ctera your files. your cloud.

THE CASE FOR A SYNC-GATEWAY

Combining the Benefits of Cloud File Sync Tools with the Speed of Local Storage

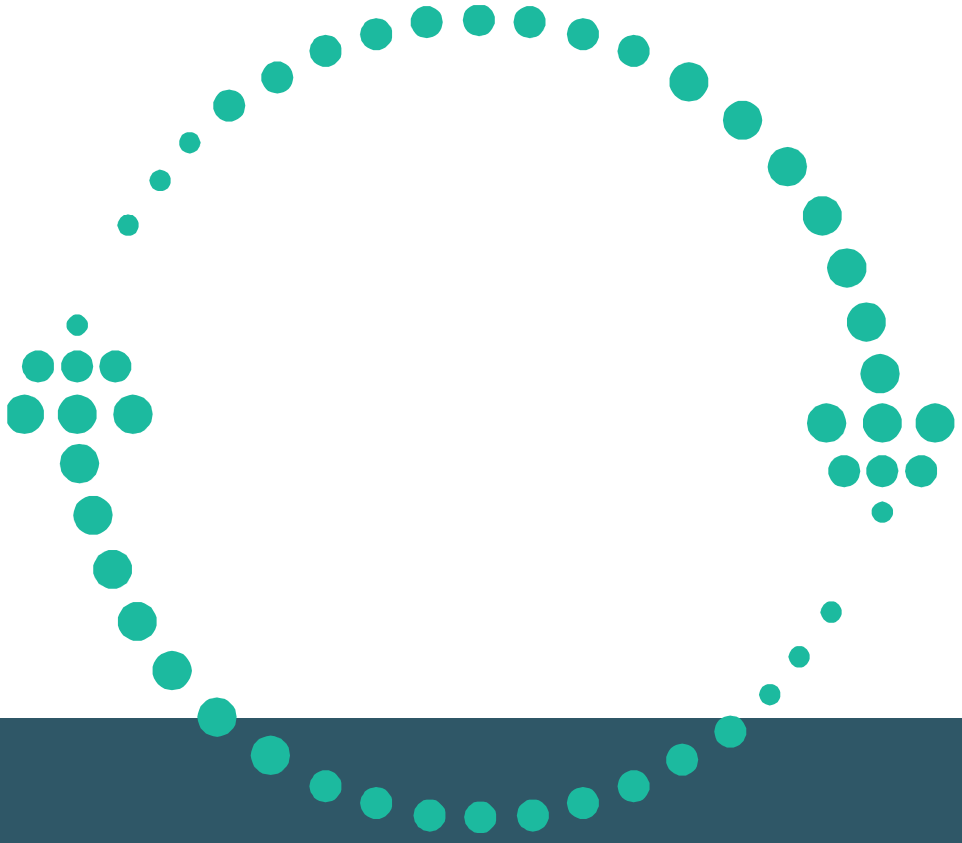

Table of Contents

www.ctera.com info@ctera.com **USA:** (650) 227-4950 **Intl.:** +972-3-679-9000

Introduction

Files are fundamental building blocks for most organizations. Spreadsheets, presentations, documents and images are created and referenced by users every day. When it comes to remote offices and branch offices (ROBOs), file services are often handled by local "file servers". The majority of these file servers are either Windows-based or network attached storage (NAS) appliances.

Local file servers are fraught with problems: provisioning, configuring, managing and protecting file servers at remote sites is expensive and error prone. But as with many IT services, cloud computing introduces new opportunities for delivering file services, especially to ROBOs.

This whitepaper describes recent developments in enterprise file services, and the impact of cloud storage on that landscape. It proposes a hybrid architecture for enterprise file services, that seamlessly integrates the cloud with traditional file server approaches, and allows users to store, protect, access and share files using any device. The proposed architecture offers performance, security, efficiency and ease of use.

Next Generation File Services

Even though file services have been around for a while, consumer oriented file services like Dropbox or Google Drive dramatically influenced users' expectations from corporate file services. Organizations must respond to these needs and evolve their enterprise file services to meet the new user expectations while preserving and enhancing business and enterprise requirements and goals:

- **Modern User Experience**: enterprise users expect to have a friendly user interface, both in the desktop OS interface and in web-based or mobile interfaces.
- **Fast storage & retrieval**: users must be able to store and quickly retrieve files when needed.
- **Data protection**: as a critical business resource, files must be backed-up and protected from both disasters (e.g. server crash) and user errors (e.g. accidentally deleting a file).
- **Collaboration**: the ability to easily share files with other users, and occasionally with customers or partners.
- **Mobile Access**: user mobility and growing support for 'bring your own device' (BYOD) require that files can be accessed anytime, anywhere and from any device.
- **Security**: files contain critical business data, and must be secured especially if stored in the cloud.

