



# HP disaster tolerant solutions using Continuous Access for HP StorageWorks Enterprise Virtual Array in a VMware Infrastructure 3 environment

Executive summary.....	2
Solution technology components.....	2
Virtualization with VMware Infrastructure 3.....	2
Suggested VM storage configuration.....	4
Enterprise Virtual Array family (EVA8100/6100/4100).....	5
HP StorageWorks Continuous Access (CA) EVA.....	5
ESX Logical Volume Manager and EVA Continuous Access (CA).....	6
Case study.....	8
Planned downtime.....	8
Unplanned downtime.....	8
Implementing disaster tolerant VMware solution in a small campus location.....	9
Scope.....	9
Configuration.....	10
Configuration details.....	10
VirtualCenter setup.....	10
Basic ESX Server installation.....	10
SAN switch zoning.....	10
Configure ESX hosts and virtual machines.....	11
Configure DR Groups in Command View.....	11
DR Group properties.....	12
Configuration considerations.....	12
Implementing Continuous Access for a metropolitan configuration.....	13
Scope.....	13
Configuration (metropolitan area).....	13
Configuration details.....	14
VirtualCenter setup.....	14
SAN setup.....	14
Configure EVA at source site.....	14
EVA LUN presentation.....	14
Configure DR Groups in Command View.....	14
DR Group properties.....	15
Configure ESX hosts and virtual machines.....	15
Failover scenarios.....	16
Implementation caveats.....	17
RDM.....	17
Loss of a complete data center.....	17
Scripting for automation: using HP SSSU.....	17
Conclusion.....	18
For more information.....	19

## Executive summary

Practically every business owner understands the importance and need for Business Continuity planning, and its significance in ensuring that organizations are around, not just for today, but are still around well into the future. To ensure that survival, it is important that organizations recognize the importance of preparing strategies to combat the effects when disasters strike. It is however almost impossible for any company to plan against every possible IT failure, which is why companies are increasingly looking at high availability disaster tolerant solutions to ensure IT system recovery from almost any failure, without any data loss.

When companies combine data replication with virtualization, the result is often a flexible, lower cost IT infrastructure that delivers higher levels of availability matched to the needs and budget of the company. The combination of HP StorageWorks Enterprise Virtual Array storage family, HP StorageWorks Continuous Access EVA disaster recovery software, and VMware Infrastructure 3 virtualization software, enables businesses of all sizes to significantly reduce their downtime risks, while maintaining a flexible replication solution that is cost-effective, easy to implement and manage.

Disaster tolerant solutions are key components of today's data centers—even for small businesses. If you are deploying VMware Infrastructure 3, solution tools such as VMotion (instantaneously moving an entire running virtual machine from one server to another), Distributed Resource Scheduling (DRS) (resource utilization monitoring and intelligent allocation across resource pools), High Availability (HA) (cost-effective failover protection), and Consolidated Backup (LAN-free, centralized virtual machine backups) offer a broad range of disaster tolerance options.

This paper describes two deployment types of a VMware tolerant solution, based on coupling key VMware features with disaster tolerance functionality of HP StorageWorks Continuous Access EVA. The first solution is most suitable for a campus-wide disaster tolerant implementation and the other is suitable for metropolitan/geographically separated areas. Both deployments provide the business continuity needed to support your desired VMware service levels. The tradeoffs associated with each solution are also explored along with configuration caveats and best practices.

**Targeted audience:** This document expects that readers are familiar with VMware Infrastructure 3, its feature set, HP StorageWorks Enterprise Virtual Array and Continuous Access. To learn more about Continuous Access for EVA, please see the documentation available on the Storage Replication Software website <http://h18006.www1.hp.com/storage/software/replication/index.html>.

## Solution technology components

### Virtualization with VMware Infrastructure 3

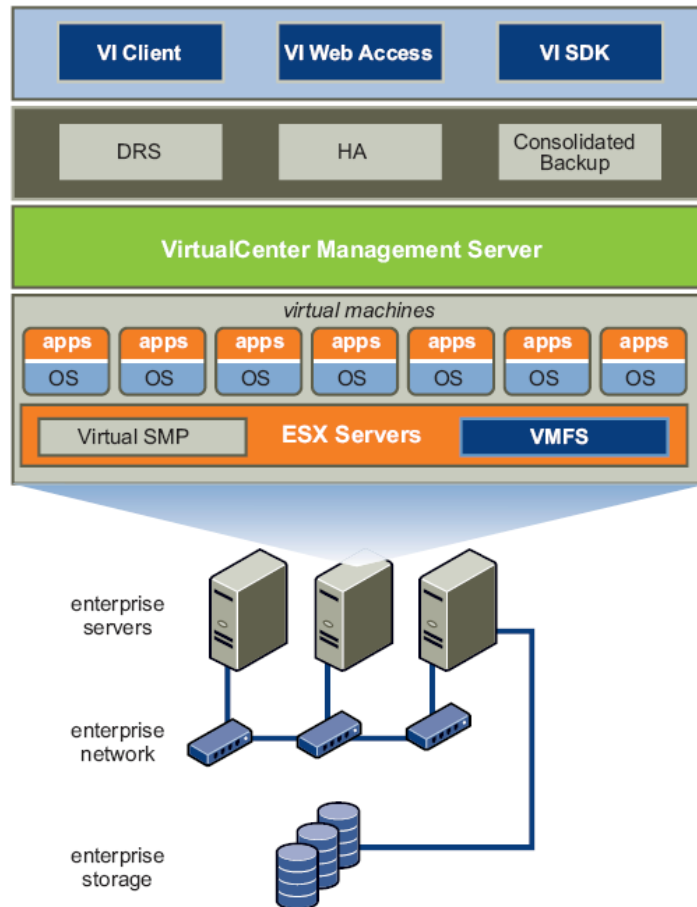
VMware Infrastructure 3 allows enterprises and small businesses alike to transform, manage, and enhance their IT environments through virtualization.

