KNOWLEDGE ENGINEERING APPROACH TO
DATA CENTRES DISASTER BACKUP/RECOVERY PLANNING

C. K. TO, V. Ma, N. Lui

Department of Computing Studies
Hong Kong Polytechnic
Kowloon, Hong Kong

Abstract

Data center disaster backup/recovery planning is an organized effort in an information processing environment to minimize the impact of disaster of any size to the information processing operations of an organization. An up-to-date disaster backup/recovery plan is crucial to the achievement of such objective. Since the planning process involves the concurrent participation of a range of highly skilled specialists, users, and vendors, keeping this plan current will definitely cause a drain to expert resources. The development of a knowledge based planning system would not only guarantee the currency of the plan but also ease the intensive demand on scarce specialist resources. This paper describes a planning system implemented in the knowledge based environment which is capable of deducing a critical application recovery sequence, data backup requirements, as well as capacity and configuration management.

1. INTRODUCTION

Computer data processing function have become the lifeline of many business concerns. Disruption in system operations could forcibly idle hundreds to thousands of employees and halting important services to customers. In more serious cases, prolonged disruption of services to customers could result in catastrophic damage to the health of the company. Disaster backup/recovery planning is directed towards avoiding the broader catastrophe by quickly controlling the effects of loss of information processing capability as service information delivery vehicle. The ultimate product of the disaster backup/recovery planning process are:

- a sufficient hardware and software configuration to restore the critical services/applications within a prescribed period as specified by top management;
- a comprehensive list of data resources required to restore the critical services/applications;
- a sufficient set of pre-defined procedures to respond to any disaster in the data center(s) under consideration.
- a manpower deployment plan to ensure the efficient deployment of skilled technical resources;
- a strategy for recovering the damaged site.

This study applies the knowledge engineering approach to perform the first two planning tasks. Knowledge of the planning methodology is acquired and represented as rules in the knowledge base and further reasoning and deduction will be performed by the inference engine of the knowledge based system rather than by human experts. The following sections will describe the basic functions to be performed in the disaster backup/recovery planning process, the mechanisms associated with the knowledge based system, the operations of the prototype system, and the basis for future enhancements.

2. THE DISASTER BACKUP/RECOVERY PLANNING PROCESS

Data center disaster backup/recovery planning is now one of the most essential activities in organizations which relies on information processing functions to operate. It is an organized effort to minimize the impact of disaster of any size to the information processing operations of the organization. The objectives of the planning process are to make sufficient preparation, to design and to implement predetermined procedures, for responding to a disaster. In order to achieve the objectives, the organization must:

- have sufficient capacity and appropriate hardware and software configuration to restore and provide critical services to the organization's users;
- have the most up-to-date version of the production software required for providing such services;
- have available the necessary files/databases required by the application systems;
- have the appropriate operations/technical skills to operate and support the systems;
- have a set of executable backup/recovery procedures to respond to an emergency;
and the backup/recovery plan must be kept current to assure it is executable.

2.1 The Planning Team

A complete disaster backup/recovery planning exercise involves a team of specialists internal or external to the organization:

- **The Users**
  - to identify the critical services and the maximum tolerable down time.
  - to project the future growth of such services.
- **The Application Analysts**
  - to identify critical applications, and their application dependencies and data resource dependencies.
- **The Technical Specialists**
  - to identify the software environment which support the critical applications.
  - to identify the hardware environment required for operating the system and application software.
- **The Vendor**
  - To give advice on hardware and software configuration and characteristics.
- **The Operations Managers**
  - To advise on the operational aspect of backup and recovery.
- **The Technical Planner**
  - to derive the recovery sequence for critical applications.
  - to derive overall data resources requirements.
  - to derive overall backup/recovery capacity and configuration requirements.
- **Executive Management**
  - to approve and make trade-off decision on the criteria in restoring critical services.

It is the function of the technical planner to coordinate the planning activities and integrate all information into a coherent and executable plan.

2.2. The Planning Cycle

The disaster backup/recovery planning process consists of a number of stages described in the following sections.