While some of these requirements may seem contradictory at first, there is a way to address all of them in a single unified architecture. So let's dig in.

On-premise and In-Cloud Hybrid Storage

Cloud storage services became integral part of cloud computing, allowing enterprises to store rapidly growing amounts of data in the cloud. Cloud storage offerings are typically based on "object storage", which is optimized for storing and retrieving data objects. The object storage is accessed via HTTP-based application programming interface (API), commonly referred to as 'RESTful API'.

While promising scale and flexibility, cloud storage services present two important challenges to ROBO users: compatibility and performance. Cloud storage protocols (e.g. RESTful API) are incompatible with traditional file access protocols (e.g. SMB, NFS), creating the need for 'protocol translation'. And since cloud storage is located at remote datacenters, ROBO users experience significantly slower performance compared to a local file server.

Cloud storage gateways (CSG) are designed to address the performance and compatibility challenges associated with delivering cloud storage services to ROBOs. In principle, the CSG serves as an intelligent intermediary between the ROBO users and applications and the newly added cloud storage.

The 'front end' of the CSG looks and behaves exactly like a file server. Users and applications within the ROBO simply access it just as they would access any standard file server or NAS. The 'back end' of the CSG connects to the cloud, handling protocol conversions and efficiently transferring data stored on it to the cloud.

This hybrid solution – combining local gateways with centralized cloud storage - offers ROBO users and applications fast and reliable local file services, while taking advantage of the cloud storage scale, flexibility and ubiquitous mobile access. It dramatically lowers the cost and complexity associated with delivering file services to ROBOs, and by efficiently uploading files to the cloud they literally make the age-old data protection problem go away.

Cloud storage gateways help address key items on the file services 'wish list': they offer fast data storage and retrieval,

and certainly alleviate the data protection problem. But what about the requirement to share and access files from any device and between any users?

Gateways that can Sync & Share

With file data stored in the cloud, new file services are made possible. File Sync and Share (FSS) introduces the ability to synchronize and share file data between multiple user devices (desktop, laptop, mobile) and selectively between users.

The usage model of FSS is straight forward: a user creates a file folder in the cloud, and is offered access to it through specialized client software on each of his devices; a copy of the cloud folder becomes automatically available on each of the user's devices; changes made on a specific device are propagated to the cloud, and reflected on any device owned by the user. Furthermore, a user can designate a specific file or folder to be shared with another user. The other user will be able to view and access the shared file or folder.

So we have cloud storage gateways that excel at delivering cloud-based file services to the ROBO, and FSS as an elegant solution for sharing files between any device owned by the user, and among different users. Wouldn't it be nice to combine the power of these two? That's exactly what the sync-gateway does.

A sync-gateway functions as a regular cloud storage gateway, but with the important addition of a built-in client for FSS. Remember, an FSS service is implemented by installing special clients on any participating device (e.g. laptop, desktop, mobile). By activating the Cloud Drive service, the Sync-Gateway simply becomes another device participating in the FSS service.

The storage administrator determines which cloud folders will be synced to any particular gateway. Once those folders are defined, the sync-gateway will display the folders as regular 'file shares'. Changes made to these special file shares will be immediately propagated to the associated cloud folder, and vice versa.

The benefit? Users within a ROBO work with shared cloud folders just as they do with any regular file shares. They benefit from the performance and simplicity of a local file share, and can access files stored within these shares from anywhere – using the CTERA Agent (an FSS client) on their laptop or mobile device, or via a browser. And just as with any FSS service, files or folders can be shared securely and selectively with other users.

The Sync-Gateway truly combines the best of all worlds: fast and simple local file services, compatibility with existing file protocols, cloud-based data protection, access to files anywhere, and streamlined collaboration.

