ctera
Cloud Storage, Enabled.

Private Enterprise File Sync & Share

Whitepaper by CTERA Networks

Highlights

- The need for file sync & share (FSS) solutions in the enterprise
- Benefits of FSS vis-à-vis traditional file sharing solutions
- Private cloud vs. public cloud FSS
- Key requirements for a private cloud enterprise-grade FSS solution
- CTERA's FSS solution architecture, features, and benefits

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

The Need for File Sync & Share (FSS)

Today's corporations employ knowledge workers who create, consume and share information. A growing portion of corporate information is stored as "unstructured data", namely files. Presentations, documents, spreadsheets, and images are but few examples of the types of files employees need to access and manipulate on a daily basis.

Many of these files are stored on users' workstations, desktops and laptops, while others are stored on departmental file servers. But wherever those files are stored, users must be able to access them at the office, at home, or on the road. Furthermore, users are no longer confined to using only workstations provisioned by corporate IT. Many organizations adopted a 'bring your own device' (BYOD) policy, allowing employees to access corporate data from smartphones, tablets, and even a random web browser.

Allowing users to access and manipulate files from multiple devices requires that files are 'synchronized' between those devices. For example, a user may edit a document using his PC at the office. Later at home, he opens the file using his tablet PC. Naturally he expects to see the changes made in the office incorporated into the file. He makes some additional changes to the file while working on it at home. The next morning he should view these changes when accessing the file from his office PC.

Additionally, given the collaborative nature of knowledge-related tasks, files must be available for access by multiple users. Frequently, files must be accessed by people outside the organization – by partners, suppliers or customers. As with any corporate data, file sharing must be carefully controlled. Who gets to see what file and when is an important decision that users must be able to make, and IT must help to enforce.

To summarize: In today's corporate environment, IT is required to support easy access and sharing of files anytime, anywhere and from any device, while maintaining security and access control policies.

Traditional File Sharing Solutions

Before the emergence of cloud technology, corporations were using a variety of methods for accessing and sharing files. While each of these methods offers some benefits to users, they each present some significant drawbacks. Among the most popular methods for file sharing are *file servers*, *email* and *content management systems*:

File Servers

Used for storing files on the corporate network. Files are organized in a hierarchical structure of folders, where each folder or file is assigned specific access rights. The data stored on file servers can be accessed by users that are logged into the corporate network, according to their assigned access rights.
File servers present a useful method for sharing files among corporate users. They maintain a single, consistent copy of each shared file and support file locking, which allow specific applications to prevent conflicting writes by multiple users.

File servers require that users be connected to the corporate network while accessing files - either by being physically present at the office, or via remote network access (e.g. VPN). Furthermore, most mobile devices do not support the file access protocols required by file servers (e.g. CIFS, NFS), and while offering good performance over the LAN, those protocols are not well adapted for good user experience over wide area networks, and are not considered to be secure enough to be used over the Internet without a VPN layer. Furthermore, those protocols offer no support for file access while offline.

File servers require significant administrative work, such as creating proper folder structure and defining user access rights. They are not suitable for BYOD support, and do not allow access or sharing of files by people who are not currently connected to the corporate network.

Email

Employees have been using email for sharing files with co-workers as well as people outside the company. The mechanism is straightforward – simply 'attach' a file to an outgoing email message and send it to the people you wish to share it with. Note that most companies restrict the size of email attachments, which limits the size of files that can be 'shared' this way.

The 'simplicity' of email-based file sharing comes with a great deal of complexity related to version management and access control. Very quickly you end up with exponential number of file versions and hardly any way to manage them. Furthermore, email attachments can be easily forwarded both inside and outside the company, so there is no simple way to control who gets to access the files and who shouldn't.

Enterprise Content Management (ECM):

These are specialized software packages that offer a central repository of files (e.g. Microsoft SharePoint, EMC Documentum). The ECM system keeps track of revisions made to files under its management. Users are assigned authorization levels, which control whether they can view or edit specific files. ECM systems typically support a process for file locking, whereby users "check out" a file, modify it and eventually perform "check in" back into the system. Some solutions require a specialized software client, while others also support a web-based interface. Installing and administering ECM requires a high degree of IT expertise, and users must be trained how to use the system. The ECM central servers may encounter scalability issues in large deployments, and cause delays in user access to files.

