Top 10 Do’s/Don’ts of Data Protection for VMware vSphere
Agenda

• Exploring Data Protection for VMware vSphere
  • vSphere Snapshots, Cloning, and Replication
  • Guest level backups
• vStorage APIs for Data Protection (VADP)
  • Data Protection Applications
  • VMware VDP
• VADP Transport Modes and Do’s and Don’ts
• Summary
Exploring Data Protection for VMware vSphere
Exploring Data Protection for VMware vSphere

- Platform Native mechanisms
  - vSphere Snapshots, Cloning and Replication
- Application Native tools
  - Oracle RMAN etc.
- Data Protection Applications
  - Inbuilt - vSphere Data Protection (VDP)
  - 3rd Party Apps - Veeam, CommVault etc.
vSphere Snapshots

• Captures a point-in-time state of the virtual machine (VM)
  • VM’s memory, power settings
  • Point-in-time of the contents .vmdk files
vSphere Cloning

• Creates a duplicate of the existing VM
  • Same computer name and network settings
  • Copy of original .vmdk and .vmx files
  • Copy of contents on original virtual disks
vSphere Replication

- Asynchronously replicates virtual machine to another location
- Integrated with Microsoft Volume Shadow Copy Service (VSS)
- Customizable retention of replicated historical points for VM recovery
- No application agent required
vSphere Snapshots, Cloning, Replication: Summary

<table>
<thead>
<tr>
<th>What do I have for data protection and disaster recovery?</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point-in-time snapshot</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Multiple copies</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VSS application consistency</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Business Continuity</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Application Log Management</td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Legal Hold and E-Discovery</td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Archive Indefinitely</td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Extended Retention</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>
Data Protection Applications

- Data Protection and Recovery Software Market
  - Total $5.6B in 2013, 9.2% annual growth*
- Key Players/Solutions
  - vSphere Data Protection (VDP)
  - EMC Avamar, EMC NetWorker
  - Symantec NetBackup, Symantec Backup Exec
  - CommVault Simpana
  - Veeam Backup Management Suite
  - Others: HP, CA, Microsoft, Dell, Acronis, PHD Virtual

* Source: IDC World Wide Data Protection and Recovery Software Forecast and Vendor Shares
Guest Level Backups

- Requires backup agents on application servers
- Similar to *backing up a physical server*
- Data protection solutions that support client-direct backups
  - EMC NetWorker
  - Symantec NetBackup

![Diagram of Guest Level Backups]

- VM Guest Network
- 10GigE Storage Network
- Exchange Backup Agent
- Microsoft Exchange 2013 Server VM
- vSphere
- ESX/ESXi
- ESXi datastore (Tintri VMstore)
- Backup Server
vStorage APIs for Data Protection (VADP)

- Enables full VM image backup and restore
- Enables file level restore
- Allows use of vStorage Changed Block Tracking for more efficient backup and restore

<table>
<thead>
<tr>
<th>VMware ESX/ESXi</th>
<th>Microsoft Hyper-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Source: Info-Tech Research Group; N = 80</td>
<td>All solutions support VMware.</td>
</tr>
<tr>
<td>VMware</td>
<td>ca technologies</td>
</tr>
<tr>
<td></td>
<td>commvault system management</td>
</tr>
<tr>
<td></td>
<td>FalconStor Software</td>
</tr>
<tr>
<td></td>
<td>Dell AppAssure</td>
</tr>
<tr>
<td></td>
<td>EMC² where information lives</td>
</tr>
<tr>
<td></td>
<td>IBM</td>
</tr>
<tr>
<td></td>
<td>Microsoft</td>
</tr>
<tr>
<td></td>
<td>Symantec</td>
</tr>
<tr>
<td></td>
<td>Unitrends</td>
</tr>
<tr>
<td></td>
<td>Veeam</td>
</tr>
<tr>
<td></td>
<td>XenServer</td>
</tr>
<tr>
<td></td>
<td>ca technologies</td>
</tr>
<tr>
<td></td>
<td>commvault system management</td>
</tr>
<tr>
<td></td>
<td>Dell AppAssure</td>
</tr>
<tr>
<td></td>
<td>HP</td>
</tr>
<tr>
<td></td>
<td>IBM</td>
</tr>
<tr>
<td></td>
<td>Microsoft</td>
</tr>
<tr>
<td></td>
<td>Symantec</td>
</tr>
<tr>
<td></td>
<td>Unitrends</td>
</tr>
<tr>
<td></td>
<td>Veeam</td>
</tr>
<tr>
<td></td>
<td>XenServer</td>
</tr>
</tbody>
</table>
Image Level Backups

