

**hp StorageWorks
multi-site disaster
tolerant solution**

**implementation
blueprint**

design guide



Confidential

This document contains confidential and proprietary information belonging to Hewlett-Packard, Inc. Access to this information is strictly limited to specifically authorized employees of Hewlett-Packard. All other persons are expressly forbidden to read or review this document without the prior written consent of Hewlett-Packard.

notice

© Copyright 2003 Hewlett-Packard Development Company, L.P.

Edition 0503

HP, StorageWorks, ServiceGuard, MetroCluster, Continental Clusters, Continuous Access, Continuous Access Extension, Business Copy, RAID Manager XP, LUN Configuration and Security Manager XP, LUN Configuration Manager XP, Secure Manager XP, and the HP logo are trademarks of Hewlett-Packard Company in the United States and other countries. UNIX is a trademark of The Open Group. All other product names mentioned herein may be trademarks of their respective companies.

Use of the terms “CA,” “sync CA,” “sync-CA,” “async CA,” or “async-CA” within this document refer to the HP StorageWorks Continuous Access or Continuous Access Extension products, and have no connection with the term “CA” copyrighted by Computer Associates.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

format conventions

note This is a Note.

contents

1 Introduction	5
audience	5
required skills and knowledge	5
related documents	5
2 Model Configuration.....	7
solution overview	7
logical view	8
physical view	9
minimum requirements	10
3 Design Process	11
assumptions	11
deliverables	11
design flowchart	12
4 Design Tasks	13
1: gather customer requirements	13
guidelines for completing the customer requirements checklist	15
2: identify customer administrative personnel.....	17
3: identify components.....	19
guidelines for completing the component checklist for site 1.....	21
guidelines for completing the component checklist for site 2.....	23
guidelines for completing the component checklist for site 3.....	25
4: diagram site configurations	25
5: complete bills of materials	29
6: continue solution design and implementation	32

1 Introduction

This design guide provides information and checklists to help HP services personnel design a Multi-Site Disaster Tolerant (MSDT) Solution for a specific customer.

audience

This guide is intended to help the HP Solution Architect and the HP Consulting and Integration Engineer determine the feasibility of implementing an MSDT Solution for a specific customer and, if feasible, define the high-level design of the solution for that customer. This guide contains a series of tables and checklists to assist in this process.

required skills and knowledge

This guide assumes that the HP representative designing the solution has an in-depth understanding of:

- Systems and network architecture
- The MSDT Solution (detailed in the *MSDT Technical Blueprint*)

This guide assumes that the HP representative designing the solution is familiar with:

- HP-UX servers
- HP StorageWorks XP disk arrays
- The HP StorageWorks software products used in the solution, including HP StorageWorks RAID Manager XP (RM), HP StorageWorks Business Copy (BC), HP StorageWorks Continuous Access (CA), and Continuous Access Extension (CA Ext)
- The HP cluster software products used in the solution, including HP ServiceGuard (SG), MetroCluster, Continental Clusters, and XP-CA toolkit for MetroCluster

related documents

For more information on the MSDT Solution, see the following documents:

- *Multi-Site Disaster Tolerant Solution Business Blueprint*
- *Multi-Site Disaster Tolerant Solution Technical Blueprint*
- *Multi-Site Disaster Tolerant Solution Implementation Blueprint: Installation and Configuration Guide*
- *Multi-Site Disaster Tolerant Solution Implementation Blueprint: Multi-Site DT Management Tools User Guide*
- *Multi-Site Disaster Tolerant Solution Implementation Blueprint: Administration Guide*
- *Designing Disaster Tolerant High Availability Clusters*: B7660-90013
- *Managing MC/ServiceGuard*: B3936-90065
- *HP ServiceGuard Quorum Server Version A.02.00 Release Notes*: B8467-90011
- *MetroCluster with Continuous Access XP Version A.04.20 Release Notes*: B8109-90013

2 Model Configuration

This chapter describes the model configuration for an MSDT Solution. This model configuration is the one that HP has tested and recommends for its high availability and redundancy.

solution overview

In the MSDT Solution, two nearby sites—less than 100 km¹ apart—protect each other in case of an in-region disaster. Critical applications are mirrored synchronously, providing high availability for online transaction processing. If a failure occurs at one site, the other site can take over application processing, with minimal interruption, at virtually the exact point where it was interrupted. A third site (Site 3) located well outside of the region offers protection should both primary sites (Sites 1 and 2) be lost. A point-in-time copy is made at Site 2 and then mirrored to Site 3 at customer-defined intervals. Copying is a scheduled, scripted process enabled by the Multi-Site DT Management Tools. The recovery point from Site 3 would be determined by the last time a copy cycle was completed.

The MSDT Solution solves the following business issues:

- Application continuance in case of a local or regional disaster while maximizing transaction-processing availability. Mirroring of Site 2 to Site 3 using a point-in-time copy allows placement of Site 3 out of the disaster region.
- High availability for 24 x 7 operations.
- ServiceGuard with MetroCluster and Continental Clusters provide a recovery time objective (RTO) of less than one hour. Synchronous capability between sites 1 and 2 allows for recovery point objective (RPO) of virtually zero.
- Customizable management scripts allow specific integration with customer environment and applications.