Virtualization creates an abstraction layer that decouples the physical hardware from the operating system to deliver greater IT resource utilization and flexibility. Multiple virtual machines (VMs), running a range of operating systems (such as Microsoft® Windows® Server 2003 or Linux) and applications, run in isolation but side-by-side on the same physical server.

VMware Infrastructure 3 delivers comprehensive virtualization, management, resource optimization, application availability and operational automation capabilities in an integrated offering.

Figure 1 provides a logical view of the components of a VMware Infrastructure 3 implementation.

Figure 1. VMware Infrastructure 3 Components



Some of the components shown in Figure 1 include:

- **VMware ESX Server** – a production-proven virtualization layer running on physical servers; abstracts processor, memory, storage and networking resources to be provisioned to multiple VMs.
- **Virtual Machine** – a representation of a physical machine implemented in software; includes an operating system and applications running on a virtual hardware configuration (CPU, system memory, disk storage, NIC, and more). The operating system sees a consistent, conventional, hardware configuration, regardless of the actual physical components. VMs support advanced capabilities such as 64-bit computing and virtual symmetric multiprocessing. A VM is implemented as an isolated file that can reside in any storage, making it easy to migrate the VM to any location (as, for example, part of a disaster tolerant strategy involving HP StorageWorks Business Copy (BC) and Continuous Access (CA)).
- **Virtual Machine File System (VMFS)** – a high-performance cluster file system for VMs
- **Raw Disk Mapping (RDM)** – a RDM LUN supports direct access<sup>1</sup> between the VM and physical storage subsystem, and is useful with SAN snapshots and other layered applications running in a VM. Because RDM volumes allow SCSI commands to pass through directly from the guest operating system, they better enable scalable backups using native SAN features. By comparison, VMFS volumes filter all SCSI commands.

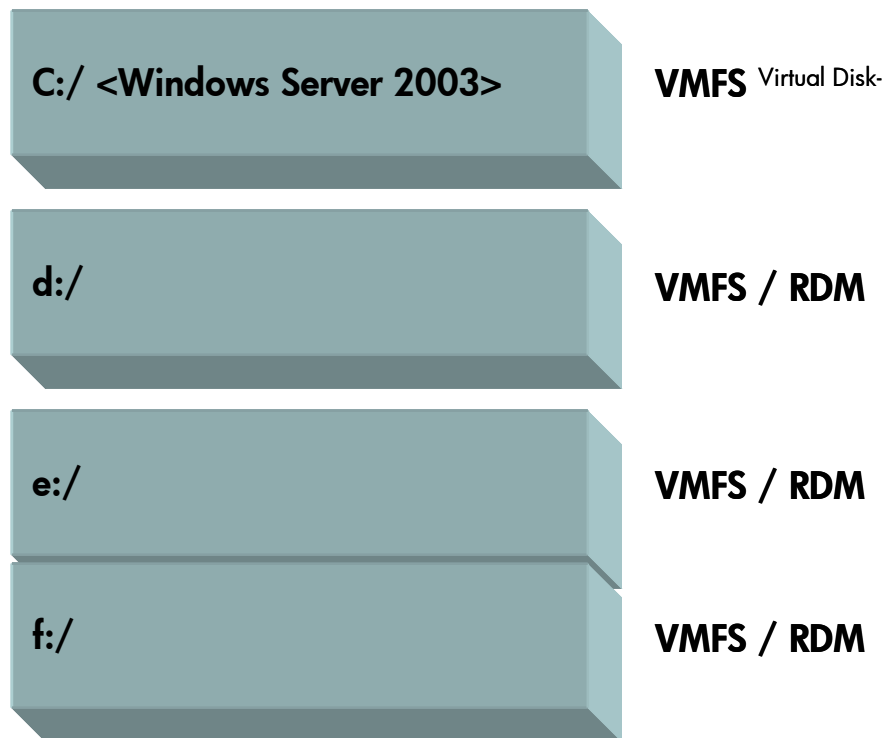
<sup>1</sup> Fibre Channel or iSCSI only

- **Virtual Symmetric Multi-Processing (SMP)** – allows a single VM to simultaneously use multiple physical processors
- **VirtualCenter Management Server** – provides a central point for configuring, provisioning, and managing a virtualized IT infrastructure
- **Virtual Infrastructure (VI) Client** – provides an interface that allows administrators and users to connect remotely to the VirtualCenter Management Server or individual ESX Server installations from any Windows PC
- **VI Web Access** – A web interface for virtual machine management and remote console access

## Suggested VM storage configuration

A suitable VM configuration is a prerequisite for successful disaster recovery with BC and CA. For example, boot disk images and data disks for VMs should be located within a RAID array on the SAN.

Figure 2. Sample configuration that is suitable for virtual machines drive configurations



HP recommends using a dedicated VMware Virtual Machine Disk Format (VMDK) file within a VMFS filesystem to separate the VM's operating system from all other data.

With this structure, the VMFS virtual disk containing the boot image can be kept to the smallest possible size so that less time is required for cloning, exporting, and backup. You can also implement separate backup policies for the operating system virtual disk and the data disks.

## Enterprise Virtual Array family (EVA8100/6100/4100)

The HP StorageWorks 4100/6100/8100 Enterprise Virtual Arrays continue to offer customers in the mid-range to enterprise market place leading high performance, high capacity and high availability "virtual" array storage solutions. Not only do these solutions reduce IT costs and complexity, they save time, space and costs as compared to traditionally architected storage, and they are supported by a powerfully simple suite of management software making it easy for users to achieve higher levels of productivity.

