Spring 2012

Senior Project Report

Computer Science Department

California State University, **Dominguez Hills**

Disaster Recovery

Steve Suttles

In
Partial Fulfillment of the requirements

For
Senior Design – CTC 492

Department of Computer Science
California State University, Dominguez Hills
Spring 2012

Committee Members/Approval

Faculty advisor *Signature* *Date*

Sandy Taylor_

Committee member *Signature* *Date*

_Howard Ross

Committee member *Signature* *Date*

Dr. Mohsen Beheshti

Department Chair *Signature* *Date*

Abstract
CTC 492 Spring 2012
Steve Suttles

Disaster recovery is the process, planning, and practice of how a company brings their computer systems backup up and running after their data center becomes unavailable. For my senior project. My team manages 320 windows servers, over ½ of these servers are virtual running on VMWare ESX 4.1. This includes internet facing, databases, email, file and print servers. I would like to present the hardware and software needed, and information on how to select the location. Critical to rebuilding the data center after the disaster is what services are most important to get back online. What services can you go without. Where is the data and how do you get it where it needs to be. Important to disaster recovery is an understanding of how long it will take to restore service and how much data will be lost because of the disaster. These are known as Recovery Time Objective (RTO) and Recovery Point Objective (RPO). There are several types of disaster recovery plans which include Hot, Warm, and Cold data recovery. The recovery plan I expect to put in place will be a combination of all 3. We have a location selected and some recovery hardware in place. In this document I would like to point out our short comings and put together a cookbook so anyone with some computer knowledge could rebuild our datacenter at the new location.

Table of Content:

Chapter 1 Introduction

Chapter 2 Background

Chapter 3 Environment outline

Chapter 4 Recovery Plan

Chapter 5 Testing Plan

Chapter 6 Conclusion

Chapter 1 Introduction to Disaster Recovery

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others[1]

1.1 Need for Disaster Recovery

Disaster recovery is how a company can get their computer systems backup up and running after their data center becomes unavailable. For my senior project I would like to build a disaster recovery plan for my company. My team manages 320 windows servers, over ½ of these servers are virtual running on VMWare ESX 4.1. This includes internet facing, databases, email, file and print servers. I would like to present the hardware needed, and how to select the location. Critical to rebuilding the data center after the disaster is what services are most important to get back online.

Important to disaster recovery is a understanding of how long it will take to restore service and how much data will be lost because of the disaster. There are several type of disaster recovery plans which include Hot, Warm, and Cold. The recovery plan I expect to put in place will be a combination of all 3. We have a location selected and some recovery hardware in place. In this document I would like to point out our short comings

[1]

and put together a cookbook so anyone with some computer knowledge could rebuild our datacenter. " In a recent survey, Coleman Parkes Research found that North American businesses lose $159,331 per year through IT downtime (average 10 hours/year) and data recovery.2 In the same survey, small companies lose more than $55,000 in revenue due to downtime and recovery, mid-sized companies lose $91,000-plus in revenue, and large enterprises more than $1 million in revenue. And that's just revenue, not counting lost employee productivity from IT downtime, harm to company brand and reputation, non-compliance with regulatory commitments, and damaged staff morale and customer loyalty."[2]

1.2 Why I selected this topic?

The current disaster recovery plan for the City is to restore all windows servers from the windows backups that we have off site. These backups are over 3 weeks old. We are slowly creating a new philosophy toward backup and disaster recovery however if we had an event today it would take several months to recover and what we could recover would be less than optimal to the business units. The balance of backup and disaster recovery and the accoiated cost is very hard to sell to management. But its insurance just like what you purchase on your house and car or your person for that matter, it is not important until you need it.

As a business you need to weigh the cost of backup and disaster recovery verses the cost of how long can you afford your business to be closed and what is the impact to your customer base and the public in the case of the City if you are not available to help your constituents. The City provides many services to the constituents, in time of a disaster none more important is the best recourse of how to sustained life. I manage a team of 4 network analyst and we support over 300 windows servers. It is important that we can restore communication and services to the City and the worker within the City as soon as possible. The management of the City is concerned about how we will continue to provide excellent service to the constituents and I would like to put a plan in place that a

[2]

doesn’t require a person knowledgeable of the City network to bring the system back on-line.

In today’s economic climate it is difficult to devote time to a disaster recovery plan. We are being asked to do more with less and just keeping the ship afloat is a large task. I am currently trying to achieve by Bachelor’s Degree and it seemed a perfect match to complete my disaster recovery project with my senior project. Parts of the project have already been decided for me (Location, Equipment, Recovery Software). There is no implementation plan and no assessment of how or if it will work. I find myself trying to build something from what I have and if I did not have a plan today but need to recover I would build it on the fly. At the end of the project I will have something that could be given so anyone with some server experience and they could recover the City’s environment with little or no problems.