- Leverage VMware’s VADP without any backup agents
- Use backup proxy for offload functionality
- VADP transport modes:
  - HotAdd
  - NBD/NBDSSL
  - SAN
Agenda

• Exploring Data Protection for VMware vSphere
  • vSphere Snapshots, Cloning, and Replication
  • Guest level backups

• vStorage APIs for Data Protection (VADP)
  • Data Protection Applications
  • VMware VDP

• VADP Transport Modes and Do’s and Don’ts

• Summary
What do data protection solutions have in common?

- Support for VMware vStorage APIs for Data Protection (VADP)
  - Image-level backups
- Application data protection support
  - Guest-level backups
- Create multiple local or off-site copies
- Allow legal holds and e-discovery
- Extended retention periods (1 year, 5 years, 7 years, indefinitely)
• Use Thin Provisioning for VDP Appliance OVF and backup storage deployment
• Use Static IP address entry for VDP Appliance
• Do vCenter Registration – test connection is mandatory
• Use FQDN entry on DNS Server
• Use port 53 DNS for proxy node access
• Provision user account with admin privileges on vCenter root node
For Guest level backups, must install VDP for Exchange Server agent

Must have network route from VDP Advanced to Exchange server

Exchange VSS GLR requires Exchange MAPI/CDO kit installed

Recommended one exchange server per backup job
Example: Exchange Backup/Recovery with VDP Advanced

- Restore to original
- Restore using RSG/RDB
VADP Transport Modes: Do’s and Don’t’s
1. VADP HotAdd Transport Mode
HotAdd Transport Mode Overview

ESX/ESXi DataStore using Tintri VMstore

Microsoft Exchange 2013 Server

10GigE Storage Network

ESX/ESXi A

vSphere

HotAdd

Backup Data (CBT) HotAdd

VDP Appliance (VM)

ESX/ESXi B

vSphere

HotAdd

Microsoft SQL 2012 Server

VM-Guest Network

VM1

VM2

VM5

VM6
Best Practices

- Use 10GigE for storage network
- Proxy server must be a virtual machine
- Proxy server can also be a Backup Server

[Diagram showing HotAdd attached VMDK]
HotAdd Transport Mode: Pitfalls

Exploring some common VADP HotAdd failures:

What is the following error an indication of?

```
ConsolidateVMDisks_Task for VM DomClones-2 failed. Reason Unable to access file since it is locked
1060 1 06/24 10:16:54 ### ### ConsolidateVMDisks --- ConsolidateVMDisks_Task for VM DomClones-2 failed. Reason Unable to access file since it is locked
```
HotAdd Transport Mode: Do’s and Don’ts

- **Do** ensure proxy host has network access to ESXi/ESXi server
- **Do** deploy additional proxy server for HotAdd on ESX/ESXi server
- **Do** manually remove .vmdk files from proxy server before new backups
- **Don’t** use HotAdd for independent disks
- **Don’t** migrate target virtual machines during backups
- **Don’t** use HotAdd if VMFS block size of VM < VMFS block size of proxy server
2. VADP NBD/NBDSSL Transport Mode
NBD/NBDSSL Transport Mode Overview

VM-Guest Network

10GigE Storage Network

ESX/ESXi DataStore using Tintri VMstore

Backup Data (CBT) NBD/NBDSSL

VDP Appliance (VM)

Microsoft Exchange 2013 Server

Microsoft SQL 2012 Server

VM1 VM2

VM3 VM4

VM5 VM6
Deployment Best Practices

• Use 10GigE for storage and backup network
• Proxy server must have network access to ESX/ESXi Server
• Proxy server can be a physical server or a virtual machine
• Proxy server can be a Backup Server
NBD/NBDSSL Transport Mode: Pitfalls

VMware VADP NBD/NBDSSL Transport Mode:

```
[NFC ERROR] NfcCheckAndReserveMem: Cannot allocate any more memory as NFC is already using 31457329 and allocating 2097152 will make it more than the maximum allocated: 33554432. Please close some sessions and try again
```