File Sync & Share (FSS) Services

A new breed of file sharing services (e.g. Dropbox, Google Drive) recently emerged within the consumer space, allowing users to share files (e.g. photos, videos) with friends and family. A user registers to the service and then downloads an agent to each of his/her PCs. The agent creates a folder on the PC, and when a user either drops a file into that folder, or modifies an existing one, it gets synchronized with a master copy in the cloud.

File sharing services also support mobile environments. By installing an FSS app on their smartphones or tablet computers, users can access the same they are sharing on the office PC. The same shared folder can also be accessed from a web browser anywhere. Users may point any web browser to the FSS service website, log in with their username/password and the shared folder becomes visible through the web browser. Users can also mark specific files or folders as favorites, to synchronize them onto the mobile device for offline access.

The usage model for FSS is very intuitive. It is fully aligned with the methods traditionally used for accessing files locally. When user A wants to share a file with user B, she simply moves that file to a shared folder. User B will see the file appear in his FSS folder. A Web-based interface allows easy collaboration with other users, even those that are not registered users of the FSS service.

Furthermore, FSS offers excellent responsiveness since all reads and writes are performed locally. FSS also offers excellent resilience to Internet connectivity loss, since they are designed from the ground up to perform transparent offline synchronization.

After taking the consumer market by storm, file sync & share services quickly found their way into the corporate world. Corporate users started to adopt these file sharing services to facilitate access from multiple devices (BYOD), and share files with colleagues, partners and customers. While consumer-grade file sharing services pride themselves on exceptional ease of use, they present significant challenges and risks when it comes to corporate data security and regularity compliance. The infiltration of these services into the corporate domain has kept many IT managers awake at night.

The Need for Enterprise FSS

Users' need for file access and sharing '*anytime, anywhere and from any device*' is part of the reality corporate IT needs to face. Ignoring the need may push even more users into the arms of consumer-grade file sharing services. This is a security threat and a legal risk that most companies simply cannot afford.

Files that may contain sensitive business details, financial information or customer data must be protected according to enterprise security policy and regulatory requirements. Letting such files 'leak' into a consumer-grade file service may open the door for competitors, or put customer relationships at risk. In some industries, failing to meet regulatory compliance when it comes to corporate data may lead to legal liability, hefty fines and negative publicity.

While some companies have tried to forbid the use of unsanctioned, consumer-grade FSS services, most understand that in order to address the need they must offer a sanctioned, secure alternative under the control of corporate IT. Beyond the basic ability to access and share files, enterprise-grade FSS should address the following requirements:

- **Data Security:** Given the sensitivity of corporate data, files stored outside the enterprise firewall must be encrypted in order to avoid access by unauthorized personnel.
- **User Identity Management:** The authentication, access rights and policies associated with each corporate user are typically managed within a directory service (e.g. Active Directory). An FSS solution should be fully integrated with such systems, so that file access rights comply with company policies and do not require setting up separate identity silos.
- **Central Administration:** IT needs a comprehensive administrative view of an FSS service. It needs to set global or individual policies, track usage, and review performance metrics.
- **Project Collaboration:** regular FSS services don't offer facilities for defining projects, which are shared workspaces with specific access rights based on users and groups which are found in the enterprise directory, as well as external guests. Projects can be centrally managed, but many organizations are finding that the flexibility of self-defined projects, which are formed by end users without IT assistance, allows for improved organizational agility and reduced IT overhead. In order not to degrade into anarchy, these self-defined projects should still be managed by a corporate policy – regarding aspects such as which users can define projects, automatic storage quotas based on the project creator, and so on.
- **Usage Metering:** many companies move to a model where IT services are internally billed to other departments. It is therefore important to measure the storage and network traffic used by each department/user.
- **Audit Trail:** In some circumstances, changes to sensitive corporate data must be tracked. The history of who made modifications to a file, and when, should be kept for future audits.
- **Integrated Backup:** A closely related service to FSS is the ability to backup and restore files on demand. FSS is not in itself a backup solution, since it is not regularly scheduled and does not support the same level of version management. When evaluating new FSS solution, corporate IT should also examine how it integrates with other file related requirements such as backup.

Public vs. Private FSS

When looking to implement Enterprise-grade FSS solutions, companies are facing two major approaches:

- **Public Cloud:** Software-as-a-Service (SaaS) offered by 3rd party vendors, hosted on shared cloud infrastructure.
- **Private or Dedicated-Hosted Cloud:** Service managed by corporate IT, and hosted within corporate datacenters or on a dedicated external cloud under corporate IT control.