Disaster recovery in not new to information technology these same issues occurred in business before computers. If you had a business where you extended credit to your customers and then lost all your credit recites due to fire or some other disaster, how do you recover from that. Do you just trust in the honesty of your clientele I don’t think so. If you are an intelligent business man you have a backup copy of the people that owe you. This is the purpose of a disaster recovery plan.

1.3 What I would like to learn?

This project is double fold it allows me to complete my CTC 492 requirements and also will assist me in the disaster recovery project I have been working on for the City. Disaster recovery is an overlook part of information technology. Disaster recovery is not important until you need it and don’t have. It is also very costly to recover with in a reasonable time with out spending big bucks. The City has made a substantial investment in disaster recovery hardware and would now like to see the plan in place to take advantage of the investment. I would like the find the major pitfalls in the design and find workarounds to resolve them. A few of the problems that have already been identified and we are working to resolved are

- Building new backup server and cataloging backups would take a very long time.
- Restoring the Oracle database servers requires the Rman server to be available so this should be one of the first servers to be restored.
- Restoring servers to dissimilar hardware takes a special

1.4 Defining the Process

There are several steps to creating a disaster recovery plan as defined in, “ The Disaster Recovery Handbook”, these steps and be used in creating a disaster recovery for any type of business.

1. Define a Project sponsor this person needs to be very high in the business structure. A person that can make all the different groups come together to complete the project plan. **Technology Services Manger**

2. Assign a Business Continuity Manager, this person will schedule the different teams that need to assist in creating a successful disaster recovery plan. **Technology Services Infrastructure Manager**

3. The Sponsor and the Business Continuity Manger need to clearly define the scope of the project. This is a critical meeting if the scope is to large the project is destine to fail and if the scope is too small it may be ineffective if truly needed. **Data Center Manager**

4. The Business Continuity Manager must select a team. This should include service level experts. **Server Support Supervisor**

5. The Business Continuity Manager and Project team should develop the project plan. **Server Support Team, Data Base Team, Application Team, LAN/WAN Team**

6. Execute the project plan.

7. Document project execution and testing.[3]

[3]

Chapter 2 Background

Considerations for disaster recovery include what does your server environment look like do you have physical or virtual servers. What is your RPO (recovery point objective) and RTO (recovery time objective)? Will you have Hot, Warm, or Cold recovery site? Is there a possibility of using replication or clustering to enhance your recovery solution?

2.1 Replication & Clustering

Other considerations of disaster recovery include what systems can be replicated or cluster with in cost restraints. In looking at our disaster recovery project it was evident that the most important systems we have related around communications and the internet. The Email system we have implemented is Lotus Notes 8.6 which was originally configured in a fail over format. The secondary node in the cluster is able to take over for the either primary node in the cluster. This format lends it self well to a disaster recovery configuration. We simply moved the secondary node to the disaster recovery site and made the necessary configuration changes to the network to allow the secondary to become the primary if the primary becomes unavailable.

Systems that have been replicated to our disaster recovery site include DNS, DHCP, Internet access, Internet proxy, Email, and Active directory. All of the systems listed above have been created to allow mutual dispersed systems and this functionality we have taken advantage of. As we define the City systems it is very important that we take advantage of all the system that can be cluster or replicated. The rest of the systems will be restored the old fashion way.

The primary DNS server is at city hall, we on a regular basis fail over to the secondary with no issues. We have more then 15 Active Directory servers. More then 3 that exists on the hardware at ECOC or on the hub of server not on the shoreline.

2.2 Physical Servers VS. Virtual Servers

In the late 80's early 90's companies started using local area networks and commodity servers. Application, file / print, and database servers sprung up very fast the created a server sprawl in the data center. The inexpensive cost allowed companies to build servers for each service needed.[4] But this caused a problem in creating a disaster recovery plan because to restore these systems requires the same hardware at the recovery site as at the production site. To have the same equipment at both sites is very expensive. To acquire the same equipment after a disaster would take quite a bit of time that most businesses cannot afford.

In the mid to late 90's the ability to virtualize servers was introduced to the commodity server market. This technology has several benefits. It allows a company to have a smaller footprint saving on electricity and less space needed in datacenter. Since the virtual server has the hardware abstracted from the operating system it is no longer necessary to have the exact same hardware at the disaster recovery site. Money is also saved because when running virtual servers it is possible to use more of the total capacity of the physical server hardware. When using physical server most of the process power goes unused. The use of virtual servers also minimizes downtime because the virtual server can be moved from one host to another without bringing the virtual server down. This allows for hardware maintenance without downtime.

2.3 Hot Warm Cold Recovery

Disaster recovery can be broken down in 3 types. My recovery plan will take advantage of all 3. Cold recovery requires your backup files be offsite. It can but doesn't require a recovery location but it could. This is the least expensive recovery method; however it does take the most time to recover. Hot recovery requires fully redundant hardware at a remote site and includes and some type of data replication. This is type of recovery is the most expensive and has the fastest recovery time. It also requires some sort of

[4]

communication between the production site and the recovery site. Warm recovery consists of a recovery site with backups on site ready to be recovered. It is as expected the middle ground between a cold recovery and hot recovery. The plans that will be use in the report will a combination of all 3 recovery types. Some services will be replicated, some services will have hardware ready to be restored to, and some systems have been deemed to costly to duplicate the hardware so in the event of a disaster hardware will need to be purchased to rebuild these systems.

