Xsan Management Guide

For Mac

v1.2

Contents

Introduction

This guide provides basic command-line instructions on how to configure and manage an Xsan storage area network (SAN). Before you begin, familiarize yourself with two command-line tools, `cvlabel` and `xsanctl`. You can do this by opening the Terminal app and typing `man cvlabel`, then pressing the Return key. This displays the manual page for the `cvlabel` command. You can do the same with the `xsanctl` command.

IMPORTANT: You should feel comfortable with using the Terminal app and have a basic understanding of how to navigate directories and use the `sudo` command. Not setting up the SAN properly or making changes incorrectly could cause failures or loss of data.

About Xsan SANs

A storage area network (SAN) is a way of connecting computers and storage devices so computers have fast, shared access to files while making it easy for administrators to expand storage capacity.

An Xsan SAN consists of:

- Shared data volumes
- RAID systems that provide storage space that's protected from disk failure
- At least one computer acting as a metadata controller that combines RAID arrays and presents their storage to clients as volumes that behave like local disks
- Client computers that access storage in accordance with established permissions and quotas
- Underlying fibre channel, Distributed LAN Client, and Ethernet networks

Shared SAN volumes
A user or app on a client computer accesses shared SAN storage as if it were a local volume. Xsan volumes are logical disks made up of pools of RAID arrays.

Metadata controllers
When you set up an Xsan SAN, you assign at least one computer to act as the metadata controller. The controller manages volume metadata, maintains a file system journal, and controls concurrent access to files. Metadata includes such information as where files are stored and what portions of available storage are allocated to new files.

To guarantee volume availability, a SAN should include more than one metadata controller. In this way, if the active controller fails, a standby controller takes over.

Clients
The computers that users or apps use to access SAN volumes are called *clients*. Clients exchange metadata with controllers over an Ethernet network, but use fibre channel or Distributed LAN Client (DLC) to send and retrieve file data to and from the RAID systems that provide storage for the volumes.

Fibre channel network connection
Xsan moves data between clients and SAN volumes over high-speed fibre channel connections. Controllers also use a fibre channel connection to move metadata to and from the volume.

Xsan can take advantage of multiple fibre channel connections between clients and storage. Xsan can alternate between connections for each read and write, or it can assign each RAID array in a volume to a connection when the volume is mounted.

Ethernet network connection
All versions of Xsan exchange file system metadata over an Ethernet network. (Controllers use fibre channels to read and write metadata on a volume.) To prevent internet or intranet traffic from interfering with metadata communications, you can optionally set up separate public (internet) and private (metadata) Ethernet networks.

Distributed LAN Client (DLC) network connection
Xsan 4.1 or later on OS X 10.11 or later supports StorNext's DLC network connection, which allows client connections to your SAN over Ethernet instead of a fibre connection. Connections for such tasks as ingesting and editing can take place over fibre, while DLC connections can be used for other tasks.

You can have a public network (internet), a private network (metadata), and a DLC network all as independent networks, with optimum performance. You could instead have all three over a single wired Gigabit Ethernet connection, but throughput won't be optimum.

Note: macOS only supports being a client using DLC. Being a metadata controller isn't supported.

Xsan security
There are several ways you can control access to a SAN volume:

- Unmount a volume on client computers that shouldn't have access to it (using the `xsanctl` command-line tool). However, users who have administrator accounts on client computers can browse and mount SAN volumes.
- Specify owner, group, and general access permissions in the Finder.
- Control user access to files and folders on a volume, by setting up access control lists (ACLs). This works only if access controls lists are enabled for a volume.

How Xsan storage is organized

Although an Xsan volume mounted on a client computer looks like a single disk, it consists of multiple physical disks combined on several levels using RAID techniques. The following paragraphs describe these elements and how you combine them to create shared Xsan volumes.

LUNs
The smallest storage element you work with in Xsan is called a SCSI *logical unit number*, or *LUN*. A LUN represents a group of drives combined into a RAID array.

You create a LUN when you create a RAID array on a RAID storage device. The RAID system combines physical drives into an array based on the RAID scheme you choose. Each array appears on the fibre channel network as a LUN. If the standard RAID arrays on your RAID systems aren't right for your application, you can use the RAID system management software to re-create arrays based on other RAID schemes or different numbers of drive modules.