VM restore operation using a 3rd party backup solution:

```
```
**NBD/NBDSSL Transport Mode: Do’s and Don’ts**

- **Do** use 10GigE for backup network
- **Do** ensure network connectivity between proxy server and ESXi server
- **Do** ensure TCP port 902 is open between proxy server and ESXi server
- **Don’t** exceed the NFS connection limits on an ESXi server
- **Don’t** use NBDSSL if over-the-wire encryption is not required
- **Don’t** forget to check and update network connection if proxy is vMotioned
3. VADP SAN Transport Mode
SAN Transport Mode Overview

- **ESX/ESXi**
- **10 GigE Storage Network**
- **Backup Server/Backup Proxy Host**
- **SAN**
- **Traditional LUN Storage Array**
- **VM-Guest Network**
- **VDP Advanced does not support SAN transport mode**
Deployment Best Practices

- Validate compatibility for Initiator FC HBA and Target FC HBA
- Configure and verify initiator and target zoning on SAN switch
- Proxy server should be a physical server
SAN Transport Mode: Do’s and Don’ts

- **Do** ensure FC HBA port on the proxy server discovers the LUNs
- **Do** set SAN policy on Windows proxy server to onlineALL
- **Do** use host-based management software for device mapping
- **Don’t** use for restore of thin provisioned disks
- **Don’t** initialize disk on proxy server
- **Don’t** delete disks from the proxy server disk management
Demo: SAN Transport Mode – Initialize LUN

- ESX/ESXi
- BackupServer05053 (Physical System)
- 10 GigE Storage Network
- SAN
- Traditional LUN Storage Array
- ESXi DataStore: TEST
- vSphere
- Disk
SAN Transport Mode: Pitfalls

1. Corrupted ESXi datastore LUN.
2. Failed backup
3. What’s next?

NetBackup Job Detail
<table>
<thead>
<tr>
<th>Number</th>
<th>Transport Mode</th>
<th>DO’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SAN</td>
<td><strong>DO</strong> ensure FC HBA ports on proxy server discovers datastore LUNs</td>
</tr>
<tr>
<td>2</td>
<td>SAN</td>
<td><strong>DO</strong> set SAN policy on proxy server to onlineALL</td>
</tr>
<tr>
<td>3</td>
<td>HotAdd/NBD/NBDSSL</td>
<td><strong>DO</strong> ensure proxy server has 10GigE backup network access to ESX/ESXi server</td>
</tr>
<tr>
<td>4</td>
<td>HotAdd</td>
<td><strong>DO</strong> manually remove .vmdk files from proxy server before new backups if consolidate VM disk fails</td>
</tr>
<tr>
<td>5</td>
<td>NBD/NBDSSL</td>
<td><strong>DO</strong> ensure TCP port 902 is open between proxy server and ESX/ESXi server</td>
</tr>
<tr>
<td>Number</td>
<td>Transport Mode</td>
<td>DON’Ts</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>SAN</td>
<td>DON’T initialize/delete disk on proxy server if in doubt of LUN ownership</td>
</tr>
<tr>
<td>7</td>
<td>SAN</td>
<td>DON’T forget to use host-based device management software for device mapping</td>
</tr>
<tr>
<td>8</td>
<td>HotAdd/NBD/NBDSSL</td>
<td>DON’T forget to update network connections if proxy server is vMotioned</td>
</tr>
<tr>
<td>9</td>
<td>HotAdd</td>
<td>DON’T use HotAdd if VMFS block size of VM &lt; VMFS block size of proxy server</td>
</tr>
<tr>
<td>10</td>
<td>NBD/NBDSSL</td>
<td>DON’T exceed NFS connection limits on an ESX/ESXi server</td>
</tr>
</tbody>
</table>
Resources

http://www.tintri.com/resources/whitepapers

- VDP Advanced and Tintri Backup and Recovery Best Practices
- Backup and Recovery Best Practices
- Veeam and Tintri Backup and Recovery Best Practices

http://www.vmware.com/support.html

- vStorage APIs for Data Protection (VADP) FAQ
- vSphere Data Protection 5.5 Administration Guide
THANK YOU