Chapter 3 Environment Outline

Before starting the disaster recovery plan it is important to define what your current environment consists of and what changes need to be made to get you to your target environment. What backup software are you using and do you need something different. Where are the backup stored and how will they get to the recovery site.

3.1 Existing Disaster Recovery Environment

At the start of this project our disaster recovery plan we had tape backups of which the 3rd week of tapes went off-site to Iron Mountain. Iron Mountain is a records storage and management company. The backup model was a daily differential backup and a weekly full back up to tape. Over the years we found that the backup window was to short so we moved to backup to disk. The weekly full backups were moved to tape and every week the 3rd week of backups was sent offsite. What that means in practical terms is that we thought we could afford 3 weeks of lost data in an actually disaster. As more systems have moved off the mainframe and more systems became automated the more the backups and disaster recovery system has come to the forefront of importance. We evolved from backup tape to disk to disk backup with secondary backup offloaded to tape. The backups were moved to a complete disk to disk backup, but it was still necessary to backup to tape to move systems offsite. Finally the backups were replicated to the offsite location which has now become our disaster recovery site. The network connection between has been upgraded to a 2 Gigabit fiber which has allowed us to backup directly from our primary data center to disk targets at our disaster recovery site. This change made the need for another company to store or backups unnecessary.

3.2 Backup Systems

The existing backup systems for all windows system include 4 core products.

- Backup Exec! Is used to backup all windows file and operating systems
- Oracle Rman is use to backup all Oracle databases
- vRanger , is used to backup all virtual servers and virtual workstations
- Microsoft SQL backup, is used to backup all MS SQL databases

We currently have 6 Backup Exec servers that point to Data Domain 565 targets. The DD565 are located at our disaster recovery site and do data deduplacation. We are getting a 25 to1 deduplication ratio. We have 2 Oracle Rman servers which backup the Oracle databases to a Dell MD3200i. The Dell MD is an iSCSI disk appliance which allow the server to present the disk as a network drive, but it does it over the network to the target at our disaster recovery site. We have 2 vRanger servers they are use to backup all the virtual server in our server environment, these backups also use the DD565 as the backup target. The SQL servers backup to local disk on the SQL server then the SQL backup file is captured by Backup Exec backup job which is copied to the DD565.

Since all of the backups have targets that are offsite we have deemed that it is not necessary to make duplicate copies of the backup jobs. The production systems are at one location and the backups are at another site therefore if the production site becomes unavailable we have the backups elsewhere and if we lose the backup site we have all of the production systems still running.

3.3 Existing Production Environment

The environment that we are trying to document for recovery, consist of 328 windows servers, there are 208 virtual server and 120 physical servers. Most of the physical servers are Oracle database and application servers. We also have a Ctrix applications server environment that will soon be converted to virtual. This plan only include the Windows servers however, the Infastructure Division includes a Mainframe team and a Open systems team (unix, linux). The mainframe disaster recovery plan is completely in place. The open systems are being ported to x86 systems to allow for easier portability and disaster recovery systems. The open systems and mainframe are not be covered in this plan.

Chapter 4 Recovery Plan

"A disaster recovery plan is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The plan should be documented and tested to ensure the continuity of operations and availability of critical resources in the event of a disaster. The primary objective of disaster recovery planning is to protect the organization in the event that all or part of its operations and/or computer services are rendered unusable. Preparedness is the key. The planning process should minimize the disruption of operations and ensure some level of organizational stability and an orderly recovery after a disaster.

Other objectives of disaster recovery planning include:

- Providing a sense of security
- Minimizing risk of delays
- Guaranteeing the reliability of standby systems
- Providing a standard for testing the plan.
- Minimizing decision-making during a disaster"[5]

4.1 Describe Preparation Steps

In looking at our current recovery plan it was apparent that our disaster recovery would take far too long. As we upgraded the network and the backup hardware we found that we could put together a plan that would allow us to recover much faster with some modifications and some planning. As more applications are moved off the mainframe the windows systems became more important to the recovery plan. There are still several important applications on the mainframe, but there are many more important applications on the windows systems. To begin the recovery plan we need to define the systems to be recovered. Determine the priority of recovery and test the recovery plan

[5]

4.2 Acquire Hardware / Software

I was asked one day how much hardware it would take to rebuild our environment if we had a disaster. I ran a report on the total number of servers, and then found out how many of these servers could not be virtualized due to hardware constraints and then divided that number by 25 because on average we are able to run 25 virtual servers on 1 physical host. We then purchased 2 fully populated Dell M1000e blade chassis's with 16 Dell M610 blade servers in each and 8 Dell R710 stand alone servers. These servers are connected to EMC NS480 Disk. It will take 12 ESX servers to recreate our existing virtual server environment. It will take another 4 ESX servers to convert the physical servers to virtual that have not yet been converted. Then we have 12 servers that have hardware dongles that require a physical server which will be install on the remain blade servers and we will need to purchase T1 cards and Fax cards for the final 4 servers.

