Implementing Effective Backup Strategies For Disaster Recovery

Kurt Lamoreaux

Consultant, Computer Networking

VMWORLD 2006

Overview

- VMware backup options
- 3rd party backup options
- Disaster recovery – which backup options work best
- Case Study
- VI3 Disaster Recovery options

VMware Backup Options

- ESX 2 Backup Options
  - Internal virtual machine backups
  - Service Console backups to local device
  - Service Console backups to network device
  - SAN Imaging
  - vmsnap/vmres
- ESX 3 Additional Backup Option
  - Consolidated Backup
    - Proxy based backup from SAN
    - Preconfigured scripts for major 3rd party backup products

3rd Party Options – Supported Backup Tools

- Symantec Backup Exec
  - Versions 10.0, 10d
- VERITAS Netbackup
  - Versions 5.0, 5.0 MP4, 5.1, 5.1 MP2 MP3, 6.0
- IBM Tivoli Storage Manager
  - Versions 5.2.1, 5.2.3, 5.3
- EMC Networker
  - Versions 7.0, 7.1.x, 7.2, 7.3
- CA, BrightStor ARCServe
  - Versions r11, r11.1, r11.5
- CommVault Galaxy
  - Version 5.9, 6.1

3rd Party Options – VMware Oriented Solutions

- Vizioncore esxRanger
- esXpress
- Vmts.net – vmbk.pl
  - Image based backups – vms are treated as a set of files
  - Tools are vm aware – support features such as REDO logs, suspend/resume of vms, export of vmdk files

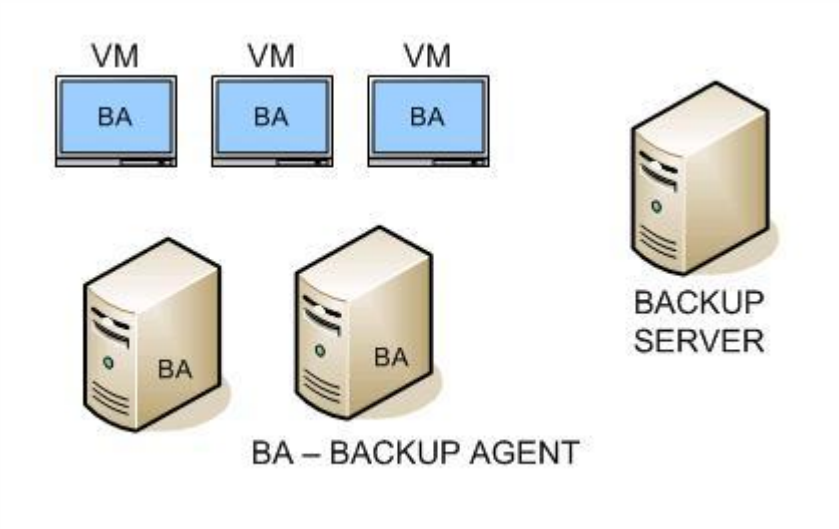
Disaster Recovery – Which Strategy Works Best?

- What is the disaster?
  - A file in the virtual machine needs to be restored
  - A virtual machine is not functioning
  - An ESX server has gone down
  - The SAN has gone down
  - Catastrophic outage (entire site/region down)

- Disaster recovery is more than backups and restores
  - It is important to develop a strategy for using backups and restores
  - A combination of solutions will often produce the best results

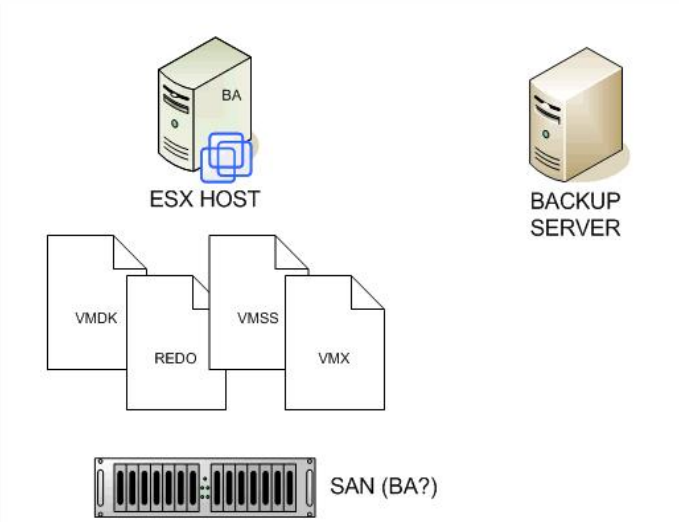
Disaster Recovery – Internal Backups

- Internal virtual machine backups considerations
  - Same strategy for virtual machines and physical servers
  - ‘Bare metal restore’ features have become easier to use
  - Can use disk imaging based tools for backups
  - Some servers do not restore well from this type of backup
  - Can allow for a V2P restore strategy