Your RAID LUNs are labeled and initialized for use with the Xsan file system when you use `cvlabel` to label the LUNs. The `addVolume` command uses those labels to create the Xsan volume. For more information, launch the Terminal app and enter `man cvlabel`, then press Return.

Storage pools
LUNs are combined to form storage pools. A storage pool in a small volume might consist of a single RAID array, but a larger volume might consist of several storage pools each of which includes several arrays.

Xsan distributes file data in parallel across the LUNs in a storage pool using a RAID 0 (striping) scheme. By distributing available storage over several LUNs in a storage pool, so you can improve a client's access speed. You can set up storage pools that have different performance or recoverability characteristics based on the RAID level of their LUNs. Users can then select where to store files based on their need for speed or safety. When you create or modify a storage pool, the number of assigned LUNs needs to be a power of 2.

You can add LUNs to storage pools and storage pools to Xsan volumes at any time. You use `xsanctl editVolume` to add available LUNs to storage pools. For more information, launch the Terminal app and enter `man xsanctl`, press Return, then locate the Storage Pool settings section.

Volumes
Storage pools are combined to create the Xsan volumes that users see. From the user's perspective, the volume looks and behaves like a large local volume, except that:

- The size of the volume can grow as you add underlying arrays or storage pools
- Multiple users on the SAN can access files on the volume at the same time

How Xsan uses available storage

Xsan stores user files and file system data on SAN volumes, and stripes data across the LUNs in a volume for better performance.

Metadata and journal data

Xsan records information about the files in an Xsan volume using metadata files and a file system journal. File system metadata includes information such as which specific parts of which disks are used to store a file and whether the file is being accessed. The journal data includes a record of file system transactions that help ensure the integrity of files in the event of a failure.

These files are managed by the Xsan metadata controller but are stored on LUNs, not on the controller itself. Metadata should be stored on the first storage pool you add to a volume. Journal data can also be stored on the same storage pool as metadata, or you can use a separate storage pool for journal data. You must have journal data on only one storage pool.

Striping at a higher level

When a RAID system writes a file using a RAID 0 (striping) scheme, it breaks the file into segments and spreads them across disk drives in the RAID array. This improves performance by writing parts of the file in parallel (instead of one part at a time) to disks in the array.

Xsan applies this same technique in the storage hierarchy. Within each storage pool in a volume, Xsan stripes file data across the LUNs that make up the storage pool. Performance is improved because data is written in parallel.

You can tune SAN performance by adjusting the type of data written to each LUN in a storage pool (mixing or separating metadata, journal data, and user data).

Xsan capacities

The following table lists limits and capacities for Xsan volumes.

Parameter	Maximum
Number of volumes on a SAN	16
Number of storage pools in a volume	512
Number of LUNs in a storage pool	32
Number of LUNs in a volume	512
Number of files in a volume	4,294,967,296
LUN size	Limited by the size of the RAID array
Volume size	Limited by the number and size of LUNs
File size	Approximately 263 bytes
Volume name length	70 characters (A–Z, a–z, 0–9, and _)
File or folder name length	251 ASCII characters
Storage pool name length	255 ASCII characters
LUN name (label or disk name)	242 ASCII characters

Xsan hardware requirements

To join a specific version of Xsan, computers must meet the following minimum requirements.

Xsan version requirements

- If you're using macOS 11 or later, you have Xsan 7.
- If you're using macOS Server 5.4 or later on macOS 10.13 or later, you have Xsan 5.
- If you're using macOS Server 5.2 or later on macOS 10.12, you have Xsan 5.
- If you're using macOS Server 5.2 on OS X 10.11.6, you have Xsan 4.1.

Memory requirements

- Client computers must have at least 4 GB of RAM.
- Computers used as metadata controllers must have at least 8 GB of RAM and one SAN volume, plus 2 GB of RAM for each additional SAN volume hosted by the controller.
  For example, a controller should have 8 GB of RAM to host one volume, or 10 GB for two volumes.

Supported operating systems

- Computers with macOS 11 can be used as Xsan 7 metadata controllers and clients.
- Computers with macOS 10.12 through 10.15 can be used as Xsan 5 metadata controllers and clients.
- To join an Xsan SAN, AIX, IRIX, Linux, Solaris, and Windows clients must be running Quantum's StorNext File System.

