Best Practices in DR using VCS & VVR

Shrikant Ghare, Yatin Nayak
Customer Forum, March 2012
Agenda

1. DR using VCS
2. DR using VVR
3. Q & A
DR using VCS

1. DR using VCS – Quick overview
2. Best Practices for DR configurations
3. Advanced DR Configurations
VCS DR Configuration Process

Application Recovery → Data Availability → DR Testing

DR using VCS – Best Practices
DR Configuration: Application Recoverability

Production Cluster

DR Cluster

Sync/Async Replication

GCO
DR Configuration: Data Availability

State diagram for HTC SVOLs

Replication configuration using HTC

DR using VCS – Best Practices
VCS integrates with several Data Availability options

<table>
<thead>
<tr>
<th>Symantec</th>
<th>Veritas Volume Replicator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Campus Cluster</td>
</tr>
<tr>
<td></td>
<td>NBU RealTime</td>
</tr>
<tr>
<td>EMC</td>
<td>SRDF, SRDF/Star, VPLEX</td>
</tr>
<tr>
<td></td>
<td>MirrorView</td>
</tr>
<tr>
<td></td>
<td>RecoverPoint</td>
</tr>
<tr>
<td>HDS/HP</td>
<td>Hitachi TrueCopy/HP XP CA,</td>
</tr>
<tr>
<td></td>
<td>Hitachi/HP XP 3DC</td>
</tr>
<tr>
<td></td>
<td>Hitachi Universal Replicator</td>
</tr>
<tr>
<td></td>
<td>3PAR, EVA CA</td>
</tr>
<tr>
<td>IBM</td>
<td>DB2 HADR</td>
</tr>
<tr>
<td></td>
<td>IBM Global Mirror, IBM Metro Mirror, DS4K</td>
</tr>
<tr>
<td></td>
<td>RemoteMirror</td>
</tr>
<tr>
<td></td>
<td>SVC CopyServices, XIVMirror</td>
</tr>
<tr>
<td>Others</td>
<td>Oracle DataGuard, DataGuard Broker</td>
</tr>
<tr>
<td></td>
<td>NetApp SnapMirror</td>
</tr>
</tbody>
</table>
Disaster Readiness Test: Firedrills

Simulate DR Failover: FireDrill

- Support for all replication technologies
  - HW rep: SRDFSnap, HTCSnap etc.
  - SW rep: DiskGroupSnap, RVGSnapshot, etc.

- Flavors: Gold/Silver/Bronze
DR using VCS

1. DR using VCS – Quick overview
2. Best Practices for DR configurations
3. Advanced DR Configurations
VCS Stretch Cluster: Best Practices

- Define Site boundaries
  - VCS: SystemZones,
  - VxVM: Host Site ID, Disk/Enclosure Site ID

- Configure the failover behavior for stretch clusters
  - AutoFailoverPolicy
    Recommended value: 2 for manual failover across SystemZones
VCS GCO: Best Practices

- Configuring DR infrastructure: Use automation tools/wizards
  - Java GUI/gcoconfig & VCS CLIs
    - Reduce time
    - Avoid human errors

- Configuring the failover behavior for Global Service Groups
  - Use Manual ClusterFailoverPolicy (default)
    - For short distances between DR sites, ClusterFailoverPolicy can be Connected
  - Use Preswitch during planned migrations
VCS GCO: Best Practices

- Configure Steward for 2-site DR setups
- Configure DNS agent for consistent name resolution after DR failover
VCS Replication Agents: Best Practices

• Install latest version of DR agent from SORT
  – https://sort.symantec.com/agents
  – Freeze SGs before upgrading/installing replication agent

• Define the takeover behavior of the replication resource
  – SplitTakeover = 0
  – AutoTakeover = 0
VCS Replication Agents: Best Practices

• Use separate Device Group per Application

• For out-of-band arrays, configure all the IP addresses in the resource definition
VCS Replication Agents: Best Practices

