be used;

Data Base Server – There are many different possibilities to replicate data bases, but for small infrastructure a "stand by" data base could be appropriate. This method save a local log file at the main data base with the updated and additional data, and those files are sent to the "stand by" data base that apply/load this transactions and keep the backup site updated [30].

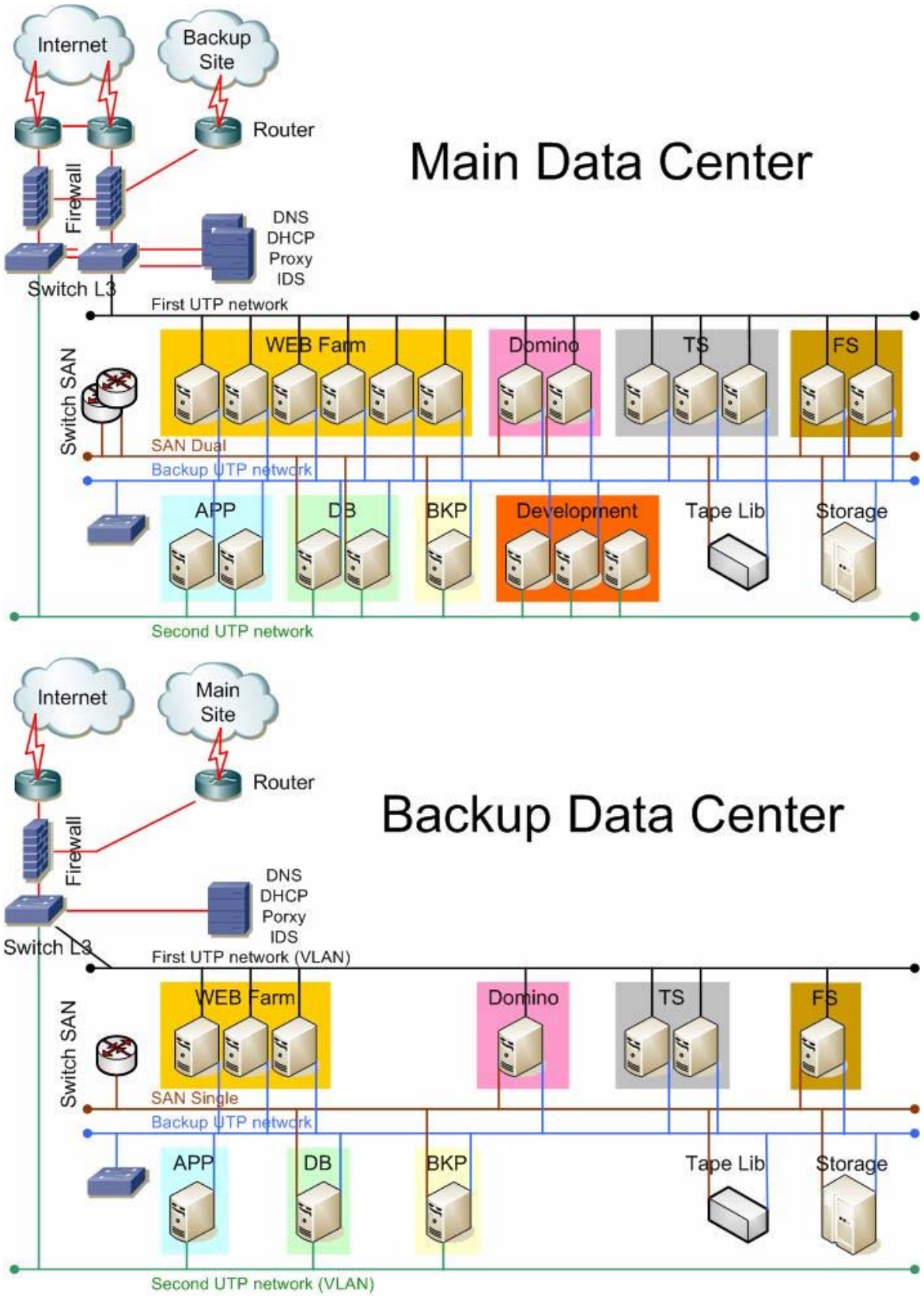


FIGURE. 3
DATA CENTER ARCHITECTURE, MAIN AND BACKUP DATA CENTERS

Backup Server – The backup "index files" should be sent to the backup site, by scripts or operating system. It's appropriate to find out the particular backup system DRP capability and flow the recommendations.

Development Server – For this scenario the idea is do not keep development files at the backup site. But the source code, configuration files and so on should be stored in backup tapes at the external company.

