Filr 2.0

How Filr Works–Overview Guide

September 2016

Novell

Legal Notice

Contents

About This Guide

This guide contains high-level overviews of Novell Filr and covers the following topics:

Audience

This guide is intended for Novell Filr administrators.

Feedback

Please use the User Comments feature at the bottom of each online documentation page to comment and suggest improvements to this guide and the other documentation included with Novell Filr.

Documentation Updates

The most recent version of this guide is available here (http://www.novell.com/documentation/novell-filr-2/filr-2-overvw/data/bookinfo.html) on the Novell Filr Web site.

Additional Documentation

For other Novell Filr documentation, see the Novell Filr Web site (http://www.novell.com/documentation/novell-filr-2/).

1 Filr Overview

Today's workers expect to access work files like they do personal files.

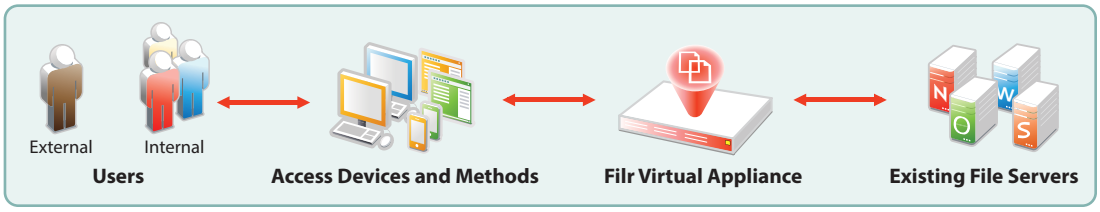
Some of them are moving work files to cloud-based services, which causes the risk managers in their organizations to lose sleep.

Novell Filr offers modern file access without compromising existing security systems.

1.1 What Is Novell Filr?

Novell Filr provides file access and sharing, and lets users access their home directories and network folders from desktops, mobile devices, and the Web. Users can also synchronize their files to their PC or Mac. Changes that they make to downloaded copies are kept in sync with the originals on their network file servers. And finally, users can also share files internally and externally, and those with the share can collaborate with each other by commenting on the files.

Figure 1-1 *Mobile Access to Enterprise Data*



- **Users:** Filr lets you control the following:
  - User authentication inside and outside your organization
  - Access to organization files and folders that were previously accessible only through mapped drives
  - Access to personal files and folders in Filr-based storage and/or in traditional Windows, OES, and NetWare home directories
  - Internal and external sharing of files and folders
- **Access Devices and Methods:** Filr provides multiple access methods.
  - A Web (browser-based) application
  - Apps for Apple iOS 8 and later, Android 2.3 and later, Windows phones 8.0 and 8.1, and BlackBerry PlayBook and Z10 personal devices
  - Clients for Windows 7 (x86 and x64) and 8 and later (x64 only) workstations
  - A client for Macintosh OS X 10.9 and later workstations
- **Filr Virtual Appliance:**
  - This runs on VMware, Xen, Citrix Xen, and Hyper-V hypervisors.

- It lets users authenticate using their eDirectory and Active Directory usernames and passwords.
- It provides access to data on NetWare, OES, Windows, and SharePoint servers that use their native file protocols (NCP and CIFS).

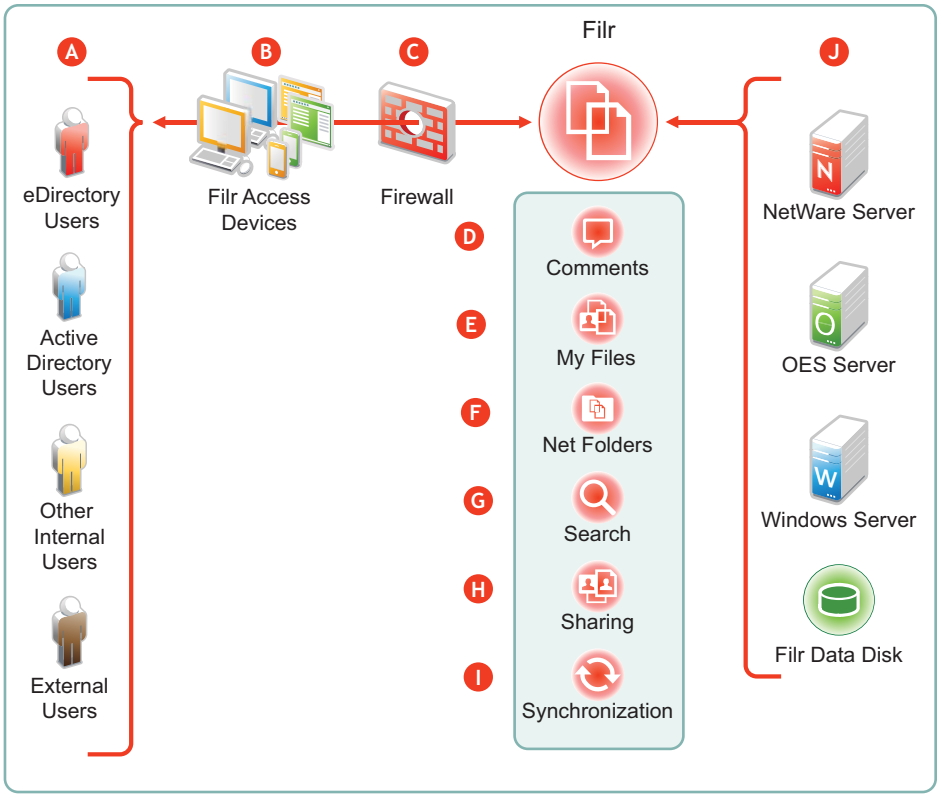
- **Existing File Servers:** Are not impacted because Filr does the following:
  - Requires no changes to file servers
  - Honors file system trustee rights and attributes

    Your Novell and Microsoft file servers and directory services retain complete control over all file- and folder-related activity.

1.2 Filr Features and Functionality

Figure 1-2 shows Filr's main features in the context of your existing network infrastructure. The table that follows the figure briefly describes each feature and how all of the components shown fit together to provide Filr services.

Figure 1-2 *What Filr Provides*



Letter	Details
A	• **eDirectory and Active Directory:** You synchronize Filr with eDirectory and Active Directory identity stores through LDAP. See "Synchronizing Users and Groups from an LDAP Directory" in the *Filr 2.0: Administration Guide*. • **Local Users:** You can create users on the Filr system independent of any LDAP source. For more information, see "Creating a New Local User" in the *Filr 2.0: Administration Guide*. • **External Users:** When a user outside the organization responds to an invitation to share a file or folder, Filr creates a username using the invitation's email address. When users accept these invitations, they can set their passwords. For more information, see "Sharing Files and Folders" in the *Filr 2.0: Web Application User Guide*.
B	Filr lets users access files and folders through the following: • A Web (browser-based) application • Apps for Apple iOS 8 and later and Android 2.3.*X* and later • Clients for Windows 7 and later and Macintosh OS X 10.9 and later workstations
C	Filr is designed to work with your security infrastructure. Your firewalls continue to protect your data while Filr provides access to it from practically anywhere. For more information, see "Site Security" in the *Filr 2.0: Administration Guide*.
D	Filr lets users collaborate by supporting user comments on files and folders. For more information, see "Filr Comments" on page 51.
E	Filr lets users access their personal files and folders on either or both traditional home directories and local Filr storage. For more information, see "My Files (Personal Storage)" on page 61.
F	Filr lets users access your organization's files and folders that were previously available only through mapped drives. For more information, see "Net Folders" on page 65.
G	Filr lets users search for files and folders that they have rights to access. If indexing is enabled on a folder, they can search within the content of the folder's files as well. For more information, see "Filr Search Appliance—Accessibility, and Searchability" on page 55.

Letter	Details
H	Filr lets users share files in Net Folders, and files and folders in My Files, with internal and external users. For more information, see “Sharing through Filr” on page 77.
I	Filr lets you synchronize eDirectory and Active Directory users as well as files and folders according to your organization’s needs. For more information, see “Filr Synchronization” on page 83.
J	Filr provides access to storage on Novell file servers, Windows file servers, and personal storage on the Filr appliance.

1.3 Why Appliances?

In contrast with servers, appliances simplify the development and delivery model for Filr so that we can provide you with new services more quickly.

Appliance benefits include the following:

- **Simplified Deployment:** Filr appliances are built on specific and tuned operating systems (SLES 11 SP3 in the case of Filr 1.2). This means that you don’t have to install the operating system, select the packages, and so on because everything needed is included and ready to configure and run.

  By the same token, packages and services that aren’t needed aren’t included, and therefore they don’t consume system resources.
- **Simplified Management:** Appliances include the following:
  - Appliance-specific configuration wizards to configure exactly and only what is required.
  - Web-based administration tools for changing configurations, adding or provisioning users, and so on, from basically anywhere that you need to be.

2 Setting Up Filr

This section presents high-level overviews of the following setup tasks. For detailed setup information and instructions, see the *Filr 2.0: Installation and Configuration Guide*.

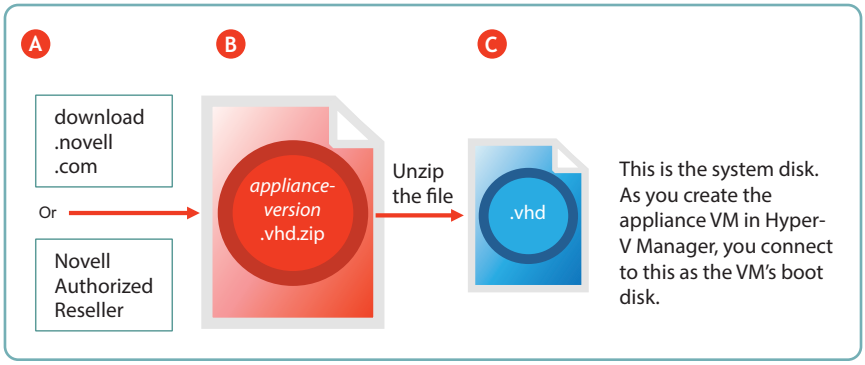
2.1 Getting and Preparing Filr Software

The process of getting and preparing Filr software is straightforward, as illustrated in the following sections.

For more information, see “Installing the Filr Appliance,” “Installing the Search Index Appliance,” and “Installing the MySQL Database Appliance” in the *Filr 2.0: Installation and Configuration Guide*.

2.1.1 Hyper-V

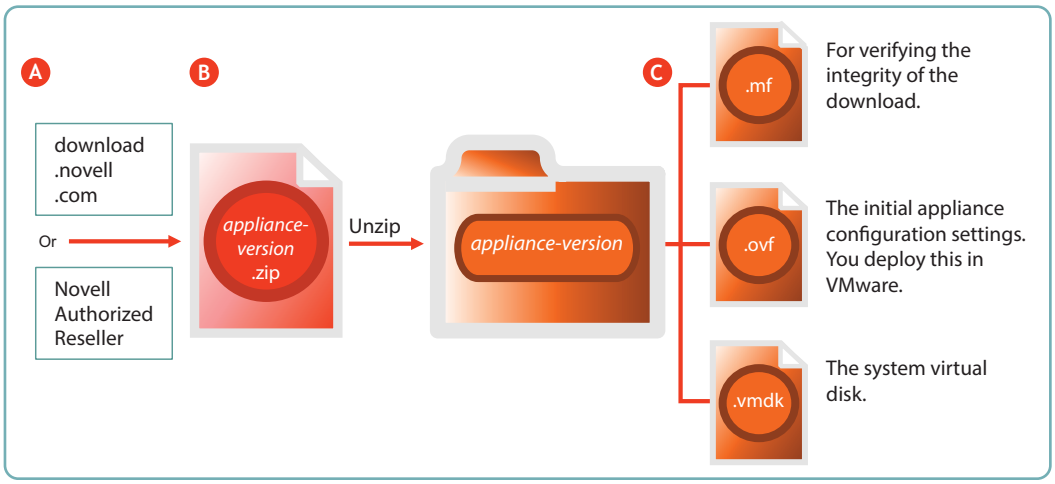
Figure 2-1 *Downloading and Preparing Novell Appliances for Hyper-V*



Letter	Details
A	You can download the `.zip` archive files for the Hyper-V build of the three Novell Filr appliances (Filr, Search, and MySQL) directly from the Novell Download Site, or you can obtain them through your Novell Authorized Reseller.
B	Unzip the archive to expose the appliance system disk image. For more information, see "Installing the Filr Appliance," "Installing the Search Index Appliance," and "Installing the MySQL Database Appliance" in the *Filr 2.0: Installation and Configuration Guide*.
C	The `.vhd` file is a Hyper-V disk image that contains all of the appliance's system files. You connect to this file in Hyper-V Manager by selecting the **Use an existing virtual hard disk** option. Unlike VMware and Xen, no pre-configured settings file is supplied for the VM. Instead you specify the RAM, network card, additional disks, and so on as instructed in the *Filr 2.0: Installation and Configuration Guide*.

2.1.2 VMware

Figure 2-2 *Downloading and Preparing Novell Appliances for VMware*

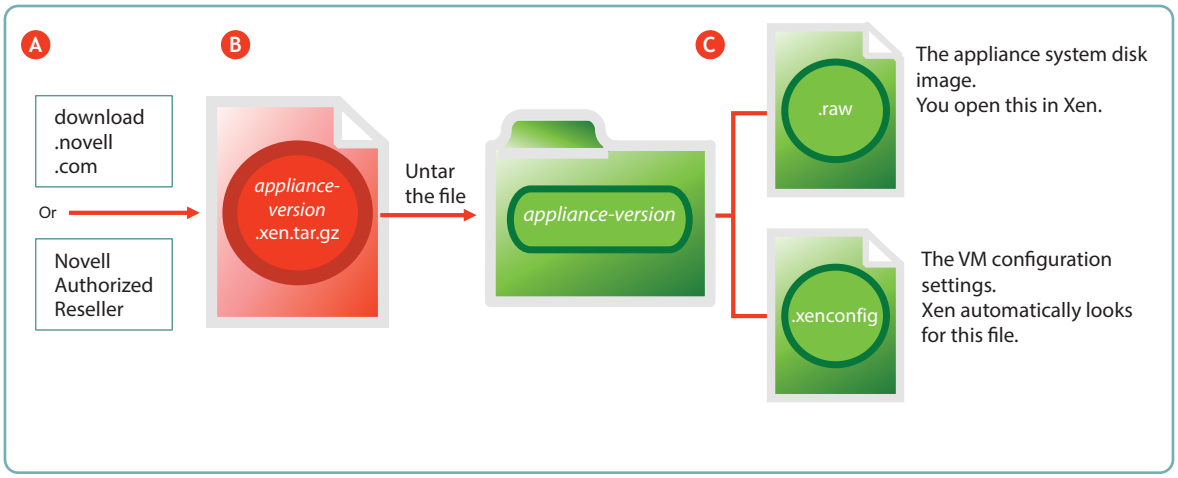


Letter	Details
A	You can download the `.zip` archive files for the VMware build of the three Novell Filr appliances (Filr, Search, and MySQL) directly from the Novell Download Site, or you can obtain them through your Novell Authorized Reseller.

Letter	Details
B	Unzip the archives to expose a folder that contains the three files needed for deployment. For more information, see “Installing the Filr Appliance,” “Installing the Search Index Appliance,” and “Installing the MySQL Database Appliance” in the *Filr 2.0: Installation and Configuration Guide*.
C	The `.mf` file contains an SHA1 digest that VMware uses to verify the integrity of the other two files. The `.ovf` file contains the virtual appliance’s configuration settings. You open and deploy this file in VMware to create the Filr appliance. You modify its settings during the initial deployment phase. The `.vmdk` file is the virtual appliance’s (VA’s) system virtual disk and contains all VA system files. It comes ready for the initial start-up and configuration.

2.1.3 Xen and Citrix Xen

Figure 2-3 *Downloading and Preparing Novell Appliances for Xen*



Letter	Details
A	You can download the `.zip` archive files for the Xen build of the three Novell Filr appliances (Filr, Search, and MySQL) directly from the Novell Download Site, or you can obtain them through your Novell Authorized Reseller.
B	Untar the archives to expose a folder that contains the two files needed for deployment. For more information, see “Installing the Filr Appliance,” “Installing the Search Index Appliance,” and “Installing the MySQL Database Appliance” in the *Filr 2.0: Installation and Configuration Guide*.

Letter	Details
C	The `.raw` file contains the system disk image. You open this file in Xen to begin the deployment process The `.xenconfig` file contains the virtual appliance's configuration settings. You modify its settings during the initial deployment phase.

2.2 Deploying Filr Appliances

NOTE: The information in this section illustrates a VMware deployment. The same basic steps apply to other supported hypervisors. For specific deployment instructions, refer to the *Filr 2.0: Installation and Configuration Guide*.

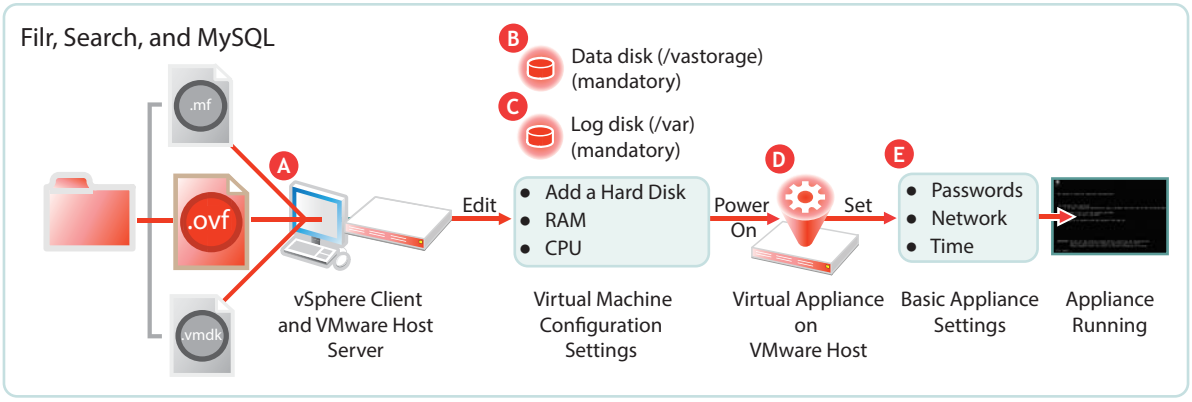
After you have obtained and extracted the appliance software, you need to deploy it on your host server, as illustrated in Figure 2-4 and Figure 2-5 and as explained in the tables that follow them. For more specific information about the different deployment models, see "Planning the Deployment Type" in the *Filr 2.0: Administration Guide*.

- Section 2.2.1, "Small Filr Deployment Overview," on page 16
- Section 2.2.2, "Large Filr Deployment Overview," on page 17

2.2.1 Small Filr Deployment Overview

NOTE: After initial VM preparation is completed, deploying on Hyper-V and Xen is comparable to the VMware steps illustrated below.