Supported storage devices

- Use only Apple-qualified RAID systems or ALUA-compliant RAID systems for storage devices.

IMPORTANT: Be sure to install the latest firmware update on your RAID systems before you use them with Xsan.

Xsan network requirements

Fibre channel connections

Unlike file system metadata, which is exchanged over Ethernet, file content in an Xsan SAN is transferred over fibre channel connections. The computers, storage devices, and switches are connected with fibre channel cables to form a *fibre channel fabric*. To set up the connections, you need a supported fibre channel adapter for each client and controller computer, a supported fibre channel switch, and fibre channel cables connecting computers and storage devices to the switches to form a fibre channel fabric.

- *Fibre channel cards or adapters:* Install a fibre channel PCI card or attach a fibre channel adapter to a compatible port of each Mac that connects to the SAN.

Note: If you're using a Mac with Apple silicon, you may need to allow the installation of kernel extensions for your fibre card or adapter. For more information, see Kernel extensions in macOS in the Deployment Reference for Mac.

- *Fibre channel switches:* Use fibre channel switches from Brocade, Cisco, and QLogic; these have been tested with Xsan.
- *Fabric configuration:* You must connect the computers, storage devices, and switches in your fibre channel network to form a fibre channel fabric. In a fabric, fibre channel cables connect node ports (F or N_Port). For more information about setting up your fabric, see the documentation that came with your fibre channel switches.

DLC connections

For Distributed LAN Client (DLC) connections, computers on the SAN must use macOS 10.13 or later connected to an Ethernet network. DLC devices for each computer can be purchased from Quantum.

Ethernet TCP/IP network connections

Computers on the SAN must be connected to an Ethernet network. Xsan controllers and clients use this network instead of the fibre channel network to exchange file system metadata.

- Using *IP addresses:* The client and metadata controller computers need static (fixed) IP addresses for Ethernet network connections. For the public intranet and internet connection, you can enter each computer's static IP address, subnet mask, router address, and DNS server address manually or configure a DHCP server to provide this information.
- *Using DHCP:* If you want the DHCP server to provide IP addresses, it must always assign the same static IP address to each SAN computer. Don't use DHCP to assign dynamic IP addresses to SAN devices.
- *Private addressing:* For the SAN metadata network, the SAN computers should have static private (nonroutable) IP addresses (unless you can't set up a separate, private Ethernet network for SAN metadata).

Directory services

To use Xsan, you must have an Open Directory infrastructure on the metadata controllers. The first metadata controller activated will be made an Open Directory master, and all additional controllers must be Open Directory replicas. If the SAN had Open Directory services active before the SAN was created, the Open Directory Master (Xsan 2 or 3 Primary MDC for SANs that managed users and groups) must be upgraded and activated first using Open Directory procedures.

The directory is also used to manage user and group privileges to control access to files and folders on the SAN. A central directory service lets you manage SAN users and groups from one computer instead of having to visit and painstakingly configure each SAN client and metadata controller.

If you have another type of directory service, such as Active Directory, you configure each Mac in the SAN to connect to it for user and group accounts by using the Users & Groups pane of System Preferences after initial setup. If your SAN doesn't have access to an existing directory service, `xsanctl createSAN` creates an Open Directory master server on your initial (primary) metadata controller.

The Open Directory master provides an LDAP directory, single sign-on user authentication using Kerberos, and password validation using common authentication methods. The replicas improve responsiveness and provide automatic failover of Open Directory services.

Plan your Xsan SAN

It's easy to add storage to an Xsan SAN, but reorganizing a SAN after you set it up isn't simple. So, it's important to plan the layout and organization of your SAN and its storage before you set it up.

An Xsan SAN is made up of:

- Storage devices (RAID systems)
- LUNs (SCSI logical unit numbers, usually RAID arrays)
- Storage pools (groups of LUNs)
- Volumes (groups of storage pools visible to users)
- Clients (computers that use volumes)
- Controllers (computers that manage volume metadata)
- An Ethernet network used to exchange volume metadata

Before you set up a SAN, you must decide how to organize these components. Take the time to create a diagram or a table that organizes available hardware into RAID arrays, volumes, client computers, and metadata controllers in a way that meets SAN users' needs and your needs as the SAN administrator.