2.2.1 Determination of Critical Services/Applications

The very first phase of the disaster backup/recovery planning cycle is the designation of critical services and the determination of their relative importance to the organization. The criteria of judging how critical a service could be any one or combination of the following factors:

- Tangible Losses
- Intangible Losses
- Legal and Statutory Requirements

Once the impact of these factors have been identified and evaluated, the user could determine the maximum tolerable outage of a service based on the order and magnitude of their impact.

2.2.2 Generation of Recovery Sequence and Data Resource Requirements

The second phase of the planning cycle is concerned with the steps to be taken to generate an application recovery sequence and the identification of data set requirements:

i) Define the system software that will be needed to run each of the critical applications in a recovery situation.

ii) Develop a priority list for the critical applications. This list should show what has to run immediately, what should be run as soon as possible, and those which can wait a few days. The information can be extracted and transformed into a chart as illustrated in Figure 1.

![Figure 1: Systems Outage Analysis Chart](image)

iii) Based on data set requirements of each of the critical applications, develop an application/data impact matrix as illustrated in Figure 2.

2.2.3 Identifying Job Dependency

After the recovery sequence is identified, there are other factors which must be considered:

i) Whether an interface exists between a critical and a non-critical application.

ii) Whether the interface between a critical application and a non-critical application can be bypassed.
iii) When a non-critical interface is bypassed, how would "catch up" processing be done to bring the files up-to-date when more processing capacity becomes available.

iv) How to avoid synchronization problems while recovering non-critical applications. Figure (3) illustrates the interfaces among the critical applications and between critical and non-critical applications.

A more realistic example is illustrated by a jobstream interface chart on Figure (4). The actual interfacing relationship at the job stream level is shown for the applications FE, CC, KK, EE, and the interrelationships between theses systems are complicated and intertwined.

2.2.4 Determination of Data Resource Requirements

The next step is to determine data resource requirements. That is, to stipulate the level of backup and the number of generations of data sets to be retained. For online processing the principal data sets residing on online storage are normally updated immediately by transactions coming through the pipeline. Batch processing of transactions against the master files provides a means for reconciliation and verification. For a batch system, a number of generations of the master file are kept and transactions are collected and validated before they are processed against the master file. If processing errors are encountered during an updating run, it is essential that the old master file and the validated transaction files are still available for re-run. For additional security, an organization may keep multiple copies and multiple generations of the master files. For an application with more than one updating cycle, it is normal practice to keep historical versions of different levels of concatenated transaction files (e.g., monthly, month-to-date, quarterly, etc.) and in some cases, intermediate processing files are also retained for each of the update cycles. Costs and storage space impose practical limits to the number of versions and generations to be retained for backup.

2.2.5 Estimating Workload and Capacity Requirements for Disaster Recovery

The fourth phase of the cycle is to plan for adequate capacity for disaster recovery and operation. Workload statistics captured by systems measurement tools are used as baseline for...
requirements estimation. There are two components of capacity demand:

- Existing critical applications workload and their natural transaction volume growth; and
- Demand generated by new critical applications or new functions.

Demand for batch applications and online applications are dealt with in different ways:

- Batch demand is usually expressed as average resource utilization per time period (e.g., per week, per month, etc). Batch processing may be constrained by a processing window, it would be necessary to consider resources requirements to meet the imposed processing deadlines.

  Online demands are normally characterized by a time-dependent profile with peaks and valleys within the time periods specified. For most online applications, consistent peaks of online demand intervals usually exist. Cost and performance are the two trade-off factors in determining online capacity requirements.

2.2.6 Development of a Disaster Backup/Recovery Configuration

After capacity requirements are estimated, it is necessary to transform the requirements into an appropriate hardware configuration capable of handling the workload. This exercise is highly vendor dependent and requires substantial knowledge of the architecture and characteristics of the vendor's hardware and software. It is also necessary to identify machine or peripheral dependent applications and accommodate such requirements.

2.2.7 Refinements and Trade-off Decisions

When a backup configuration is fully developed, the costs for backup are readily computable.
Management could evaluate the cost-effectiveness of different scenarios:

- Proceed as planned.
- Employ a service degradation strategy and relax the initial requirements.
- Employ a commercial recovery strategy by making full or arrangements with service bureaus or vendors.
- Reciprocal arrangements with other organizations.