Figure 2-4 *A Small Deployment of Filr on VMware*

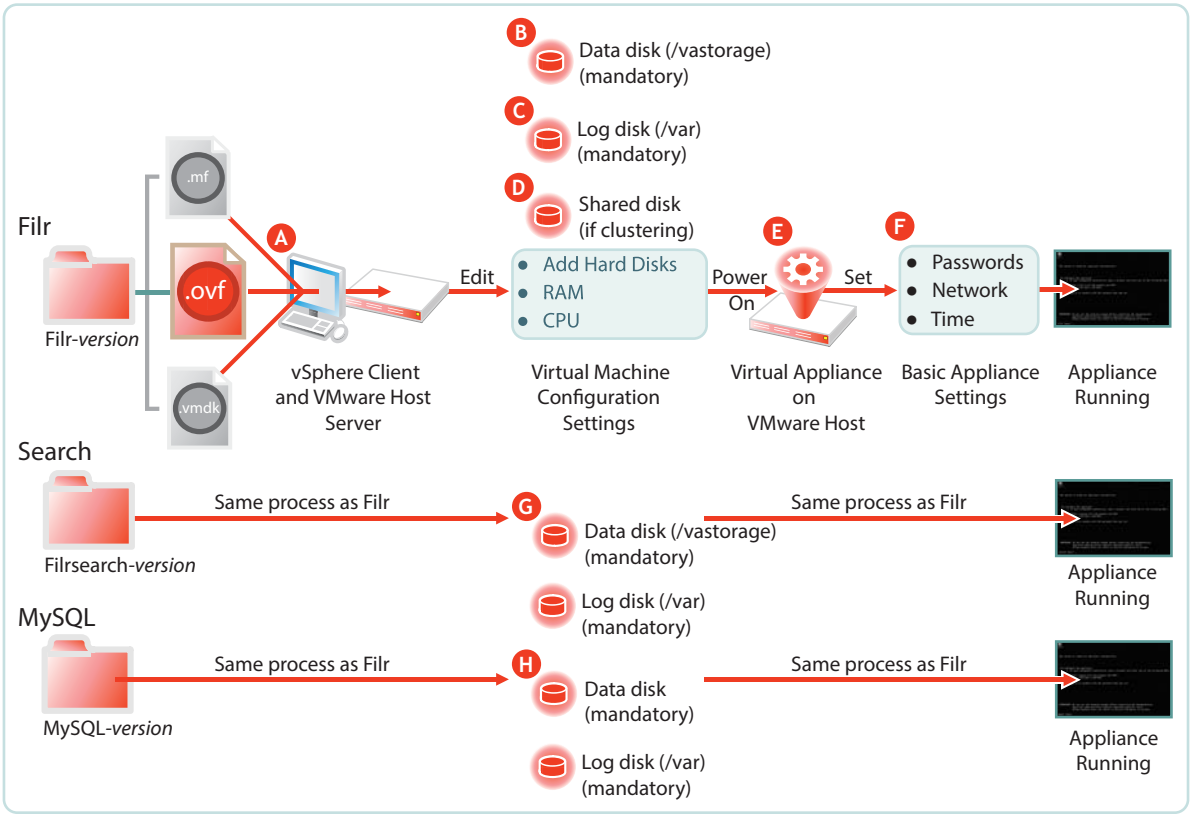


Letter	Details
A	Using the vSphere client, access the VMware host server and deploy the `.ovf` template file. Specify the hostname and IP address. If possible, the system determines the mask and gateway, and automatically populates those fields. The network interface is bridged by default. Make sure this setting matches the network configuration in your VMware environment.
B	A second disk is needed for the following reasons: ◆ Adequate personal storage disk space—personal files are stored here. ◆ Separation of system and data files to facilitate appliance updates—data files are stored here. You might want to also change the RAM allocation and the number of CPUs.
C	A third disk is needed for storing log files, which prevents the system disk from running out of space.
D	Start the appliance.
E	Specify the appliance's basic configuration, which includes administrative users' passwords, IP address settings, and the time zone and NTP time source. These settings are common to all Novell appliances.

2.2.2 Large Filr Deployment Overview

NOTE: After initial VM preparation is completed, deploying on the other hypervisors is comparable to the VMware steps illustrated below.

Figure 2-5 *A Large Deployment of Filr*



Letter	Details
A	Using the vSphere client, access the VMware host server and deploy the `.ovf` template file. Specify the hostname and IP address. If possible, the system determines the mask and gateway, and automatically populates those fields. The network interface is bridged by default. Make sure this setting matches the network configuration in your VMware environment.
B	A second disk is needed for the following reasons: ◆ Adequate personal storage disk space ◆ Separation of system and data files to facilitate appliance updates You might want to also change the RAM allocation and the number of CPUs.
C	A third disk is needed for storing log files, which prevents the system disk from running out of space.

Letter	Details
D	If you are clustering the Filr VA, add a shared CIFS or NFS disk to all of the Filr VAs in the cluster to use. This only applies to the Filr VA, not to the Search or MySQL appliances.
E	Start the appliance.
F	Specify the appliance's basic configuration, which includes administrative users' passwords, IP address settings, and the time zone and NTP time source. These settings are common to all Novell appliances.
G	If you are installing separate appliances, you need to deploy at least one and preferably two search appliances as well. The process is very similar to a Filr VA deployment, except that the search appliances don't use shared storage.
H	Installing separate appliances also requires configuring a MySQL or MS SQL database. Deploying the MySQL appliance that comes with Filr is very similar to the process for Filr and the search appliances. If you already have a MySQL or MS SQL database in your organization, you can use it instead of the MySQL appliance that comes with Filr.

2.3 Initial Configuration of Filr Appliances

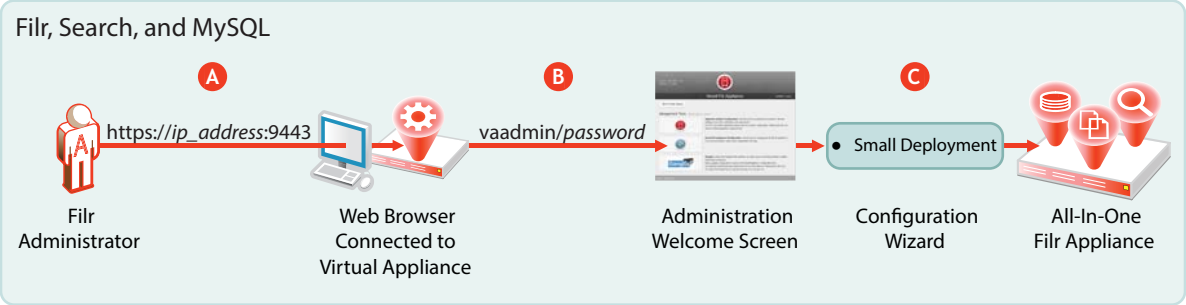
After you have deployed the appliances and set a few basic system settings, such as passwords, you must perform an initial appliance configuration. The process varies, depending on which deployment scenario you are implementing.

- Section 2.3.1, "Small Filr Deployment Configuration," on page 19
- Section 2.3.2, "Large Filr Deployment Configuration," on page 20

2.3.1 Small Filr Deployment Configuration

Starting and configuring an all-in-one Filr appliance is quite straightforward, as illustrated in Figure 2-6 and explained in the table that follows it.

Figure 2-6 *Configuring an All-in-One Filr Appliance*



Letter	Details
A	Access and configure the Filr appliance through a browser.
B	Log in to the administration console.
C	Run the configuration wizard. When you finish, your all-in-one appliance is running and ready to provide Novell Filr services.

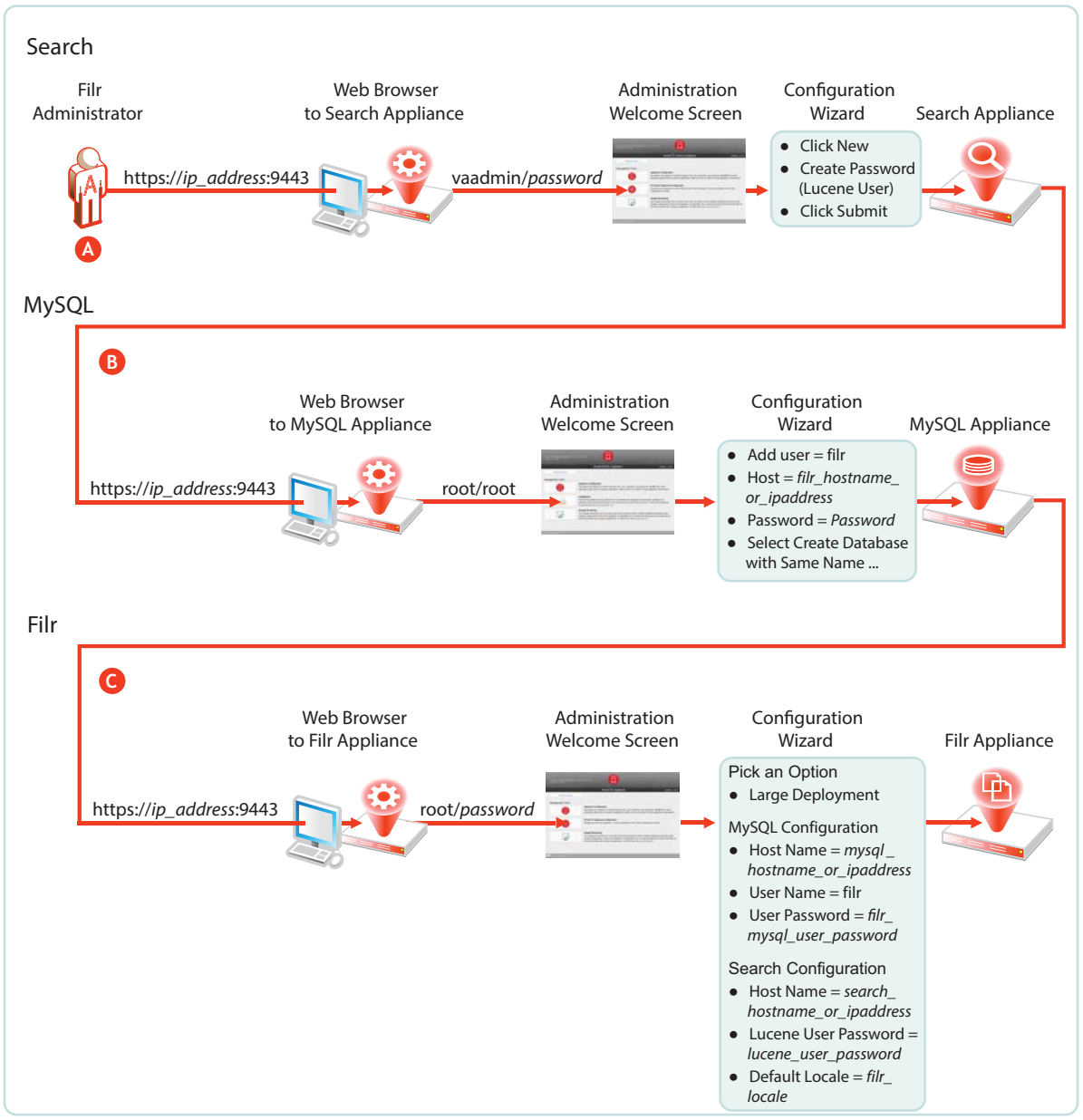
For more information, see“Configuring a Small Deployment for the First Time” in the *Filr 2.0: Installation and Configuration Guide*.

2.3.2 Large Filr Deployment Configuration

Starting and configuring the appliances for a large deployment is more involved than for a single appliance. However, the process is well documented and also very straightforward, as illustrated in Figure 2-7 and explained in the table that follows it.

Notice that the order of working with the three appliance types is reversed from the order in Figure 2-5 on page 18.

Figure 2-7 *Configuring Separate Appliances*



Letter	Details
A	First, access and configure the Search appliances through a browser, logging in to the administration console, and running the configuration wizard. When you finish this step, your Search appliances are running and ready to provide indexing services for Filr. For details, see "Installing the Search Index Appliance" in the *Filr 2.0: Installation and Configuration Guide*.

Letter	Details
B	Second, access and configure the MySQL database appliance through a browser, or configure your database server. If using the MySQL database appliance, use the phpMyAdmin utility to configure the appliance, as instructed in "Installing the MySQL Database Appliance" in the *Filr 2.0: Installation and Configuration Guide*. When you finish this step, your database appliance is running and ready to provide services to the Filr appliance.
C	Finally, access and configure the Filr appliance through an administrative browser, logging in to the administrative console, and running the configuration wizard. For more information, see "Configuring a Large Deployment for the First Time" in the *Filr 2.0: Installation and Configuration Guide*. When you finish this step, your virtual appliances are all running and working with each other, providing your network with Filr services.

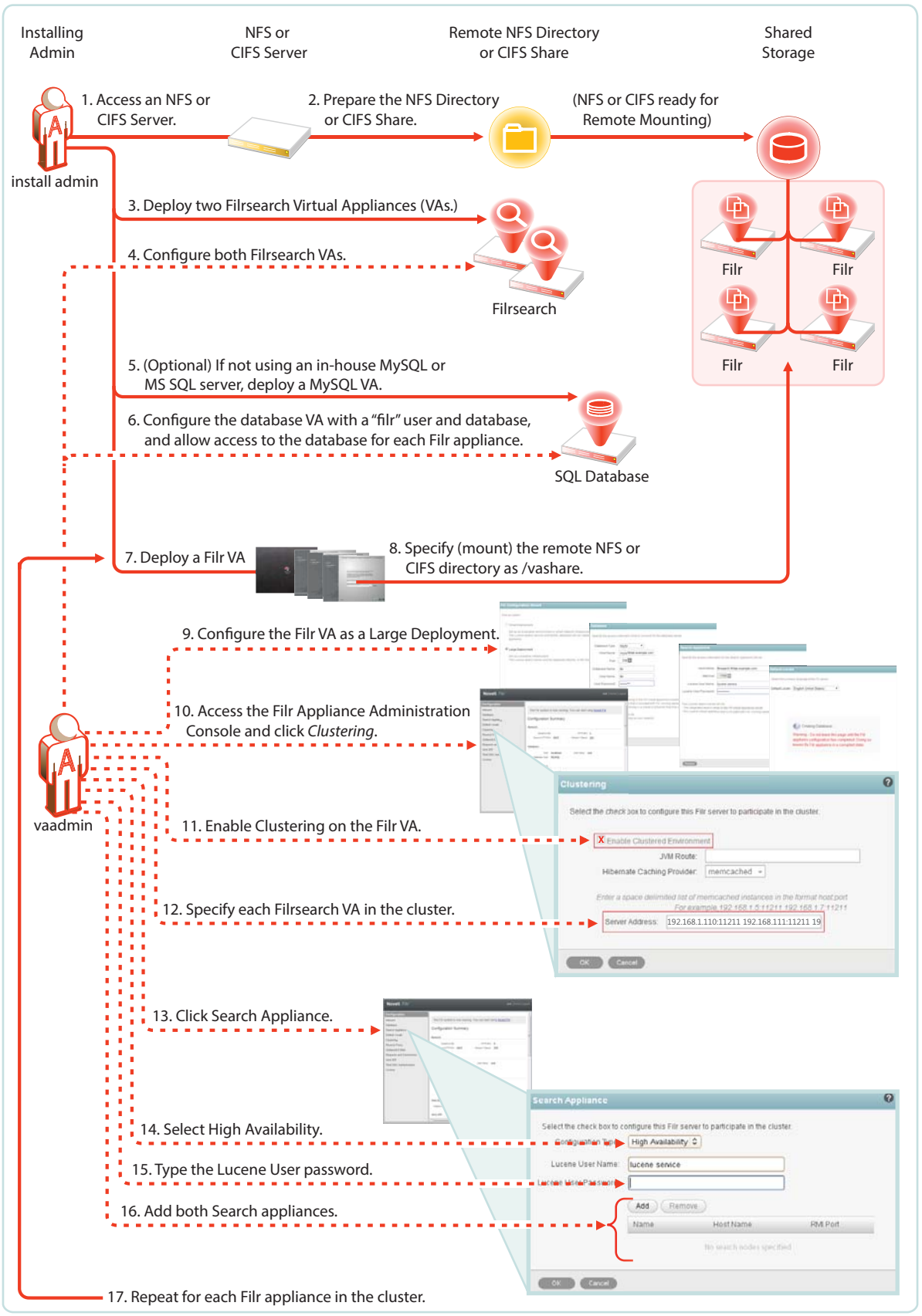
For more information, see"Creating a Large Deployment" in the *Filr 2.0: Installation and Configuration Guide*.

2.4 Filr Clustering (Expanding a Deployment)

Filr clustering involves two or more Filr VAs sharing the same NFS or CIFS data storage location (`/vashare`). You can only create a cluster if your Filr appliances were deployed pointing to the same `/vashare` disk.

Basic steps for setting up Filr clustering are included in Figure 2-8.

Figure 2-8 *Clustered Filr VAs*



For step-by-step instructions, see “Setting Up a Large, Expandable (Clustered) Deployment” in the *Novell Filr 2.0 Planning and Deployment Best Practices Guide*.

For more information about clustering, see “Multi-Server (Clustered) Deployment” in the *Filr 2.0: Installation and Configuration Guide*.

2.5 Integrating Filr Inside Your Network Infrastructure

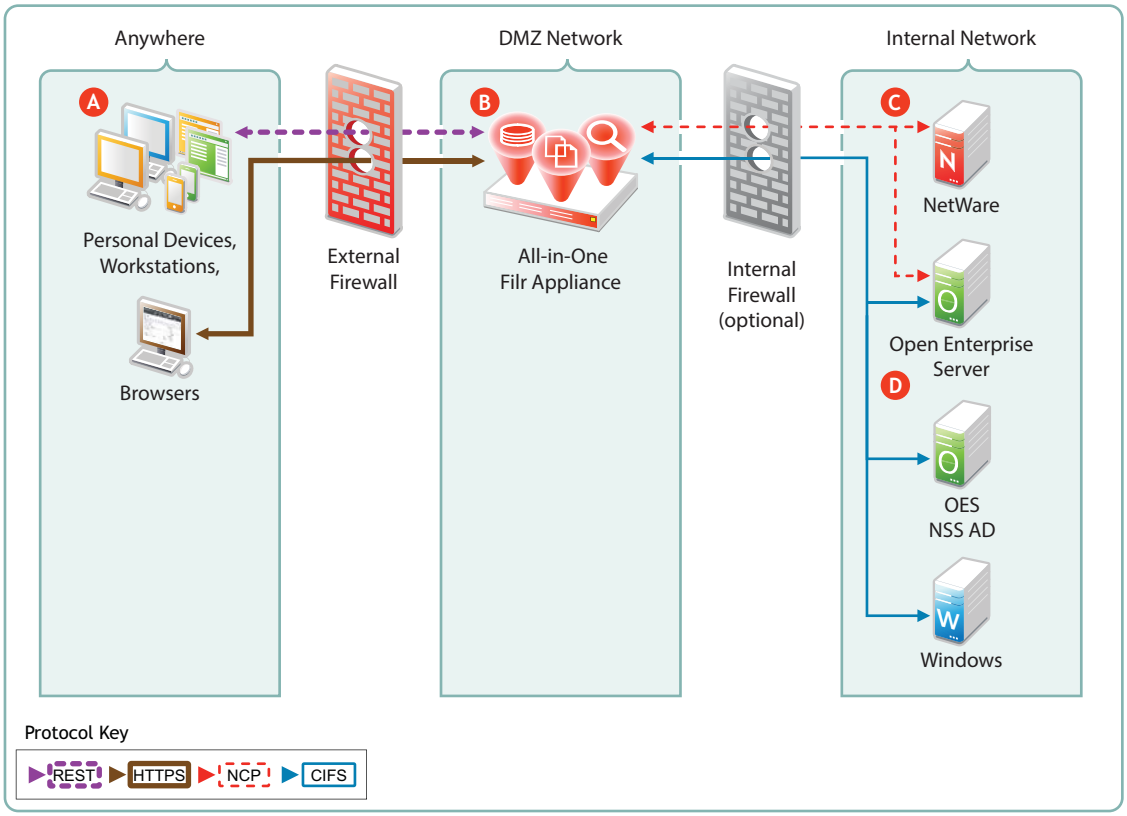
The following examples illustrate two possibilities out of many potential network configurations for deploying Filr.