Preliminary planning

As you plan, consider the following questions:

- How much storage do you need?
- How do you want to present available storage to users?
- What storage organization makes the most sense for your users' workflow?
- What levels of performance do users require?
- How important is high availability?
- What are your requirements for security?

Your answers to the questions above will help you decide the following:

- What RAID schemes should you use for your RAID arrays?
- How many SAN volumes do you need?
- How should individual volumes be organized?
- Which clients, users, and groups should have access to each volume?
- Which computer will act as the primary metadata controller?
- Do you need more than one standby metadata controller?
- Do you need to adjust a volume's allocation strategy?
- How should you configure your Ethernet network?

How much storage?

Because it's easy to add storage for user data to an Xsan SAN, you only need an adequate starting point. You can add storage later as needed. However, you

can’t add storage for journal data, so try to allocate enough space for journal data right from the start. You can add an entire storage pool for metadata and another storage pool for journal data.

Workflow considerations

How much file sharing is required by your users’ workflow? For example, if different users or groups work on the same files, simultaneously or in sequence, store those files on a single volume to avoid needing to maintain or hand off copies. Xsan uses file locking to manage shared access to a single copy of the files.

Performance considerations

If your SAN supports an app (such as high resolution video capture and playback) that requires the fastest possible sustained data transfers, design your SAN with these performance considerations in mind:

- Set up the LUNs (RAID arrays) using a RAID scheme that offers high performance.
- Use RAID 1 for metadata LUNs and RAID 5 for data LUNs.
- To increase parallelism, spread LUNs across RAID controllers. Xsan then stripes data across the LUNs and benefits from simultaneous transfers through two RAID controllers.
- To increase throughput, connect both ports on client fibre channel cards to the fabric.
- For clients using Xsan 5 or Xsan 7 and DLC, real-time operations should be done over a fibre connection.
- Store file system metadata on a separate storage pool from user data and make sure the metadata LUNs aren’t on the same RAID controller as user data LUNs.
- You can use a separate storage pool for journal data when you create a new volume. This significantly improves performance for some operations, such as creating and deleting files.
- Use a second Ethernet network (including a second Ethernet port for each SAN computer) for SAN metadata.

Availability considerations

If high availability is important for your data, set up multiple metadata controllers to accommodate metadata controller failover. Also, consider setting up dual fibre channel connections between each client, metadata controller, and storage device using redundant fibre channel switches.

Security considerations

If your SAN supports projects that must be secure and isolated from each other, create separate volumes for each project and set appropriate ACLs on the volume to eliminate any possibility of the wrong client or user accessing files stored on a volume.

As the SAN administrator, you control which computers are SAN clients. Users whose computers aren't SAN clients or controllers can't browse for or mount SAN volumes.

However, you can't control which Xsan computers can use a volume. Users whose SAN computers have macOS can mount all SAN volumes themselves.

You can also set up access control lists (ACLs) or assign user and group permissions to folders using standard file access permissions in the Finder.

Prepare LUNs using RAID arrays

Much of the reliability and recoverability of data on a SAN is provided not by Xsan but by the RAID arrays you combine to create storage pools and volumes. Before you set up a SAN, use the RAID system configuration or administration software to prepare LUNs based on specific RAID schemes.

WARNING: Losing a metadata controller without a standby metadata controller can result in the loss of all data on a volume. A standby controller is strongly recommended.

LUNs configured as RAID 0 arrays (striping only) or LUNs based on single drives are difficult or impossible to recover if they fail. Unprotected LUNs such as these should be used only in storage pools that store scratch files or other data that you can afford to lose.

WARNING: If a LUN in the metadata storage pool fails and can't be recovered, all data on the volume is lost. It's strongly recommended that you use only redundant LUNs (LUNs based on RAID schemes other than RAID 0) to create Xsan volumes.

Most RAID systems support all popular RAID levels. Each RAID scheme offers a different balance of performance, data protection, and storage efficiency, as summarized in the following table.