4.3 Determine Priority

Determining the priority was a very difficult task. We first asked the application team to prioritize the systems by using a numbering system.

1. Cirtical must never go down
2. Important server must be up in less than 24 hours
3. Important server must be up in less than 72 hours [6]

The applications team can back and said that all of the applications were critical. After hearing this it was evident we would need to make this decision for them. At this point we have decided that Email, Active Directory, DNS, DHCP, and Internet access. All of these services are replicated across the network. Next we will restore the virtual server and then the physical server.

[6]

4.4 Provision Hardware / Software

To not completely waste the hardware that was purchased it was decided to use it for test systems. Several blade servers have been loaded with VMWare ESXi and connected to the disaster recovery SAN. There is a total of 5 blades setup for test and in the event that a disaster does occur the test systems will be removed and the test environment will be used for production. Additional VMWare system will need to be provisioned but there will already be a starting point for the recovery. Copies of all necessary software has been copied to a data store at the disaster recovery site. This includes ISO files of all Operating Systems disks and all applications software.

Chapter 5 Testing Plan

Just as important as creating a disaster recovery plan is testing the plan. Types of test include checklist tests, simulation tests, parallel tests, and full interruption tests. It's also important to determine what can be tested, how it could be tested, and then evaluating the test. And documenting what could not be tested.

5.1 What Can We Test?

With the several different types of servers the question in this report is what can we test, and how many systems do we need to test to validate that our test plan is well documented. It was decided that all of the hot site components should be tested because the expectation is that the hot site systems will fail over automatically whenever either side fails. Every weekend the mail servers are rebooted and automatically fail over the to the clustered server which is a weekly test of the mail system. The DNS and DHCP servers re rebooted on a monthly schedule which validates the fail over process of that system. Active Directory replication is check once a week and system that are closest to the disaster recovery site get there the authentication from this site which validates its replication.

5.2 How do we test it?

It is very important to come up with a well thought disaster recovery testing plan. What can be tested? There are some systems that may not be able to test due to financial constraints hardware or other constraints.

- How long will the test take? Most tests will require system down time of the production system, which may cause hardship to the business unit. This down time is due to the fact that other production systems are production at the disaster recovery site already.

- Who should be involved? The current testing plan the IT team will do the testing in phases. The IT staff will test system recovery, databases, application servers, and file / print services, and web servers. The staff will validate that the process works as expected. The next phase will include the customer.

- Does the test involve system down time? The test will be taken of a case by case basis with the objective to have the least impact on the customer as possible.

The first of theses test is planned for March 3, 2011 see the appendix 1.1 for the project plan and time line. In this test we will restore the Occupation Health System. This system includes an Oracle database and an Oracle Tomcat web server. The Oracle database is on a physical server and will be converted to a virtual server and the web server is a virtual server and will be restored from vRanger the virtual server backup software. This test will also include a database restore from the Rman server. The Server support team will bring down the production servers and change the DNS IP Addresses for the restored servers to allow the Rman restore to work and to allow the applications administrator to test the system. After the system has been tested the server support team will bring down the disaster recovery system and bring the production systems back online.

5.3 Evaluate what was tested

Looking at what was tested it was a very good exercise to build a plan and test the plan. It is evident that the original plan was lacking any structure and was doomed to fail. By going through this exercise it we found numerous problems which have been fixed. All test were finally completed successfully now comes the difficult part which is to document all components of the restore process. I've asked all the parties involved to completely document there portion of the recovery process and will continue to put all of the documents together to create a full disaster recovery plan.

5.4 Explain what was not tested

The only systems that were not tested were the system that had hardware constraints that could not be duplicated these systems will be noted in the project plan that they could not be test and the constraint that kept them from being tested.

Chapter 6 Conclusion

Disaster recovery is more than off-site storage, it requires planning, detailed documentation, and extensive testing. A good disaster recovery plan is a company's insurance that they will recover from a disaster.