- Section 2.5.1, “A Small Filr Deployment,” on page 24
- Section 2.5.2, “A Large Filr Deployment,” on page 26

2.5.1 A Small Filr Deployment

Figure 2-9 illustrates a high-level view of how an all-in-one appliance might be integrated into a small organization’s network. Each letter is explained in the table that follows the figure.

Figure 2-9 *Example of a Small Filr Deployment*

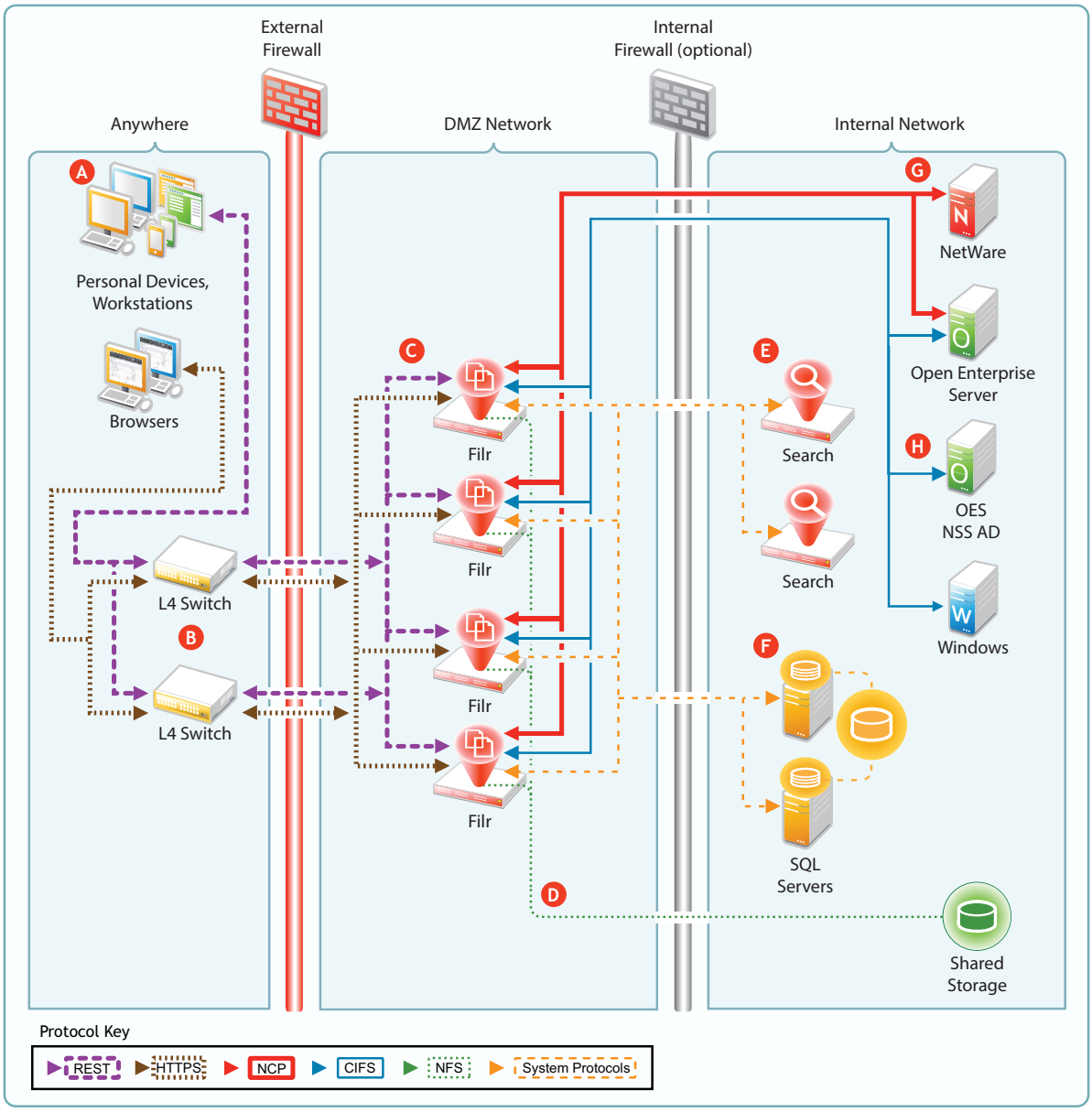


Letter	Details
A	Filr brings Novell and Windows file services to personal devices, Macintosh and Windows workstations, and Web browsers.

Letter	Details
B	Filr is built for fitting in with your security infrastructure and can be deployed in a DMZ network, allowing your organization's data to remain safely inside your internal network.
C	Filr provides full NCP protocol support. Users have access to files stored on both NetWare and Open Enterprise Server file servers.
D	Filr provides full CIFS protocol support to servers providing CIFS file services, such as Windows file servers.

2.5.2 A Large Filr Deployment

Figure 2-10 *Example of a Large Filr Deployment*



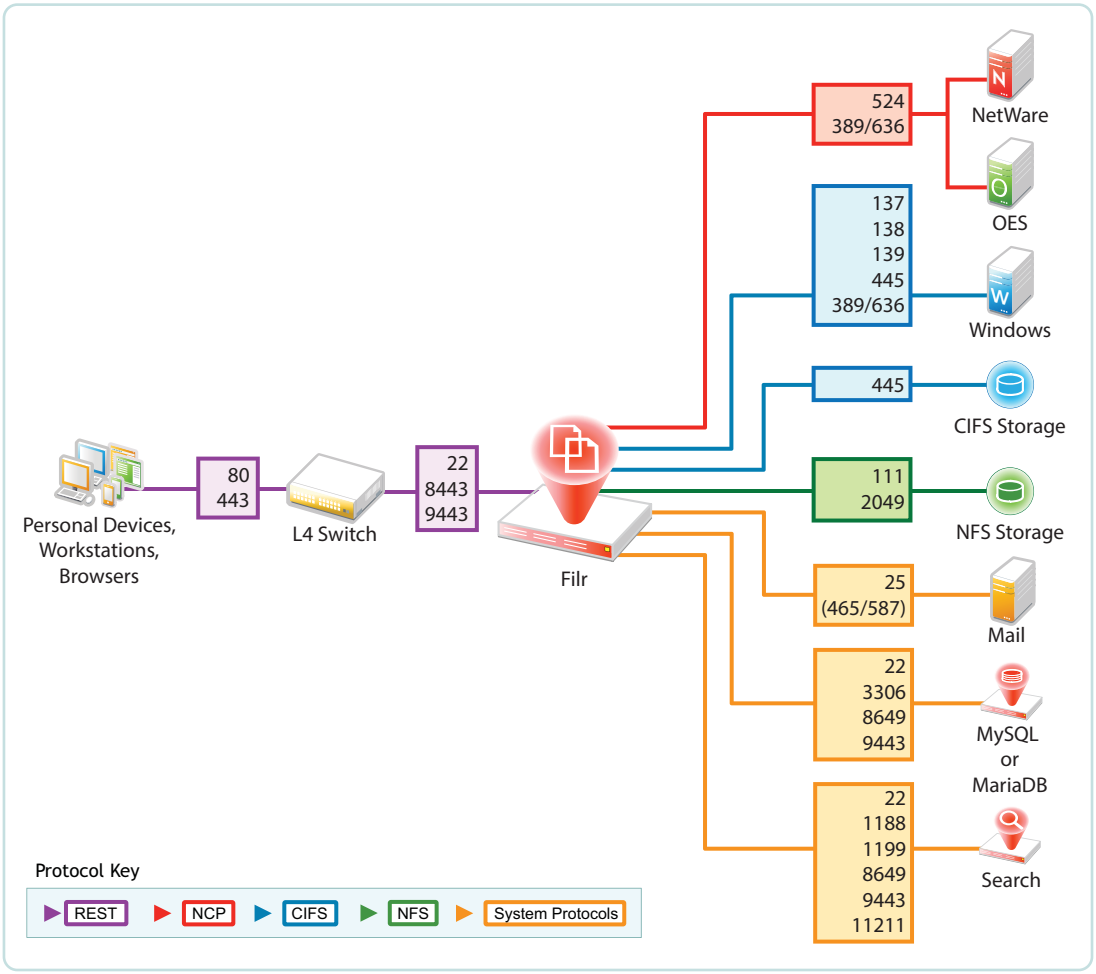
Letter	Details
A	Filr brings Novell and Windows file services to personal devices, Macintosh and Windows workstations, and Web browsers.
B	You can use L4 switches to provide load balancing of REST requests to your Filr appliances. Although not shown, you can, of course, also use software-based load balancers for this.

Letter	Details
C	You can deploy Filr appliances inside a front-end DMZ and configure multiple Filr VAs to share NFS- of CIFS-based storage (D), thus providing scalability and high availability.
D	Shared storage (`/vashare`) lets you expand your Filr deployment to include multiple Filr VAs (C). Although an exported NFS disk is shown in the illustration, CIFS shares are also supported.
E	You can deploy multiple search appliances in an internal network, each of which maintains indexes of Filr data to provide failover for search and other requests coming through the Filr appliances.
F	Your organization's MySQL or MS SQL servers can be deployed in the internal network and configured to access the same database.
G	As with small deployments, this configuration supports NCP file services.
H	CIFS file services are also supported.

2.6 Ports Used in Filr Deployments

Figure 2-11 illustrates the ports that can be used in Filr deployments, including insecure ports. For information on configuring and securing Filr securely, see Setting Up Filr in a DMZ in the Filr 2.0: Administration Guide.

Figure 2-11 *Filr Port Usage*



2.7 There Are No Changes to Existing File Servers or Directory Services

- **File Servers:** Filr requires no changes to existing file servers or directory services. There is no new software to install on existing file servers.
- **File Systems:** There are no changes to existing file systems. File system rights, trustee assignments, storage quotas, and so on are all honored. This is because all file access is controlled by the file systems just as it was before Filr was installed.
- **Directory Services:** There are no schema extensions or other changes required to existing directory services.

3 Filr Administration

Filr administration is very straightforward as outlined in the following sections.

3.1 Filr Administrative Users

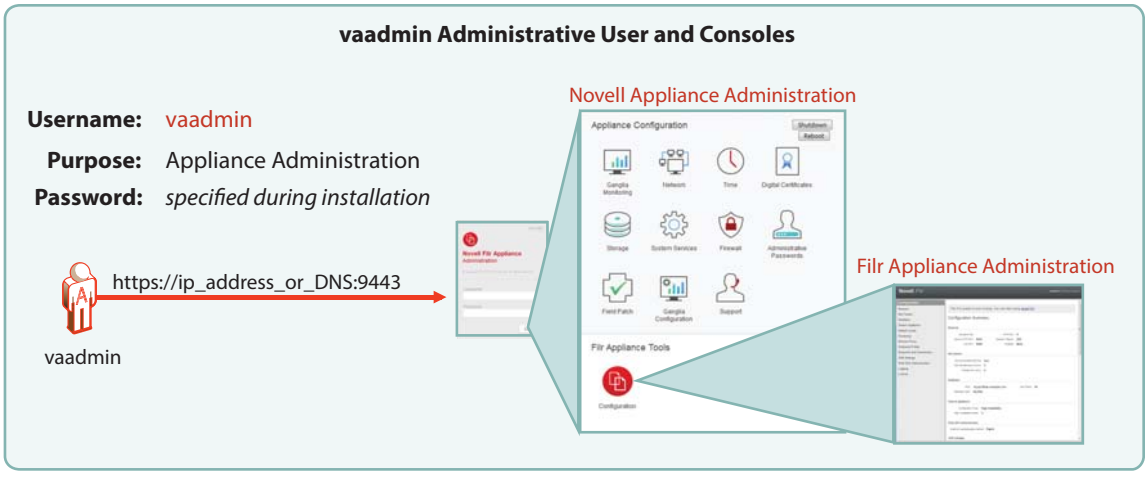
Filr appliances are installed and administered in two phases and require two different administrative users, each with different Web-based administrative tools, as explained in the following sections:

3.1.1 vaadmin

`vaadmin` takes over the installation process after the initial deployment is finished. It then configures appliance services so that they are fully operational.

Use vaadmin to change or adjust appliance settings. For example,

- Installing certificates and licenses
- Adjusting the network configuration
- Setting up Filr clustering



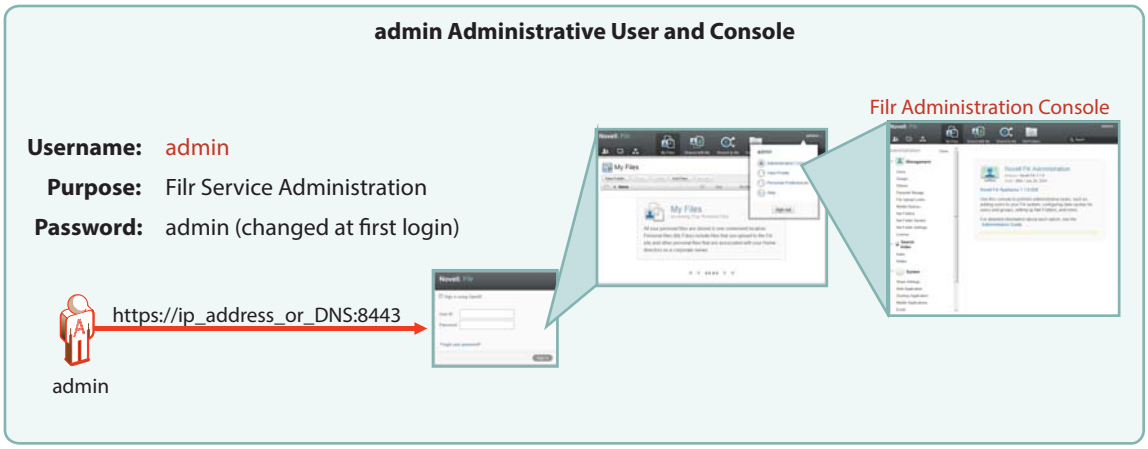
3.1.2 admin

After the appliances are fully operational, most of the administrative work is accomplished using the Filr `admin` user account.

The first time you log in, the username/password are admin/admin. You are prompted to change this. See "Changing the Filr Administrator User ID or Password" in the *Filr 2.0: Administration Guide*.

You use this administrative user to do the following:

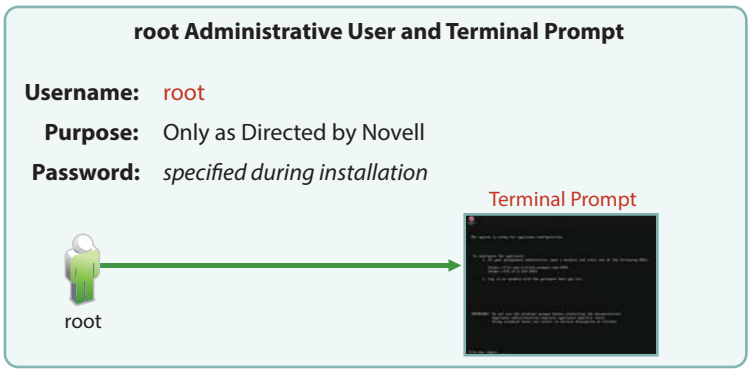
- Import (synchronize) users and groups from LDAP identity stores
- Create additional Filr users
- Set up My Files personal storage
- Set up Net Folders
- Set synchronization schedules
- Manage access
- Manage quotas
- Manage shares



3.1.3 root

Novell Filr and the appliances associated with it are special-purpose virtual machines. They are designed to be configured and managed using the Web-based management consoles (above). Although it is possible to access the appliance using the terminal prompt or through an SSH connection, Novell strongly discourages this practice because it can result in service disruption or more serious problems, including data loss.

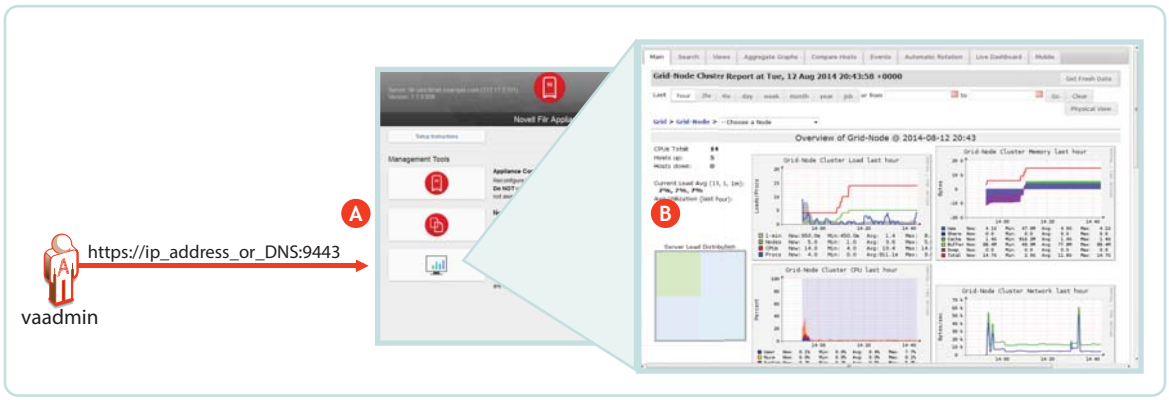
If you contact Novell Support with a Filr support incident, you might be asked to access the appliance's terminal prompt as the `root` user. Otherwise, there are no Filr administrative tasks that involve `root` or the bash interface.



3.2 Ganglia Appliance Monitoring

By launching the Ganglia monitoring page, as shown in Figure 3-1, you can access various real-time monitoring statistics for all of the Ganglia-enabled machines on your network segment.

Figure 3-1 *Ganglia Appliance Monitoring*



Letter	Details
A	The `vaadmin` administrative user has access to Ganglia monitoring, via the Appliance Configuration and Maintenance Web page.
B	At the top of the Ganglia Web page are graphs that represent an aggregation of all of the Ganglia-enabled machines that are being monitored on your network segment. At the bottom of the page are graphs for each machine that is being monitored. By clicking an individual machine's graph, you can get its details. For example, on a Filr appliance you see Filr metrics, `/vastorage` monitoring, CPU load, disk statistics, memory usage, and all of the standard Ganglia metrics.