¹ 100 km is the current tested limit although recent technology may allow for greater distances.

logical view

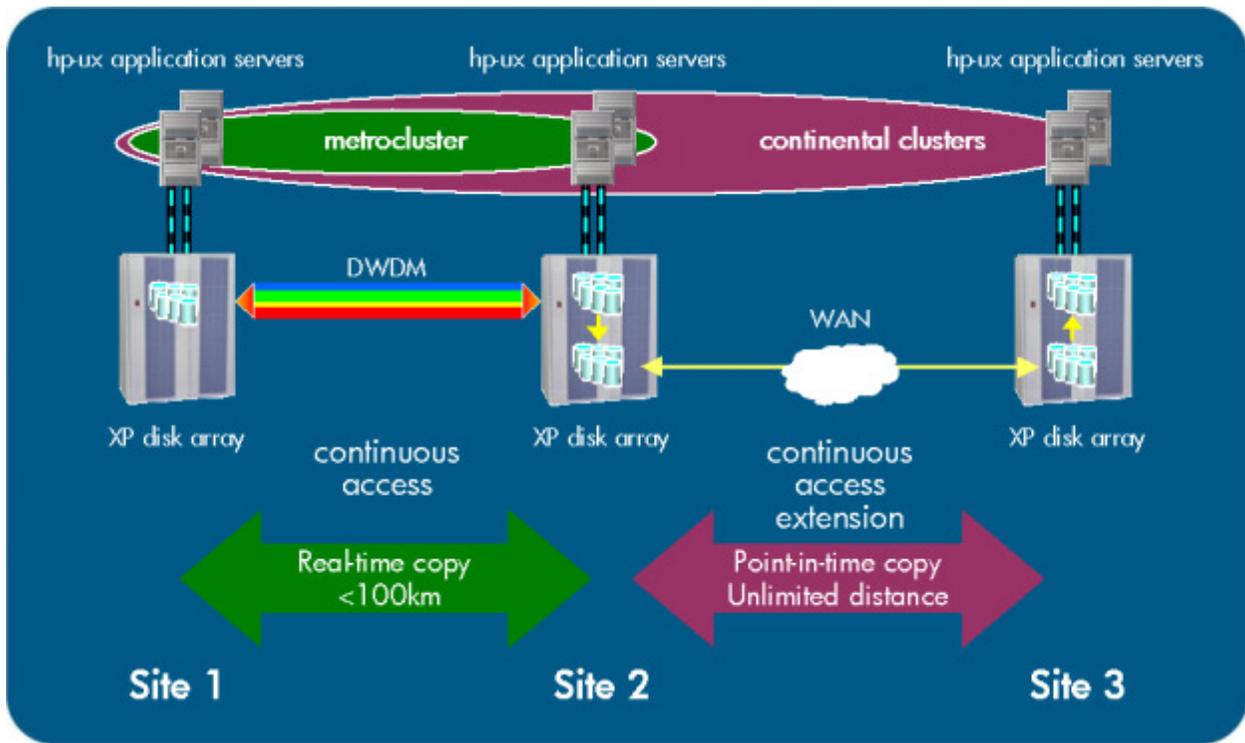


figure 1. logical view of the MSDT solution model configuration

Figure 1 provides a high-level logical view of the model configuration for an MSDT solution.

- Both Site 1 and Site 2 are fully operational sites with application hosts available.
- The host at Site 2 can be used to run development or other applications, or can be used as a client for the host application running at Site 1. In the event of a system failure at Site 1, the application that normally runs at Site 1 can fail over to Site 2.
- Remote point-in-time copying can be automatically performed at regular, customer configurable intervals from Site 2 to Site 3. All three sites have at least one host capable of running applications.