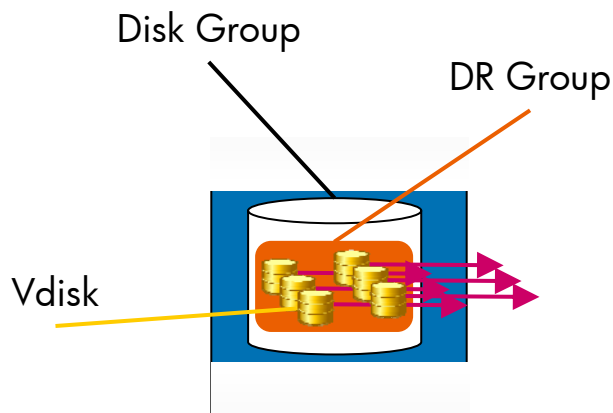
### HP StorageWorks Continuous Access (CA) EVA

Continuous Access EVA is a feature of the Enterprise Virtual Array (EVA) that allows data replication between two or more EVAs. Data replication can be done synchronously or asynchronously. Continuous Access EVA supports various interconnection technologies such as Fibre Channel over IP (FCIP) and Fibre Channel. Additionally, the EVA also supports bi-directional replication. Data replication between sites is most widely used when creating a true disaster tolerant data center.

EVA Continuous Access (CA) enables data replication between all models of the EVA family. EVA CA can replicate data synchronously and asynchronously between source and destination arrays.

A copy set is a replicated Vdisk and a Data Replication (DR) group is comprised of replicated Vdisks (Copy Sets). Each DR group acts as a consistency group and all copy sets within that group share a single write history log. Thus a Data Replication (DR) group is the primary level of CA management. All CA management actions such as Write Mode, Failsafe mode, Suspend Mode and Failover are performed on a DR group and not on each copy set. Replication Solution Manager is the preferred tool to manage BC and CA on EVA.

Figure 3. CA data replication group



The number of replication groups created should be tailored to the specific user environment. For instance, the creation of replication groups can be based on a number of decision factors, for example:

- The disk resources for each application running in a virtual machine may require their own DR group. This allows failing over just one or multiple applications individually to a different virtual machine without having to fail over the VM they are running on.
- A virtual machine or group of virtual machines may need to have all of their disk resources in a single DR group. Virtual machines booting off of VMDK files on the same VMFS volume would need to all be failed over together when the LUN where the VMFS resides is failed over.

The EVA provides a limited number of DR groups<sup>2</sup> so understanding your environment and its replication granularity requirements can help you reduce the number of DR groups required for your environment and provide improved efficiency. Consult with your HP field representative for data replication groups' implementation strategies.

## ESX Logical Volume Manager and EVA Continuous Access (CA)

VMware Infrastructure 3, tracks disk metadata inside the VMFS3 volume. When creating a VMFS3 filesystem, metadata is written to the Logical Volume Manager (LVM) header containing the following information:

- LUN ID of the disk (Example: 4)
- The storage system product ID retrieved from the SCSI Inquiry string (Example: HSV210)
- A unique LUN identifier also known as WW LUN ID (Example: 6006-0e80-0527-1600-0000-2716-0000-050). This is a hex number, unique for each LUN.

Whenever an ESX Server finds a LUN with a VMFS3 filesystem, the information returned from the LUN is compared with the LVM metadata header that resides on the VMFS filesystem.

The VMkernel treats a volume as a snapshot if there is a mismatch between the information that exists in the LVM header of the VMFS volume and the data retrieved from the LUN. By default, VMFS3 volumes residing on LUNs determined as snapshots are hidden from access. The examples below describe when a LUN will be interpreted as a snapshot:

- A LUN is presented to multiple ESX Servers, however the LUN ID is not the same as seen by all ESX Servers.
  - **Possible cause:** The most likely cause is misconfiguration. Reconfiguring the environment so that all servers see the LUN with the same ID can address this issue.
- The LUN is a real storage snapshot
  - **Possible cause:** An actual snapshot was created using array replication technology such as EVA Business Copy. Advanced LVM parameters discussed below help address this.
- A LUN is replicated using Continuous Access from one EVA to another EVA with both EVAs having different product ID (controller models) and a failover has occurred. Advanced LVM parameters discussed below help address this.

In the ESX kernel logs (/var/log/vmkernel) an entry similar to the following is added for each snapshot found:

---

ALERT: LVM: 4903: vmhba2:2:2:1 may be snapshot: disabling access.

---

It may be desirable in some cases to allow an ESX Server access to a snapshot LUN. For this, ESX Server provides two methods:

1. Allow access to snapshots through the use of the **LVM.DisallowSnapshotLun** advanced LVM parameter. ESX default setting is LVM.DisallowSnapshotLun=1 (See Figure 4). To allow access to snapshots, this value must be set to 0 (LVM.DisallowSnapshotLun=0) and then trigger a manual ESX SAN rescan.

---

<sup>2</sup> Max number of DR groups may vary depending on the EVA firmware. Consult the EVA Continuous Access release notes for the number of DR groups.

---

**CAUTION:** When access is allowed to snapshots, no “real” EVA snapshots can be presented to the ESX Servers as long as the original Vdisks are presented to the same ESX host.