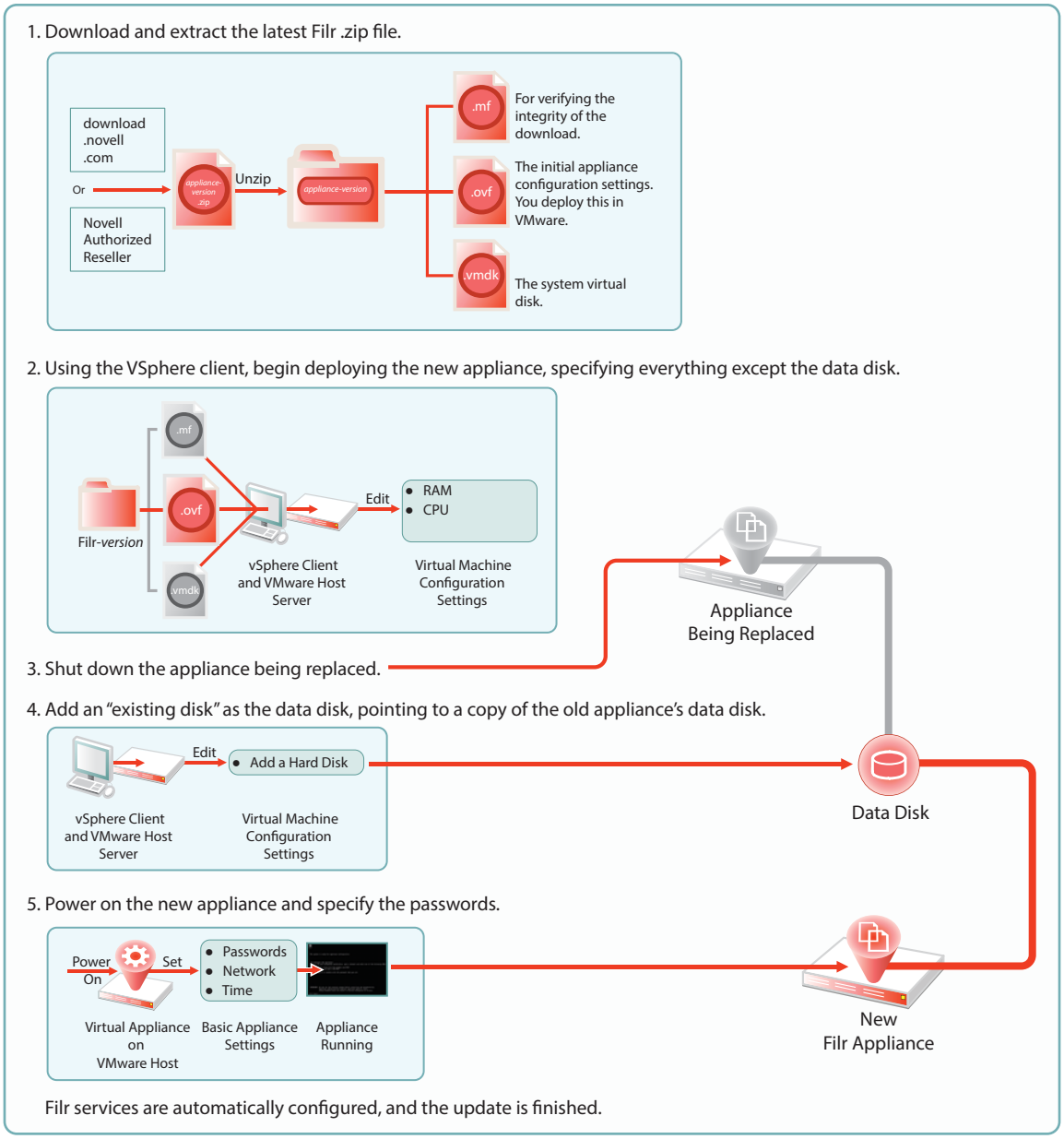
If you want to learn more about using and customizing Ganglia, you might consider investing in publications on the subject, such as the book Monitoring with Ganglia, which was written by developers and others associated with the Ganglia project.

3.3 Updating Appliances

Filr and Search appliances are updated by simply installing a new appliance system disk and linking it to the existing data disk, as illustrated in Figure 3-2.

IMPORTANT: While performing an upgrade, be sure to consult the detailed instructions in "Upgrading Filr" in the *Filr 2.0: Installation and Configuration Guide*. A successful upgrade depends on following sub-tasks that are not illustrated here, such as the order in which appliances are shut down and then restarted.

Figure 3-2 *Updating a Filr or Search Appliance*

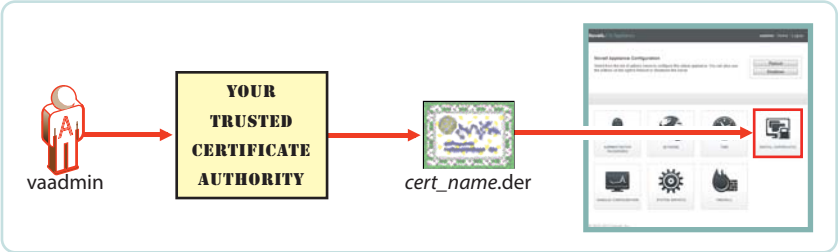


3.4 Certificate Management in Filr

So that your Web client users don't receive security warnings when accessing Filr, we recommend that you configure Filr with a certificate from your CA, as illustrated in Figure 3-3. This will ensure that browsers will trust the Filr appliance as a valid server.

You can also set up Filr as a client to trust other servers. For example, if your LDAP identity store requires SSL communications (LDAPS), you can import the trusted CA certificate from your identity store server.

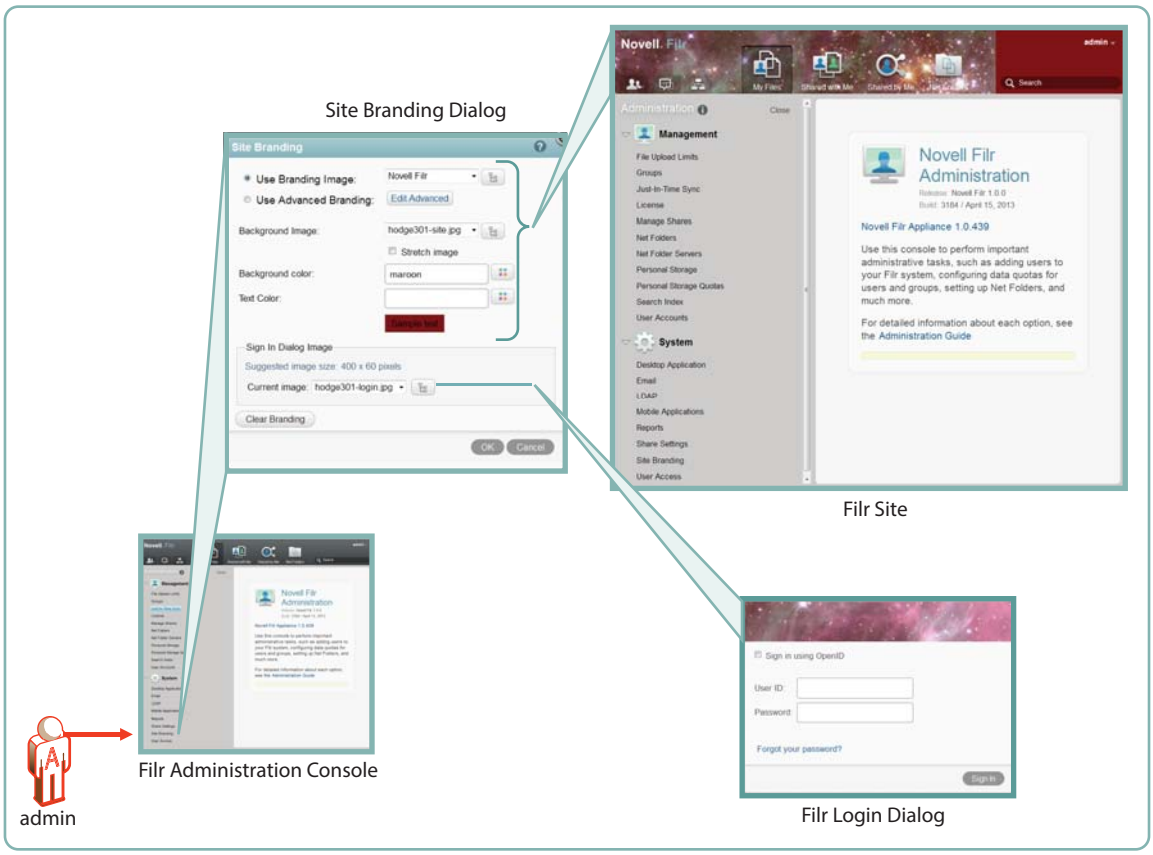
Figure 3-3 *Importing a CA certificate*



3.5 Filr Site Branding

You can customize the colors and images displayed on the Filr site and the login dialog box, as illustrated in Figure 3-4. Customizations are retained when Filr is upgraded. For more information, see "Setting Up Site Branding" in the *Filr 2.0: Administration Guide*.

Figure 3-4 *Branding Filr*



4 Access Roles and Rights in Filr

Filr administrators need to have a good understanding of how Filr leverages the file system and other rights that are already in place, and also how user rights to use Filr functionality are determined.

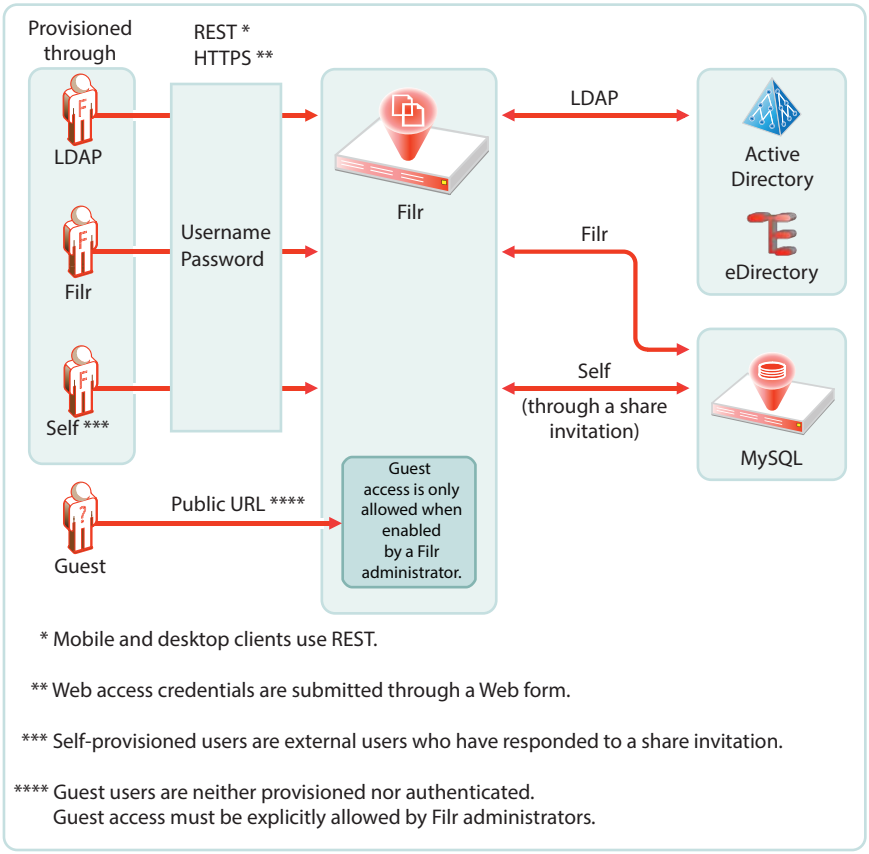
4.1 Filr Authentication

Filr clients for mobile devices and workstations use a REST protocol for Filr authentication. Inside the protocol are the user-supplied credentials. Filr validates these against the identity source (LDAP or local).

Web access is through a Web form that lets Filr take the credentials supplied and validate them as with REST.

This is illustrated in Figure 4-1.

Figure 4-1 *User Authentication in Filr*



4.2 Access to Files and Folders Is Controlled by the File System

The NSS file system on OES and NetWare, the NTFS file system on Windows servers, and the SharePoint Document Libraries on SharePoint servers always control access to the files and folders they contain. Users seeking access through a file browser, such as Windows explorer, must generally have the required permissions on the file system or document library to gain access.

This is absolutely true when accessing files and folders through Filr. You cannot gain more access through Filr than the underlying file system or document library allows.

Sharing through Filr is no exception. Obviously, users must have access to files in order to share them, and they cannot grant a higher shared-access role than they have.

- Shared access to files in Net Folders and Home Folders depends on the Net Folder proxy user having the required file system or document library rights.
- Shared access to folders and files in Personal Storage is controlled by the Filr system itself because the files and folders are contained in Filr-based storage.

4.3 Access Permissions and Filr

- Section 4.3.1, “Access Permissions to Net Folders,” on page 37
- Section 4.3.2, “Access Permissions to My Files,” on page 37

4.3.1 Access Permissions to Net Folders

From a Filr perspective, users can get the required permissions to access files and folders in Net Folders in one of three ways:

- **Directly:** Users are assigned permissions to the files and folders on the file system or SharePoint Document Library where they reside. After they are imported as LDAP users, Filr administrators can then grant them access to the Net Folder. The system then derives a role based on their file system rights.
- **Group Membership:** Users can also inherit permissions to the files and folders through membership in a group that has been assigned the required permissions on the file system. After the group is imported through LDAP and granted access to a Net Folder, group members have the same rights as if they were directly assigned.
- **Shared Access:** Users who receive and accept share invitations to Net-Folder-based files, access the shared files through the Net Folder's assigned proxy user. Each proxy user must have the required permissions on the file systems that are targeted by the assigned Net Folders.

4.3.2 Access Permissions to My Files

My Files can contain Home folders and/or personal storage.

Home folder access is controlled by the file system where the folder is located. Personal Storage is located in Filr-based storage and access is directly controlled by Filr.

- **Direct Ownership:** Filr users have full ownership of their personal files and folders, whether in Filr-based personal storage or in their home folders.
- **Shared Access:** If sharing is enabled at the system level, then by default, users can share their personal folders and files within system constraints.

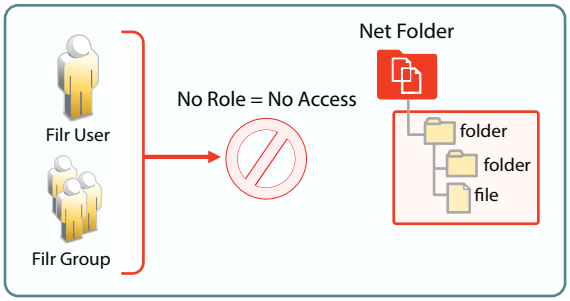
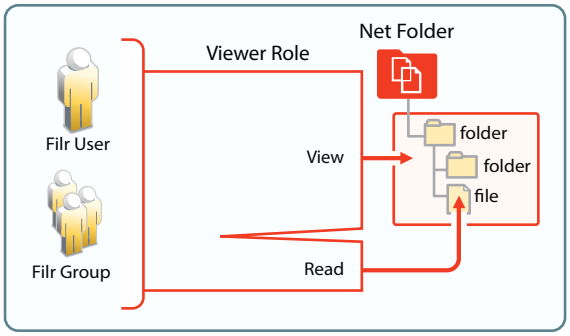
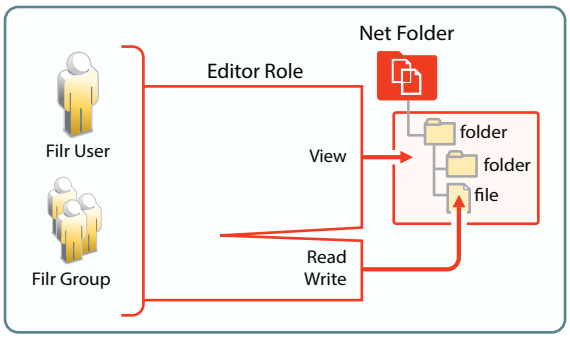
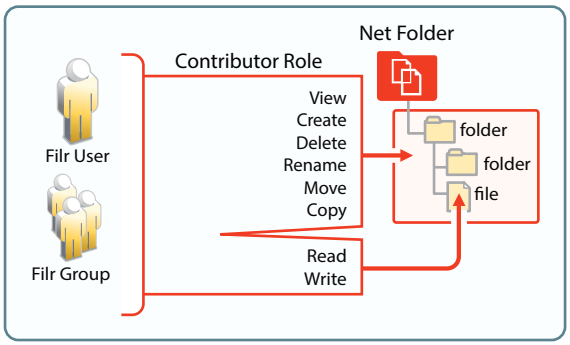
  The sharing process involves assigning a shared-access role to the folder or file being shared.

IMPORTANT: Before granting access to their personal storage, users should clearly understand each shared-access role, especially the Contributor shared-access role, which allows share recipients to rename or delete the shared folder.

4.4 Net Folder Access Involves Four Roles

When users are assigned to a Net Folder, then depending on the rights that users have on the file system or library (see Access Permissions and Filr), Filr assigns them one of four roles, as outlined in Table 4-1.

Table 4-1 *Net Folder Roles and the Rights That They Represent*

Role	Rights Through Filr	Rights Illustrated
None	No rights	
Viewer	• View Net Folder contents • Read existing files	
Editor	• View Net Folder contents • Read and Write to existing files	
Contributor	• View, Create, Delete, Rename, Move, and Copy inside the Net Folder • Read and Write to existing files .	

The file system and library rights required for each Net folder role are illustrated and explained in the following sections.

- Section 4.4.1, “Net Folder Roles are Derived, Not Assigned,” on page 39
- Section 4.4.2, “Net Folder Role Requirements on NSS File Systems,” on page 39

- Section 4.4.3, “Net Folder Roles on NTFS File Systems,” on page 40
- Section 4.4.4, “Net Folder Roles on SharePoint,” on page 41

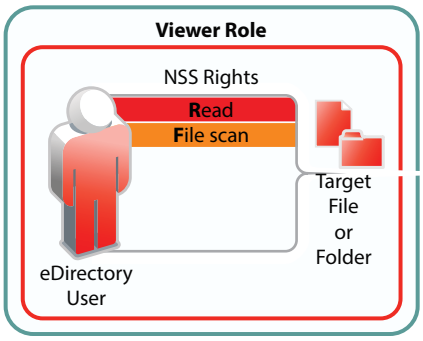
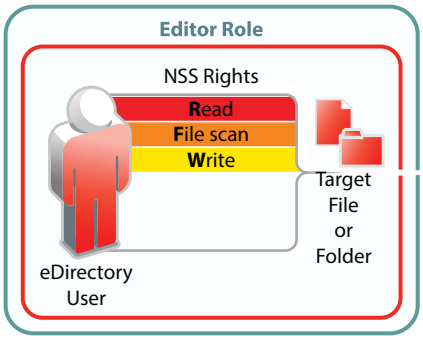
4.4.1 Net Folder Roles are Derived, Not Assigned

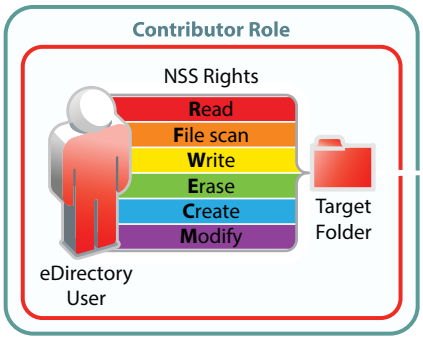
For Filr users to access Net Folders, Filr administrators must simply grant them access. Granting access is the only Net Folder access control mechanism in Filr. Net Folder Roles are not assigned; they are derived from the access rights that users have on the target file systems, as outlined in the sections that follow.