• For Virtual machines managing in-band arrays, map the Control Devices in Raw device mode to the Guest
  – e.g. Physical RDM in Vmware

• Adjust the OnlineTimeout of the resource
  – For EMC SRDF, use sigma script to assist in setting DevFOTime
  – Increase ActionTimeout for Oracle DataGuard

• EMC RecoverPoint (CDP/R), use latest FailoverImage
  – e.g. latest (recommended), bookmark_name, TIME=Timestamp

• Set PanicSystemOnDGLoss on DiskGroup
Disaster Readiness Test: Best Practices

- Identify Firedrill flavor (recommended: Gold)

- Use space optimized snapshots wherever possible
  - E.g. EMC CLARiiON Snapview, EMC Symmetrix Snap
Disaster Readiness Test: Best Practices

• Use fdsetup wizard to configure Firedrill Service Group

• Schedule periodic Firedrills using fdsched

• Configure only one System for Firedrill SG
DR using VCS

1. DR using VCS – Quick overview
2. Best Practices for DR configurations
3. Advanced DR Configurations
Multi Tier applications

Production Site

Cluster Fault Event

DR Site

1. Disaster event: (GCO) Cluster Fault
2. On DR site, run “VBS Showplan” to check whether VBS can be started
3. Perform “VBS Start” on DR Site
4. For the GCO Tier force takeover is done to start DB Tier SG
5. Subsequently App and Web Tier SGs Started

Symantec
DR for Virtual Machines

- VM images replicated to DR site
  - To maintain consistent application environment (no config drifts) across Data Centers
  - Replicated Network parameters may be incorrect in the DR site because of different subnet

Best Practices

- Use VCS Virtualization Agents to manage Virtual machines
  - E.g. Solaris Ldoms, Solaris Zones, AIX WPARs
- Use VCS Virtualization agents’ DROpts attributes
  - IP Address, Netmask, Gateway, DNS, etc.
  - VM Network Reconfiguration after DR failover
Multi site replication

- Use VCS Replication agents to handle multi site replication configurations
  - SRDF (Concurrent), SRDFstar, HTC3DC, RVGPrimary (with Bunker), etc.
- Configure single stretch cluster covering the synchronous sites
- Separate cluster for the asynchronous site, connected by VCS GCO
Replication Options: where VVR fits in

**Primary Site**

- Application-Based Replication
- Host-Based Replication
- Storage-Based Replication

**Secondary Site**

- Application-Based Replication
- Storage-Based Replication

**Replication Options:**

- **Storage-Based Replication**
  - Symantec

- **Host-Based Replication**
  - Symantec

- **Application-Based Replication**
  - Oracle
  - Oracle

**DR using VVR**
VVR – Replication objects

Primary Datacenter

Secondary Site

APP

Primary RVG

Secondary RVG

Production Data

Storage Replicator Log (SRL)

Secondary Data

Storage Replicator Log (SRL)

RLINK

DR using VVR
VVR - Flexible replication modes to meet your SLA

**Synchronous**
- Maximum Protection: Zero RPO
- Ideal for small distances (< 100 KM)

**Asynchronous**
- Maximum Performance
- Ideal for any distance between sites

**Bunker**
- Maximum Protection + Maximum Performance
- Cost effective 3-site solution
VVR Asynchronous Replication
High performance replication across any distance

**Performance Path**

- **Write I/O**
- **I/O ack**
- **Next I/O**
- **Write I/O in order**

**Primary Datacenter**

- Application host
- Storage array

**Secondary Site (DR site)**

- Application host
- Storage array

- **Transfer I/O**
  - (distance = more time)
- **Store I/O**
  - **Transfer ack**
    - (distance = more time)

**NOT in Performance Path**
Best Practices in VVR - Overview

- Planning Replication
  - VRAvisor
- Configuring Replication
  - General practices
  - Configuring a secondary
  - HA-DR agents
- Advanced Replication features
  - Bunker replication
  - Compression
  - Off-host processing
- Optimizing Replication
  - VVR memory pool tuning
Our Disaster Recovery Plan Goes Something Like This...
VRAdvisor – a VVR Planning tool

How can I achieve desired RPO/RTO?
How do I tolerate network outages?