6.1 Lesson Learned!

This project is double fold it allows me to complete my CTC 492 requirements and also will assist me in the disaster recovery project I have been working on for the City. Disaster recovery is an overlook part of information technology. Disaster recovery is not important until you need it and don't have. It is also very costly to recover within a reasonable time with out spending big bucks. The City has made a substantial investment in disaster recovery hardware and would now like to see a plan in place to take advantage of the investment. The more I discuss the disaster plan the more hidden issue are uncovered. Problems that have already been identified and we are working to resolved are

- Building new backup server and cataloging backups would take a very long time.
- Restoring the Oracle database servers requires the Rman server to be available so this should be one of the first server to be restored.
- Restoring servers to dissimilar hardware is very difficult

References

[1] Paul Kirvan, IT Disaster Recovery Plan, TechTarget, 2009

[2] Tim Clark, The Best Practice for Backup Disaster Recovery for SMB's, The FactPoint Group, 2011

[3] Michael Wallace; Lawrence Webber, The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, AMACOM, December 1, 2010

[4] John Arrasjid, Duncan Epping, Steve Kaplan, Foundation for Cloud Computing with VMware vSphere, TheUSEIX Association, January 2010

[5] Geoffrey H. Wold, Disaster Recovery Planning Process, Disaster Recovery World© 1997, and Disaster Recovery Journal© 1997

[6] Darrill Gibson, Managing Risk in Information Systems, Jones & Bartlett Learning, August 19, 2010

Project Proposal
CTC 492
Spring 2012

TITLE: Disaster Recovery

Prepared by: Steve Suttles

Disaster recovery is the process, planning, and practice of how a company brings their computer systems backup up and running after their data center becomes unavailable. For my senior project I would like to build a disaster recovery plan for my company. My team manages 320 windows servers, over ½ of these servers are virtual running on VMWare ESX 4.1. This includes internet facing, databases, email, file and print servers. I would like to present the hardware needed, and information on how to select the location.

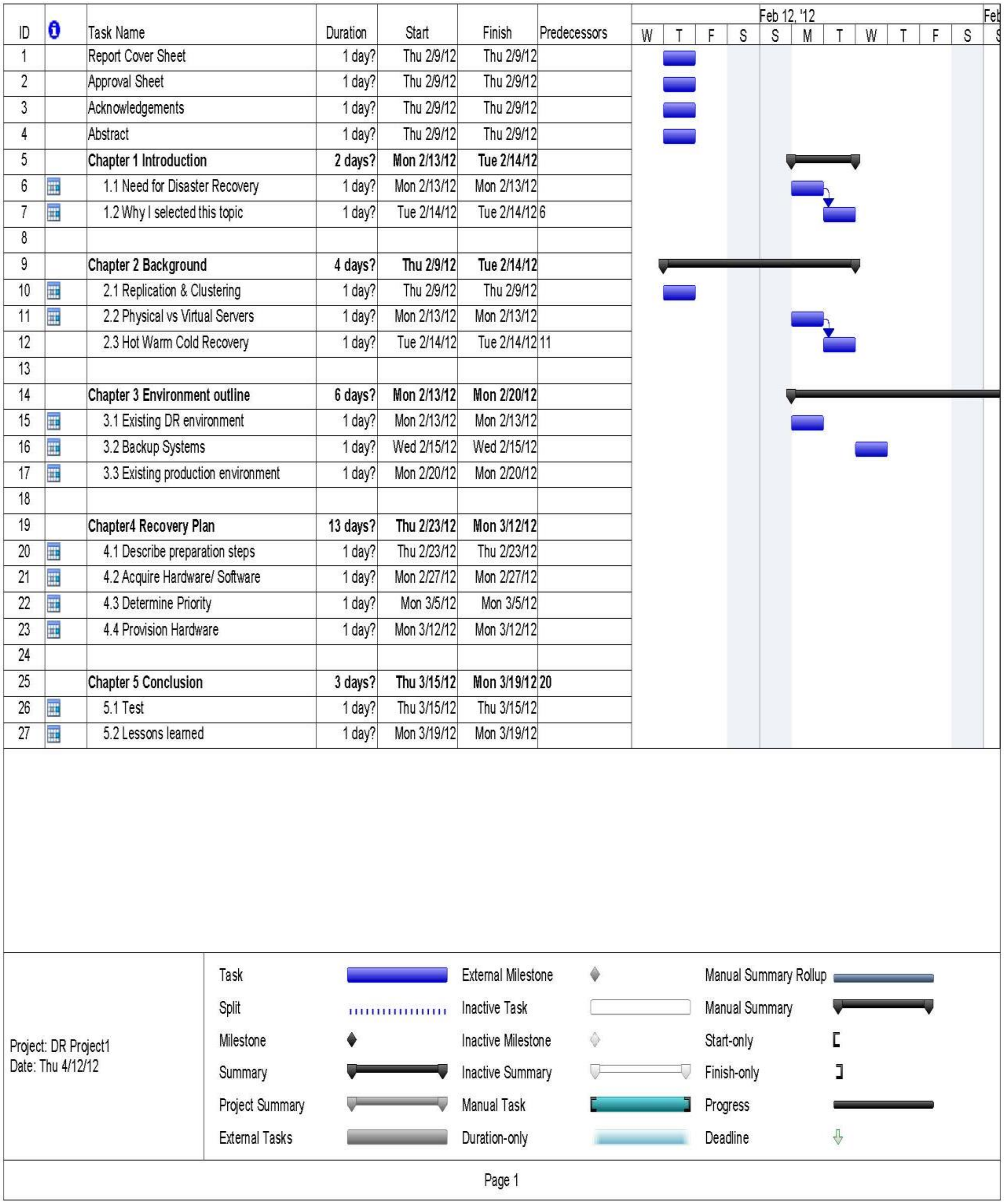
Critical to rebuilding the data center after the disaster is what services are most important to get back online. What services can you go without. Where is the data and how do you get it where it needs to be.