Storage replication can be considered for all high priority systems (1 Hour RTO), it is efficient for data bases for example, and for disk less solution (servers that don't have local hard drive). But, one system can fail at backup site even with storage replication, if some required file or configuration is applied at the local OS, and not applied to the backup site by an administrator or operator.

Storage replication can be done in two different ways (for most brands): 1. Synchronous, extend the Storage Area Network (SAN) with a Dense Wavelength Division Multiplexing (DWDM) [31, 15] link connected by Fiber Channel (FC) directly to the SAN Switch at booth data centers in 4Gbps; 2. Asynchronous, make use of an appliance that converts and cache storage written blocks that pass thought the SAN switch, and convert it to iSCSI, send by an standard Ethernet 100Mbps link [41].

Virtualization allied to Storage replication is another possibility to avoid human errors and consolidate physical servers at backup site.

Storage replication and virtualization can be considered for medium to large architectures.

MAIN SITE ARCHITECTURE

The process introduced at this paper get most of information based at the main site architecture. The HS main site is described as follow, and figure 3, with its high availability resources:

- Dual internet connection by two different ways;
- Routers, firewalls and switches layer 3 in cluster;
- Two serves (no cluster) to provide basic network services like: Domain Name System (DNS); Dynamic Host Control Protocol (DHCP); Proxy; Intrusion Detection System (IDS) and so on;
- Dedicated telecommunication Ethernet link to the backup site (starting with 100Mbps);
- Three physical Ethernet networks: "first" the MZ (Militarized Zone) front end network with internet access; "second" the MZ back-end network without internet access; isolated "backup" network with dedicated switch, all server are connected on it;
- SAN fiber network, two SAN Switches, each server has 2 Fiber Channels HBAs;
- Tape library (LIB) connected to backup network and SAN network, to provide disk-to-disk and disk-to-tape backup;
- Storage system connected to the backup, SAN and second networks.

BACKUP SITE ARCHITECTURE

The backup site is designed as a kind of 50% infrastructure, as follow (figure 3):

- Single internet connection, with Virtual Private Network (VPN) access to key users, administrators and operators (for home office support);
- Single network device: Router, firewall and switcher layer 3;
- One server to provide network services (DNS, DHCP – IDS and Proxy optional);
- Dedicated link to the main site;
- Two physical Ethernet networks: "first" the MZ with two Virtual Local Area Networks (VLANs) "front end" with internet access; and "back-end" without internet access; isolated "backup" network with dedicated switch, all server are connected on it;
- SAN fiber network, one SAN Switcher, each server has 1 Fiber Channel HBAs;
- Tape library connected to backup network and SAN network, to provide disk-to-disk and disk-to-tape backup;
- Storage system connected to the backup, SAN and first networks (VLAN).

FINAL THOUGHTS

A DRP, BCP or BIA should be used to approve and validate the backup site project designed with the IT architecture point of view. Nevertheless the process is efficient to small and medium companies that do not have a plan in place.

The key users should define if the backup site need to keep the same performance and processing power of the main data center, 50% of performance may be suitable to find out an economic solution.

Check out the replication and high availability capabilities of each application/software, operation system and the possible strategies for DRP, according their manufacturer orientation and documentation.

Some actions can help to prevent human errors: training; updated documentation; periodic tests.

To keep the backup site ready to go:

- Keep the documentation updated and published, with easy access is fundamental. In an emergency, people do not need to remember the process, just to follow the script;
- All application should use name services (DNS), in order to provide redirecting of services between data centers.

- The backup tapes should be sent daily to external archiving at a digital document management company. And the software and type of tape should be the same at booth sites;
- The key users need to test VPN access frequently.
- At least two tests with all personal should be executed per year basis.

A backup site Project is a complex issue, which involves technical skills, business needs and economic equilibrium, the "Architecture Based Backup Site Project" can help small and medium size institutions to quickly design a solution.

REFERENCES

[1] Adamopoulos, A, "Data Classification and Storage Optimization".

[2] ADC Telecommunication,"TIA-942 Data Center Standards Overview", White Paper, 2006.

[3] Advertise UK Resilience, FEMA, SBA, "The Business Continuity Planning & Disaster Recovery Planning Directory", hyperlink: http://www.disasterrecoveryworld.com/, 2007.

[4] Ameinfo, "The A to Z of Windows disaster recovery", hyperlink: http://www.ameinfo.com/49091.html, 2004.