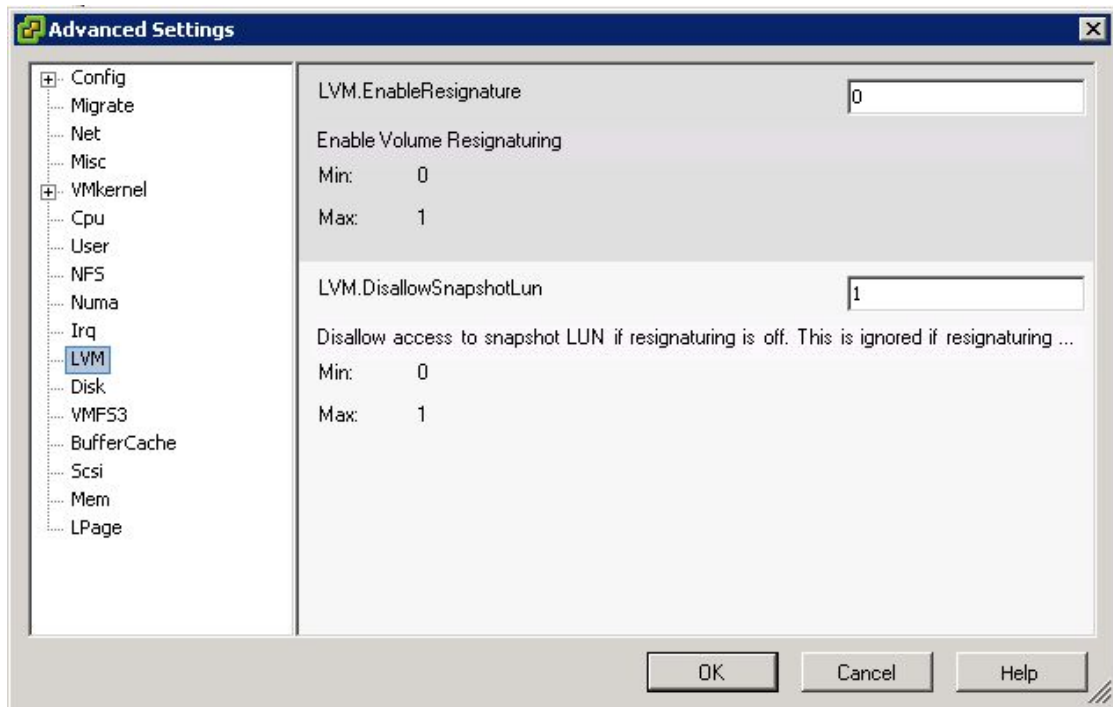
---

2. Write a new LVM header on the snapshot LUNs through the use of the **LVM.EnableResignature** advanced LVM parameter. ESX default setting is LVM.EnableResignature = 0 (See Figure 4).
- 

**CAUTION:** When LVM.EnableResignature = 0, all datastore names will be changed to a name similar to: snapxxx\_datastorename. All VMs residing on these datastores will have to be re-imported. Only apply on one ESX Server at a time, rescan the SAN; then set the parameter value back to its default value.

---

Figure 4. LVM advanced parameter default settings



## Case study

Building an effective disaster tolerant solution can often be a very complex and time consuming task. Furthermore most disaster tolerant solutions, implemented at customer sites, are often untested and fail to protect customers when failure occurs. Depending on the data center solution or application, the recovery point objective and recovery time objective are different from customer to customer.

Any disaster tolerant solution must be able to accommodate both planned and unplanned downtime.

### Planned downtime

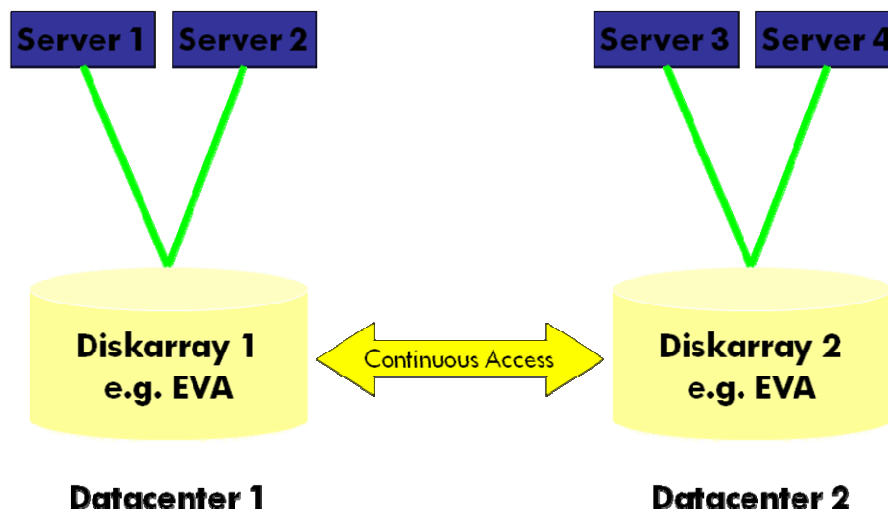
Planned downtime (for equipment or software maintenance) can jeopardize data at local or centrally-located data centers. You must be able to preserve these data at a centralized location.

### Unplanned downtime

Unplanned downtime results from a natural disaster or sudden hardware or software failure and may impact an entire site. CA offers an ideal solution, allowing you to move your data to a safe offsite data center, away from harm.

When implementing a VMware disaster recovery solution two configuration options are available, each providing pros and cons to the overall solution. The first configuration is the most standard Continuous Access configuration as illustrated in the following figure.

Figure 5. A standard Continuous Access configuration

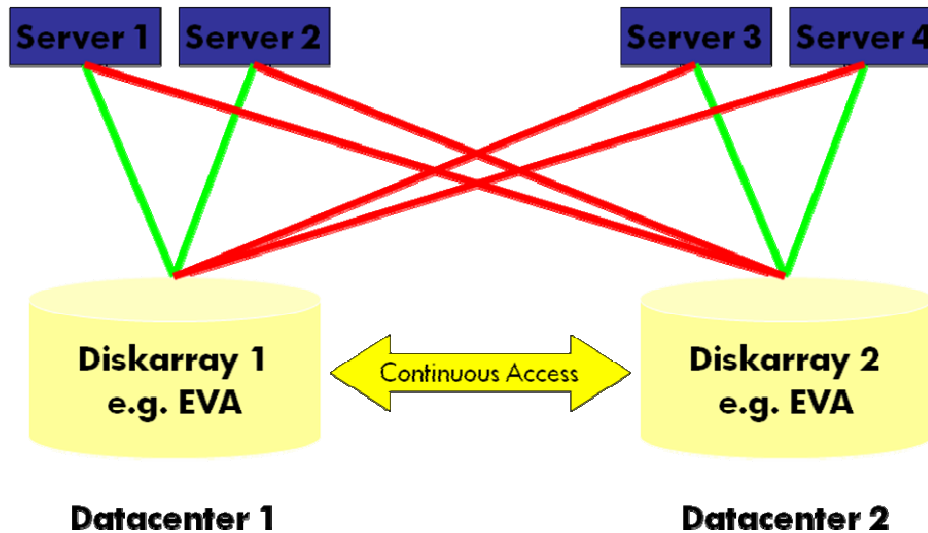


In this configuration, the servers in each data center can only access the local storage they are connected to. Any failure to the servers or the storage in Datacenter 1 will trigger a failover to Datacenter 2 and vice versa. Nonetheless this configuration is well suited for long distance (metro or continental) replication. Furthermore, optimal resource utilization can be attained by using multiple DR groups each replicating in one direction or the other.