Sync-Gateway Deployment Model

The CTERA solution includes the following components:

- **CTERA Cloud Storage Gateway**: installed in every participating ROBO, and connects to the CTERA Portal. The CTERA gateway appliance is available either in a physical form factor, or a virtual one.
- **CTERA Portal**: installed within a private, virtual-private or public cloud. The Portal aggregates traffic from all gateways, agents and mobile apps and interfaces with the backend cloud storage. It serves as a hub and gate-keeper for file synchronization and sharing, supporting the FSS functions for all clients, and it is the central management console for all gateways, software agents and mobile apps.
- **CTERA Agent**: loaded on each client – desktop, laptop or server. The CTERA Agent is an 'FSS client' providing access to, and synchronization with designated cloud folders. Additionally, the CTERA Agent can be used to back-up client file and application data either to a local gateway, or directly to cloud via the CTERA Portal
- **CTERA Mobile App**: loaded on mobile devices (e.g. iOS, Android, etc.) and serves as an FSS client for cloud folder access and synchronization.

A sample deployment of a sync-gateway is shown in figure 1. The CTERA gateway functions as a regular file server, supporting common file protocols such as NFS, SMB, AFP, FTP, etc. Local ROBO users and app servers access the gateway just like a regular file server. Based on policies, files stored on the gateway are compressed, de-duplicated and encrypted, then uploaded to the cloud (via the CTERA Portal) where they are stored. Traffic between the CTERA gateway and the Portal uses a secure and highly optimized CTERA transfer protocol (CTTP).

your files.
your cloud.

In addition to regular file server functionality, the sync-gateway provides each user with a unified view of their cloud folders. The user's personal and shared cloud folders are accessible through the sync-gateway via common file service protocols (SMB, NFS) at the remote branch office. All modifications performed by a user are instantly synced with CTERA Portal and are available for access and collaboration from anywhere via web-based browser access, mobile devices, and more.

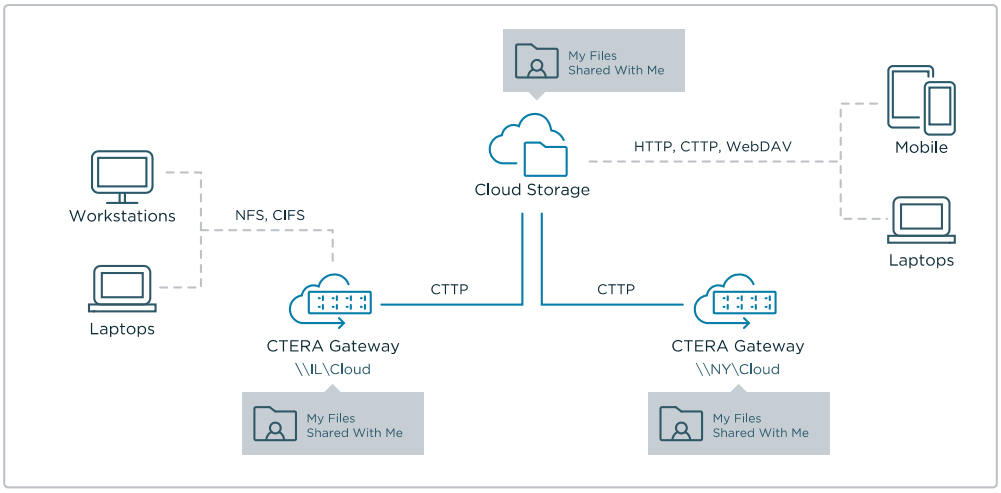

Figure 1

Users who are away from the office can access their personal and shared cloud folders using the CTERA Agent on their laptop, or the CTERA mobile app. Users located at other sites can access shared cloud folders or files in a similar way via the CTERA sync-gateway located in their site.

Apart from addressing performance requirements and bandwidth limitations, the sync-gateway is used to address site-to-site collaboration needs while ensuring security when collaborating with users outside of the corporate firewall. A geo-dispersed enterprise can sync and share data effectively across sites while preserving access control lists.

What about security?

Many organizations are rightfully concerned about migrating sensitive file data to the cloud. We must however distinguish between private cloud, virtual private cloud and public cloud.

With private clouds, the storage infrastructure is owned and managed by the organization. Private clouds are no different than tradition datacenters in terms of security. Virtual private clouds are hosted by 3rd party service providers, but are entirely 'fenced-off' and the security policies are controlled by the organization IT team. Other than the fact that physical assets aren't owned by the organization, virtual private clouds are similar in terms of security to private clouds.