RAID level	Storage efficiency	Read performance	Write performance	Data protection
RAID 0	Highest	Very High	Highest	No
RAID 1	Low	High	Medium	Yes
RAID 3	High to very high	Medium	Medium	Yes
RAID 5	High to very high	High	High	Yes
RAID 0+1	Low	High	High	Yes

Use RAID 1 for metadata LUNs

RAID 1 (mirroring) can give slightly better performance than the default RAID 5 scheme for the small, two-drive metadata LUNs that Xsan uses to store volume information. A single drive is almost always adequate for storing the primary volume metadata (10 GB of metadata space is enough for approximately 10 million files.) The second, mirror drive protects you from metadata loss.

Use RAID 5 for data LUNs
Most RAID systems are optimized for excellent performance and data redundancy using a RAID 5 scheme. (RAID 5 stripes data across available drives and distributes parity data across the drives.) Some RAID systems ship preconfigured as RAID 5 LUNs. RAID 0 (striping with no parity) might give slightly better write performance, but it provides no data recovery protection, so RAID 5 is always a better choice for LUNs used to store user data.

Adjust RAID system performance settings

To get the best performance and reliability from your RAID systems, install the latest firmware.

RAID system performance settings, which affect parameters such as drive caching, RAID controller caching, and read prefetching, can have a significant effect on Xsan volume performance. Follow these guidelines.

Enable drive caching
In addition to the caching performed by the RAID controller, each drive in an array can perform caching at the drive level to improve performance.

Enable RAID controller write caching
Without RAID controller write caching, a request to write data to the associated LUN isn't considered finished until the data is written to the physical disks that make up the array. Only then can the next write request be processed. (This is also known as write-through caching.)

WARNING: If you enable drive caching for a RAID set, make sure the system is connected to an uninterruptible power supply (UPS). Otherwise, you could lose cached data if the power fails.

When RAID controller write caching is enabled, a request to write data is considered finished when the data is in the cache. This is also known as write-back caching. Write requests are processed more quickly because the file system only needs to write to the fast cache memory and doesn't need to wait for the slower disk drives.

Be sure to enable write caching on RAID controllers that support metadata storage pools.

Although some large write requests might benefit from caching, often they don't. By placing a volume's metadata storage pool on a RAID controller separate from the data storage pools, you can enable caching on the RAID controller used for metadata and disable caching on the RAID controller used for data.

When the file system is relying on caching in this way, you must guarantee that data in the cache isn't lost before it's written to disk. Data written to disk is safe if the power fails, but data in a cache isn't. To be sure that a power failure can't cause the loss of cached data, protect your RAID systems with RAID controller backup batteries or a UPS.

Enable read prefetching

Read prefetching is a technique that improves file system read performance when data is being read sequentially, as in the case of audio or video streaming, for example, when read prefetching is enabled, the RAID controller assumes that a read request for a block of data will be followed by requests for adjacent data blocks. To prepare for these requests, the RAID controller reads the requested data and the following data, and stores it in cache memory. Then, if the data is requested, it's retrieved from the fast cache instead of from the slower disk drives.

Decide on the number of volumes

A volume is the largest unit of shared storage on the SAN. If users need shared access to files, store those files on the same volume. This makes it unnecessary for them to pass copies of the files among themselves.

However, if security is critical, remember you can't control client access by unmounting volumes on Xsan clients. Users with Mac computers can mount SAN volumes themselves.

For a typical balance of security and shared access, create one volume and control access with folder access privileges or ACLs.

Decide how to organize a volume

You can help users organize data on a volume or restrict users to specific areas of the volume by creating predefined folders. You can control access to these folders by assigning access permissions.

Choose metadata controllers

You must choose at least one computer to be the SAN primary metadata controller, the computer which is responsible for managing file system metadata.

Note: File system metadata and journal data are stored on the SAN volume, not on the metadata controller itself. See "Store user data with metadata and journal data" below.

If high availability is important for your data, set up multiple metadata controllers to accommodate metadata controller failover.

If performance is critical, don't run other server services on the metadata controller and don't use the controller to reshare a SAN volume using NFS.

Estimate metadata and journal data storage needs

The metadata and journal data that describe a volume are stored not on the volume's metadata controller, but on the volume. Metadata is stored on the first storage pool in the volume. Journal data can be stored on any storage pool in the volume. You must have only one storage pool with journal data.

To estimate the amount of space required for Xsan volume metadata, assume that 10 million files on a volume require approximately 10 GB of metadata on the volume's metadata storage pool.