The second configuration is a less conventional yet very flexible crosslink approach. The following figure illustrates this configuration:



Figure 6. A flexible crosslink Continuous Access configuration



In this configuration, the servers have access to both the local and remote storage systems. This crosslink architecture allows for storage failures to not require a server failover and similarly, server failures, do not require a storage failover. For instance, if the servers in Datacenter 1 failed, the VMs can be restarted on server 3 and 4 in Datacenter 2 directly by accessing the storage in Datacenter 1. This configuration allows for great flexibility but may present some latency issues when deployed over long distances (metro, continental) making it most suitable for campus-wide deployment.

This paper explores these two configurations in more details and provides key implementation schemes to enable ease of use and management while offering robust data replication solutions which address various recovery time objectives (RTO) and recovery point objectives (RPO) needs in a small campus, metropolitan area or both.

## Implementing disaster tolerant VMware solution in a small campus location

### Scope

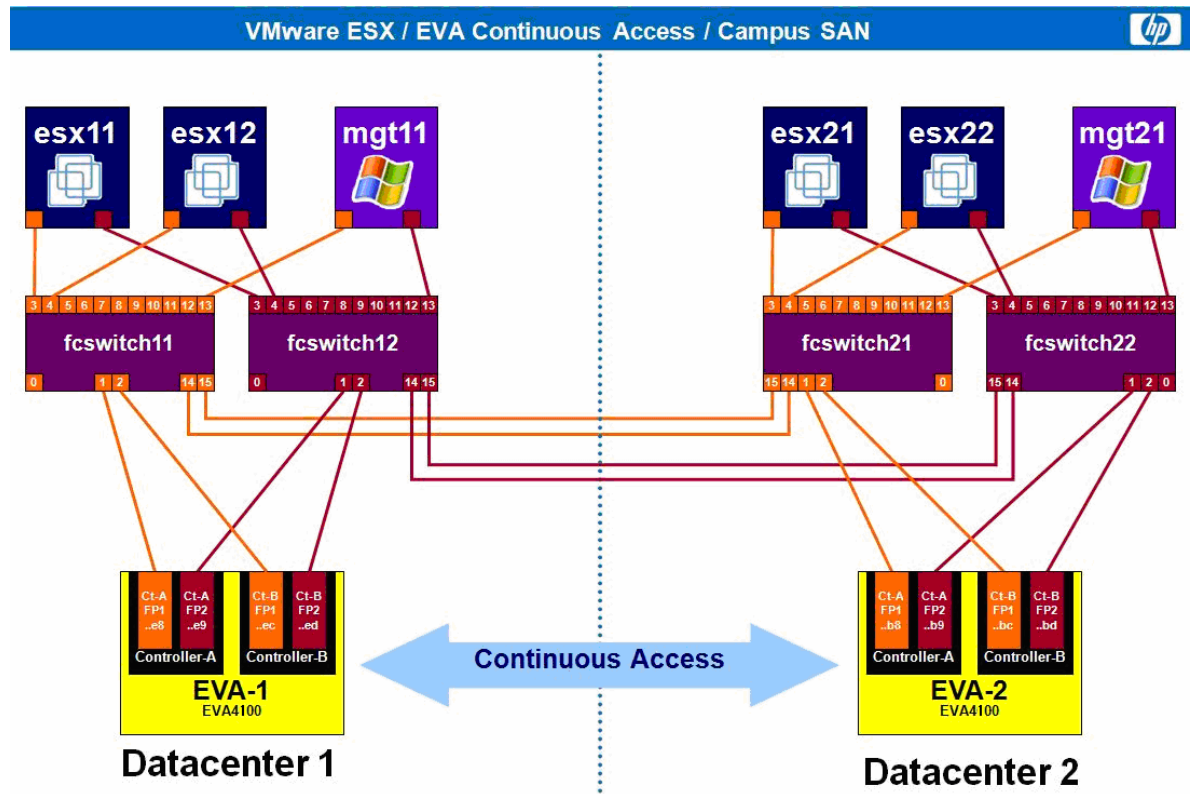
This case study demonstrates a disaster tolerant solution for a small campus area. In this scenario the data centers are merged through a shared SAN (See Figure 7). EVA-1 and EVA-2 are connected through a Continuous Access link through the shared SAN. Failures to esx11 and/or esx12 only require that VMs be restarted on esx21 and esx22 from the replicated data and boot LUN on EVA-2. Failures to EVA-1 may cause esx11 and esx12 to run their VMs directly from EVA-2 on the replicated volumes. A manual failover of the corresponding DR group must be performed prior to restarting the VM. This proof of concept is ideal for small office or campus wide solutions where distances are minimal and potential latency issues are not a concern.

- Recovery Point Objective: Low (Varies depending on replication mode)
- Recovery Time Objective: Medium

[Low=(0 to seconds); Medium=(minute to half hour); High=(half hour to several hours)]

# Configuration

Figure 7. Campus-wide CA configuration topology



## Configuration details

### VirtualCenter setup

- Create a single data center in VirtualCenter
- Add the local and remote ESX hosts to this data center

### Basic ESX Server installation

- Follow your best practices for installing and configuring VMware Infrastructure 3. For this scenario it is required to boot the ESX Server from local disks.

### SAN switch zoning

- Configure zoning in a way that all ESX Servers see both EVAs. When zoning is properly configured, ESX Servers (esx11, esx12) in Datacenter 1 have access to both the local storage (EVA-1) and the destination storage (EVA-2) in Datacenter 2. Furthermore ESX Servers in Datacenter 2 (esx21, esx22) also have access to both storage systems (EVA-1 and EVA-2) in this topology.
- HP considers a best practice to create separate zones per server HBA and storage devices (for example, 2 zones per ESX Server in each fabric). This configuration provides a shared SAN environment in which the SAN from Datacenter 1 and Datacenter 2 are merged through inter-switch links (ISL) into one SAN. For more information, please refer to HP SAN design reference guide for more zoning and SAN design considerations.