Important to disaster recovery is a understanding of how long it will take to restore service and how much data will be lost because of the disaster. These are known as Recovery Time Objective (RTO) and Recovery Point Objective (RPO). There are several types of disaster recovery plans which include Hot, Warm, and Cold data recovery. The recovery plan I expect to put in place will be a combination of all 3. We have a location selected and some recovery hardware in place. In this document I would like to point out our short comings and put together a cookbook so anyone with some computer knowledge could rebuild our datacenter at the new location.

Dr. Mohsen Beheshti
Faculty advisor

Sandy Taylor
Committee member

Howard Ross
Committee member

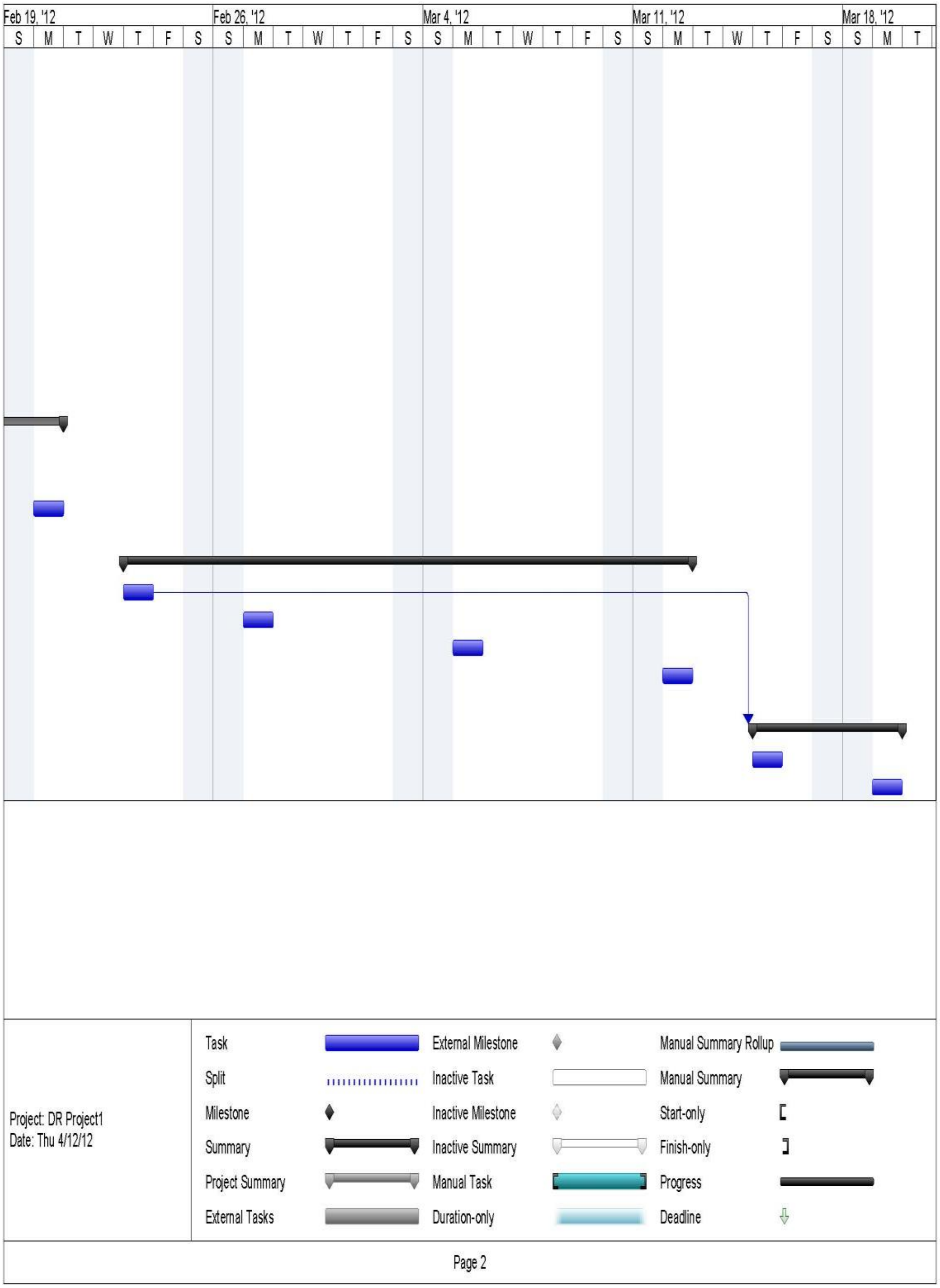


ID	ℹ	Task Name	Duration	Start	Finish	Predecessors
1		Report Cover Sheet	1 day?	Thu 2/9/12	Thu 2/9/12	
2		Approval Sheet	1 day?	Thu 2/9/12	Thu 2/9/12	
3		Acknowledgements	1 day?	Thu 2/9/12	Thu 2/9/12	
4		Abstract	1 day?	Thu 2/9/12	Thu 2/9/12	
5		**Chapter 1 Introduction**	**2 days?**	**Mon 2/13/12**	**Tue 2/14/12**	
6	▦	1.1 Need for Disaster Recovery	1 day?	Mon 2/13/12	Mon 2/13/12	
7	▦	1.2 Why I selected this topic	1 day?	Tue 2/14/12	Tue 2/14/12	6
8						