The journal requires between 64 KB and 512 MB. Xsan configures a fixed size when you create a volume. Due to the small size, you can use a single RAID 1 LUN for the journal storage pool. To maximize the performance benefit of a separate journal storage pool, dedicate entire physical disks to the RAID 1 LUN.

Store user data with metadata and journal data
Although it's possible to create a volume with only one storage pool (containing metadata, journal and user data), it isn't recommended if performance is of concern.

Plan the Ethernet portion of your Xsan network

Ethernet connections are used in several ways in an Xsan SAN:

- Xsan clients and metadata controllers use Ethernet to exchange volume metadata.
- Xsan clients can use Ethernet for access to networks outside the SAN (campus or corporate intranet or the internet).
- Xsan metadata controllers can use Ethernet connections for remote management.
- RAID systems can use Ethernet connections for system management.
- Fibre channel switches can use Ethernet connections for switch management.

Plan the fibre channel portion of your Xsan network

Xsan uses fibre channel connections to:

- Transfer user data between clients and data storage pools.
- Transfer metadata between metadata controllers and metadata storage pools. If you have connections operating below the data rate supported by your equipment, verify fibre channel performance and troubleshoot the fabric.

Because the devices connected to a fibre channel network adjust their speed to match the slowest device on the fabric, be sure that all connections in the fabric are operating at the expected speed.

Check with the manufacturers of the devices you're connecting to your fabric to be sure that the transceivers (GBICs) you're using are qualified for use with their devices.

Check fibre channel connection performance
Use the management software provided with your fibre channel switches to test the performance of your fibre channel fabric.

First-time Xsan SAN setup

Before you begin using Xsan, you need to configure a number of infrastructure settings.

Connect to Ethernet networks

Before you create or configure your SAN, you must connect client computers, controller computers, and storage devices to the SAN's fibre channel and Ethernet networks.

1. Connect each controller computer, RAID storage device, and client to the Ethernet networks.
   Configure any managed Ethernet network switches and VLANs for each Ethernet network used.
2. Connect each controller computer, RAID storage device, and client to a fibre channel switch to create a fibre channel fabric for the SAN.
3. Configure the switch and make the connections so you create a fibre channel fabric according to the manufacturer's instructions.
4. Verify all physical links and cable integrity.

Verify IP addresses of metadata controllers

Each computer that is designated as a metadata controller (primary and all secondary) must have a static IP address and resolve to a fully qualified domain name (FQDN). The FQDN must match the hostname of the computer. Use the Terminal app to match the FQDN to the hostname:

1. `sudo scutil --set HostName <FQDN-name>`

Also, make sure the DNS server on the SAN network is properly maintained and always available. A secondary DNS server is also recommended.

Create an Xsan SAN

To create an Xsan SAN, use the Terminal app to complete the following tasks on the initial computer. This creates an Open Directory master, sets up the initial SAN, and becomes the primary metadata controller. Before you begin, make sure you have the following:

- A local account that has administrator privileges. In this example, the user name is *localadmin* and the password is *72DERjx1*.
  Note: in this example, the account and user are both localadmin. These two accounts can be different.
- The name of the SAN. In this example, the name is *VIDEOSAN*.
- A certificate auth name. In this example the certificate auth name is *videocert*.

- A certificate auth email address. In this example the certificate email address is *administrator@example.com*.
- At least three Mac computers that will be part of the SAN are recommended (a primary metadata controller, a standby metadata controller, and a client computer).

Press Return after each step and, if necessary, enter the administrator password.

1. Make sure all network and fibre connections are functioning properly.
2. `sudo xsanctl createSan 'VIDEOSAN' --account localadmin --pass 72DERjx1 --user localadmin --cert-auth-name videocert --cert-admin-email administrator@example.com`

After you press Return, the `xsanctl` command creates the SAN.

Join a SAN

To join a SAN, use the Terminal app to complete the following tasks on the secondary computer. The task creates an Open Directory replica and joins the existing SAN as a standby metadata controller. Press Return after each step and if necessary, enter the administrator password.