<http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/c00403562/c00403562.pdf>.

## Configure EVA at source site

- Present the Vdisks to all ESX Servers

## EVA LUN presentation

---

Figure 8. EVA LUN presentation

Vdisk	LUN
staticVDisks\i2esx-kalmcluster\i2esx-kalmcluster_01_admin	1
staticVDisks\i2esx-kalmcluster\i2esx-kalmcluster_02_vms	2
staticVDisks\i2esx-kalmcluster\i2esx-kalmcluster_03_vms	3

---

## Configure ESX hosts and virtual machines

- ESX Server
    - ESX advanced parameter LVM.EnableResignature is left at default 0.
    - ESX advanced parameter LVM.DisallowSnapshotLun is left at default value of 1.
    - Scan and format the Vdisks with VMFS
  - Virtual machine
    - Create your virtual machine and use the newly formatted VMFS
- 

### Note:

In case there are two different EVA controller models (for example, EVA4100 and EVA8100) it is necessary to set the Advanced setting "LVM.DisallowSnapshotLun" to 0.

No real EVA snapshot can be presented to the ESX Servers as long as the original Vdisks are presented through the same server.

---

## Configure DR Groups in Command View

- On the source EVA create one DR group for all existing ESX Vdisks. Multiple groups can also be created.
- Leave the default settings:
  - Synchronous mode
  - Destination Hosts Access = None
- On the destination EVA (here: EVA-2) present all corresponding Vdisks with the same LUN IDs as on the source EVA-1.

## DR Group properties

Figure 9. DR group properties

Save changes		?
<div style="display: flex; border-bottom: 1px solid black; margin-bottom: 5px;"> <span style="padding: 2px 10px;">General</span> <span style="padding: 2px 10px;">Log</span> <span style="padding: 2px 10px;">Members</span> <span style="padding: 2px 10px;">Connections</span> </div>		
Destination system: i2eva8k		
<b>Connection Attributes</b>		
Write mode:	Requested:	Synchronous ▼ Actual: Synchronous
Replication I/O:		Resumed ▼
Destination host access:		None ▼
Auto-suspend:		Disabled ▼
Log state:		✔ Not in use
Connection state:		✔ Good
UUID:	6005-08b4-0010-712a-0001-f000-004b-0000	

## Configuration considerations

In a failover situation it is important to understand the proper course of action to avoid unexpected behaviors. For instance, in the event EVA-1 loses Fibre connection from the ESX Servers and its CA link to EVA-2, when the administrator switches EVA-2 disk access to being Source (Failover) and the VMs are restarted on EVA-2, if EVA-1 returns to the SAN at a later time, it will return with its disk access also set to Source and the ESX Servers may have LUNs with the same ID from two different storage systems presented to it. This situation is highly undesirable. To avoid this behavior, after setting EVA-2 disk access to Source mode during a manual failover the following steps can facilitate proper recovery of the CA configuration:

1. Logically separate (using Fibre Channel switch zoning) the ESX Servers from the failed EVA by disabling the relevant zones (CA and Host access zones).
2. After EVA-1 is repaired and its SAN connection restored, power cycle the array.
3. Re-enable the previously disabled zone to re-establish the CA link between the two arrays.
4. Allow all replication groups to fully synchronize.
5. Enable host access zones to re-establish host access to EVA-1.
6. Schedule a planned failover to validate the functionality of EVA-1 and/or to return the environment to its original configuration.

Table 1. Pros and cons of data centers merged through a shared SAN (small campus area case study)

<b>PROS</b>	<ul style="list-style-type: none"> <li>• Efficient resource utilization even in a failure case</li> <li>• Very flexible architecture and rapid recovery time</li> </ul>
<b>CONS</b>	<ul style="list-style-type: none"> <li>• Does not protect in the event of natural disaster, blackouts, and other disasters which impact the campus-wide area</li> <li>• If proper recovery steps are not followed, potential for EVA split brain scenario</li> <li>• Configuration slightly complex (Zoning)</li> </ul>