Disaster Recovery – External Backups

- External virtual machine backups are simple
  - File level backups
  - Simple restore process
  - Require down time for virtual machine or REDO files
  - Require VMware based host for restore



Disaster Recovery – Best of Both Worlds

- Combination of internal and external backups of virtual machines provides maximum flexibility
- Example
  - Monday – external based backup of virtual machine
  - Daily – internal based backup using 3rd party software
- Can perform simple file restore inside virtual machine for restoration of corrupt or deleted file
- Can perform complete server restore by restoring virtual machine from last external backup, with the ability to restore any internal backups that occurred on subsequent days

Disaster Recovery – Other Considerations

- Backup Storage – Onsite and Offsite
- Hardware for recovery
- Software for recovery
- Location for recovery
- Instructions for recovery
- How does the virtual machine strategy tie in to the rest of the environment?

Case Study – Disaster Recovery Strategy

- Utility in Alaska
- Multiple ESX server (2.5.x) on SAN
- Single Site
- Majority of servers running as virtual machines
- Network based backup solution already in place (IBM Tivoli)

- Goal – one solution that works for all backups, including virtual machines

Case Study – Disaster Recovery Levels

- Missing or corrupt files on a server
- Service failure on a server
- Single server failure
- Site level failure

- All recoveries must work for both physical and virtual machines

Case Study – Site Level Disaster Recovery

- Identify critical services that must be restored
- Identify and collect necessary software and store securely
- Identify critical contacts and store securely offsite
- Store all critical data offsite
- Arrange offsite hardware
- Develop documentation for recovery process and store securely offsite
- Test recovery process

Case Study – VMware backup strategy

- Centralized backup strategy using IBM Tivoli
- Combination of internal and external virtual machine backups
- Schedule outage of virtual machines for external backup
- Use different namespace in Tivoli for hosts than for external virtual machine backups
- Use same namespace in Tivoli for all external virtual machine backups

Case Study – Tivoli Configuration

- Each ESX server backed up separately
  - Tivoli client installed
  - No vmfs partitions included
- All virtual machines run Tivoli client internally
  - Internal backup performed nightly
- All virtual machines backed up as files through scripts
  - Separate dsm.opt file
  - Separate section in dsm.sys
  - Separate node name

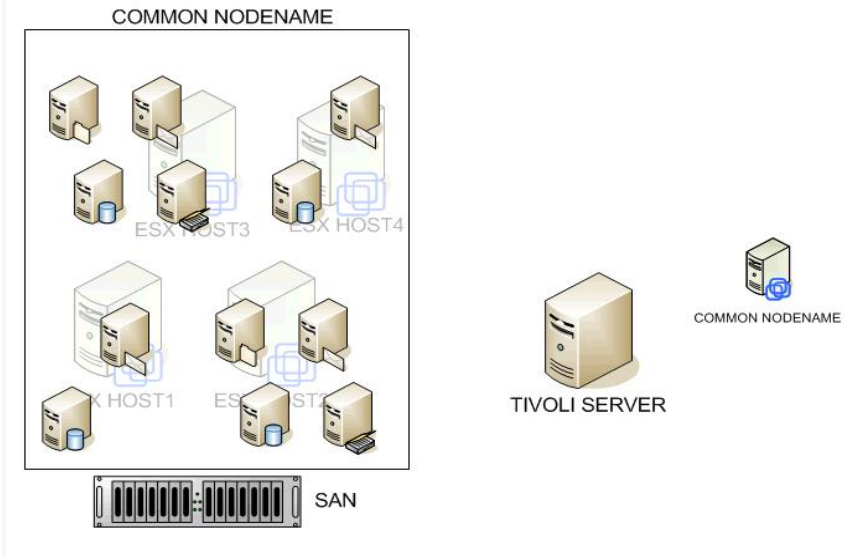
Case Study – dsm.sys file

```
Servername esxserverx
CommMethod tcpip
TcpPort 1500
TcpServerAddress tivoli.server.address

Servername virtualmachines
CommMethod tcpip
TcpPort 1500
TcpServerAddress tivoli.server.address
MAKESPARSEFILE NO
NODENAME virtualmachines
VIRTUALMOUNTPOINT /vmfs/san
VIRTUALMOUNTPOINT /vmfs/local
```

Case Study – Why Use Tivoli Nodenames?