Use VRAdvisor

Graphic interface
No need to install VVR
VRAdvisor – a VVR Planning tool

The problems

- Tolerance to network & secondary outages
- Tolerance to I/O spikes
- RPO & RTO planning

What VRAdvisor does

- Data collection and analysis
- Graphical charts
- SRL size planning
- Network bandwidth recommendations for
  - sync & async modes of replication
  - specified RPO & RTO
- What-if analysis
VRAdvisor – a VVR Planning tool

Analysis Results

- Network Bandwidth required for replication in Synchronous / Synchronous Override mode is: **1.61 Gbps**

Since the specified Network Bandwidth is less than what is required for replication in Synchronous mode, there may be a degradation of application performance due to a delay in application writes.

- SRL Size without outage: **1.89 GB**
- SRL Size with outage: **678.2 GB**

*These results are based on theoretical calculations. We recommend that you add a buffer of 10-20% to these results to take care of variations in real life scenarios.*
VRAdvisor – a VVR Planning tool

Type of Analysis:

- Calculate SRL Size for a specified Network Bandwidth and Outage.
- Calculate Network Bandwidth for data loss specified in bytes.
- Calculate Network Bandwidth for Bunker Bandwidth and RTO.

Common Parameters:

Network Bandwidth Available for Replication from Bunker to Secondary

RVG Parameters:

- Replication Method (File or Volume Group)
- % Disk Writes
- Bandwidth Limit
- RTO

What-If Analysis Results:

<table>
<thead>
<tr>
<th>RVG</th>
<th>Host</th>
<th>% Writes</th>
<th>B/W Limit</th>
<th>RTO</th>
<th>P-&gt;B BW/RVG</th>
<th>P-&gt;B BW</th>
<th>P-&gt;S BW</th>
</tr>
</thead>
<tbody>
<tr>
<td>RVG_sample2.vra</td>
<td>host02</td>
<td>100</td>
<td>N/A</td>
<td>6 Hour(s)</td>
<td>38.14 Mbps</td>
<td>98.1 Mbps</td>
<td>92.96 Mbps</td>
</tr>
<tr>
<td>RVG_sample1</td>
<td>host01</td>
<td>100</td>
<td>N/A</td>
<td>6 Hour(s)</td>
<td>74.34 Mbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DR using VVR
Best Practices in VVR – Configuring Replication

- General practices
- Configuring a VVR secondary
- Setting up HA-DR agents
Configuring VVR – 101

• Create the primary Replicated Volume Group (RVG)
  
  \#> vradmin –g diskgroup createpri rvg volumelist srl

• Add the secondary site to this RVG
  
  \#> vradmin –g diskgroup addsec rvg primary secondary

• Replication is now configured, and can be started by
  
  \#> vradmin –g diskgroup –a startrep rvg secondary

• Monitor replication status by running
  
  \#> vradmin –l repstatus rvg
### General Practices for Configuring Replication

#### Better availability
- 1 RVG per application
- 1 RVG per disk group

#### Better performance
- Use different physical disks for SRL and data volumes
- Stripe the SRL over several physical disks
- Tier-1/SSD storage for SRL: all writes go through the SRL!