If the service degradation scenario is chosen it would be necessary to go back to stage one and restart the planning cycle.

3. THE KNOWLEDGE BASED SYSTEM FOR DISASTER BACKUP/RECOVERY PLANNING

The rationale for using a knowledge engineering approach for disaster backup/recovery planning is the nature of the task:

- The preparation and update of the disaster backup/recovery plan require expert knowledge of the domain, which involves complex reasoning, inductive inference, intuition, fact, and most of all, timeliness in producing the plan.

Many of the rules employed are heuristics or rules of thumb especially for capacity and configuration planning. These rules can be represented in a knowledge based system in a more readable and understandable form. Rules can readily be added, modified, and deleted to reflect the dynamic nature of the information processing environment.

A knowledge based system possesses built-in control mechanism that specifies the order in the application of rules and it also specifies a way of resolving conflicts when more than one rule match a pre-condition at any one time.

A knowledge based system could employ both backward and forward chaining which allows the system to be both goal-driven and data-driven.

3.1 System Flow

The system is made up of 2 major components:

i) The knowledge based system component.

ii) The database management component.

Functional flow of the system is represented in Figure (5) and Figure (6).
3.1.1 The Knowledge Based System Component

The knowledge based system will inference through the knowledge base and retrieve requirements information from the database files. The application recovery sequence and data backup requirements are then prepared and stored in database files. The knowledge based system is developed under the Teknowledge M.1 expert system shell. It retrieves information from the priority list of critical applications and information from the applications/data impact matrix, workload statistics, and equipment characteristics from the database, process through the inference engine then produces the application recovery sequence, the data backup requirements, the capacity requirements, and the set of configuration requirements.

3.1.2 The Database Management Component

This component maintains the information required by the knowledge based system. It is used to create, update and delete the priority list of critical applications and the applications/data impact matrix. Interactive enquiry and hardcopy reporting facilities are available for the users to examine the application recovery sequence, data backup requirements, and critical application workload statistics and forecasts.

3.2 Operation of the Disaster Backup/Recovery Knowledge Based System

In order to realized the conceived system architecture, five system modules are developed. Each performs a self-contained task, the conglomeration of the 5 modules constitute the knowledge based system:

i) Application recovery sequence and data backup requirements generation module.

ii) Capacity requirements and configuration deduction module.

iii) Database Manipulation Interface Module.

iv) Database Reporting Module.

v) Database Maintenance Module.

3.2.1 Applications Recovery Sequence and Data Backup Requirement Generation

This module retrieves information from the database and deduces the application recovery sequence and data backup requirements using formalized design rules. The operation sequence of this generation module is:

i) invoke the database manipulation interface to obtain critical application outage information.

ii) store the information in cache memory.

iii) deduce the application recovery sequence and data backup requirements with rules in the knowledge base.

iv) store the output generated in cache memory.

v) use the database manipulation interface to output the deduced results to the database.

Both forward chaining and backward chaining are used to produce recovery sequence and its data set backup requirements for an application. The forward chaining process is used for dependent application and data set searching. Backward chaining is applied to derive the recovery sequence of each application to develop the complete recovery sequence and to find individual data set requirements to derive overall data set backup requirements. Figure (7a) illustrates application dependency. The knowledge based system acts as a backtracker, it first searches the critical application AA and then the non-critical application DD. Then it backtracks and searches the non-critical application EE. When the system is scanning for application BB and discovers that EE has been previously searched it would backtrack to perform scanning for another application (CC). Since an application may use several data sets and a data set maybe used by several applications (Figure (7b)) the knowledge based system will determine the recovery requirements for data sets in the same manner. It will examine data set and application relationships and determine whether a data set has been search before.

3.2.2 Capacity Requirements and Configuration Deduction Module

This module deduces sufficient capacity and an appropriate configuration required for recovery and operation of all critical applications within the current planning horizon.