1. `sudo xsanctl joinSan 'VIDEOSAN' --controller-name v1-mdc1-example.com --controller-user localadmin --controller-pass 72DERjx1 --master v1-mdc1-example.com --account localadmin --pass 72DERjx1`

After you press Return, the `xsanctl` command will join the secondary computer to the SAN as an Open Directory replica and a standby metadata controller.

Create an Xsan volume

Before you can use your SAN, you must create at least one volume. Before you create the volume, you need to consider the specifics of the volume.

- For the volume name, use only uppercase letters (A–Z), lowercase letters (a–z), numbers (0–9), and underscores (_). Don’t include spaces or hyphens. The maximum length is 70 characters.

Use the `cvlabel` command to do the following:

- Make sure LUNs are labeled.
- Assign a LUN to metadata and journaling.
- Assign a LUN to store user data.
  For more information, launch the Terminal app and enter `man cvlabel`, then press Return.

In this example:

- The name of the volume is FinalVideoFiles.

- The name of the metadata and journaling LUN is automatically named MetadataAndJournal
- The name of the user data LUN is FirstUDLUN.

This is done on the initial computer, now known as the primary metadata controller. Press Return after each step and if necessary, enter the administrator password.

1. `sudo xsanctl addVolume FinalVideoFiles --defaultFirstPool --addLUN FirstMDLUN --storagePool data --addLUN FirstUDLUN`
2. Verify the volume was created: `sudo xsanctl list`

Perform software updates on all your computers

When a software update to your operating system becomes available, you should update all your SAN computers. Update your primary metadata controller first, followed by all secondary metadata controllers. Next you can update the Xsan clients. When all software updates are complete, run the following command on the master metadata controller. Press Return after each step and if necessary, enter the administrator password.

1. Update the operating system on the primary metadata controller, then restart the Mac if necessary.
2. Enter the following on the primary metadata controller: `sudo xsanctl activateSAN`
3. Update the operating system on the standby metadata controllers, then restart the Mac computers if necessary.
4. Enter the following on each standby metadata controller: `sudo xsanctl joinSan`
5. Update the Mac clients, then restart them if necessary.

Export the Xsan configuration profile

You can create configuration profiles with the Xsan payload that allow client computers to join the SAN. This is done on the any computer that is part of the SAN. Press Return after each step and if necessary, enter the administrator password.

- `sudo xsanctl exportClientProfile`

After you press Return, the Xsan configuration profile is saved in the current working directory. In this example, the file is named VIDEOSAN.mobilconfig. You can securely copy the profile to other locations if you choose. For more information on how to specify the file's destination, see the `xsanctl` man page.

Install the Xsan configuration profile

After the configuration profile is created, you can install it on computers that you want to have access to the SAN.

1. Securely copy the configuration profile to the computers that you want to have access to the SAN.
2. Make sure all network and fibre connections are functioning properly.
3. Double-click the profile, open System Preferences, then click the Profiles preference pane.
4. Select the Xsan configuration profile from the sidebar, click the Install button, then click Continue.
5. Enter the user name and password of the administrator account on the computer where the Xsan configuration profile was created, click Install, then click Install.
6. Enter the local administrator name and password, then click OK.
7. Verify that you can see and add files to the Xsan volume.

Manage Xsan volumes

Mount or unmount an Xsan volume

You can mount or unmount an Xsan volume—typically from a client computer, not from the primary metadata controller. In this example, the volume name is FinalVideoFiles. Press Return after each step and, if necessary, enter the administrator password.

1. Do one of the following:
   - To unmount the volume: `sudo xsanctl unmount FinalVideoFiles`
   - To mount the volume: `sudo xsanctl mount FinalVideoFiles`
2. Verify the volume is either mounted or unmounted: `sudo xsanctl list`

Add storage to an Xsan volume

Adding a storage pool to a volume increases available storage and also requires that you stop the volume and unmount it. Adding storage pools is a quick way to expand a volume and doesn't require defragmenting the volume to recover performance. Press Return after each step and, if necessary, enter the administrator password. In this example, the volume is FinalVideoFiles, the new storage pool is NewPool, and it contains two LUNs (NewLUN1 and NewLUN2).

- Type the following on the Primary Metadata Controller: `sudo xsanctl editVolume FinalVideoFiles --storagePool NewPool --addLUNs NewLUN1 NewLUN2`

Remove an Xsan volume

If you no longer need a volume, you can remove the volume from the SAN. When you remove a volume, all data is deleted from that volume. In this example, the volume name is FinalVideoFiles. Press Return after each step and, if necessary, enter the administrator password.