A public cloud FSS service utilizes infrastructure built by a 3rd party and shared amongst multiple customers in a multi-tenant environment. To use the service, the company typically pays a "subscription fee" per each employee, plus a capacity-based fee for storage used. The files are uploaded to the 3rd party datacenter, where they are stored and managed by the service provider. Security is typically addressed through encryption of the data at rest, and/or in transit. File synchronization speed depends on available Internet bandwidth.

A private cloud FSS solution is constructed and managed by corporate IT staff, using off-the-shelf software/hardware/service solutions. The FSS solution can take advantage of existing corporate storage, and can benefit from existing storage services such disaster recovery and business continuity. Files are stored within the corporate datacenter, under full corporate control. Users who access files from within the corporate network benefit from 'LAN-speed' synchronization. Since the solution is created by the corporate IT, it can be easily integrated with other storage services, such as backup.

A close variant of a private-cloud FSS involves hosting corporate data on a *dedicated* cloud service. The file storage is managed by a Cloud Service Provider (CSP) or hoster as a 'virtual private-cloud'. It isn't shared among multiple corporations, but rather dedicated to a specific company. Since dedicated-hosted cloud FSS provides similar levels of corporate control as private cloud FSS, this paper will hereafter refer to both as private-cloud FSS.

The following table summarizes the differences between the public and private cloud approaches:

Criteria	Private FSS	Public FSS
Cost model	Leverage datacenter storage CapEx for FSS solution	OpEx for service Pay-per-Use for storage
File storage	Within datacenter or dedicated cloud, under full corporate control	At 3rd party datacenter Subject to 3rd party control
Sync Performance	LAN-speed when onsite, Internet-speed when offsite	Internet-speed

CTERA Private Enterprise FSS

CTERA provides an enterprise-grade FSS alternative to consumer cloud applications, utilizing either private or hosted cloud infrastructure while maintaining end-to-end security. The solution allows enterprises to set up file sync & share services for their users, based on a variety of object storage or cloud storage platforms. It enables the use of existing datacenter storage infrastructure to deliver mobile file collaboration, and control the storage of corporate data. CTERA is interoperable with leading private cloud storage solutions from EMC, IBM, HDS, Openstack, and others, as well as public cloud services such as Amazon Web Services, IBM SmartCloud, and others. Customers can also customize the user interface to apply their corporate brand to the service.

CTERA's FSS solution bi-directionally synchronizes folders to and from a private cloud, making files readily accessible on users' laptops, desktops and mobile devices - also when offline. CTERA's Mobile App integrates with its cloud file sharing mechanism and provides file access and collaboration capabilities from mobile devices including iPhone, iPad and Android devices.

In order to facilitate multi-user collaboration, CTERA's solution allows users to set up joint cloud storage workspaces ('projects') for sharing files with colleagues. These project-specific folders support read/write privileges, allowing multiple users to share data and resolving any conflicts generated in the process. Folder owners can also perform ad-hoc file sharing using time-limited 'invitations' to selected users.

CTERA's FSS solution seamlessly utilizes existing Active Directory or LDAP services for identity management and user authentication, including complex AD tree and