Fig. (7) Application Recovery Sequence and Data Set Backup Requirement Preparation
### 3.2.2 Capacity Requirements and Configuration Deduction Module

This module deduces sufficient capacity and an appropriate configuration required for recovery and operation of all critical applications within the current planning horizon.

- **i) Capacity Requirements Deduction**
  
  The planned capacity includes the current workload, the workload generated by natural growth in transaction volumes, and workload generated by new critical applications or new functions. Projection of new workload are performed at the job stream level using benchmark or simulation results. Capacity requirements for recovering online applications are deduced by finding the maximum capacity requirements for the peak of the combined profile of all online application workload. Capacity requirements for batch applications are deduced in a different way. Deductions are carried out at the job stream level. The recovery process is simulated using the deduced recovery sequence and then compute the capacity requirements. Batch application utilizes the capacity not required by online applications. Under two conditions will batch requirements dominate:

  - Batch requirements within the batch processing window exceed capacity required by peak online demand.
  - Total requirements (online plus batch) exceed peak online demand.

- **ii) Configuration Requirements Deduction**

  The final step of the deduction process produces a set of configuration requirements for recovery and operation. Capacity requirements deduction provide the following input to this final step:

  - MIPS required.
  - Real memory required.
  - Channel capacity required
  - Disk I/Os required.
  - Number of tape drives required.
  - Print capacity required.
  - Number of display terminals required.

  A configuration is deduced by computations and heuristics. The deduced configuration requirements is a vector containing the following elements and their associated quantities:

  - CPU model.

---

**Fig. (7) Application Recovery Sequence and Data Set Backup Requirement Preparation**

```
   critical   critical  non-critical
   app AA    app BB    app KK

   critical   critical  critical  non-critical
   dataset X1  dataset X2  dataset X3  dataset X4
```

**Fig. (8) Online Workload Profile**

```
 100
 90
 80
 70
 60
 50
 40
 30
 20
 10

CPU Utilization

<table>
<thead>
<tr>
<th>CPU Utilization</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>***</td>
</tr>
<tr>
<td>40</td>
<td>***</td>
</tr>
<tr>
<td>30</td>
<td>***</td>
</tr>
<tr>
<td>20</td>
<td>***</td>
</tr>
<tr>
<td>10</td>
<td>***</td>
</tr>
</tbody>
</table>

**Fig. (9) Application Recovery Sequence and Data Set Backup Requirement Preparation**

```
3.2.3 Database Manipulation Interface

This module provides database manipulation utilities so that the expert system shell could create, delete, retrieve, manipulate, and update database files.

3.2.4 Database Reporting

The function of this module is to produce reports for output.

3.2.5 Database Maintenance

This module provides facilities for the user to update the database it also supports online enquiry of information stored in the database.

4. CONCLUSIONS AND FUTURE ENHANCEMENTS

A knowledge based system has been built to embrace the basic rules and facts required for consistent disaster backup/recovery data resources, capacity, and configuration requirements planning. It has successfully demonstrated the application of the knowledge engineering approach could be an effective and efficient approach to perform disaster backup/recovery planning functions:

i) The system allows users without high degree of technical knowledge on application, capacity, and configuration requirements planning knowledge to operate.

ii) The need of scheduling all specialists in collective, lengthy, and time consuming meetings is reduced to a minimum. Expert participation is limited to the update of the knowledge base and the database.

iii) Specialists from various areas of the organization could contribute their expertise or information to update the knowledge base and database at any time convenient to them. When the system is interfaced to a change control management -- a mechanism which oversees and record changes in the information processing environment such as the release of new applications, and changes in hardware and software configurations, a large portion of the information updating tasks could be eliminated since all changes would have been recorded and updated. The system could further be extended, recorded, and updated by change control management activities. The system could further be extended to incorporate capabilities to evaluate potential impact of change activities.

iv) Scenario evaluation for backup/recovery strategies could be performed by applying the system on different sets of tolerable outage programs corresponding to each scenario. The deduced Configurations requirements output could be use as a basis for cost-effective analysis. With further extensions, it is also possible to make refinements of the disaster backup/recovery programs to achieve an optimization objective.

REFERENCES