physical view

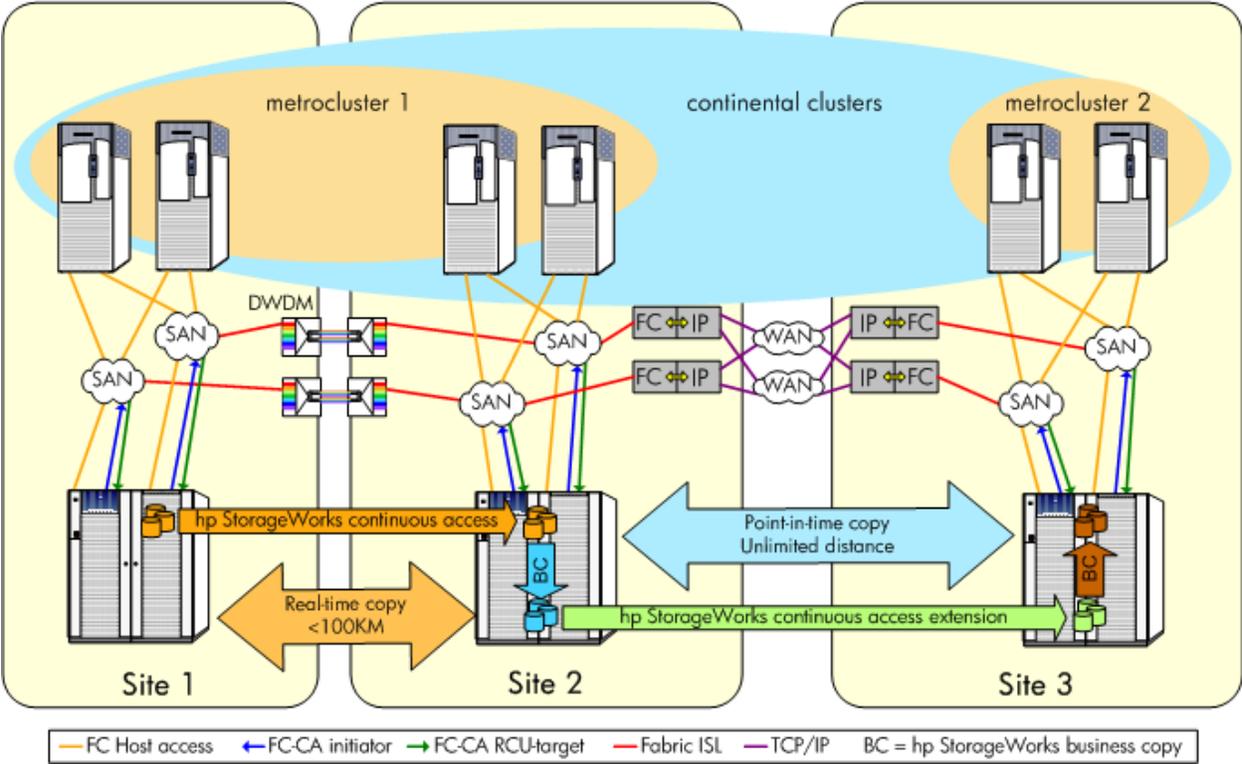


figure 2. physical view of the MSDT solution model configuration

minimum requirements

The following table lists the minimum number, size, and/or level of hardware and software components that will work with the HP MSDT Solution:

minimum required solution components

site 1	site 2	site 3
HP-UX RP series or Superdome server running HP-UX 11.11 or higher	HP-UX RP series or Superdome server running HP-UX 11.11 or higher	HP-UX RP series or Superdome server running HP-UX 11.11 or higher
HP StorageWorks Disk Array (xp48, xp128, or xp512)	HP StorageWorks Disk Array (xp48, xp128, or xp512)	HP StorageWorks Disk Array (xp48, xp128, or xp512)
HP StorageWorks SAN switch (one for each SAN node)*	HP StorageWorks SAN switch (one for each SAN node)*	HP StorageWorks SAN switch (one for each SAN node)*
Dense wave division multiplex (DWDM) repeater*	DWDM repeater*	—
—	FC-IP converter such as INRANGE 9801 Storage Networking System SNS or CNT UltraNet Edge Storage Router (one for each WAN connection)*	FC-IP converter such as INRANGE 9801 Storage Networking System SNS or CNT UltraNet Edge Storage Router (one for each WAN connection)*
HP StorageWorks Continuous Access (CA)	HP StorageWorks Continuous Access and Continuous Access Extension (CA Ext) and appropriate cache	HP StorageWorks Continuous Access and Continuous Access Extension and appropriate cache
—	HP StorageWorks Business Copy (BC)	HP StorageWorks Business Copy
HP StorageWorks MetroCluster A.04.20. (Only one copy needed; resides on all nodes.)		
HP StorageWorks Continental Clusters A.04.00. (Only one copy needed; resides on all nodes.)		
XP Multi-Site DT Management Tools (provided with solution)	XP Multi-Site DT Management Tools (provided with solution)	XP Multi-Site DT Management Tools (provided with solution)
HP ServiceGuard (SG) 11.14	HP ServiceGuard 11.14	HP ServiceGuard 11.14
HP StorageWorks RAID Manager XP v01.11.00 or later	HP StorageWorks RAID Manager XP v01.11.00 or later	HP StorageWorks RAID Manager XP v01.11.00 or later
HP StorageWorks LUN Configuration Manager XP†	HP StorageWorks LUN Configuration Manager XP†	HP StorageWorks LUN Configuration Manager XP†
HP StorageWorks Secure Manager XP†	HP StorageWorks Secure Manager XP†	HP StorageWorks Secure Manager XP†

* Ideally, there should be two SAN switches at each site, two Fibre Channel links between Site 1 and Site 2, and two WAN links between Site 2 and Site 3. At least one of each is required, but two are recommended for failover redundancy.

† The combination of HP StorageWorks LUN Configuration Manager XP and HP StorageWorks Secure Manager XP is compatible only with the HP StorageWorks Disk Array xp48 and the HP StorageWorks Disk Array xp512. If the customer selects the HP StorageWorks Disk Array xp128 or the HP StorageWorks Disk Array xp1024, then the customer must use the HP StorageWorks LUN Configuration and Security Manager XP, which is one package.