4.4.2 Net Folder Role Requirements on NSS File Systems

For eDirectory users to function in Net Folder roles, they must have the NSS rights illustrated and explained in Table 4-2. If the minimum requirements for the Net Folder Viewer role are not met, they have no access through Filr as explained in Section 4.7, “Net Folder Role Requirements Are Rigidly Enforced,” on page 46.

Table 4-2 *NSS File System Rights Required for Net Folder Roles*

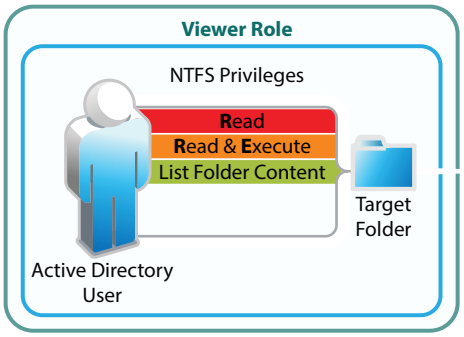
Role and Minimum NSS Rights Required	Comments
	To view files through Filr, eDirectory users must have both `Read` and `File Scan` file system trustee rights on the target file or folder.
	To modify file content through Filr, eDirectory users must have the `Write` file system trustee right in addition to `Read` and `File Scan`.

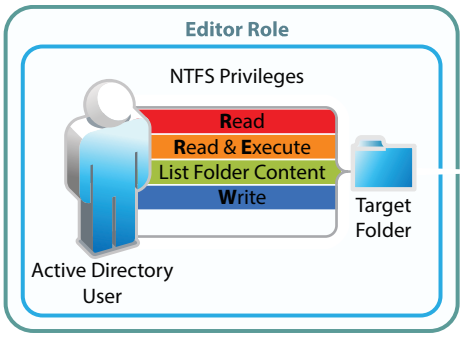
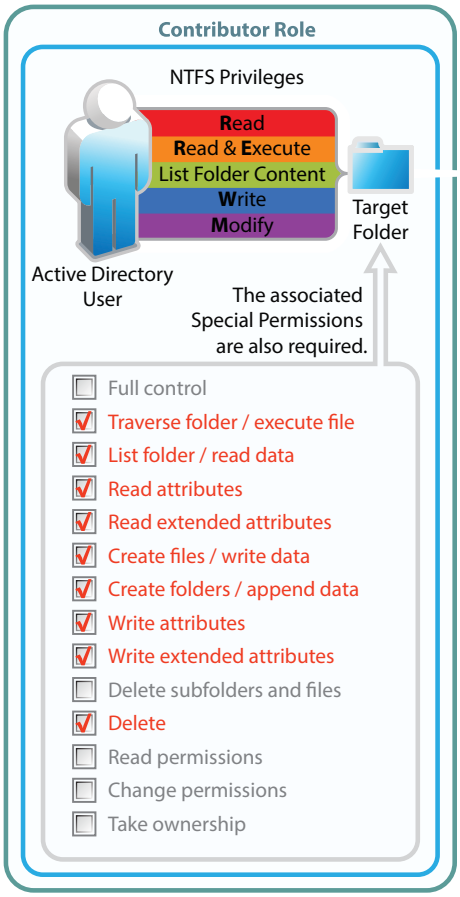
Role and Minimum NSS Rights Required	Comments
	To perform contributor functions, eDirectory users must either have • All file system trustee rights to the file or folder (except for `Access Control`) Or • The `Supervisor` right to the file or folder The presence or absence of `Access Control` has no meaning in Filr because Filr cannot modify file system trustee rights. A Filr user with the `Access Control` right on the file system cannot grant *file system* access to another user through Filr. It is true that Filr users with sufficient Filr permissions can *share* access to files and folders with other users, but this is a Filr function that leverages the file system rights of Net Folder proxy users. Access to shared files and folders is independent of any file system rights that individual users have or do not have.

4.4.3 Net Folder Roles on NTFS File Systems

For Active Directory users to function in Net folder roles, they must have the NTFS file system permissions illustrated and explained in Table 4-3. If the minimum requirements for the Net Folder Viewer role are not met, they have no access through Filr as explained in Section 4.7, “Net Folder Role Requirements Are Rigidly Enforced,” on page 46.

Table 4-3 *NTFS Permissions Required for Net Folder Roles*

Role and Minimum NTFS Permissions Required	Comments
	To view files and folders through Filr, Active Directory users must have `Read`, `Read & Execute`, and `List Folder Content` basic permissions on the target folder. The default special permissions associated with these basic permissions are also required.

Role and Minimum NTFS Permissions Required	Comments
	To modify file content through Filr, Active Directory users must have the basic `Write` permission in addition to `Read`, `Read & Execute`, and `List Folder Content` basic permissions on the target folder. The default special permissions associated with these basic permissions are also required.
	To perform contributor functions, users must either have ◆ The basic `Full Control` permission Or ◆ The basic `Modify` permission included with the privileges required for the Editor role (`Write`, `Read`, `Read & Execute`, and `List Folder Content`) **IMPORTANT:** The default special permissions associated with these basic permissions are also required as illustrated.

4.4.4 Net Folder Roles on SharePoint

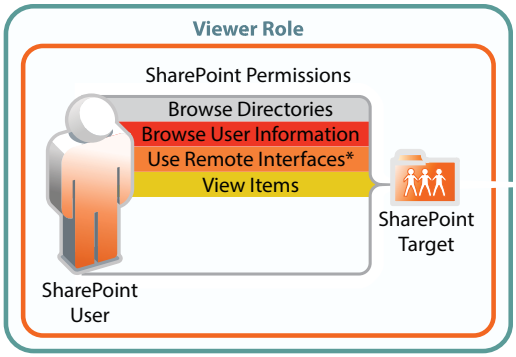
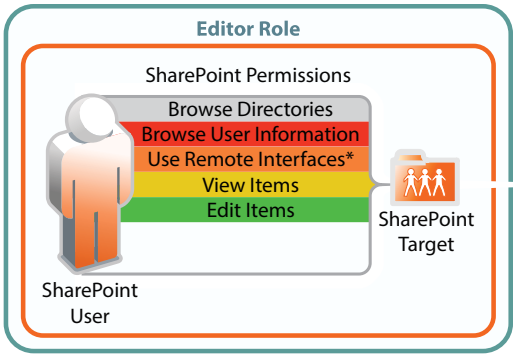
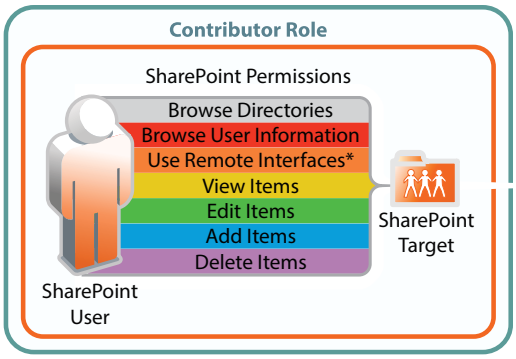
For SharePoint users to function in Net folder roles, they must have the SharePoint permissions illustrated and explained in Table 4-4. If the minimum requirements for the Net Folder Viewer role are not met, they have no access through Filr as explained in Section 4.7, “Net Folder Role Requirements Are Rigidly Enforced,” on page 46.

IMPORTANT: It is a common practice for SharePoint administrators to create customized permission lists that do not include the `Use Remote Interfaces` permission.

Filr uses a REST interface to communicate with the SharePoint system. Therefore, you must ensure that the `Use Remote Interfaces` permission is enabled for all SharePoint users and groups that access Filr. Otherwise, those using desktop clients and mobile devices will not be able to access SharePoint using Filr.

The `Use Remote Interfaces` permission is marked with an asterisk (*) in Table 4-4 below to emphasize this point.

Table 4-4 *SharePoint Permissions Required for Net Folder Roles*

Role and Minimum SharePoint Permissions Required	Comments
	To view files and folders in SharePoint document libraries, SharePoint users must have the `Browse Directories`, `Browse User Information`, `Use Remote Interfaces*`, and `View Items` permissions in the document libraries.
	To modify file content, SharePoint users must have the `Edit` permission in addition to the permissions required for the Viewer role.
	To perform contributor functions, users must have the `Add Items` and `Delete Items` permissions in addition to all of the permissions required for the Viewer and Editor roles.

NOTE: SharePoint integration with Filr is available only when you purchase an enhanced Filr license.

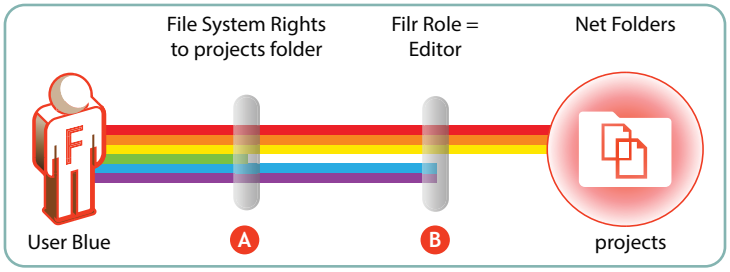
4.5 User Access Inside Filr

The Filr User Interface lets users access files in different categories. The My Files category can contain files from two different locations: Home folders or Personal Storage.

4.5.1 Net Folders

Users who are granted access to a Net Folder are not restricted by Filr. The file system of the target folder retains complete access control. The level of rights that users have through Filr depends on the system-derived role they have, as explained in, “Net Folder Access Involves Four Roles (page 37).” Roles are automatically derived from users’ permissions on NSS and NTFS file systems, and on SharePoint document libraries.

Figure 4-2 *Users’ effective rights to Net Folders are controlled by the file system or library where the Net Folder resides and the Net Folder role that these rights qualify them for*

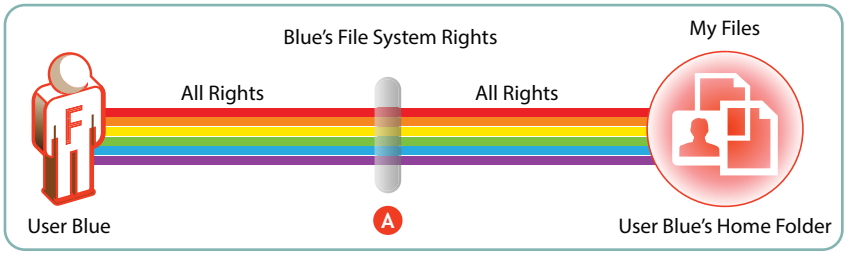


Letter	Details
A	User Blue is granted all rights to the NSS-based `projects` folder, except the `Erase` right (green bar).
B	Because User Blue doesn’t have the `Erase` right, Filr assigns the Editor role. This means that even though Blue has `Create` (blue) and `Modify` (purple) rights on the file system, and could exercise them through a file browser, such as Windows Explorer, Blue’s Filr functionality is limited to editing files within the `projects` folder.

For more information, see Section 10.5, “Granting Access to Net Folders,” on page 74.

4.5.2 My Files (Home Folders)

Users should have all rights to their server-based home folders.



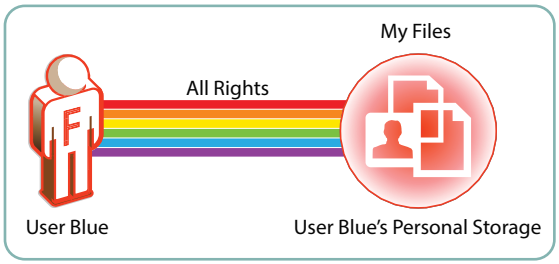
Letter	Details
A	Although it is certainly possible that an administrator might choose to limit the file system rights to a home folder, that would seem to defeat the whole purpose behind providing home directories in the first place. Of course, rights restrictions are completely separate from limiting the available file storage space. In all cases, if there are file system restrictions, Filr honors them.

4.5.3 My Files (Personal Storage)

Users automatically have all access rights to the Filr-based personal storage assigned to them.

To be available to users, personal storage must be administratively enabled because it is turned off by default.

Figure 4-3 *Filr users have all rights to their personal storage through My Files*



For more information regarding My Files, see Chapter 9, "My Files (Personal Storage)," on page 61.

4.5.4 Shared with Me

User shared-access roles relative to Shares are assigned by the user sending the invitation.

Users sending invitations can only assign shared-access roles up to the level that they have.

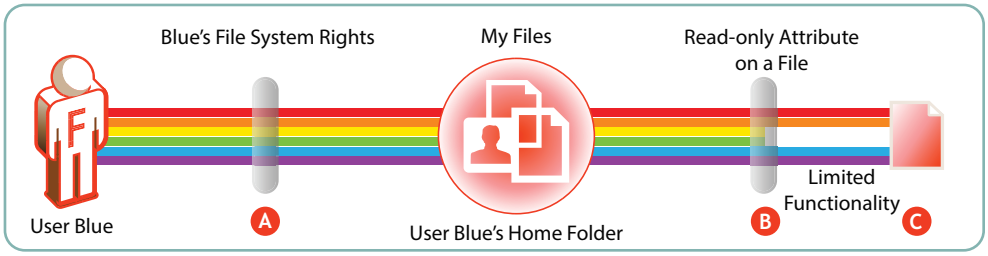
Users receiving and accepting share invitations might or might not have direct rights on the file system or in SharePoint, but that is irrelevant when accessing a file through a share. Individual user rights do not apply to shared items. Shared items in Net Folders (including Home Folders) are accessed on behalf of users by the Net Folder proxy user; shared items in personal storage are accessed through the Filr system itself.

NOTE: Shared files that live in SharePoint are not accessed through Shared with Me, but rather in Net Folders. However, the same principles apply as explained in this section.

For example, if a user already has Viewer access to a file in a SharePoint Net Folder and someone shares the file with the user and grants Editor shared-access role, the user then has Editor access for that file within the Net Folder.

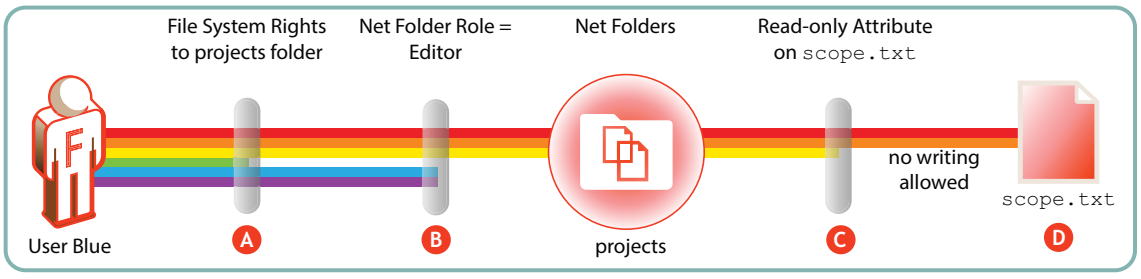
4.6 File Attributes Are Always Honored

Figure 4-4 *File attributes affect functionality in home folders*



Letter	Details
A	User Blue is granted all rights to an NSS-based home folder.
B	Using a file browser, such as Windows Explorer, Blue applies the Read-only attribute to one of the files in the home folder to ensure that it doesn't get modified by mistake.
C	A few weeks later, Blue opens the file through Filr and having forgotten about the Read-only attribute, tries to change it. The file system doesn't allow this because of the file's Read-only attribute. Of course, Blue could remove the attribute using a file browser and then modify the file. Filr always honors the file system. As long as the file is Read-only, it cannot be modified through Filr.

Figure 4-5 *File attributes also affect functionality in Net Folders*



Letter	Details
A	As shown in Figure 4-2 on page 43, Blue doesn't have `Erase` rights on the `projects` folder.
B	Therefore, Blue only qualifies for the Filr Editor role.
C	The project leader maintains strict control of the `scope.txt` file by using the `Read-only` attribute.
D	This means that, even though Blue is an Editor in the `projects` folder, the `scope.txt` file is off-limits for making any changes.

4.7 Net Folder Role Requirements Are Rigidly Enforced

On NSS, NTFS, and SharePoint, it is possible to define customized permissions. For example, you can create a directory in which users can create files even though they have no permission to view them afterward.

Customized permissions do not apply to Filr.

The NSS, NTFS, and SharePoint requirements set forth in Table 4-2, Table 4-3, and Table 4-4 are very rigid.

If any permissions are missing for a given role, Filr defaults to a more restrictive role.

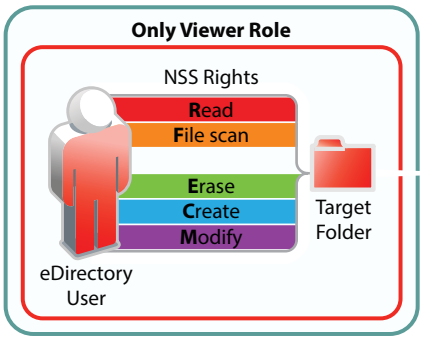
For NSS, the permissions must all be available as either user/group rights or container rights because, unlike the NSS file system, Filr doesn't combine the two (see Section 4.8, "Filr Roles and NSS File System Rights Might Not Match," on page 48).

Additionally, if each and every permission required for the Viewer role is not present, then Filr grants no role to the user, as illustrated in the following sections.

4.7.1 NSS Example

Figure 4-6 shows that if the NSS `write` right is missing, the user can only function as a viewer, even though all of the other Contributor-level rights are present.

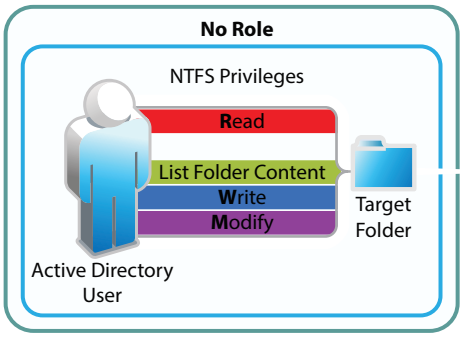
Figure 4-6 Missing Write right limits to only Viewer role



4.7.2 NTFS Example

Figure 4-7 shows that for NTFS, if the `Read & Execute` privilege is missing, the user has no Net folder role, even though all of the other permissions are present.

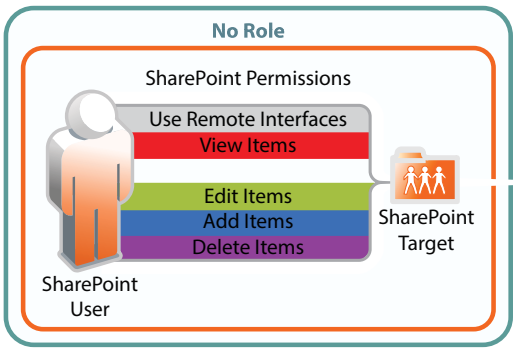
Figure 4-7 Missing Read & Execute privilege prevents access through Filr



4.7.3 SharePoint Example

Figure 4-8 shows that, for SharePoint, if the `Browse User Information` privilege is missing, the user has no Net folder role, even though all of the other permissions are present.