Public clouds do introduce security challenges. Encryption is one approach to protecting sensitive data in the cloud, but attention should be paid to where data is first encrypted, encryption keys management and the potential exposure of meta-data (i.e. file names and attributes) and user identities. Furthermore, data sovereignty guidelines may dictate that it stays within a specific country, something hard to enforce with public cloud.

CTERA offers solutions that seamlessly integrate with private clouds and virtual private clouds. Hence using its hybrid cloud storage solution in that context introduces no new security vulnerabilities. CTERA is also used by 3rd party service providers to build and deliver their own cloud storage services.

CTERA has taken great care to ensure the security of enterprise data. For example: source-based AES 256bit encryption ensures that no data leaves the organization boundaries without being encrypted first; all data transmissions are done using secure protocols; encryption keys are managed within the CTERA portal, giving administrators full control; robust multi-tenancy guarantees that different enterprises' data never gets mixed; and fine-grained policies enable customers' choice of cloud-storage targets; These and other measures are designed to ensure the security of enterprise data - without compromising the end user experience.

Sample Use Cases

The CTERA sync-gateway offers a powerful set of capabilities that can be applied in a variety of ways. A few examples for potential use cases are described below:

ctera your files. your cloud.

- **File Server replacement**: cloud storage offers cost-effective and flexible platform for storing enterprise files. Plus, it supports access and sharing of files anywhere, anytime, from any device. File servers on the other hand provide convenience and local performance. Using the CTERA sync-gateway, enterprises can comfortably replace existing file servers, benefiting from cost savings, simplicity, performance and seamless collaboration.
- **File-based collaboration**: file sync & share (FSS) services are a new way for sharing files among users, yet they present security challenges and are detached from the familiar file server model. The sync-gateway seamlessly combines the performance and familiarity of a local file server with new FSS functionality. It offers a secure FSS service that nicely blends with the familiar file share model.
- **Roaming users**: users who alternate work locations (e.g. executives traveling between corporate offices, or relocated employees) no longer have to choose between the speed of a local file server, and having access to their files in another location. The user's folders are synchronized to each of the desired locations so they're available over LAN speed. Any changes are automatically propagate to all of the other synchronized locations. These user data synchronization policies are all centrally managed through the CTERA Portal. No matter what office they are in, users will find the latest copy of their files safely residing on a local gateway.
- **Software distribution**: enterprises often have large central file repositories they need to distribute to all their users. Examples include the library of the latest anti-virus updates, copies of updated corporate applications, TFTP/PXE boot shares, etc. Using the sync-gateway, IT can designate selected folders (e.g. the anti-virus files) to be shared with users in designated offices. CTERA's network-optimized protocol assures fast and efficient distribution of such large file repositories, allowing each user to easily access the repository via the cloud folder that was shared for that purpose.

A Case Study

A global company explored ways to modernize the file services it offers its distributed work force. The existing architecture was based on file servers deployed at each remote site, with unreliable backup capability. The IT team wanted to reduce Windows server footprint, while preserving file access performance for users. Other key requirements were: reliable data protection and disaster recovery options, as well as support for a BYOD (bring your own device) policy that allows employees to access and share files anywhere.

The company evaluated several options for addressing its broad file services needs, and selected CTERA for implementing their new, cloud-based file services architecture.

The CTERA Portal was installed at the company newly formed storage cloud, and CTERA gateways were deployed at each remote office. In addition, CTERA agents were loaded on users' laptops while CTERA mobile app installed on smartphones and tablets.

In addition to supporting file shares, the IT team created 'cloud folders' for users, allowing them to access those folders at the office (via the sync-gateway), or away from the office using the CTERA Agent or Mobile App. Beyond having fast access to file shares, users can also easily sync and share files between devices and other users. To quote the company director of IT ops:

"CTERA has enabled the IT team to transform its file services and become an internal service provider capable of delivering on-demand, cloud-based data access and protection services throughout the organization. CTERA supports the company vision of centrally managed, comprehensive and simple-to-use remote data services."

Summary

Cloud storage has introduced a positive disruption to the way organizations deliver file services to their end users. The traditional model of deploying a Windows file server or NAS at each ROBO is no longer necessary. Cloud storage gateways can easily and cost-effectively replace the aging file servers offering cost, simplicity and data protection advantages. The next generation of cloud storage gateways offers support for cloud folder synchronization. The CTERA sync-gateway successfully combines the speed and convenience of local file services with data protection, flexible and ubiquitous file access, and seamless collaboration. It represents the next generation of file services for remote offices and branch offices.