3 Design Process

The first step in the design process is to qualify a customer as a candidate for an MSDT Solution. For instance, the customer must have three separate sites available. The distance between Site 1 and Site 2 must not exceed 100 km. Site 1 and Site 2 must be able to be linked by a direct Fibre Channel (FC) connection². Site 3 must be far enough away from Site 1 and Site 2 to assure that it is out of the region of a potential disaster. If these qualifications are not and cannot be met, this solution is not appropriate for the customer. Before beginning the design of a MSDT Solution, consider a number of factors. These include:

- Customer requirements
- Existing customer components
- MIS/system administration personnel requirements

assumptions

- The customer has identified possible locations for the solution sites and is familiar with the existing layout and equipment (if any) at each location.
- The customer has access to a direct FC link between Site 1 and Site 2, which does not exceed 100 km³.
- The customer has access to a Wide Area Network (WAN) link between Site 2 and Site 3.

deliverables

The goal of the design process is to produce the following deliverables:

design deliverables

physical diagrams	Basic physical diagrams of the customer-specific solution. Physical diagrams show: <ul style="list-style-type: none">• The general interconnection of the solution design scheme• The various types of hardware used for this solution, including cable routes, switches, and converters• Redundant local clusters and XP enclosures supporting CA and BC• High-level software layers such as MetroCluster, Continental Clusters, and CA Figure 2 on page 9 is an example of such a physical diagram.
bills of materials	Lists of components to be used in the solution, including suitable existing components and new components that the customer needs to purchase. Produce a separate bill of materials for each site, so that installers can easily identify which components belong to which site.

² Where “direct” means a dedicated, low latency adequate bandwidth link, however that is achieved. Any use of protocol converters for the site 1 to 2 link falls outside the model and must be factory approved prior to the sale.

³ 100 km is the current tested limit although recent technology may allow for greater distances. This recommendation is for performance and is not a technical limitation of the XP array.

design flowchart

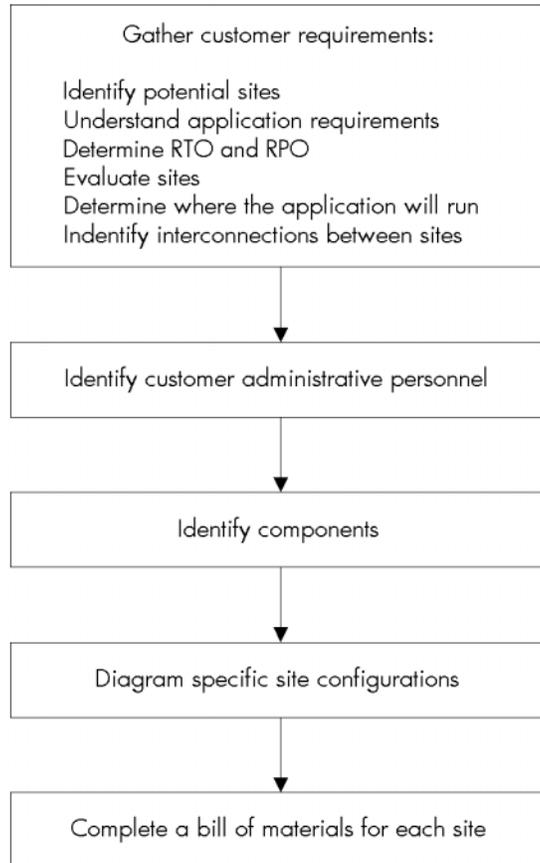


figure 3. design process steps

4 Design Tasks

The first step of solution design is assessing the customer's requirements: business needs, price range, existing infrastructure, and what actions the customer will need to perform in order to prepare for the installation of the solution.

1: gather customer requirements

Use the customer requirements checklist on the next page and the guidelines that follow to determine general customer requirements for the solution.

customer requirements checklist

	question	answer
1	Where is Site 1, and what are its characteristics?	
2	Where is Site 2, and what are its characteristics?	
3	Where is Site 3, and what are its characteristics?	
4	What are the characteristics of the link between Site 1 and Site 2 (including length, number of links, connection type, etc.)?	
5	What are the characteristics of the link between Site 2 and Site 3 (including length, number of link, link type, latency, packet loss, etc.)?	
6	What is the customer's desired Site 1 to Site 2 RTO?	
7	What is the customer's desired Site 1 to Site 2 RPO?	
8	What is the customer's desired Site 2 to Site 3 RTO?	
9	What is the customer's desired Site 2 to Site 3 RPO?	
10	What are the customer's major application requirements?	
11	What are the customer's current processing requirements? When will the point-in-time-copy be created?	
12	What is the customer's desired failover/failback configuration (e.g., redundant servers at local sites)?	
13	What are the customer's current storage requirements?	
14	What will the customer's storage requirements be in three years?	

guidelines for completing the customer requirements checklist

1. The answer is a physical address and description. Site 1 is the primary application site where the application will be actively running under normal conditions, and where most of the users will access the system most of the time. Select the most secure available site as Site 1. Some less secure locations include:

- On or near an earthquake fault line
- A high-rise building in a city center
- Close to an airport or in the path of regular low-flying aircraft
- An area known to have tornados, floods, or bison stampedes
- A building without adequate physical & perimeter security
- A building powered by a single source of electricity

All sites must have adequate space, properly grounded electrical sources, sufficient electrical outlets, and sufficient ventilation. For details about storage site requirements, see the HP-UX specification documents.