#### Better protection
- Mirror all data volumes and SRLs across arrays
Best Practices in VVR – Configuring Replication

- General practices
- Configuring a VVR secondary
- Setting up HA-DR agents
## Best Practices for Configuring a VVR secondary

### Virtual IP
- Plan ahead for application clustering by configuring the replication IP addresses as virtual IPs

### Network bandwidth
- Enable bandwidth limit for VVR, if network bandwidth is constrained or shared
- Use autosync with SmartMove for efficient initial synchronization (SF 6.0+)
- Use compression feature (SF 6.0+)

### Firewall
- Open all the VVR heartbeat and data ports (vrport)
- For NAT-based firewalls, `vol_vvr_use_nat` tunable must be set to 1
Best Practices in VVR – Configuring Replication

- General practices
- Configuring a VVR secondary
- Setting up HA-DR agents
HA-DR Agent hierarchy – an example

Mount Service Group (Parallel & Global)
- CFSmount
- RVGSharedPri

RVGShared Service Group (Parallel)
- RVGShared
- CVMVoldg

RVGLogowner Service Group (Failover)
- RVGLogowner
- IP
- NIC

GCO Service Group (Failover)
- App
- IP
- NIC

CVM Service Group (Parallel)
- CFSfsckd
- CVMCluster
- CVMVxconfigd

Online local firm dependency

DR using VVR
Best Practices in VVR – Optimizing replication

- VVR memory pool tuning
- Performance tuning
VVR Memory Pools - overview
Best Practices in VVR – Advanced Features

- Using bunker replication
- Using off-host processing
- Using compression
Best Practices for bunker replication

- Follow bunker proximity guidelines
- Dedicate separate disks to bunker SRL
- Dedicate separate controllers to bunker SRL
Summary

Planning VVR configuration
- VRAadvisor

Configuring Replication
- Adding VVR secondary
- HA-DR agents

Optimizing Replication
- VVR memory pool tuning

Advanced Replication Features
- Bunker replication
Thank you!

Shrikant Ghare
shrikant_ghare@symantec.com

Yatin Nayak
yatin_nayak@symantec.com
Multi Tier applications: Planned migration (TBD)

1. VBS contains mix of Global & Local SGs
2. Global SG is ONLINE on Production Site
3. “VBS Showplan” on DR site would show that VBS on DR cannot go online
4. Stop the VBS on Production site
5. Start the VBS on DR site
Planning for Disaster Recovery

Ensure Business Continuance after Disaster

- Reduce downtime cost and recovery time (RTO)
- Reduce data loss (RPO)
- Automatic detection and notification of disaster/site failures
- Automated application component startup in the right order
- Ability to do planned migration of application to DR site

Veritas Cluster Server (VCS) for DR automation

- Single solution for local High Availability & Disaster Recovery
DR Events in VOM

[Diagram of DR Events in VOM]

Advanced DR Configurations
DR Events in VOM

Advanced DR Configurations
Futures

• DR SLA computation
  – Instant computation of DR SLAs like RPO and RTO
• VOM based recovery plan for SG and VBS
• Multi Tier Firedrills
Replication Configuration: Best Practices

• Identify hosts for replication management and install appropriate vendor tools on all control hosts
  – These could be the same as Application’s SystemList, or different

• For in-band arrays, map the control devices to Control hosts
  • E.g. EMC Gatekeepers, Hitachi Command Device
  – For virtual machine control hosts, map the control devices in Raw device mode e.g. Physical RDM

• Configure security wherever possible
  – Install secure vendor tools wherever available e.g. NaviSecCli
  – Generate appropriate array security files
Multi Tier Application: DR Best Practices

• Use VBS to manage multi-tier applications

• Use Showplan to check the readiness of the Business Service on DR Site for planned/unplanned operations

• There should be at least one global service group configured in VBS DR setup on at least one of the VBS Cluster Tier
  • Recommended: Global SGs at all tiers

• The failover policy of the global service group should be Manual

• Multiple tiers can be consolidated into the same tier at the DR site
DR Configurations: Topologies

Veritas Cluster Server (VCS) for Disaster Recovery

Local HA

Metropolitan HA (Stretch Cluster)

Wide-Area DR (Global Cluster)

VCS Benefits

- Reduce
  - Failover time
  - Operator dependency
  - Operator error
  - Complexity
- Provide comprehensive data and application availability

DR using VCS – Best Practices