- Nodename used to track files
- Regardless of number of ESX servers, same nodename can be used for backing up virtual machines
- If virtual machine is moved to another ESX server, manually or using VMotion, file will be consistently tracked.
- Restores of virtual machines can include prior versions using Tivoli storage features.



Case Study – When To Back Up Virtual Machines

- Suspends for backups were acceptable for all virtual machines
  - It was simply a matter of timing
  - Did not impact the view in the organization of server downtime
  - Monitoring software modified to allow server to be down without triggering events
- Backups were scheduled based on size and when services could be down
  - Tried to keep total amount of data backup up each day steady
  - Gigabit connection – able to backup 1GB/min

Case Study – Scheduling Backups

- Perl script used to perform backups
- Scheduled to run hourly
- Master file of all vms was created and used to control backups
  - Day of week and time of day controlled in file
  - Multiple days could be selected
- If virtual machine was moved from one host to another, backup schedule not affected
- Script could also be used for manual backups
- Tivoli logs parsed and used to create web based report of results

Case Study – Backup Script Overview

- List of registered virtual machines on host created
- List compared to master file to flag any not in file
- For each virtual machine, identify if time to backup
  - Read vmx file to determine vmdk files to backup and suspend location
  - Suspend virtual machine
  - Use Tivoli to backup vmdk files, REDO files (if any), suspend file, and corresponding home directory
  - Resume virtual machine
- Collect log files for reporting
- Copy of script available – kurt@cncsinc.com

Case Study – Disaster Recovery Plan

- Create Tivoli server
- Restore Tivoli database
- Load tapes into system
- Create ESX server
- Install Tivoli client
- Restore virtual machine drives (and home dirs if needed)
- Register or create virtual machines using restored drives
- Restore physical servers using Tivoli bare metal restore functions

- Prior to VMware - success rate was very low – over 5 days with no access to data actually available
- Using VMware in DR strategy, in 3 days they can have most critical systems up and completely functional

Case Study – Benefits of Approach

- Simple approach
- Eliminates the use of redo files for backups
- Perl script approach could be adapted for other uses, such as database and other file backups
- Disaster Recovery plan kept simple
- Solution works well for site disaster, SAN disaster, and server or service disaster

Virtual Infrastructure 3 – Disaster Recovery

- Consolidated Backup
- Controlled using /etc/vmware/backuptools.conf
- Additional Information at VMworld 2006
  - LAB3801 - VCB for Disaster Recovery
  - BCT9552 - VI3 Capabilities for Improving Disaster Recovery
  - BCT4540 - Integrating VCB into Your Backup Infrastructure: Best Practices for Implementation and Customization
  - BCT5070 - Leveraging VMware ESX Server in Disaster Recovery Solutions
  - TAC4016 - Integrating ESX Server 3 with Data Protection Software
  - TAC9816 - Hot Backups and Restores for VMware ESX Server: A '1-2' Punch Backup Methodology
  - TAC9912 - Nondisruptive Backup of VMware Environments Using VERITAS NetBackup
  - MDC9870 - Backup and Recovery of Virtual Machines

Conclusion

- For an effective disaster recovery plan
  - Identify scope of disaster
  - Determine acceptable down time for virtual machines
  - Implement a strategy that is simple and flexible
  - Document process
  - Have 3rd party test process

Presentation Download

Please remember to complete your
session evaluation form
and return it to the room monitors
as you exit the session

The presentation for this session can be downloaded at
http://www.vmware.com/vmtn/vmworld/sessions/

Enter the following to download (case-sensitive):

Username: cbv_rep
Password: cbvfor9v9r

Some or all of the features in this document may be representative of feature areas under development. Feature commitments must not be included in contracts, purchase orders, or sales agreements of any kind. Technical feasibility and market demand will affect final delivery.

VMWORLD 2006