2. The answer is a physical address and description. Site 2 is the target for the synchronous replication copy, and will act as the immediate failover site for the application running on Site 1. Ideally, Site 2 is located within 10 km of Site 1.
3. The answer is a physical address and description. Site 3 should be located outside of the potential disaster region.
4. The answer is the length of the FC link, the number of links, and the connection method. The length of the link is most likely greater than the direct distance between the two sites. Links between sites must cross geographical obstacles and do not run in a straight line. The answer helps determine RPO and copy time characteristics. Ideally, Sites 1 and 2 are less than 10 km (6 miles) apart. Up to 100 km is supported, but this will cause some degradation in performance. Redundant physical connections, using different paths, are strongly recommended.

HP recommends using DWDM equipment to provide the best utilization of FC connections between the sites. DWDM units from various vendors have certain built-in redundancy options. The vendor agreement details the expected characteristics of the link, including latency and packet loss. Most DWDM units can transmit on two independent FC links and switch between these links without impacting the protocol transmitted. If the customer decides to use only one DWDM unit on each site, HP recommends that the customer extend two inter-switch connections from two different switches through this connection. This improves performance and provides redundancy for the switches.

Alternatively, the customer can use direct switch connection between the sites, such as long wave interfaces on the switches, which can span a distance of up to 10 km between sites. Using ultra long wave interfaces on some switch units allows distances up to 80 km between sites. Direct switch connections require a dedicated FC connection for each interconnection. The FC connection can only be used for fiber protocol and is limited by the switch performance. HP recommends using at least two interconnections from two different switches (four switches in total).

5. The answer is the distance of the IP link, the number of links, and their characteristics, including the latency and packet loss. Site 3 should be located well outside of the potential disaster region. Distances of several hundred to several thousand kilometers are considered ideal for this solution.
6. The answer is measured in minutes. If desired RTO cannot be met, the customer must either compromise or determine another solution. The RTO may be influenced by the distance between Site 1 and Site 2 as well as the size of the database at Site 1. If the two sites are located at the maximum supported distance (100 km), then it will be necessary to adapt the heartbeat interval to allow for the time delay between the sites.
7. The answer is measured in data transactions. The RPO establishes the amount of IO transactions that might be at risk in the worst-case scenario. All Site 1 mirrored data should be recoverable at Site 2 at any time, with the exception of data that is in transit at the time of a Site 1 failure.

8. The answer is measured in hours. This RTO is influenced by the distance between the sites, the size of database being recovered, and administrator response time. The desired RTO influences customer decisions on bandwidth of the long distance link and the time between cycling point-in-time data.
9. The answer is measured in data transactions. The performance of the data link between Site 2 and Site 3 determines the time intervals between data cycles and, therefore, determines the point to which applications must be rolled back after a wide-area disaster. The RPO is determined by the time required to cycle new data from the production systems, the amount of data that is expected to change, and the bandwidth available for transmitting data. In some case the RPO to site 3 will be 0 if a communication link to Site 2 remains available and the last data-cycle process can be completed. If the link fails, then the RPO is determined by the completion of the last cycle process. If the cycle process has completed, then the data will be only one cycle time old. If the cycle was still in progress when failure occurred, then the customer must revert to the BC copy on site 3 and the data will be two cycle times old. The long distance link requires an FC-IP converter. A number of converter types and options exist for this interconnection.
10. The answer is a list of the customer's critical application requirements, including server and storage requirements. Solution Architects and C&I Engineers use this information to determine the solution details. Not all applications will work with the MSDT solution. The application must be able to recover automatically from a system failure and be able to rollback any uncommitted data in the event of a restart after a failure. If the application cannot perform these actions automatically, then automated failover might not be possible. If the application cannot recover from a system failure or cannot restart from a point-in-time copy, then the MSDT Solution might not be appropriate for the customer.

When determining which applications are critical, examine up-stream and down-stream applications and the user access path to the application(s).

11. The answer depends on the number of CPUs, and the best time of the day to create the point-in-time copy. HP-UX servers are available with multiple CPUs. An RP-series server can have from 1 to 16 CPUs, while the high-end HP Superdome servers are available with 16, 32, or 64 CPUs. The customer must decide if additional CPUs are required based on the current server performance characteristics.

Determine the best time of the day for creating point-in-time copies. Examine the performance and operation characteristics of the application, as well as the amount of data expected to be updated per day, per hour, and per work period. Look at events that generate large amounts of information at once; for example, creating large archive files, running batch processes, or loading large databases. In some applications there is a logical point during the day (for example, at the end of the working day) to make the point-in-time copy.