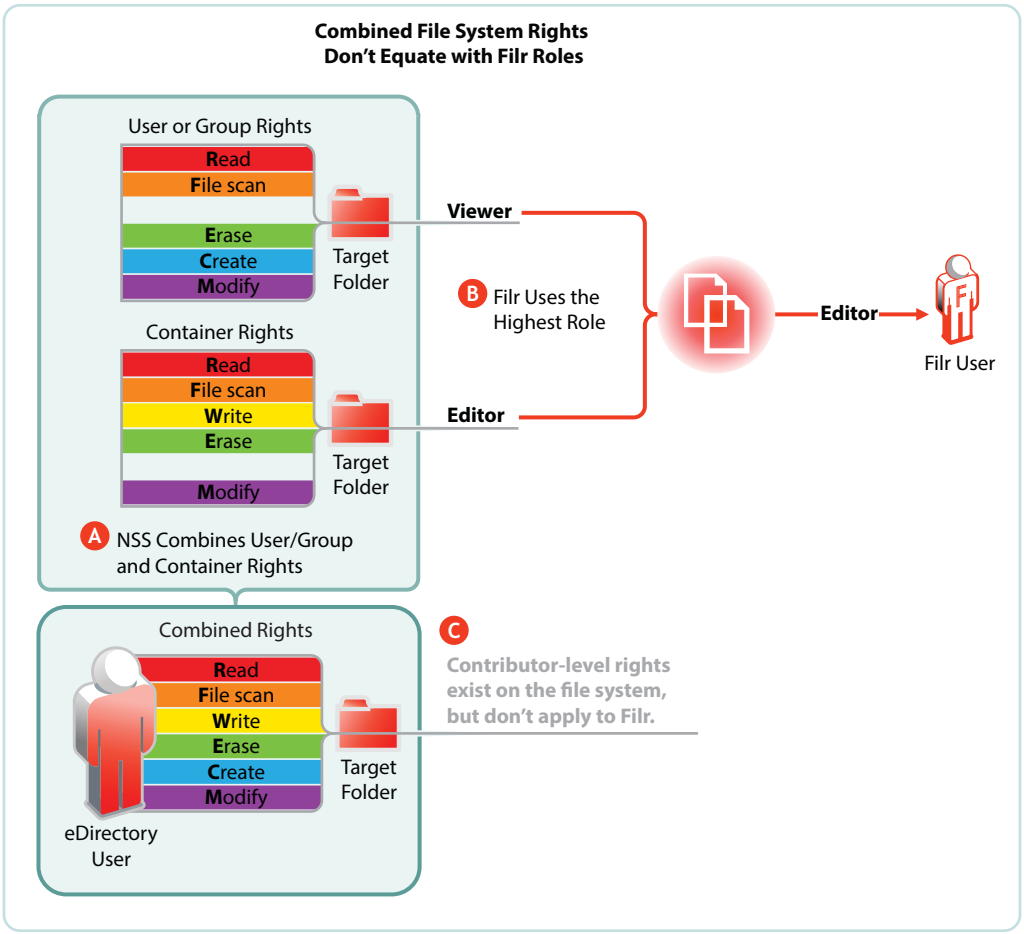
Figure 4-8 Missing Browse User Information permission prevents access through Filr



4.8 Filr Roles and NSS File System Rights Might Not Match

Figure 4-9 illustrates that NSS file system rights are calculated differently than Filr roles on NSS-based Net Folders.

Figure 4-9 *Roles and Rights Might Not Match*



Letter	Details
A	◆ NSS combines User/Group rights and Container rights to derive File System rights.
B	◆ Filr uses the highest role derived from either ◆ The assigned User/Group rights or ◆ The assigned Container rights
C	◆ Filr doesn't consider the combined NSS file system rights when deriving Net Folder roles In this case, the Contributor right would be available to the Filr user only if the Write right were added as a User or Group file system rights, or the Create right were added as a Container file system right.

4.9 Sharing Rights

In contrast to file and folder rights, which are controlled by the file system, Filr controls all My Files and Net Folder sharing.

For more information about sharing, how it is managed, and how it works, see Chapter 12, “Sharing through Filr,” on page 77.

4.10 Windows Share Rights Don’t Affect Filr

Windows Shares are leveraged by Filr to create Net Folders. It might seem logical, therefore, that the rights settings exposed on the **Sharing** tab in Windows would affect Filr functionality. That is not the case.

Setting Windows Share rights on a Windows Share has no effect on Filr. This is in keeping with the best practice recommendation from Microsoft that Share rights not be used to grant or control file access.

Remember, Filr Sharing is only enabled through the Net Folder proxy user and the file system privileges assigned to it.

4.11 Access-based Enumeration (Windows) Doesn’t Affect Filr

Access-based Enumeration settings on an NTFS file system have no effect on Filr.

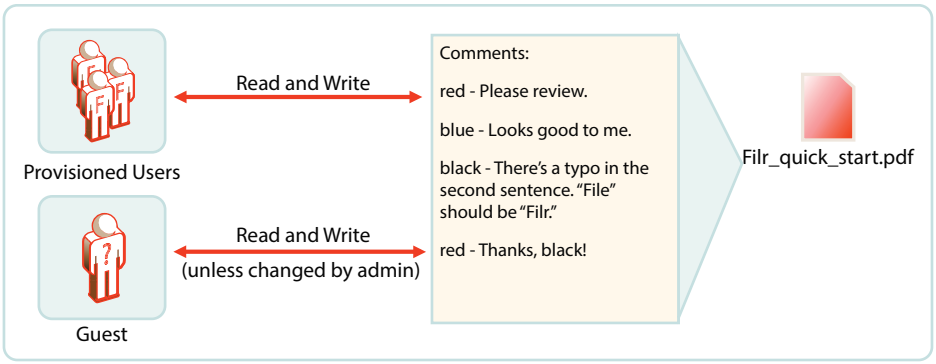
For example, a Windows administrator might disable Access-based Enumeration so that the files in a shared folder always display in Windows Explorer no matter what the user’s rights.

The administrator might then expect that users would also be able to see the files through Filr. That is not the case. Disabling Access-based Enumeration has no effect on Filr. Only those users who have all of the NTFS permissions required for the Viewer role (Read, Read & Execute, and List Folder Content) can see the files.

5 Filr Comments

Comments are linked to the files that are commented on. All users, including Guest, have Read and Write access to comments on the files and folders that they are allowed to see. If there is a risk of Guest users logging inappropriate comments, rights can be changed to Read Only, as indicated in Figure 5-1.

Figure 5-1 *Who Can Log Comments in Filr*

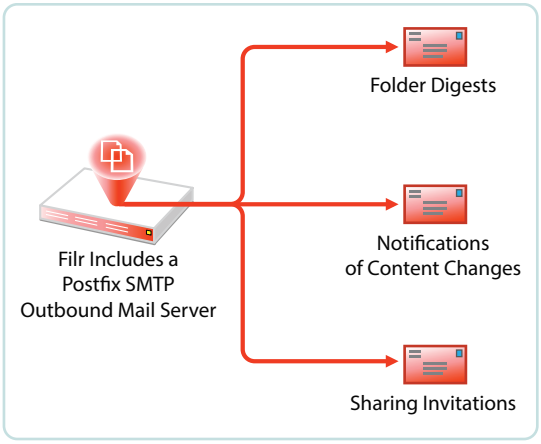


For more information about Filr comments, see "Comments" in the *Filr 2.0: Administration Guide*.

6 Filr Email Notifications

Filr includes a Postfix mail server for outbound email notifications, as illustrated in Figure 6-1.

Figure 6-1 *Filr Outbound Email Functionality*



Although the default mail server should work well for most Filr installations, you can configure Filr to use your outbound SMTP mail server. For more information, see "Configuring Outbound Email Services" in the *Filr 2.0: Administration Guide*.

Beginning with Filr 2.0, you can also customize parts of the email notifications that are generated by Filr, For more information, see "Customizing Email Templates" in the *Filr 2.0: Administration Guide*.

7 Filr Search Appliance—Accessibility, and Searchability

The Filr Search (Lucene) appliance performs critical functions within Filr deployments as described in the following sections.

7.1 "Indexing" Refers to Two Linked but Separate Processes

The term "Indexing" as used in Filr can become a bit confusing. There are two types of indexing that are handled by the Filr Search appliance:

- **Metadata Indexing:** For files, folder, users, and groups to be visible and accessible in Filr, their associated metadata must be transferred to the Filr system and processed or indexed. The process of making objects visible in Filr is described in Section 14.1, "How Filr Makes Files and Folders Visible to Users," on page 89 and Section 16.3, "How Filr Makes LDAP Users and Groups Visible," on page 103.
- **Content Indexing:** Only after file metadata has been indexed can Filr begin processing the words in files for searchability. For details about this process, see Section 7.4, "About File-Content Searchability," on page 57 and Section 13.3, "Net Folder File Content Indexing Overview," on page 87.

7.2 Object Accessibility Requires Search Appliances

7.2.1 Only Objects That Have Their Metadata Indexed Are Accessible

Administrators and users can only access a file, folder, user, or group in Filr after

1. The Search server has processed/indexed the associated metadata for the file, folder, user, or group that has been synchronized to the SQL database.
2. The resulting metadata index is stored in the SQL database.

As objects have their metadata synchronized and indexed by Filr Search, they become accessible. If the metadata index is unavailable because the Filr Search appliance is down, objects disappear from Filr.

7.2.2 Both Metadata Indexing and Content Indexing Require Planning

For new Filr deployments, the initial processing/indexing of file and folder metadata can take anywhere from a few seconds to a few hours, depending on the number of files and folders involved.

Content indexing for searchability can take much longer.

Therefore, anticipating the time that will be required to get Filr services functioning is important and requires that you complete the process described in "Planning the Amount of Data to Synchronize" in the *Filr 2.0: Administration Guide*.

After the initial synchronization and indexing of file and folder metadata and content is complete, Filr handles metadata and content changes quickly and automatically.

NOTE: User and group metadata processing happens as the objects are created and doesn't require separate planning.

7.2.3 Having Two Search Servers Is Critical

Because Filr requires an accessible metadata index, if the only available search server goes down or if its index is lost (for example during an metadata index rebuild), access to files and folders, etc. is also lost (at least temporarily). For this reason, Novell strongly recommends that every large deployment have two search servers. (See "Setting Up Two Filr Search Appliances" in the *Novell Filr 2.0 Planning and Deployment Best Practices Guide*.)

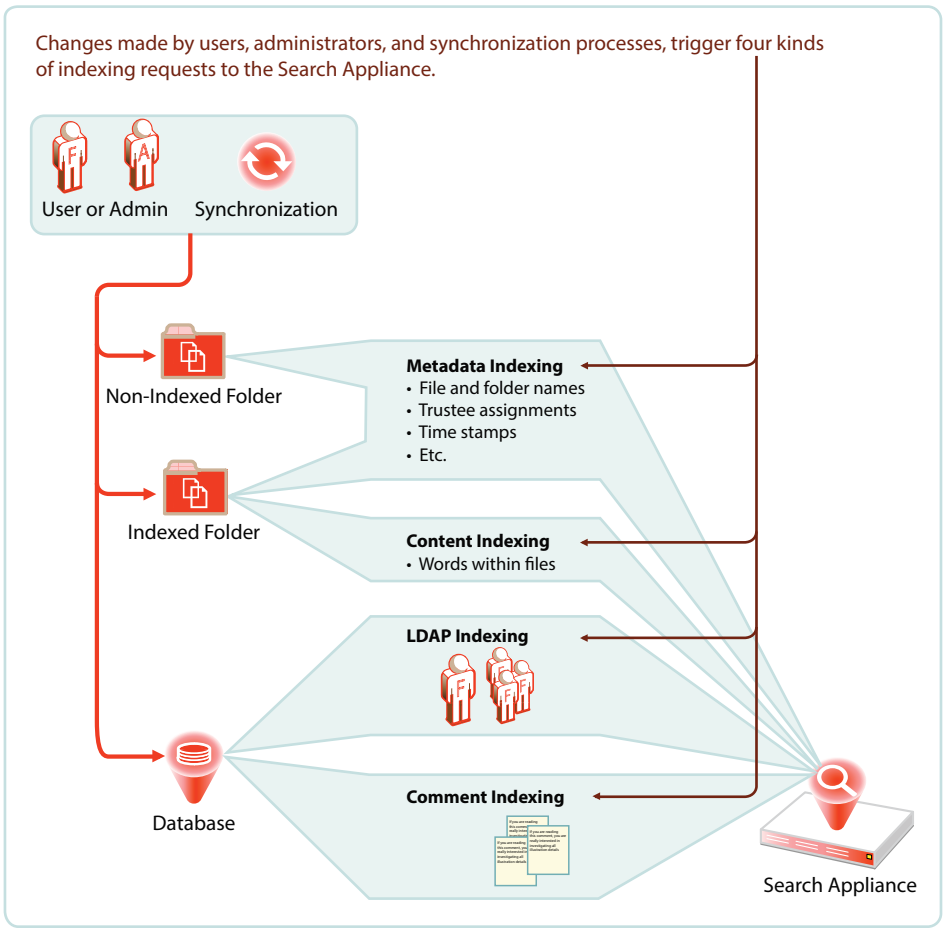
7.3 What Is Indexed and When

As illustrated in Figure 7-1, indexing occurs each time that Filr detects a data change. Index triggers include the following:

- Modifications made by a user or administrator
- Synchronization of files and folders

  When a folder is indexed, the only files re-indexed are those whose time stamps or hash sums have changed since the last index was performed.
- Synchronization of users and groups

Figure 7-1 When Indexing Occurs



7.4 About File-Content Searchability

7.4.1 FAQs

- **When Does Content Indexing Begin?** After all file and folder metadata has been indexed for accessibility.
- **Is My Files Content Searchable?** Yes. Files in home folders and personal storage are always indexed for searchability.
- **What About Net Folders?** Net Folders must be enabled for indexing as described in “Configuring and Managing Net Folder Servers” and “Creating and Managing Net Folders” in the *Filr 2.0: Administration Guide*.

7.4.2 Content Indexing Is Resource-Intensive

Although content indexing is performed as a background process, it is resource-intensive.

Depending on the number of files, initial content indexing can take hours or even days.

It is vital to carefully define your organization's content-indexing scope by carefully identifying exactly which files your organization requires to be content-searchable.

7.4.3 More Information

For an overview of when indexing occurs in conjunction with Net Folder synchronization, see Section 13.2, "Net Folder Synchronization Detail Overview," on page 85.

Filr indexing is also discussed in "Managing the Lucene Index" in the *Filr 2.0: Administration Guide*.

8 Filr Licensing

Filr comes with a 60-day evaluation license pre-installed. You must install a full license in order for Filr to continue functioning beyond the 60-day evaluation period.

For instructions on viewing and installing Filr licenses, see “Viewing and Updating the Filr License” in the *Filr 2.0: Administration Guide*.

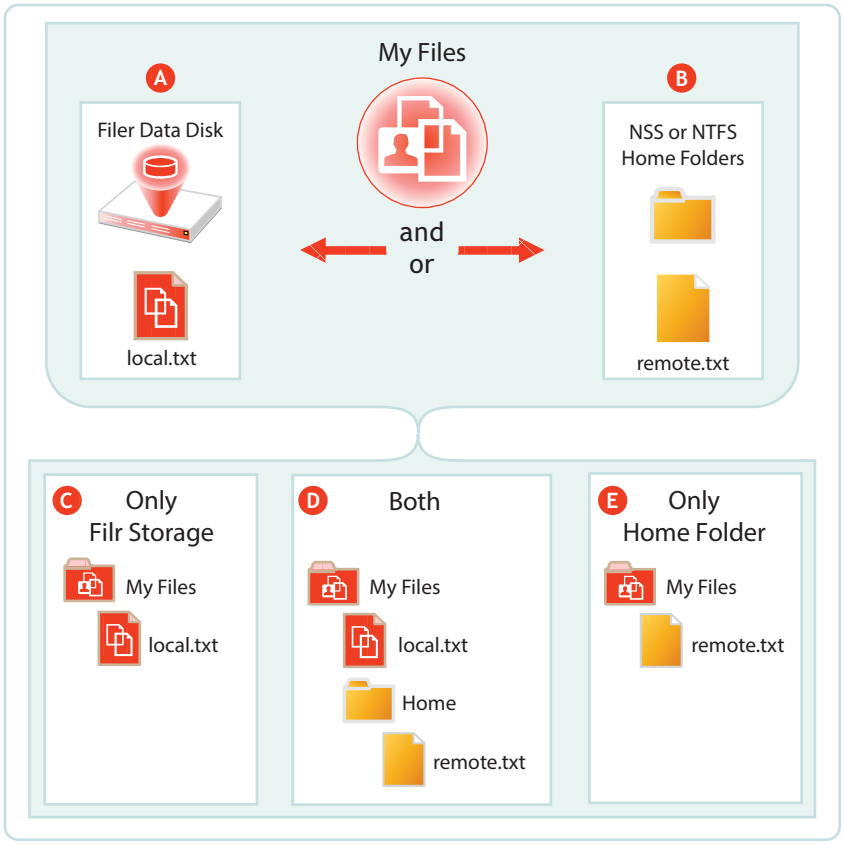
9 My Files (Personal Storage)

Many organizations let their network users store personal files on organization file servers. Filr supports this practice through My Files, which can include access to personal storage on Filr as well as to traditional home directories.

9.1 Understanding My Files

My Files is an optional personal storage area that you can make available to your Filr users. It can include two possible data storage locations, as illustrated in Figure 9-1 and explained in the table that follows it.

Figure 9-1 *My Files' Possible Storage Locations*



Letter	Details
A	If you enable personal storage for users as outlined in Figure 9-2 on page 63, then Filr automatically creates a personal storage directory on its data disk.
B	If your LDAP users have home directory attributes associated with them in the identify store (eDirectory or Active Directory), then when their users accounts are synced, Filr creates special Net Folders that link to their home directories.
C	If you have enabled personal storage for users who do not have home directories as described on the previous row, then those users see only what is stored in the Filr data store in their **My Files**.
D	If you have enabled personal storage for users, and those users also have home directories associated with them in the identity store, they see what is stored in the Filr data store and a folder named **Home** under **My Files.** The **Home** folder provides a distinction between files and folders in the Filr data store and those in Home directories on the file server.
E	If you haven't enabled personal storage, but your users have home directories, then the files and folders in their home directory display as direct entries within **My Files**.

NOTE: Of course, if you don't enable personal storage, and users don't have home directories, then their **My Files** is empty and not usable.

9.2 Enabling Personal Storage

Personal storage can be enabled for all users on the Filr system or on individual users and/or groups level, as fits your organization's needs.