9		**Chapter 2 Background**	**4 days?**	**Thu 2/9/12**	**Tue 2/14/12**	
10	▦	2.1 Replication & Clustering	1 day?	Thu 2/9/12	Thu 2/9/12	
11	▦	2.2 Physical vs Virtual Servers	1 day?	Mon 2/13/12	Mon 2/13/12	
12		2.3 Hot Warm Cold Recovery	1 day?	Tue 2/14/12	Tue 2/14/12	11
13						
14		**Chapter 3 Environment outline**	**6 days?**	**Mon 2/13/12**	**Mon 2/20/12**	
15	▦	3.1 Existing DR environment	1 day?	Mon 2/13/12	Mon 2/13/12	
16	▦	3.2 Backup Systems	1 day?	Wed 2/15/12	Wed 2/15/12	
17	▦	3.3 Existing production environment	1 day?	Mon 2/20/12	Mon 2/20/12	
18						
19		**Chapter4 Recovery Plan**	**13 days?**	**Thu 2/23/12**	**Mon 3/12/12**	
20	▦	4.1 Describe preparation steps	1 day?	Thu 2/23/12	Thu 2/23/12	
21	▦	4.2 Acquire Hardware/ Software	1 day?	Mon 2/27/12	Mon 2/27/12	
22	▦	4.3 Determine Priority	1 day?	Mon 3/5/12	Mon 3/5/12	
23	▦	4.4 Provision Hardware	1 day?	Mon 3/12/12	Mon 3/12/12	
24						
25		**Chapter 5 Conclusion**	**3 days?**	**Thu 3/15/12**	**Mon 3/19/12**	**20**
26	▦	5.1 Test	1 day?	Thu 3/15/12	Thu 3/15/12	
27	▦	5.2 Lessons learned	1 day?	Mon 3/19/12	Mon 3/19/12	

Project: DR Project1
Date: Thu 4/12/12

Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┅	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Progress	▬
External Tasks	▬	Duration-only	▬	Deadline	⇩

