OXYGEN
CONSULTING SERVICES
PROGRAMMED FOR PROGRESS

Disaster Recovery Plan and Backup Strategy for a website

Sanjiv Agarwala
CISSP,CISA,CISM,CGEIT,ITIL,MBCI,ISO27001,ISO9001
Director, Trainer and Principal Consultant
Oxygen Consulting Services Pvt. Ltd.
sanjiv.agarwala@o2csv.com
ska262001@yahoo.co.in

Session Topics:

Disaster Recovery Plan

- **What may cause a Down Time for a Website?**
  - **Hardware Failure**
  - **Site Down**
  - **Power Failure**
  - **User's part**
  - **Infection/ Attack**
  - **Software Failure**
  - **High Availability (HI)**
  - **Load Balancing (LB)**

Points to consider:

1. **What is the application in question**
2. **Where is it running – which system, server**
3. **Who is operating it**
4. **Who all have access to it**
5. **Security controls – physical and logical security**
6. **What are the various disasters that can impact this web server**
7. **Some disaster recovery concepts – natural and man-made disasters, business impact analysis, recovery time objective, recovery point objective**

Load balancing is a computer networking methodology to distribute workload across multiple computers or a computer cluster, network links, central processing units, disk drives, or other resources, to achieve optimal resource utilization, maximize throughput, minimize response time, and avoid overload. Using multiple components with load balancing, instead of a single component, may increase reliability through redundancy. The load balancing service is usually provided by dedicated software or hardware, such as a multilayer switch or a Domain Name System server.

High availability is a system design approach and associated service implementation that ensures a prearranged level of operational performance will be met during a contractual measurement period.

OXYGEN
CONSULTING SERVICES
PROGRAMMED FOR PROGRESS

Session Topics:

Backup Strategy for a Web Site

- Incremental Backup
- Differential Backup
- Full Backup
- Daily Backup
- Copy Backup
- What is a Backup Policy
- Efficient ways of designing a Backup and Restore Strategy
- Business Continuity and Disaster Recovery (BCDR) plan for the Web Server

Copy backup

A copy backup copies all selected files but does not mark each file as having been backed up (in other words, the archive attribute is not cleared). Copying is useful if you want to back up files between normal and incremental backups because copying does not affect these other backup operations.

Daily backup

A daily backup copies all selected files that have been modified the day the daily backup is performed. The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

Differential backup

A differential backup copies files created or changed since the last normal or incremental backup. It does not mark files as having been backed up (in other words, the archive attribute is not cleared). If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.

Incremental backup

An incremental backup backs up only those files created or changed since the last normal or incremental backup. It marks files as having been backed up (in other words, the archive attribute is cleared). If you use a combination of normal and incremental backups, you will need to have the last normal backup set as well as all incremental backup sets in order to restore your data.

Normal backup

A normal backup copies all selected files and marks each file as having been backed up (in other words, the archive attribute is cleared). With normal backups, you need only the most recent copy of the backup file or tape to restore all of the files. You usually perform a normal backup the first time you create a backup set.

Backing up your data using a combination of normal backups and incremental backups requires the least amount of storage space and is the quickest backup method. However, recovering files can be time-consuming and difficult because the backup set can be stored on several disks or tapes.

Backing up your data using a combination of normal backups and differential backups is more time-consuming, especially if your data changes frequently, but it is easier to restore the data because the backup set is usually stored on only a few disks or tapes.

Elements of backup policy

1. What will be backup
2. At what frequency
3. Who will backup what data – desktop, server, application, filesystem
4. Accountability for backup
5. Approval for data backup
6. Backup option – daily, weekly, monthly, full, incremental, differential etc
7. Media for backup
8. Backup encryption
9. Protection of backup media
10. Data restore procedures
11. Review and audit of backup policy

Elements of backup strategy

1. Volume of data
2. Time to backup and restore and dependency on RTO and RPO
3. Live data or stored data only – system backup
4. Media to be backup on – tapes, SAN, NAS, DVD etc
5. Data transmission over links as backup option
6. Backup software
7. Encryption needs
8. Location of DR site or backup site
9. Data, Applications and the order of backup

BC and DR for web server

- **What is the importance of the application**
- **Network diagram, what data is processed, data is stored where**
- **If a disaster happens, within what time the data needs to be restored- before what data needs to be backup, last data, time provided for recovery**
- **Complexity of application, order of application restoration**
- **Hot, warm, cold site options and mutual agreement**
- **Recovery strategy based on disaster involved – virus infection, just hardware and application failure, or complete webserver is hacked etc**

OXYGEN
CONSULTING SERVICES
PROGRAMMED FOR PROGRESS

Disaster Recovery Plan and Backup Strategy for a website

Sanjiv Agarwala
CISSP,CISA,CISM,CGEIT,ITIL,MBCI,ISO27001,ISO9001
Director, Trainer and Principal Consultant
Oxygen Consulting Services Pvt. Ltd.
sanjiv.agarwala@o2csv.com
ska262001@yahoo.co.in