- Section 9.2.1, "Personal Storage for All LDAP Users," on page 62
- Section 9.2.2, "Personal Storage for Individual Users and/or Groups," on page 63

9.2.1 Personal Storage for All LDAP Users

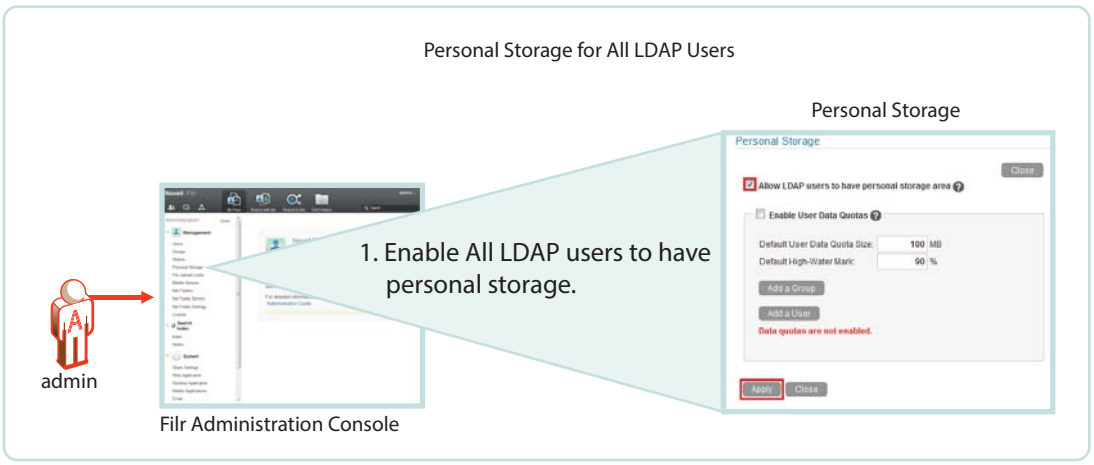
If personal storage is enabled, then space is allocated to users for personal storage. Figure 9-2 illustrates how to enable personal storage for all of the LDAP users on the Filr site.

After enabling personal storage for everyone, you can then use the **Users > More** and/or **Groups > More** menu to disable or modify personal storage settings for individual users and/or groups.

Alternatively, you can choose to not use this dialog at all, but rather enable personal storage for only specific users or groups by using the **Users > More** and/or **Groups > More** menu.

For an overview of personal storage disk space quotas, see Section 9.3, "Restricting Disk Space Usage," on page 64.

Figure 9-2 *Enabling Personal Storage for All Users*

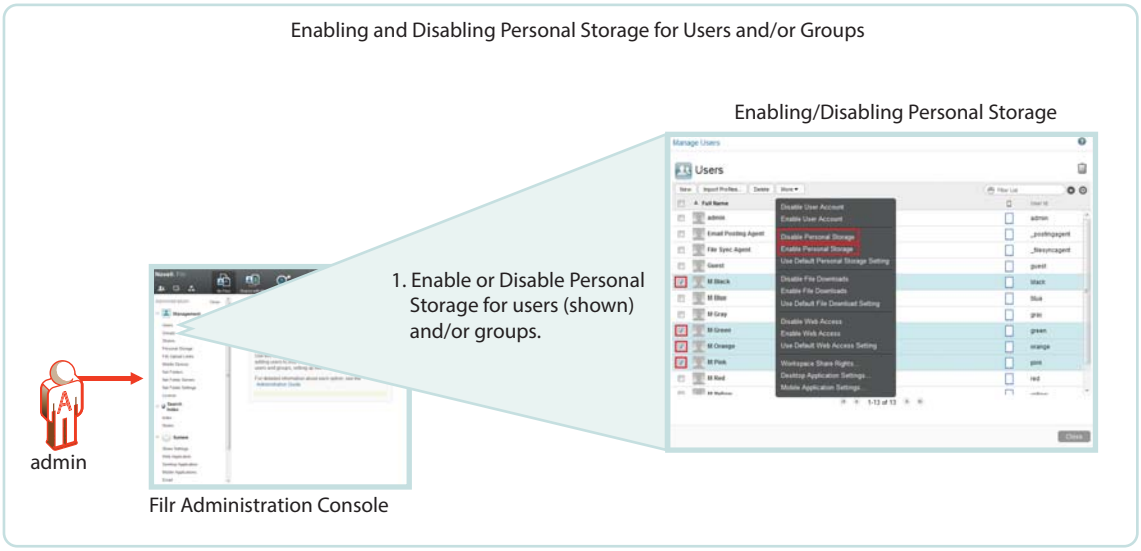


9.2.2 Personal Storage for Individual Users and/or Groups

Filr 1.2 and later lets you directly enable personal storage for individual users and/or groups as illustrated in Figure 9-3.

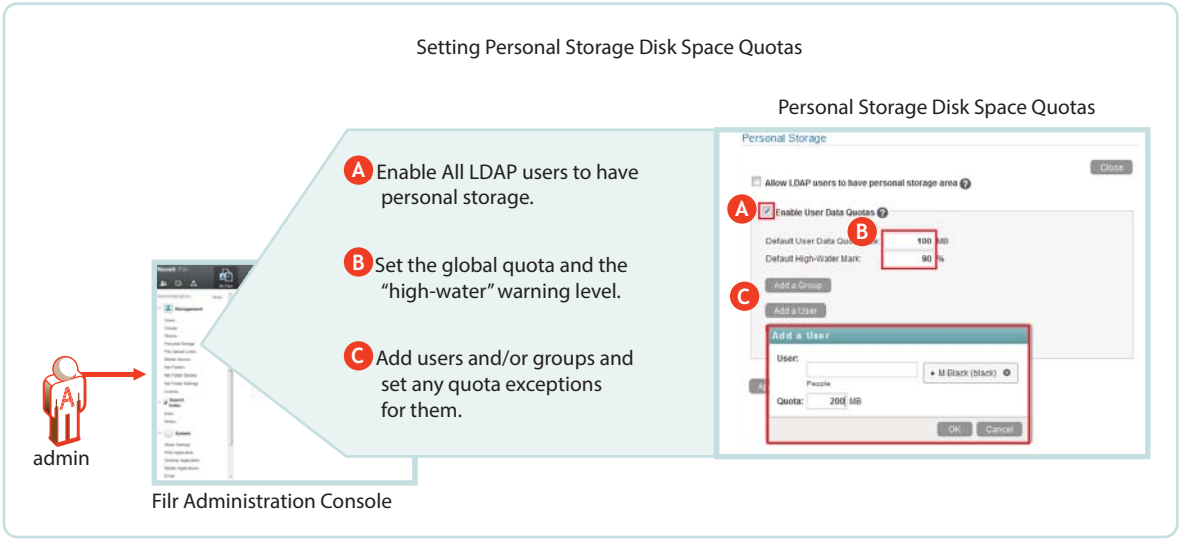
For an overview of personal storage disk space quotas, see Section 9.3, “Restricting Disk Space Usage,” on page 64.

Figure 9-3 *Setting Default and Individual Storage Quotas*



9.3 Restricting Disk Space Usage

Figure 9-4 *Enabling Personal Storage for All Users*



9.4 Home Folders Vs. Net Folders

A home folder is a special kind of Net Folder that is included in **My Files**.

Home folders allow for the sharing of files and sub-folders, while Net Folders only allow for the sharing of files, not sub-folders.

	Home Folders	Net Folders
File-server-based	Yes	Yes
Focus	Individual users	Groups or teams of users
Appear under Net Folders icon	No	Yes
Appear under My Files icon	Yes	No
Indexing	◆ Accessibility - Yes ◆ Searchability - Yes	◆ Accessibility - Yes ◆ Searchability - Optional Must be manually enabled.
Sharing granularity	Files and sub-folders	Files only

9.5 My Files Sharing Rights

See Section 12.1.3, "My Files Sharing Is Automatic," on page 79.

10 Net Folders

Filr introduces a new way of accessing file server data—Net Folders—a new file access method that shares some similarities with Novell's long-standing concept of mapped network drives.

10.1 Overview

To understand Net Folders, it is useful to see the similarities and differences between them and the mapped drives that you probably have on your current network. Figure 10-1 and Figure 10-2 illustrate such a comparison.

Figure 10-1 *File Servers and Mapped Drives*

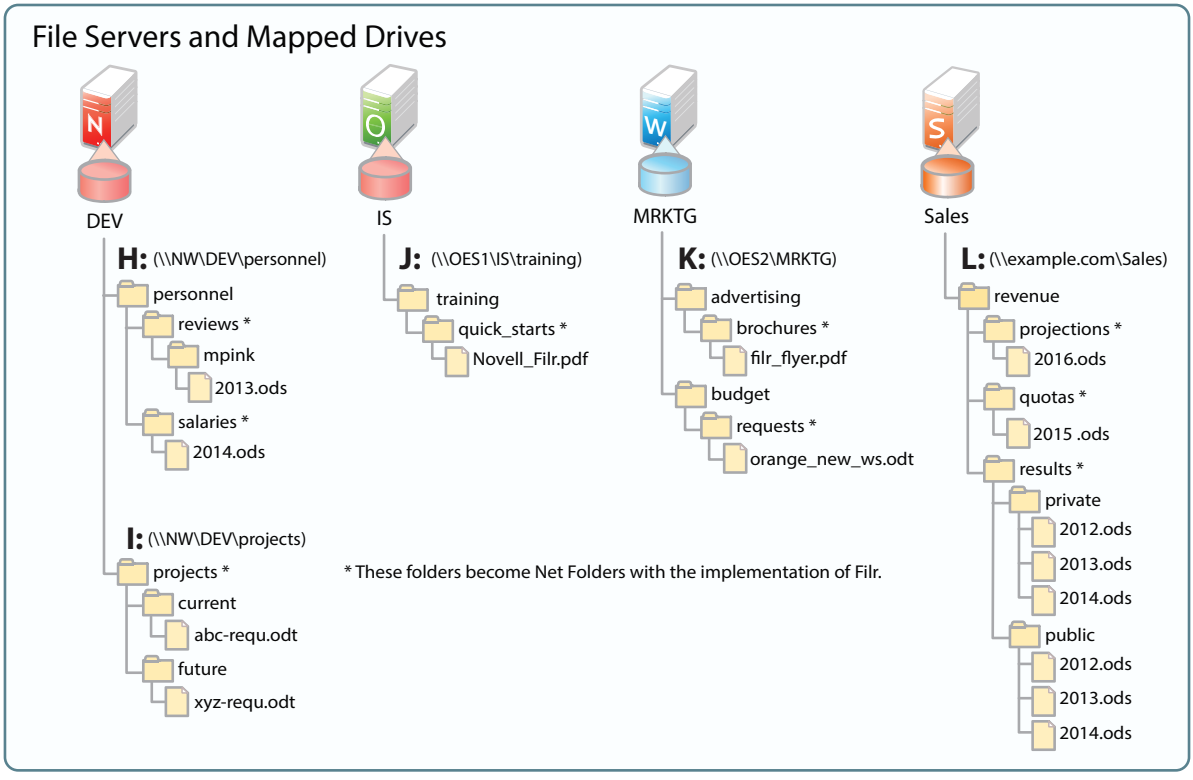
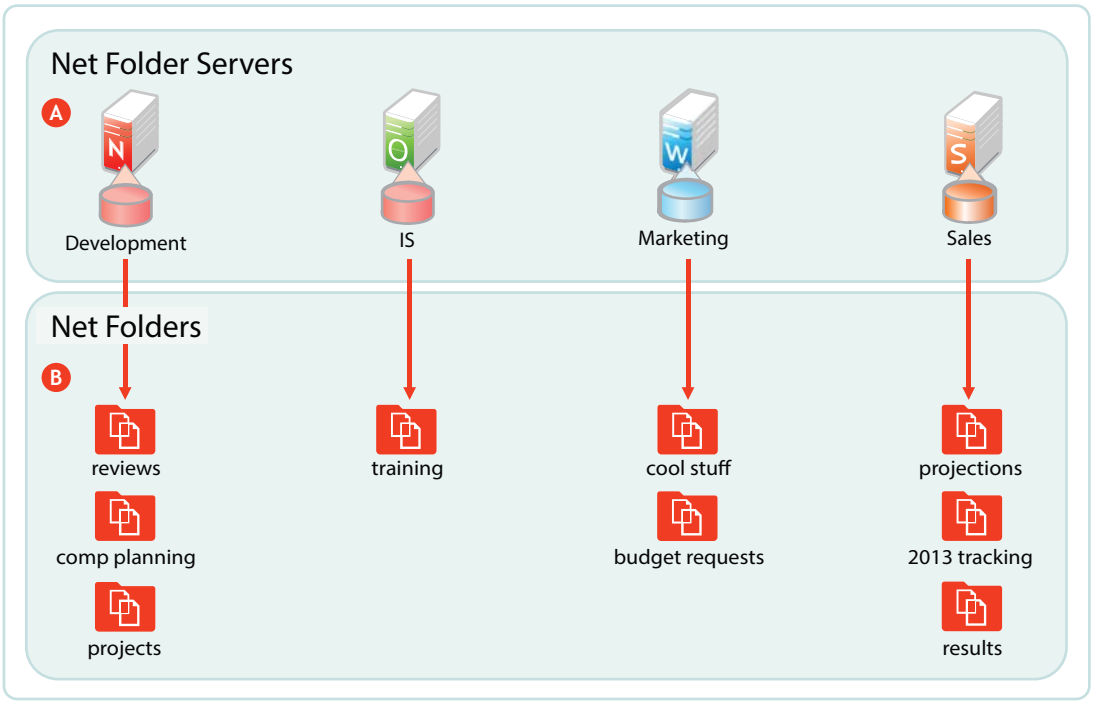


Figure 10-2 shows the same servers as in Figure 10-1, with their volumes defined as Net Folder Servers. Notice that the Net Folder Server names do not need to match the volume names, which can sometimes be rather cryptic.

The asterisk-marked folders in Figure 10-1 are shown as Net Folders here.

As with the Net Folder Server names, some of the Net Folder names in Figure 10-2 are different from the Figure 10-1 volume and folder names that they represent. This illustrates that Net Folder names are not tied to their corresponding actual folder names. Instead, you can name them whatever best communicates their purpose and content to those who access them.

Figure 10-2 *Net Folder Servers and Net Folders*



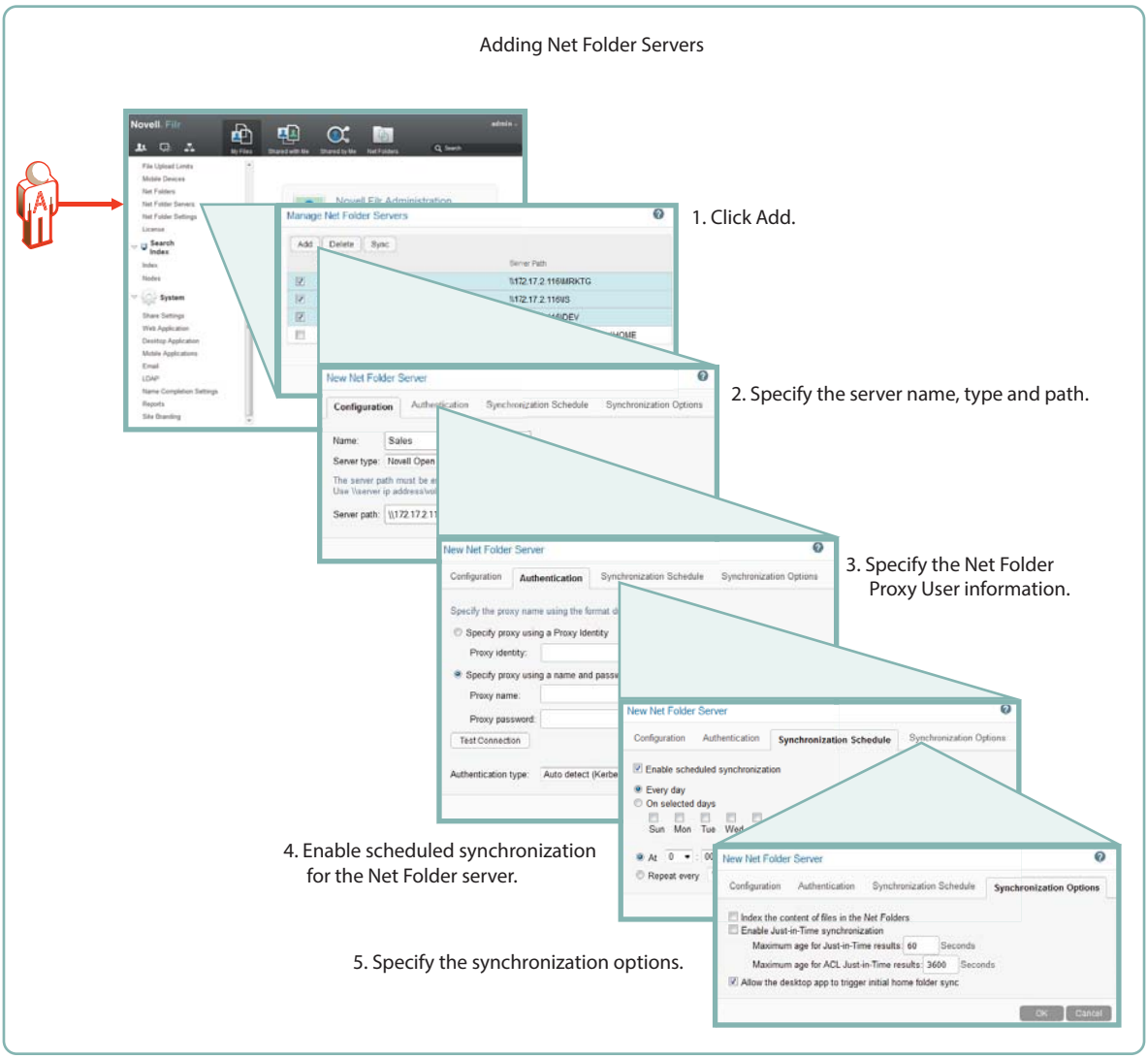
Letter	Information
A	A Net Folder Server represents a volume or share on a NetWare, OES, or Windows file server. In this example, Net Folder Servers for OES point to the root of an NSS volume on the server, but they can also point to a directory or sub-directory. Net Folder Servers for Windows servers point to a Windows share, which is usually defined at a folder level other than at the root of the file system. Therefore, it is common for a Net Folder Server for Windows to point to the same folder as an associated Net Folder does. There is usually one Net Folder Server per volume or share, but you can create multiple Net Folder Servers to the same volume or share if needed.

Letter	Information
B	A Net Folder is a pointer or reference to a specific folder within a Net Folder Server. Often there is just one Net Folder for every Net Folder Server, but you can create multiple Net Folders that point to a single Net Folder Server. You can even create multiple Net Folders that point to the same relative path. Why might you want to duplicate Net Folders? Possibilities include the following: ◆ Different synchronization schedule requirements ◆ Different access rights requirements ◆ Different usage patterns ◆ Different access loads

10.2 Specifying Net Folder Servers

The first step in creating Net Folder is to set up Net Folder Servers.