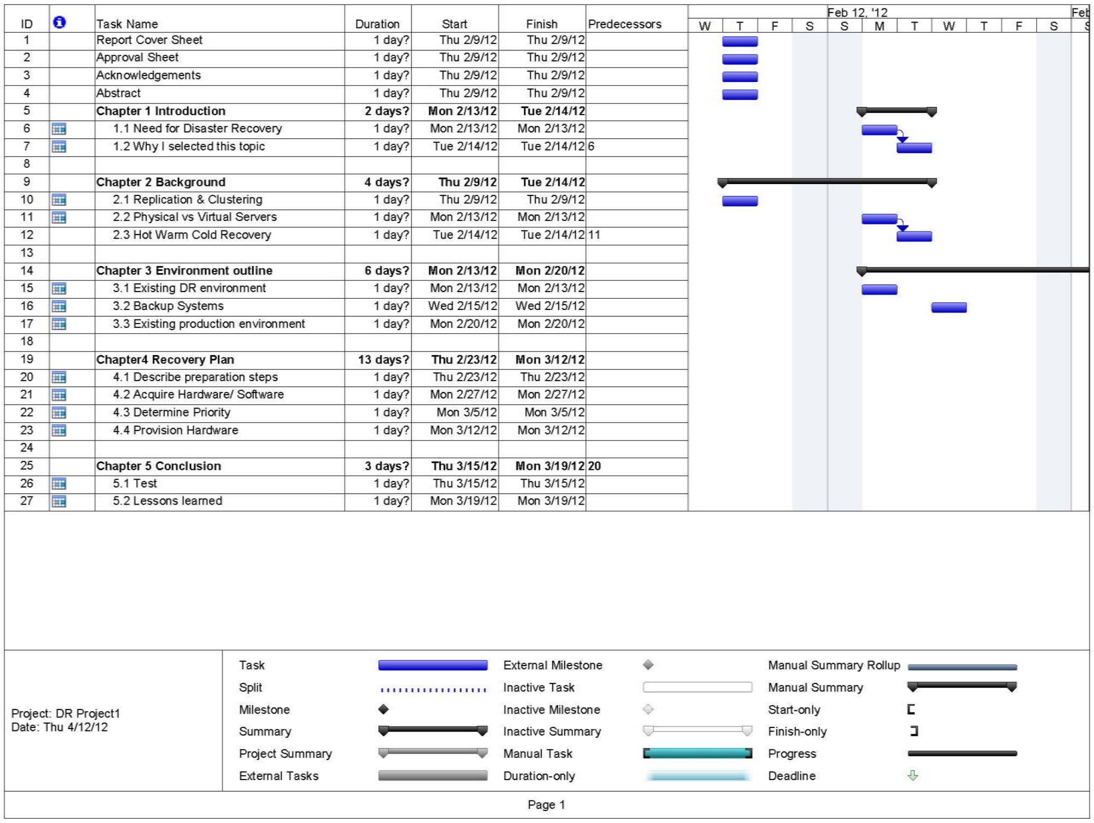
Page 1



Project: DR Project1
Date: Thu 4/12/12

Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┈	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Progress	▬
External Tasks	▬	Duration-only	▬	Deadline	⇩

Page 2



ID	ℹ	Task Name	Duration	Start	Finish	Predecessors
1		Report Cover Sheet	1 day?	Thu 2/9/12	Thu 2/9/12	
2		Approval Sheet	1 day?	Thu 2/9/12	Thu 2/9/12	
3		Acknowledgements	1 day?	Thu 2/9/12	Thu 2/9/12	
4		Abstract	1 day?	Thu 2/9/12	Thu 2/9/12	
5		**Chapter 1 Introduction**	**2 days?**	**Mon 2/13/12**	**Tue 2/14/12**	
6	▦	1.1 Need for Disaster Recovery	1 day?	Mon 2/13/12	Mon 2/13/12	
7	▦	1.2 Why I selected this topic	1 day?	Tue 2/14/12	Tue 2/14/12	6
8						
9		**Chapter 2 Background**	**4 days?**	**Thu 2/9/12**	**Tue 2/14/12**	
10	▦	2.1 Replication & Clustering	1 day?	Thu 2/9/12	Thu 2/9/12	
11	▦	2.2 Physical vs Virtual Servers	1 day?	Mon 2/13/12	Mon 2/13/12	
12		2.3 Hot Warm Cold Recovery	1 day?	Tue 2/14/12	Tue 2/14/12	11
13						
14		**Chapter 3 Environment outline**	**6 days?**	**Mon 2/13/12**	**Mon 2/20/12**	
15	▦	3.1 Existing DR environment	1 day?	Mon 2/13/12	Mon 2/13/12	
16	▦	3.2 Backup Systems	1 day?	Wed 2/15/12	Wed 2/15/12	
17	▦	3.3 Existing production environment	1 day?	Mon 2/20/12	Mon 2/20/12	
18						
19		**Chapter4 Recovery Plan**	**13 days?**	**Thu 2/23/12**	**Mon 3/12/12**	
20	▦	4.1 Describe preparation steps	1 day?	Thu 2/23/12	Thu 2/23/12	
21	▦	4.2 Acquire Hardware/ Software	1 day?	Mon 2/27/12	Mon 2/27/12	
22	▦	4.3 Determine Priority	1 day?	Mon 3/5/12	Mon 3/5/12	
23	▦	4.4 Provision Hardware	1 day?	Mon 3/12/12	Mon 3/12/12	
24						
25		**Chapter 5 Conclusion**	**3 days?**	**Thu 3/15/12**	**Mon 3/19/12**	20
26	▦	5.1 Test	1 day?	Thu 3/15/12	Thu 3/15/12	
27	▦	5.2 Lessons learned	1 day?	Mon 3/19/12	Mon 3/19/12	

Project: DR Project1
Date: Thu 4/12/12

Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┅	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Progress	▬
External Tasks	▬	Duration-only	▬	Deadline	⇩

Page 1

Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

External Contacts

Name, Title	Contact Option	Contact Number
Landlord / Property Manager		
Account Number None		
	Work	
	Mobile	
	Home	
	Email Address	
Power Company		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Telecom Carrier 1		
Account Number	Work	
	Mobile	
	Fax	
	Home	
	Email Address	
Telecom Carrier 2		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Hardware Supplier 1		
Account Number	Work	
	Mobile	
	Emergency Reporting	
	Email Address	
Server Supplier 1		
Account Number.	Work	
	Mobile	
	Fax	
	Email Address	
Workstation Supplier 1		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Office Supplies 1		
Account Number C3095783	Work	
	Mobile	
	Home	
	Email Address	

Disaster Recovery Plan for Each System

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER	Provide details
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details
Offsite Storage	Provide details

BACKUP STRATEGY FOR SYSTEM ONE	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM ONE	

DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	Provide details
Scenario 2 Total Loss of HW	Provide details