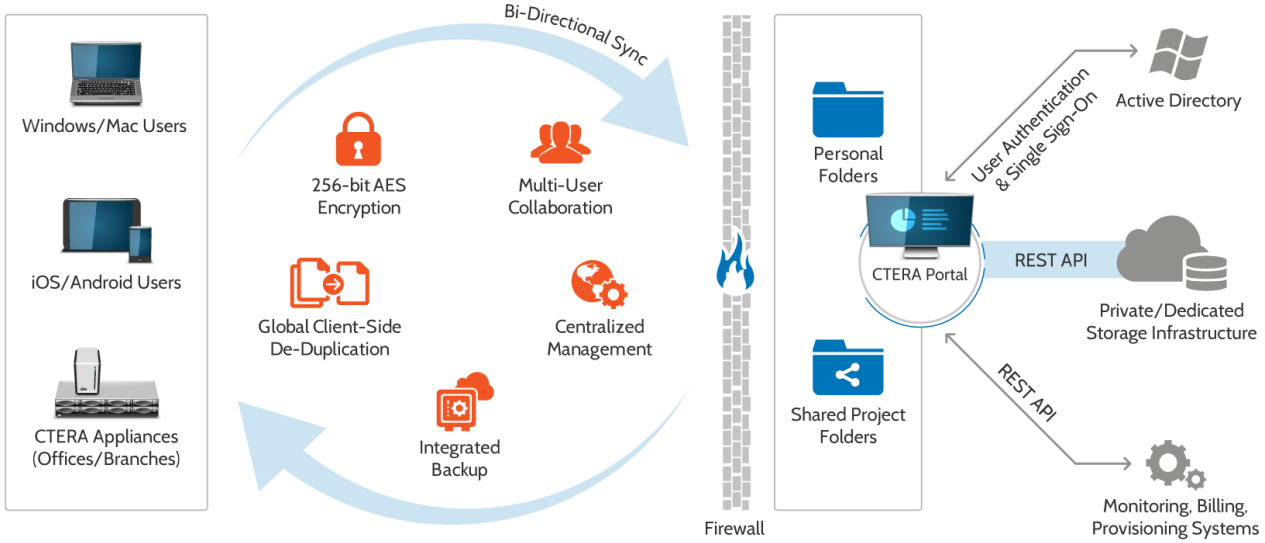

Figure1 : CTERA's Private Enterprise FSS Topology

forest topologies. Enterprises avoid duplicate directory services, and benefit from rapid deployment and compliance with role-based access privileges. With client-side encryption, data-at-rest encryption in the cloud, and true multi-tenancy with separation of data, CTERA provides a secure, private alternative to public cloud services. Enterprises who need to rapidly deploy a private cloud FSS solution will benefit from the following CTERA advantages:

- **Data Control:** The CTERA solution can be deployed within the enterprise datacenter, or on dedicated cloud storage. Corporate data resides on highly secured and protected corporate storage – leaving it under full IT control.
- **Security:** Data is encrypted both at-rest and in-transit with full control over encryption keys, proving security from the end-point all the way to the datacenter.
- **Directory Services:** Integration with existing AD/LDAP services and Single Sign On (SSO) mechanisms ensures that user authentication and access rights are fully compliant with corporate policies.
- **Leverage Enterprise Storage Pool:** CTERA's solution can leverage existing datacenter storage, integrating with data protection and disaster recovery policies.
- **Central Management:** CTERA offers a comprehensive central management dashboard that allows administrators to provision, manage, monitor and support individual service users.
- **Access Performance:** On synchronized PCs, users benefit from local access speeds and full access to their data even while offline. De-duplication and compression techniques minimize the amount of data transferred across the corporate network or over the Internet.
- **Reigning in BYOD:** Support bring-your-own-device mobile and tablet users, allowing them to access corporate data securely, with "sandboxing" that prevents other mobile apps from accessing this data and remote wipe capabilities.
- **Integrated Backup:** CTERA delivers file sync & share as well as hybrid local/cloud backup from a single, small-footprint software client. Data residing on users' PCs can be backed-up directly to the cloud, or to a local 'cloud storage gateway' appliance which later uploads the data to the cloud. Backup and FSS are also centrally managed from the same system, thus reducing both management overhead as well as complexity on end-point devices.

Summary

Employees require access to their files at the office, at home or on the road. Using a variety of devices to access corporate files – laptops, desktops, smartphones and tablets – is quickly becoming the norm. The collaborative nature of work in most companies requires users to share files with co-workers, partners and customers. These trends have made file synchronization and sharing (FSS) a key requirement for most corporations.

Companies must tackle the demand for FSS services head-on, or face the use of consumer-grade FSS services within the organization, compromising corporate data security. IT departments should therefore offer alternative, enterprise-grade FSS services. Organizations that prefer to or need to retain full control of their corporate data are now able to build a private-cloud FSS solution. Such a private FSS solution must be based entirely on the organization's infrastructure, integrate seamlessly with its authentication mechanisms, provide no-compromise enterprise-grade security and avoid using external cloud services for metadata, encryption key management or use access control.

CTERA is the leading vendor for private / dedicated FSS enterprise-grade solutions, taking into account the need to leverage a common storage infrastructure for multiple applications. CTERA's solution offers a comprehensive platform, enabling companies to rapidly deploy an FSS solution that is fully integrated with their existing storage and IT infrastructure.

CTERA Networks revolutionizes storage, data protection and collaboration for enterprise and SMBs. Its hybrid architecture combines secure cloud storage services with on-premises appliances and managed agents.
CTERA's scalable cloud storage platform is used by leading service providers and enterprises, on the public or private cloud infrastructure of their choice.

For more information, visit www.ctera.com