12. The answer is a description of the customer's strategy for host types and utilizing local or remote failover. Although each site requires only one host, HP recommends two hosts each at Sites 1 and 2. This allows the primary server to automatically fail over to the secondary server at the same site, without the need to fail over to a second site. The physical device usage stays exactly the same and there is no effect on the cycling of data between sites. If the customer prefers that the application remain at Site 1 at all times, then local failover is the best strategy. You should also discuss automated vs. manual failover. In the MetroCluster environment (Site 1 to 2), HP recommends automated failover and manual failback. Note that it is not always necessary to fail back after a failover. It is possible to recover the primary node and re-enable it for automated failover, leaving the application to run and automatically failback if there is an error on the current node. The failback process is normally a controlled process that can be scheduled and performed during a planned downtime.

Another decision is where the point-in-time copy originates, preferably at Site 2. With the point-in-time copy originating from Site 2 and the application primarily running at Site 1, a failure at Site 1 causes the application to move to Site 2 without affecting the point-in-time copy. It is important to ensure that Site 2 is resilient enough to withstand local failures. A failure at Site 2 causes the point-in-time copy to stop functioning. If the customer selects Site 1 for the point-in-time copy, then a failure at Site 1 will stop all point-in-time copies. In this case, the customer must decide whether to continue running the application at Site 2 without data loss but with no connection to Site 3, or run the application at Site 3 from the point-in-time copy at Site 3.

The customer must also decide how many hosts are application hosts, device control hosts, and management hosts. Application hosts run the application on either primary or secondary servers. These hosts are part of the cluster and have all the network and device resources. Application hosts have to be connected to the individual arrays and must access only one copy of the data. Device control hosts are connected to one or more of the arrays in the solution and have access to command devices on those arrays. Management hosts are not able to run the application, and are not connected to the array and, therefore, not able to control the device groups. These hosts can be used to manage the cycle process of the device groups or maintain a remote log of events.

Discuss any quorum disk/server facilities that may be required in the cluster. If any host fails, then more than 50% of that cluster must remain active.

13. The answer is measured in terabytes (TB). Is the current storage at each site getting full? Supported XP disk arrays are available with capacities of 48, 128, 512, and 1024 physical drives. They provide maximum unformatted storage capacities of up to 8.7, 18, 93, and 149 TB respectively. Remember that the customer's total storage need is roughly five times the production site storage.
14. The answer is measured in TB. Consider the customer's growth requirements and the possibility that additional storage is needed now or will be needed later.

2: identify customer administrative personnel

A system administrator performs routine maintenance, system upgrades, and, in the event of a disaster, oversees disaster recovery operations. Use the administrative personnel checklist to determine if the necessary system administrators are available and qualified. Each customer data site should have at least one backup administrator who can handle disaster recovery tasks, in the event that the primary administrator is unavailable. For instance, the primary administrator for site 1 may be the backup for site 2, and visa-versa. The customer should select one system from which to perform all system maintenance, preferably at site 3. Selecting a primary management system allows a single point of management and the creation a central log of daily events for the MSDT topology.

Once this checklist is filled out, the customer should keep a copy of it at each site to contact system administrators in an emergency.

administrative personnel requirements checklist

required administrator(s)		currently available administrator(s)
Site 1	Primary administrator	Name: Phone: Email: Familiar with necessary HP products? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with solution? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with disaster recovery process? <input type="checkbox"/> Yes <input type="checkbox"/> No Primary solution management system at this site? <input type="checkbox"/> Yes <input type="checkbox"/> No If yes, which host?
	Backup administrator	Name: Phone: Email: Familiar with necessary HP products? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with solution? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with disaster recovery process? <input type="checkbox"/> Yes <input type="checkbox"/> No
Site 2	Primary administrator	Name: Phone: Email: Familiar with necessary HP products? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with solution? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with disaster recovery process? <input type="checkbox"/> Yes <input type="checkbox"/> No Primary solution management system at this site? <input type="checkbox"/> Yes <input type="checkbox"/> No If yes, which host?
	Backup administrator	Name: Phone: Email: Familiar with necessary HP products? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with solution? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with disaster recovery process? <input type="checkbox"/> Yes <input type="checkbox"/> No
Site 3	Primary administrator	Name: Phone: Email: Familiar with necessary HP products? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with solution? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with disaster recovery process? <input type="checkbox"/> Yes <input type="checkbox"/> No Primary solution management system at this site? <input type="checkbox"/> Yes <input type="checkbox"/> No If yes, which host?
	Backup administrator	Name: Phone: Email: Familiar with necessary HP products? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with solution? <input type="checkbox"/> Yes <input type="checkbox"/> No Familiar with disaster recovery process? <input type="checkbox"/> Yes <input type="checkbox"/> No

3: identify components

There is a good chance that many solution components are already in place at one or more of the customer's selected sites. Use the component checklists and the guidelines that follow them to determine what components, suitable for use in the solution, are already present at the sites.

note Not all existing components may be suitable for use in the solution. In some cases, the component might not have the capacity available to be useful in this solution (for example an XP array may be nearly full, or a server may be underpowered). This checklist and the resulting bills of materials are only as accurate as the information agreed upon by you and the customer.