# Implementing Continuous Access for a metropolitan configuration

## Scope

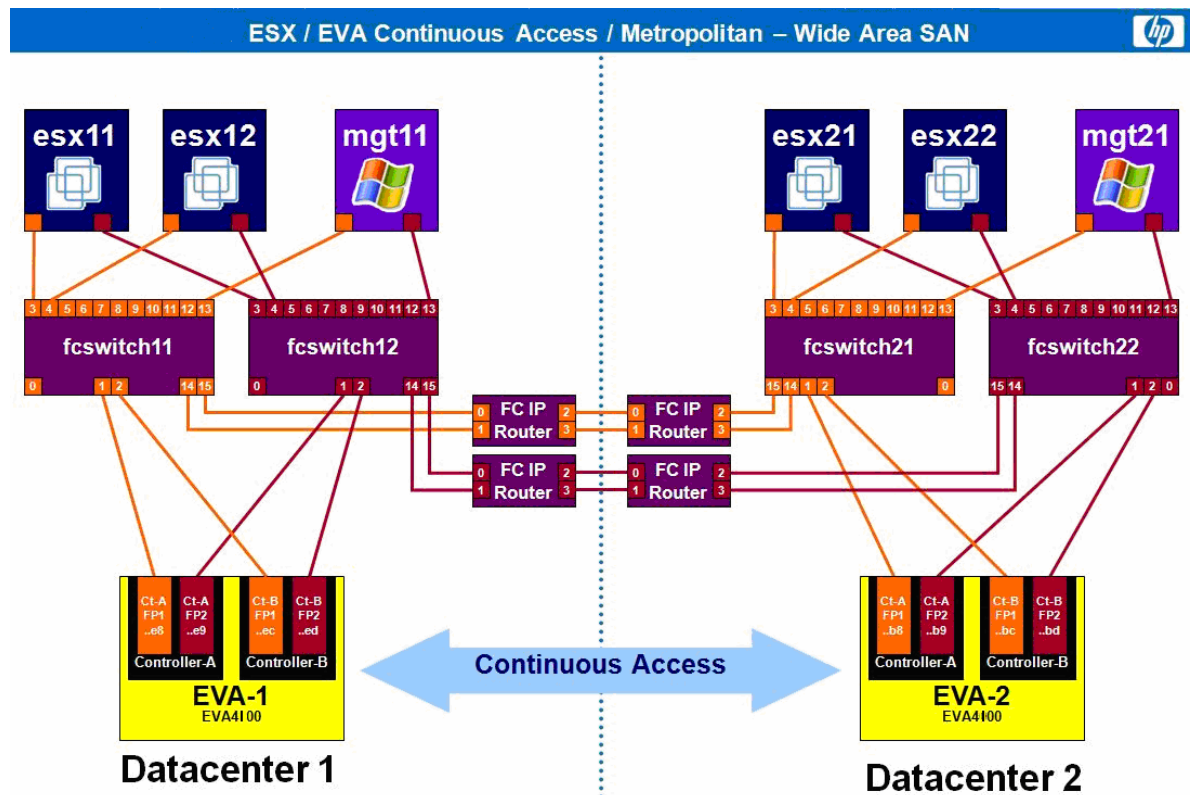
This case study demonstrates a disaster tolerant solution for a metropolitan area. In this scenario the data centers are linked through a non-shared extended SAN (See Figure 10). EVA-1 and EVA-2 are connected through a Continuous Access link through a zone in the extended SAN. Failures to esx11 or esx12 can only be recovered from by restarting the VMs on the replicated LUNs visible only through esx21 or esx22. Failures to EVA-1 are recovered from by failing over system operation to EVA-2 and restarting all VMs on esx21 and esx22 on the replicated LUNs. In either failure scenario, a manual failover is required to put EVA-2 in source access mode for the LUNs of the appropriate DR group. This process can be scripted using the HP StorageWorks Storage System Scripting Utility (SSSU) to provide some level of automation. See scripting discussed below. In this case study, the ESX Servers in Datacenter 1 have no visibility of EVA-2 in Datacenter 2 and esx21 and esx22 also have no visibility of EVA-1 in Datacenter 1. This case study is ideal for enterprise data centers that require long distance replication for protection against disasters at a local site.

- Recovery Point Objective: Low (Varies depending on replication mode)
- Recovery Time Objective: Medium

[Low=(0 to seconds); Medium=(minute to half hour); High=(half hour to several hours)]

## Configuration (metropolitan area)

Figure 10. Metropolitan Area configuration topology



## Configuration details

### VirtualCenter setup

- Create two data centers in VirtualCenter, each representing a physical data center
- Add the local ESX hosts to each data center or cluster

### SAN setup

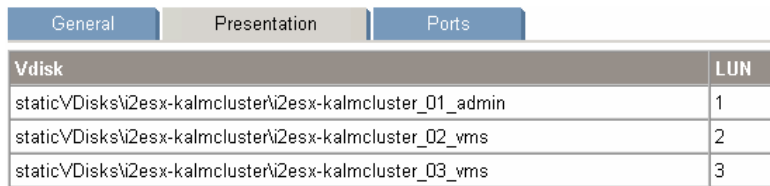
- Configure zoning in such a way that each ESX Server sees only its respective local EVA. This configuration provides an extended SAN environment in which the SAN from Datacenter 1 is extended to the SAN in Datacenter 2 through the use of FCIP routers. HP considers a best practice to create separate zones per server and storage devices (for example, 2 zones per ESX Server in each fabric).

### Configure EVA at source site

- Create the Vdisks
- Present the Vdisks to all ESX Servers

### EVA LUN presentation

Figure 11. EVA LUN presentation



Vdisk	LUN
static\VDisks\i2esx-kalmcluster\i2esx-kalmcluster_01_admin	1
static\VDisks\i2esx-kalmcluster\i2esx-kalmcluster_02_vms	2
static\VDisks\i2esx-kalmcluster\i2esx-kalmcluster_03_vms	3

### Configure DR Groups in Command View

- On the source EVA, create one DR group for all existing ESX Vdisks. Multiple groups can also be created.
- Leave the default settings:
  - Synchronous mode
  - Destination Hosts Access = None
- On the destination EVA-2 present all corresponding Vdisks with the same LUN IDs as on the source EVA-1.

## DR Group properties

---

Figure 12. DR Group properties

Save changes ?

General Log Members Connections

Destination system: i2eva8k

Connection Attributes	
Write mode:	Requested: Synchronous Actual: Synchronous
Replication I/O:	Resumed
Destination host access:	None
Auto-suspend:	Disabled
Log state:	<input checked="" type="checkbox"/> Not in use
Connection state:	<input checked="" type="checkbox"/> Good
UUID:	6005-06b4-0010-712a-0001-f000-004b-0000

---

### Configure ESX hosts and virtual machines

- ESX Server
    - Set ESX advanced parameter LVM.EnableResignature = 0
    - Set ESX advanced parameter LVM.DisallowSnapshotLun = 1 if not already set (Default value=1).
    - Scan and format the Vdisks with VMFS
  - Virtual machine
    - Create your virtual machine and use the newly formatted VMFS
- 

#### Note:

In case there are two different EVA controller models (for example, EVA4100 and EVA8100) it is necessary to set the advance setting "LVM.DisallowSnapshotLun" to 0.

No real EVA snapshot can be presented to the ESX Servers as long as the original Vdisks are presented through the same server.

