Product Brief

XenData Object Storage Interface Creates a Private Cloud

Overview

The XenData S3 Server Object Storage interface provides remote access to a XenData data storage system. The interface may be added to an LTO data tape archive or to a Windows disk volume.

Access an LTO Archive from Anywhere

Adding an object storage S3 Server Interface to a XenData LTO archive system allows files to be written to and read from the archive from anywhere worldwide using fast and secure HTTPS. The on-premises interface and associated permissions are not affected: the LTO archive continues to be accessible locally using SMB, FTP or NFS. Consequently, the S3 interface is available as a simple upgrade to existing users, as well as for new installations.

Using the new object storage interface allows an organization to keep the attractive aspects of LTO on-premises archives which include cost effective scalability and adds the ease of distributed access which has traditionally been associated with public cloud storage. And, unlike most public cloud services, files may be remotely downloaded free of any egress charges.

Access a Windows Disk Volume from Anywhere

The S3 Server interface may be installed on a Windows machine to create a disk volume which can be accessed from anywhere as object storage. Files may be written to and read from the disk volume remotely using secure HTTPS. The disk volume can also be accessed locally as a logical drive letter and over the local network using SMB, FTP, NFS or HTTP.

About S3 and HTTP/HTTPS

About S3

Amazon S3, or Simple Storage Service, is a service developed by Amazon Web Services (AWS) that provides object storage through a web services interface. The S3 interface is an extension of Amazon's global ecommerce infrastructure that has been adopted by many other companies, including XenData, as an interface for both private and public cloud object storage.

S3 stores objects. When storing files in object storage, a standardized approach is to store each file as a single object and to include the file name and its path within the object name. This is the approach used by XenData; it allows object storage to be used as a self-describing file system storage repository that is accessible using third party tools.

S3 organizes objects in buckets. Various policies can be assigned to individual buckets, including for access security.

About HTTP and HTTPS

HTTP, or HyperText Transfer Protocol, is a transport protocol which is the foundation of almost all data exchange on the Web. HTTPS, or HyperText Transfer Protocol Secure, is an extension to HTTP which encrypts data while in transit. Furthermore, it uses a certificate issued by a certification authority to verify that the connection is legitimate. The certificate is known as an SSL Certificate.

HTTP and HTTPS may be used to transfer files to an S3 interface. They may be implemented in a multi-threaded fashion which, for example, breaks large files into multiple parts that are transmitted in parallel. This provides very fast file transfers over large distances.

HTTPS, which requires an SSL Certificate, is strongly recommended when implementing remote access via the Internet to your LTO or Windows disk volume.

Adding an SSL Certificate

To securely access via HTTPS, a Domain Validation SSL certificate is required. It should be purchased from a certification authority such as GoDaddy. This has a typical cost of around $70 per year. Additional requirements are:

- An external static IP address is required from your Internet Service Provider
- Your router/firewall must be configured to map the external IP address to the machine running the XenData software.
- A subdomain for the S3 Server interface. This is a name that you chose and will be a subdomain of a domain that you own. For example, XenData might choose s3server.xendata.com. This becomes the web URL used for remote access of your storage.
- DNS record change. The Domain Name System is used to map your external static IP address to your chosen subdomain. It takes time to propagate the DNS record change. This is typically a few hours, but it can take up to 72 hours to propagate a DNS record change throughout the entire Internet.

Adding the S3 Server Interface to a XenData LTO Archive

Adding the S3 interface an existing XenData archive system is very straight forward:

- Install the XenData S3 extension software
- License the S3 interface by adding a valid activation code using the XenData License Administration Utility

Creating a Windows Disk Volume with an S3 Server Interface

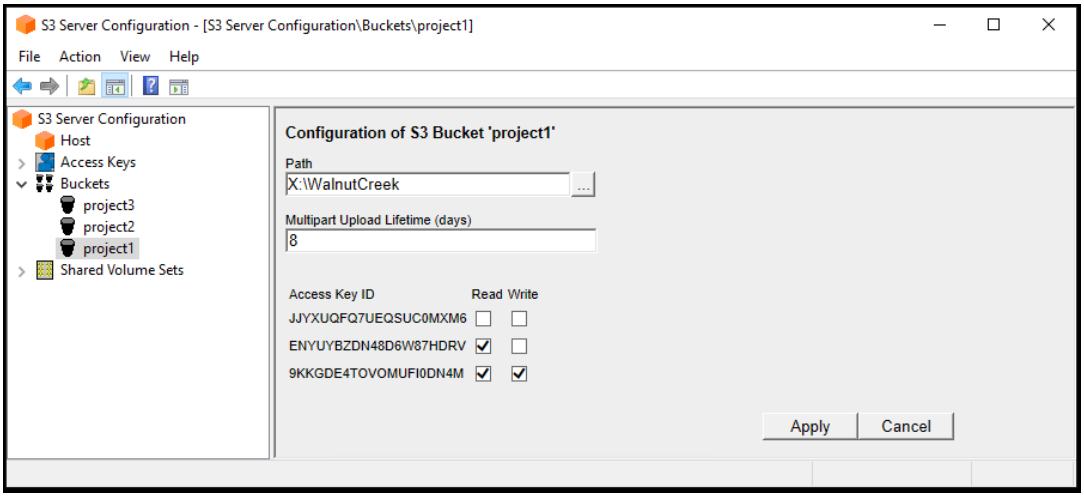
An S3 Server interface may be added a reformatted Windows NTFS disk volume as follows:

- Install XenData Cloud File Gateway (CFG) software and configure at installation to manage the NTFS disk volume. The XenData Alert Module will also be automatically installed.
- Install the XenData S3 extension software
- License the CFG software, the Alert Module and the S3 interface by adding valid activation codes using the XenData License Administration Utility

Configuring the S3 Interface

After installing the S3 Interface software, an S3 Server Configuration utility is available. This should be used to set the permissions that allow access to the LTO archive via S3. These permissions do not affect the local access, including via SMB, FTP and NFS. The configuration utility is used to create buckets and S3 access keys. The permissions apply to existing files stored on the archive, as well as to new files.

The S3 Server Configuration utility is illustrated below.

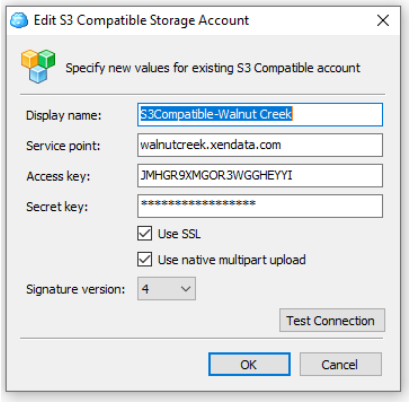


The configuration utility allows the administrator to define highly granular access permissions to the archive file system, as follows:

- One or more access keys is defined, perhaps one per user or group of users. The access key and associated secret key are entered into the S3 storage browser that will be used for remote access.
- One or more buckets are then defined. A folder, together with its sub-folders, is allocated to each bucket.
- Permissions for each access key are then defined for each bucket. When read permissions are not granted, the bucket's contents are not visible to the user. When read permissions are granted, a remote user may browse and restore files from the archive file system. And if write permissions are granted, an S3 storage browser may be used to upload files directly to the storage volume.

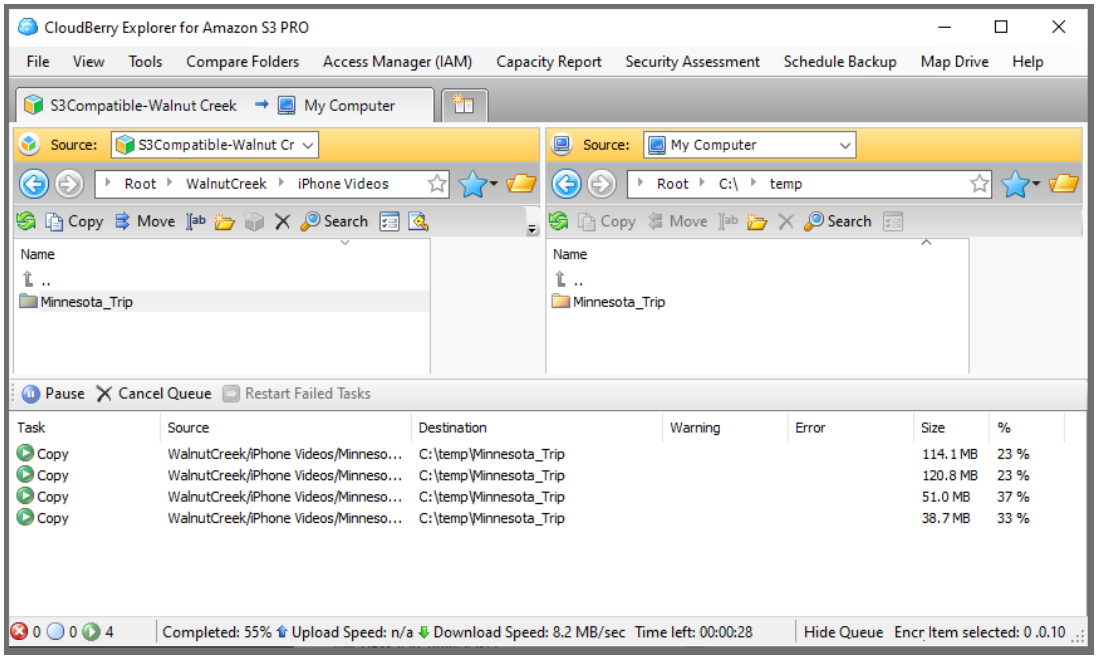
Example of Remote Access using an S3 Storage Browser

The S3 enabled storage volume may be accessed remotely using a certified third-party storage browser such as Cloudberry Explorer which is illustrated here.



One of the access keys and associated secret key that were defined using the XenData Server Configuration Utility are entered for a new S3 Compatible storage account in Cloudberry Explorer.

The contents of the S3 enabled storage volume are then available as illustrated below.



Contact Us

XenData USA: Walnut Creek, California | +1 925 465 4300
XenData Europe: Cambridge, UK | +44 1223 370114
Email: xendata@xendata.com | Web: www.xendata.com

Last Updated: May 12, 2022