component checklist for site 1

	component	quantity required	quantity and model/version # of existing, suitable components	quantity and model/version # of needed components
1	RP-series or Superdome servers running HP-UX 11.11 or later			
2	StorageWorks XP arrays			
3	StorageWorks SAN Switches (2/8 EL or 2/16 EL)			
4	DWDM equipment			
5	ServiceGuard (11.14. or later)			
6	MetroCluster (A.04.20. or later) with XP-CA Toolkit			
7	Continental Clusters (A.04.00 or later)			
8	Continuous Access			
9	RAID Manager XP version 01.11.00 or later			
10	LUN Configuration and Security Manager XP (if using xp128 or xp1024 arrays)			
	LUN Configuration Manager XP (if using xp48 or xp512 arrays)			
	LUN Secure Manager XP (if using xp48 or xp512 arrays)			

guidelines for completing the component checklist for site 1

1. This is the primary application server. An additional host can be used for local redundancy and failover protection. The specific model is chosen for the number of CPUs. Greater number of CPUs gives more processing speed and power.
2. Storage capacity at BC sites must be double the capacity at the production site. The xp256 array is not supported.
3. One switch is required for each SAN node at each site. Ideally, there should be two SAN switches at each site, two FC links between Site 1 and Site 2, and two WAN links between Site 2 and Site 3. At least one of each is required, but two are recommended for failover redundancy.
4. One for each FC link. DWDM equipment is available from several vendors with vendor-specific options.
5. Note if the customer must purchase the full product or only an upgrade.
6. Note if the customer must purchase the full product or only an upgrade. Only one copy is required for the solution. This copy resides on all nodes.
7. Note if the customer must purchase the full product or only an upgrade. Only one copy is required for the solution. This copy resides on all nodes.
8. Note if the customer must purchase the full product or only an upgrade.
9. Note if the customer needs an upgrade.
10. Note if the customer must purchase the full product or only an upgrade.

component checklist for site 2

	component	quantity required	quantity and model/version # of existing, suitable components	quantity and model/version # of needed components
1	RP-series or Superdome servers running HP-UX 11.11 or later			
2	StorageWorks XP arrays			
3	StorageWorks SAN Switches (2/8 EL or 2/16 EL)			
4	DWDM equipment			
5	FC-IP converters (e.g., CNT UltraNet Edge Storage Router or INRANGE 9801 SNS)			
6	ServiceGuard (11.14. or later)			
7	Continuous Access			
8	Continuous Access Extension			
9	Business Copy			
10	RAID Manager XP version 01.11.00 or later			
11	LUN Configuration and Security Manager XP (if using xp128 or xp1024 arrays)			
	LUN Configuration Manager XP (if using xp48 or xp512 arrays)			
	LUN Secure Manager XP (if using xp48 or xp512 arrays)			

guidelines for completing the component checklist for site 2

1. An additional host can be used for local redundancy and failover protection. Applications may run on this server, but they cannot be the same applications that run at Site 1.
2. Storage capacity at BC sites must be double the capacity at the production site. The xp256 array is not supported.
3. One for each SAN node at each site. Ideally, there should be two SAN switches at each site, two FC links between Site 1 and Site 2, and two WAN links between Site 2 and Site 3. At least one of each is required, but two are recommended for failover redundancy. Select switches that are supported by the customer's FC-IP converters.
4. One for each FC link. Equipment is available from several vendors with vendor-specific options.
5. One for each WAN link. These converters are available from several vendors.
6. Note if the customer must purchase the full product or only an upgrade.
7. Note if the customer must purchase the full product or only an upgrade.
8. Note if the customer must purchase the full product or only an upgrade.
9. Note if the customer must purchase the full product or only an upgrade.
10. Note if the customer needs an upgrade.
11. Note if the customer must purchase the full product or only an upgrade.

component checklist for site 3

	component	quantity required	quantity and model/version # of existing, suitable components	quantity and model/version # of needed components
1	RP-series or Superdome servers running HP-UX 11.11 or later			
2	StorageWorks XP arrays			
3	StorageWorks SAN Switches (2/8 EL or 2/16 EL)			
4	FC-IP converters (e.g., CNT UltraNet Edge Storage Router or INRANGE 9801 SNS)			
5	ServiceGuard (11.14. or later)			
6	Continuous Access			
7	Continuous Access Extension			
8	Business Copy			
9	RAID Manager XP version 01.11.00 or later			
10	LUN Configuration and Security Manager XP (if using xp128 or xp1024 arrays)			
	LUN Configuration Manager XP (if using xp48 or xp512 arrays)			
	LUN Secure Manager XP (if using xp48 or xp512 arrays)			

guidelines for completing the component checklist for site 3

1. An additional host can be used for local redundancy and failover protection. Applications may run on this server, but they cannot be the same applications that run at Site 1.
2. Storage capacity at BC sites must be double the capacity at the production site. The xp256 array is not supported.
3. One for each SAN node at each site. Ideally, there should be two SAN switches at each site, two FC links between Site 1 and Site 2, and two WAN links between Site 2 and Site 3. At least one of each is required, but two are recommended for failover redundancy. Select switches that are supported by the customer's FC-IP converters.
4. One for each WAN link. These converters are available from several vendors.
5. Note if the customer must purchase the full product or only an upgrade.
6. Note if the customer must purchase the full product or only an upgrade.
7. Note if the customer must purchase the full product or only an upgrade.
8. Note if the customer must purchase the full product or only an upgrade.
9. Note if the customer needs an upgrade.
10. Note if the customer must purchase the full product or only an upgrade.