---

### Failover scenarios

- Initiate DR Group failover at the destination EVA in Datacenter 2
- Rescan the ESX Servers in Datacenter 2
- ESX Servers in Datacenter 2 see the VMFSs, but the VMs on those VMFSs are not registered to those ESX Servers.
- Now register those VMs at the service console using<sup>3</sup>
  - `vmware-cmd -s register `find /vmfs/volumes/ -name "*.vmx" ``

If multiple VMs need to be registered, a simple script similar to the one show below can automate this process:

```
for i in `find /vmfs/volumes/ -name "*.vmx" `
do
  echo "### Registering VM $i ..."
  vmware-cmd -s register $i
done
```

Table 2. Pros and cons of data centers linked through a non-shared extended SAN (metropolitan case study)

---

<b>PROS</b>	<ul style="list-style-type: none"><li>• Protects against natural disasters, blackouts, and other disasters which impact the local/regional data center</li><li>• Less intricate configuration (Zoning)</li></ul>
<b>CONS</b>	<ul style="list-style-type: none"><li>• Inefficient resource utilization during failure</li><li>• Additional hardware resources required (FCIP routers)</li></ul>

---

<sup>3</sup> Note: This step only needs to be performed the first time a virtual machine is registered on an alternate ESX server. It is not required during all subsequent failovers



## Implementation caveats

### RDM

RDMs are referenced differently than VMDKs. In the event of a failover to the storage system in the other data center, the path to all RDM LUNs will have to be manually re-configured into each VM configuration.

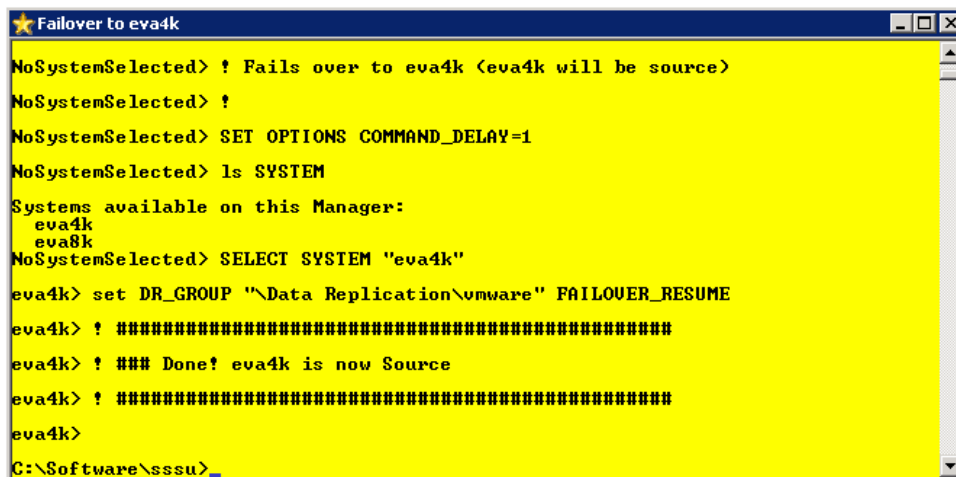
### Loss of a complete data center

If VMware HA is not used then the VMs hosted on the failed ESX Servers will have to be manually removed from inventory in VirtualCenter and will need to be re-registered on the surviving ESX Servers.

### Scripting for automation: using HP SSSU

HP SSSU (HP StorageWorks Storage System Scripting Utility) enables the creation of simple scripts that can automate the process of failing over a storage system, deleting or creating LUNs and presenting these LUNs to ESX Servers in the configuration. For example the following figure shows the output of a basic SSSU script which fails over a data replication group access status.

Figure 13. Output of a basic SSSU script which fails over a data replication group access status



```
Failover to eva4k
NoSystemSelected> ? Fails over to eva4k <eva4k will be source>
NoSystemSelected> ?
NoSystemSelected> SET OPTIONS COMMAND_DELAY=1
NoSystemSelected> ls SYSTEM
Systems available on this Manager:
  eva4k
  eva8k
NoSystemSelected> SELECT SYSTEM "eva4k"
eva4k> set DR_GROUP "\Data Replication\vmware" FAILOVER_RESUME
eva4k> ? #####
eva4k> ? ### Done! eva4k is now Source
eva4k> ? #####
eva4k>
C:\Software\sssu>
```

To further reduce recovery time, these SSSU scripts, after careful creation and testing, can be launched from basic Windows shortcuts as shown in Figure 14. Each of the shortcuts will launch SSSU and execute the preconfigured operation scripted. For information on SSSU please consult the SSSU user guide at [http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01077522/c01077522.pdf?jumpid=reg\\_R1002\\_USEN](http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01077522/c01077522.pdf?jumpid=reg_R1002_USEN)

Figure 14. Windows shortcuts for SSSU scripts



## Conclusion

This white paper concludes that there are two deployment types which provide a VMware disaster tolerant solution, based on VMware features with disaster tolerance functionality of HP StorageWorks Continuous Access EVA and HP StorageWorks EVA. Both deployments provide the business continuity needed to support your desired VMware service levels.

## For more information

HP virtualization with VMware	<a href="http://www.hp.com/go/vmware">http://www.hp.com/go/vmware</a>
VMware Infrastructure 3, planning (white paper)	<a href="http://h71019.www7.hp.com/ActiveAnswers/library/GetPage.aspx?pageid=571045">http://h71019.www7.hp.com/ActiveAnswers/library/GetPage.aspx?pageid=571045</a>
HP StorageWorks EVA replication software release notes	<a href="http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00746629/c00746629.pdf">http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00746629/c00746629.pdf</a>
Data storage from HP	<a href="http://www.hp.com/go/storageworks">http://www.hp.com/go/storageworks</a>
VMware Virtual Infrastructure 3	<a href="http://www.vmware.com/products/vi/">http://www.vmware.com/products/vi/</a>
VMware <b>"Storage/SAN Compatibility Guide for ESX Server 3.0.x"</b>	<a href="http://www.vmware.com/pdf/vi3_san_guide.pdf">http://www.vmware.com/pdf/vi3_san_guide.pdf</a>
VMware <b>"SAN Configuration Guide"</b>	<a href="http://www.vmware.com/pdf/vi3_esx_san_cfg.pdf">http://www.vmware.com/pdf/vi3_esx_san_cfg.pdf</a>

To help us improve our documents, please provide feedback at [www.hp.com/solutions/feedback](http://www.hp.com/solutions/feedback)

© Copyright 2007, 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

4AA1-0820ENW, Revision 4, February 2008