[5] Ameinfo, "Why does backup still matter?", hyperlink: www.ameinfo.com/49843.html, 2004.

[6] Anthes, G, "Data Centers Get a Makeover", Computer World, November, 2004.

[7] Arnold, R, L, CBCP, "Recovery From Sept. 11 Events Is Slow Process", Disaster Recovery Journal, Attack on America, Special Report.

[8] Baser, E, "A Guide to the Perplexed Business Owner: Helping your business survive the unexpected shutdown", Ennovatec inc, 2007.

[9] Benton, D, "Disaster Recovery: A Pragmatist's Viewpoint", Disaster Recovery Journal, Data Recovery, 2007.

[10] Bredemeyer, D, Malan, R, "The Role of the Architect", Architecture Resources for Enterprise Advantage, Bredemeyer Consulting, WhitePaper, 2006.

[11] Castro, F, "Oracle Application Server 10g Release 2 Disaster Recovery", Oracle, WhitePaper, 2005.

[12] Cisco Systems, "Cisco Integrated Firewall Solution", Data Sheet, C78-345384-01, 2007.

[13] Cisco Systems, "Data Center Infrastructure Architecture Overview", USA, March, 2004.

[14] Cisco Systems, "The Cisco Enterprise Data Center Architecture – Data Center Security Solutions", 2005.

[15] Cisco, "Introduction DWDM Technology", Chapter 1, OL-0884-01.

[16] Citrix, "IBM Lotus Notes Server Consolidation and Client Deployment", Citrix AccessAnswers, 2005.

[17] Cocchiara, R, "Beyond disaster recovery: becoming a resilient business", IBM, October, 2005.

[18] Fishman, M, EMC, "Disk and Tape Backup Mechanisms", SNIA – Storage Networking Industry Association, 2007.

[19] Gartner, "Sample Company: Business Impact Analysis", 2002.

[20] Haag, S, Cummings, M, McCubbrey D, J, "Management Information Systems for the Information Age", McGraw-Hill/Irwin, June 2004.

[21] HP, "Building a disaster-proof data center with HP Extended Cluster for RAC", Hewlett-Packard Development Company, 5982-3575EN, Rev. 3, July, 2007.

[22] HP, "HP Extended Cluster for RAC: Continuous availability with the flexibility of virtualization", Hewlett-Packard Development Company, 5982-3575EN, Rev. 2, August, 2005.

[23] IBM, "IBM Data Replication Summary", Presentation, 2007.

[24] IBM, "IBM Storage Infrastructure for Business Continuity", Presentation, 2007.

[25] Martin, J, "Overview of a Disaster Recovery Plan", PLUSS Corporation.

[26] Massiglia, P, "High Availability and disaster recovery for NAS data", Agami Systems, SNIA, Presentation, 2007.

[27] Miller Jr, T, A, "Unisys Safeguard Solutions for Disaster Recovery and Business Continuity", Unisys, WhitePaper, May 2007.

[28] Muller, G, "The role and task of the System Architect", Embedded Systems Institute, April, 2007.

[29] Oracle, "Executive Brief: Disaster Recovery Planning", 2006.

[30] Oracle, "Oracle Backup and Recovery Workshop", v1, July, 1998.

[31] Padtec, "CWDM – DWDM Tecnologias para alta capacidade", Presentation, http://www.padtec.com.br, 2007.

[32] Peterson, E, "RAC on extended distance clusters", Oracle, 2007.

[33] Records Management Services, "Vital Records: How Do You Protect And Store Vital Records?", Washington University, hyperlink: http://www.washington.edu/admin/recmgt/vital.store.html, 2004.

[34] RedHat, "Planning for Disaster", Red Hat Linux 8.0 Manual: The Official Red Hat Linux System Administration Primer, 2002.

[35] Schimidt, J, Nickolett, C, "Business Continuity Planning Description and Framework", Comprehensive Consulting Solutions, WhitePaper, April, 2001.

[36] Shimonski, R, J, "Planning for High Availability: Disaster Recovery Planning", WindowsNetworking.com, 2004.

[37] Stringfellow, S, "Disaster Recovery Requirements Analysis", Sun BluePrints, July, 2000.

[38] TechRepublic, "Disaster recovery plan updated checklist", V. 2, April, 2005.

[39] The Business Continuity Institute, http://www.thebci.org/, 2007.

[40] Tuerner, W, P, Seader, J, H, Brill, K, G, "Tier Classification Define Site Infrastrucutre Performance", The Uptime Institute, 1996.

[41] Unisys, "Unisys SafeGuard 30m Solution", 2006.