4: diagram site configurations

In the diagram template on the next page, fill in customer information as appropriate:

- The number and type (application, device control, or management) of hosts at each site.
- The number of SAN nodes and switches at each site.
- The number and types of links between the sites.
- The number and type of converters at each site.
- The number and type of arrays at each site.
- Where BC copies will be located. In the model configuration, these are at sites 2 and 3.

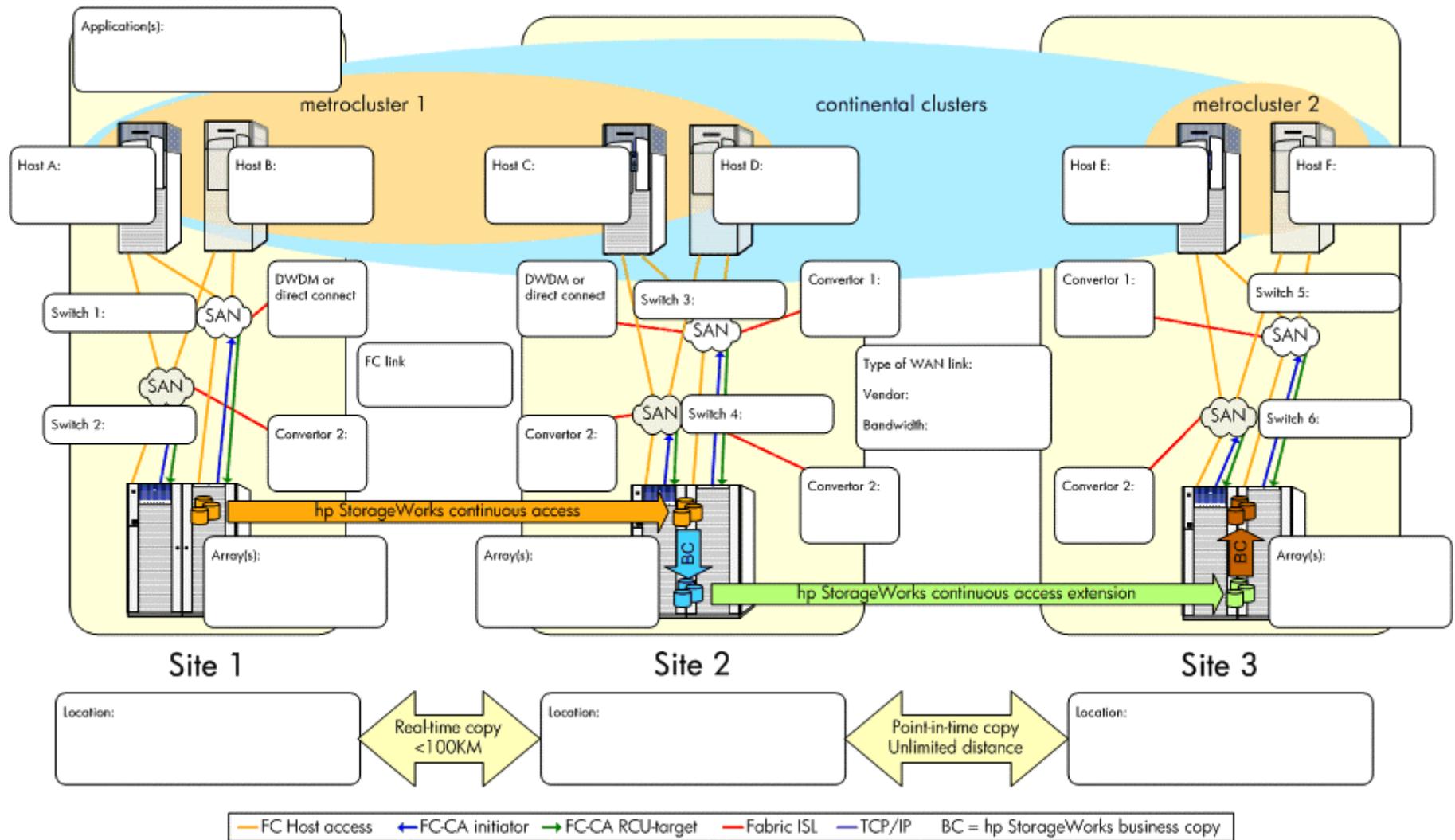


figure 4. physical view of customer's MSDT solution

5: complete bills of materials

Review the component checklists to produce specific bills of materials for each site.

bill of materials for site 1

component to purchase	quantity	part number	comments

existing component	quantity	comments

bill of materials for site 2

component to purchase	quantity	part number	comments

existing component	quantity	comments

bill of materials for site 3

component to purchase	quantity	part number	comments

existing component	quantity	comments

6: continue solution design and implementation

Once the high-level design is complete, you are ready to continue with the detailed design and implementation described in the *Multi-Site Disaster Tolerant Solution Implementation Blueprint: Installation and Configuration Guide*.