1. Make sure the volume is unmounted on all computers.
2. Type `sudo xsanctl dropVolume FinalVideoFiles`

Manage access to SAN content

Manage access control lists on the SAN

You can manage access to specific folders on the SAN. By default, all access control lists (ACLs) are turned off on new volumes. After ACLs are turned on, they can't be turned off. This is done on the initial computer, now known as the *primary metadata controller*. Press Return after each step and if necessary, enter the administrator password.

Do one of the following on the Primary Metadata Controller:

- To turn on ACLs when you create the volume, add `--enableACLs` to the initial creation of the volume: `sudo xsanctl addVolume FinalVideoFiles --defaultFirstPool --addLUN FirstMDLUN --storagePool data --addLUN FirstUDLUN --enableACLs`
- To turn on ACLs after a volume has already been created, type: `sudo xsanctl editVolume FinalVideoFiles --enableACLs`

Manage users and groups on the SAN

You can choose to use UIDs from LDAP or GUIDs for your SAN. These are disabled by default. Press Return after each step and, if necessary, enter the administrator password. In this example, the name of the volume is FinalVideoFiles.

Do one of the following on the primary metadata controller:

- If the volume is already created: `sudo xsanctl editVolume FinalVideoFiles --idsFromLDAP` *or* `--idsFromGUIDs`
- If this is a new volume: `sudo xsanctl addVolume FinalVideoFiles --defaultFirstPool --addLUN FirstMDLUN --storagePool data --addLUN FirstUDLUN --idsFromLDAP` *or* `--idsFromGUIDs`

Manage controllers

Promote a standby metadata controller

You can promote a Standby Metadata Controller/Open Directory Replica to be the Primary Metadata Controller/Open Directory Master. The new Open Directory Master (promoted Replica) uses the directory and authentication databases of the replica. Press Return after each step and, if necessary, enter the administrator password. In this example, the primary Metadata Controller/Open Directory Master volume is INGESTVIDEOFILES, the user name is localadmin, and the password is 72DERjx1.

On the Primary Metadata Controller/Open Directory Master:

1. Run the following command to remove the computer from the SAN: `sudo xsanctl removeControllerFromSan INGESTVIDEOFILES`
2. On the previous Primary Metadata Controller/Open Directory Master, run the following command to remove the Open Directory Master database: `sudo xsanctl destroyMaster —account localadmin —pass 72DERjx1`

On the Standby Metadata Controller/Open Directory Replica:

1. Verify that the computer you want to promote is a Standby Metadata Controller/Open Directory Replica: `sudo slapconfig -getstyle`
2. Promote the Standby Metadata Controller/Open Directory Replica (you must know the Primary Metadata Controller/Open Directory Master user name and password): `sudo slapconfig -promotereplica localadmin`
3. Enter the Primary Metadata Controller/Open Directory Master user name password: 72DERjx1
4. Verify that the computer is now a Primary Metadata Controller/Open Directory Master: `sudo slapconfig -getstyle`

Remove a metadata controller from the SAN

You can remove a metadata controller from the SAN. When you remove a metadata controller, it will still keep the Open Directory database. Press Return after each step and if necessary, enter the administrator password. In this example, the controller to be removed has the fully qualified domain name (FQDN) `thirdmdc.example.com`.

- In Terminal, type the following on a metadata controller you want to keep: `sudo xsanctl removeControllerFrom thirdmdc.example.com`

Add a Mac client to a Quantum SAN

You can add a Mac client to your Quantum SAN. Do the following on the Quantum DLC metadata controller. Press Return after each step and if necessary, enter the administrator password. In this example, the name of the SAN is VIDEOSAN.

NOTE: The path below is for the Quantum xcellis node. The path for other controllers may be different.

1. Navigate to the following directory and create a profile: `/usr/cvfs/lib/make_profile`
2. Use your favorite text editor to add the following to the file:
   - <key>useDLC</key>
   - <true>
3. Save and close the file.
4. Securely copy the file to the client Mac computer.
5. Open the file on the Mac computer, then add the configuration profile.