Figure 10-3 *Net Folder Server Creation*



As illustrated in Figure 10-3, adding a Net Folder Server includes the following:

- **Specifying the Name, Type, and Path**
  - **Name:** Net Folder users don't see this name, so use a name that makes sense from an administrative perspective. For example, you might include the IP address or DNS name of the server, or you could use a location name, such as `Third_Floor_Server`.
  - **Type:** Select the server type being targeted: Microsoft Windows, Novell OES, Novell OES (NSS for AD), or Novell NetWare
  - **Server Path:** This is the full UNC path to the NSS volume or directory on OES, or to the Windows share on NTFS where your Net Folder is located.
- **Specifying the Net Folder Proxy User Information**
  - **Proxy Identity:** If you have defined a Proxy Identity that applies to this Net Folder, select **Specify proxy using a Proxy Identity**, begin typing the identity's name, then select it. For more information, see "Proxy User Identities" in the *Filr 2.0: Administration Guide*.
  - **Proxy Name:** This is the name of the Net Folder proxy user that provides access to this volume. For more information, see Section 10.4, "Net Folder Proxy Users," on page 71.

IMPORTANT: Be sure to follow these guidelines when specifying the proxy user

- **OES, NetWare, and NSS AD:** Always use a fully qualified name, such as `cn=admin,o=myorganization`.

  If you specify only a simple name, such as `admin`, then Filr accesses the Net Folders for the server using CIFS rather than NCP.

  When you test the connection, the test succeeds and data synchronizes using CIFS.

  Unfortunately, when Filr attempts to determine a user's effective rights, the request fails because that function requires NCP and the simple name doesn't provide enough information to the NCP process.

- **Windows:** Use *domain\username* as the syntax.

  DFS for Windows requires this, and the syntax will always work with Active Directory and Windows.

- **Proxy Password:** This is the password of the Net Folder proxy user. If the password changes in the identity store, it must be updated here.
- **Test Connection:** This lets you test the path and the credentials of the proxy user that you have specified.

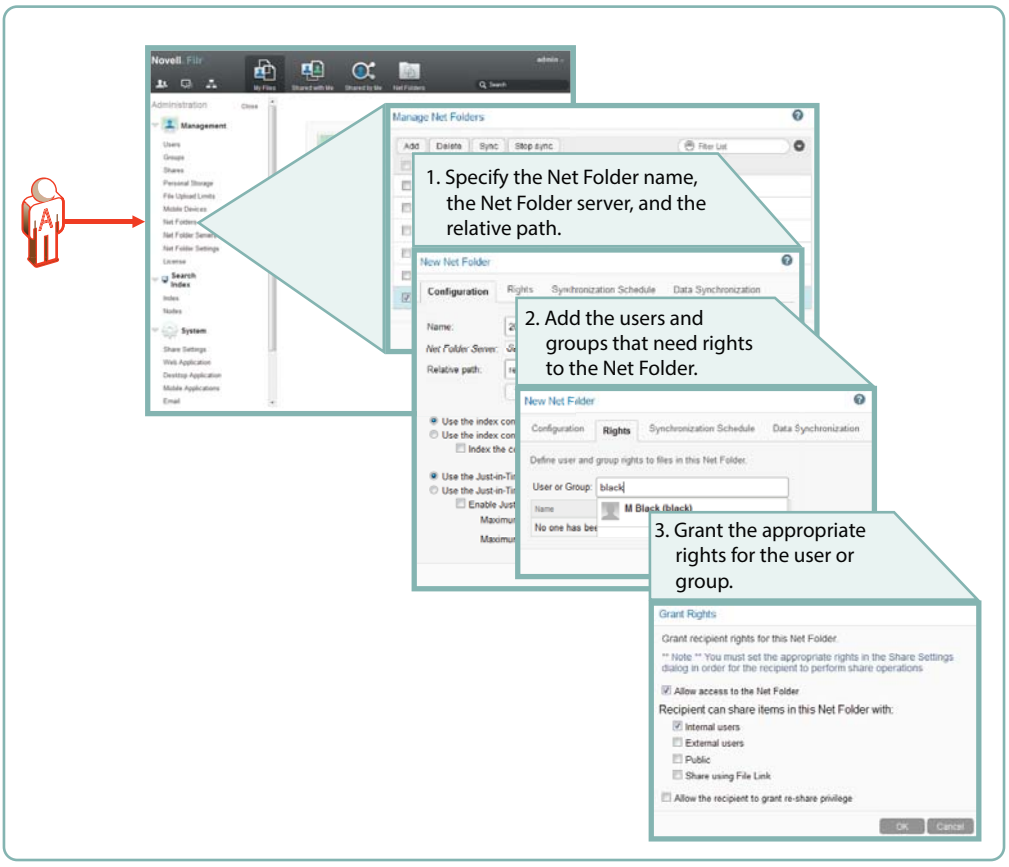
- **Enabling Synchronization for the Net Folder Server**
  - **Enable Scheduled Synchronization:** This creates a synchronization schedule for this Net Folder Server. You can then specify when you want the synchronization to occur. Any Net Folders for this server that don't have their own synchronization schedules will be synchronized according to this schedule.
- **Specifying the Synchronization Options** This lets you specify whether you want Net Folder contents indexed for searching, whether to enable Just-in-Time synchronization, and whether to allow desktop users to request Net Folder synchronizations.

For more information about Net Folder Server creation, see "Configuring and Managing Net Folder Servers" in the *Filr 2.0: Administration Guide*.

10.3 Specifying Net Folders

After creating Net Folder Servers, you can create Net Folders for users to access.

Figure 10-4 *Net Folder Creation*



The minimum tasks required for adding a Net Folder are illustrated in Figure 10-4. Setting a synchronization schedule and specifying the data synchronization options are not specifically called out because they are summarized in Figure 10-3 on page 68.

- **Specify the Net Folder Information**
  - **Name:** Filr users with rights to the Net Folder see this name, so you should use a name that they will recognize and that will help them to understand what the Net Folder contains.
  - **Net Folder Server:** The Net Folder Servers you have created appear in a drop-down list. You also have the option to create an additional Net Folder Server from within the Net Folder creation dialog.
  - **Relative Path:** This is the path to the folder relative to the UNC path entered for the Net Folder Server. A blank path creates a Net Folder that points to the Net Folder Server's UNC path.
  - **Test Connection:** This lets you verify that you have typed the path correctly.
- **Add Users and/or Groups**
  - **User or Group:** As you type a user or group name, a list populates from which you can make your selection. When you click the name, the Access Rights dialog displays
- **Access and Sharing rights:** After you enable access to the Net Folder for the user or group, you can specify sharing privileges as well.

For more information about Net Folder creation, see "Creating and Managing Net Folders" in the *Filr 2.0: Administration Guide*.

10.4 Net Folder Proxy Users

For more information about Net Folder Server proxy users, see “Providing Net Folder Server Proxy Users” in the *Filr 2.0: Administration Guide*.

10.4.1 Net Folder Proxy Identities

Beginning with Filr 2.0, administrators can define Net Folder Proxy Identities, which greatly simplify proxy user management and maintenance.

Rather than specifying the same proxy user information within the definition of multiple Net Folder Servers, you can create a Proxy Identity to represent the proxy user. Then as you create Net Folder Servers, you simply select the Proxy Identity that you created.

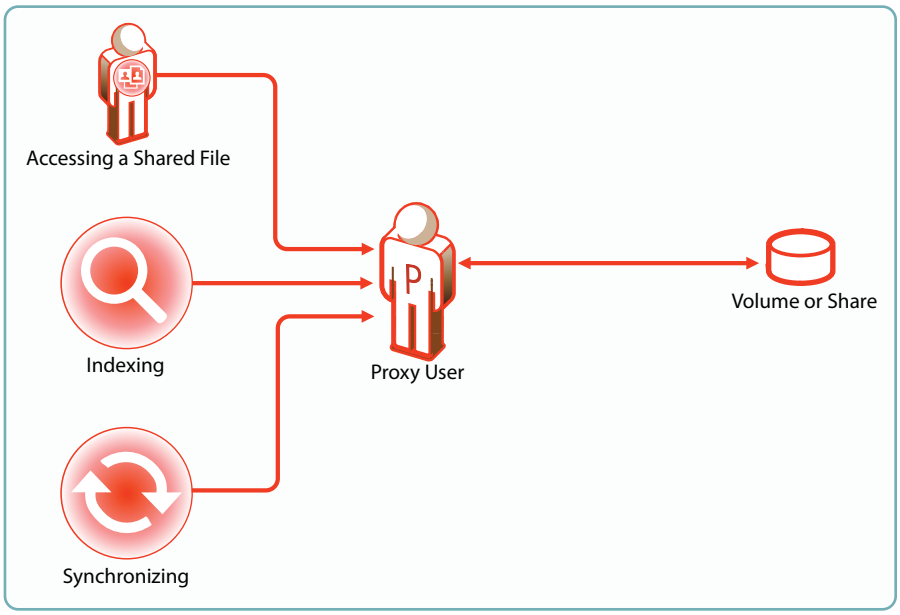
As a proxy user’s password or other information changes, you simply change the information for the appropriate Proxy Identity rather than needing to modify the information within each affected Net Folder Server.

For more information, see “Proxy User Identities” in the *Filr 2.0: Administration Guide*.

10.4.2 The Functions Facilitated by Net Folder Proxy Users

Net Folder proxy users provide Net Folder access for three Filr functions: file sharing, indexing, and synchronization, as illustrated in Figure 10-5.

Figure 10-5 *Functions of a Net Folder Proxy User*

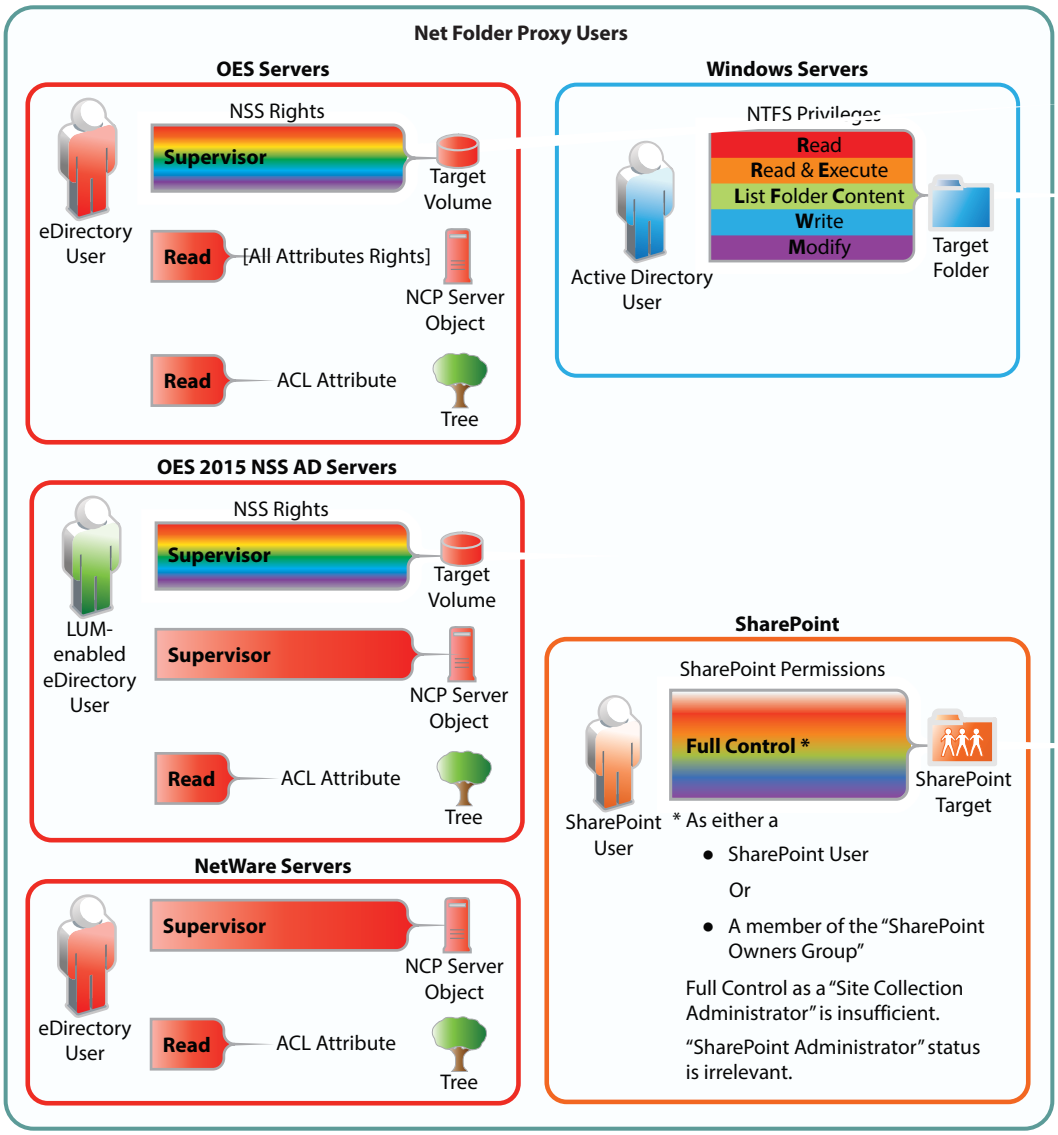


- Access to shared files always involves the proxy user, even for users who have file system rights to the shared files.
- Proxy users have no role when users with Net Folder rights access Net Folders directly.

10.4.3 Rights Required for Net Folder Proxy Users

Net Folder proxy users must have the rights shown in Figure 10-6.

Figure 10-6 *Proxy User Rights Summary*

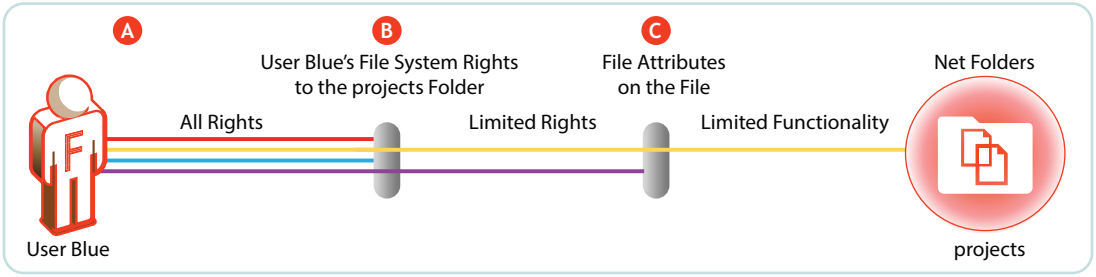


10.4.4 Net Folder Proxy User Passwords

If the proxy user password changes in the LDAP identity store, it must also be changed in the Net Folder Server definition. Proxy User password maintenance overhead can be greatly reduced starting in Filr 2.0 by leveraging Proxy Identities.

10.5 Granting Access to Net Folders

Figure 10-7 *Net Folder Access Involves Filr and the File System*



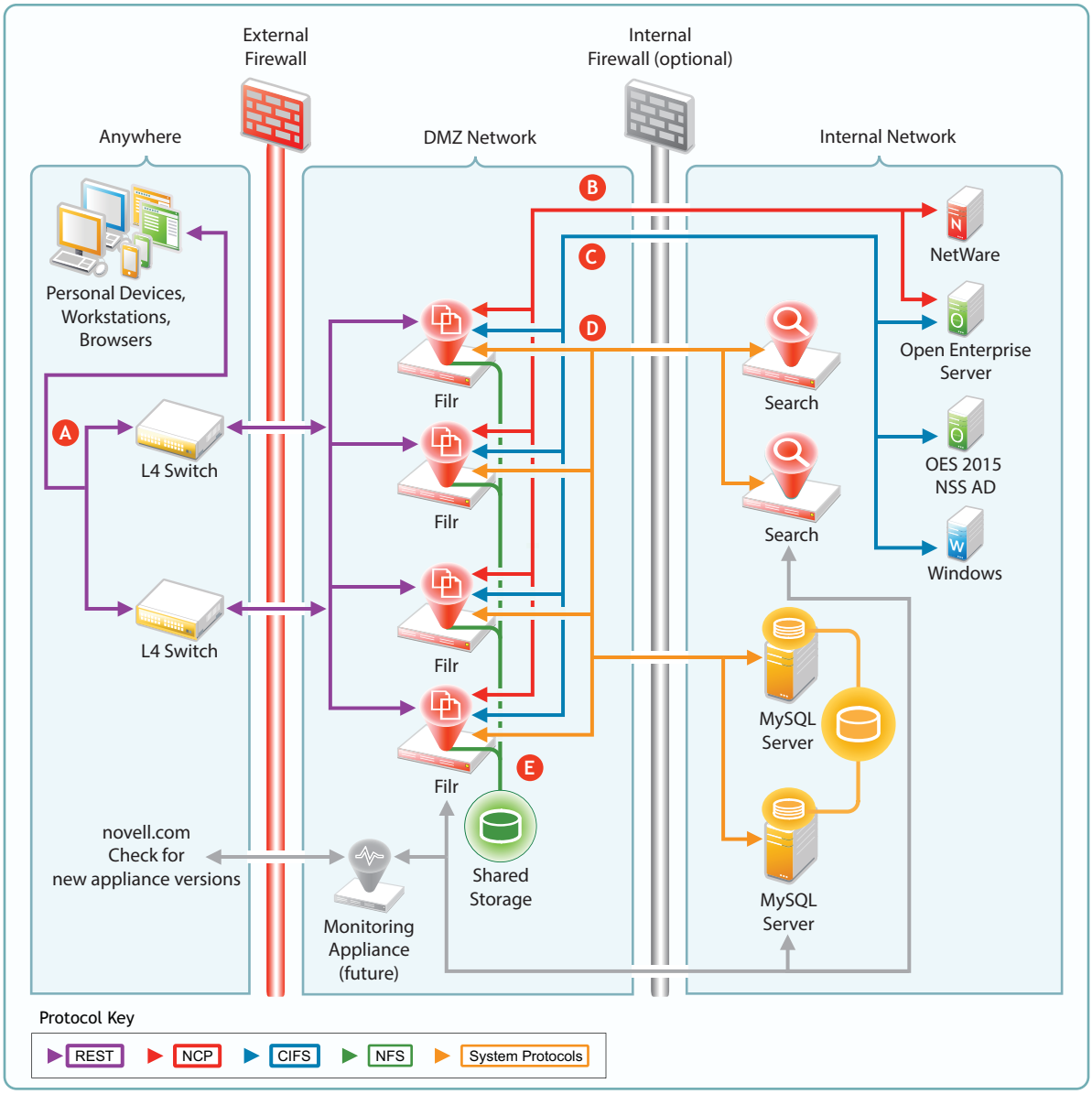
Letter	Explanation
A	When you grant a user access to a Net Folder, either individually or as a member of the group by using the Rights tab (see the explanation for Figure 10-4), then from a Filr perspective, the user has all rights to that folder. However, the file system is the access master controller.
B	The user must have file system trustee rights that allow the file to be viewed and accessed. For example, if the user has Read, Write, and File Scan rights to a file on an NSS volume, then the file is not only visible, but can, in theory, be modified. However, there's one more part to the access equation.
C	Files can have attributes that prevent them from being modified, such as Read Only. They might also be hidden, in which case they would not be visible to the Filr user.

For more information about Net Folders, see "Setting Up Net Folders" in the *Filr 2.0: Administration Guide*.

11 Protocols and Filr

The components in a Filr deployment use a number of different protocols to communicate and provide Filr services, as shown in Figure 11-1. The optional internal firewall is shown to facilitate the illustration of a separate (and also optional) DMZ network.

Figure 11-1 *Protocols Used in Filr Installations*



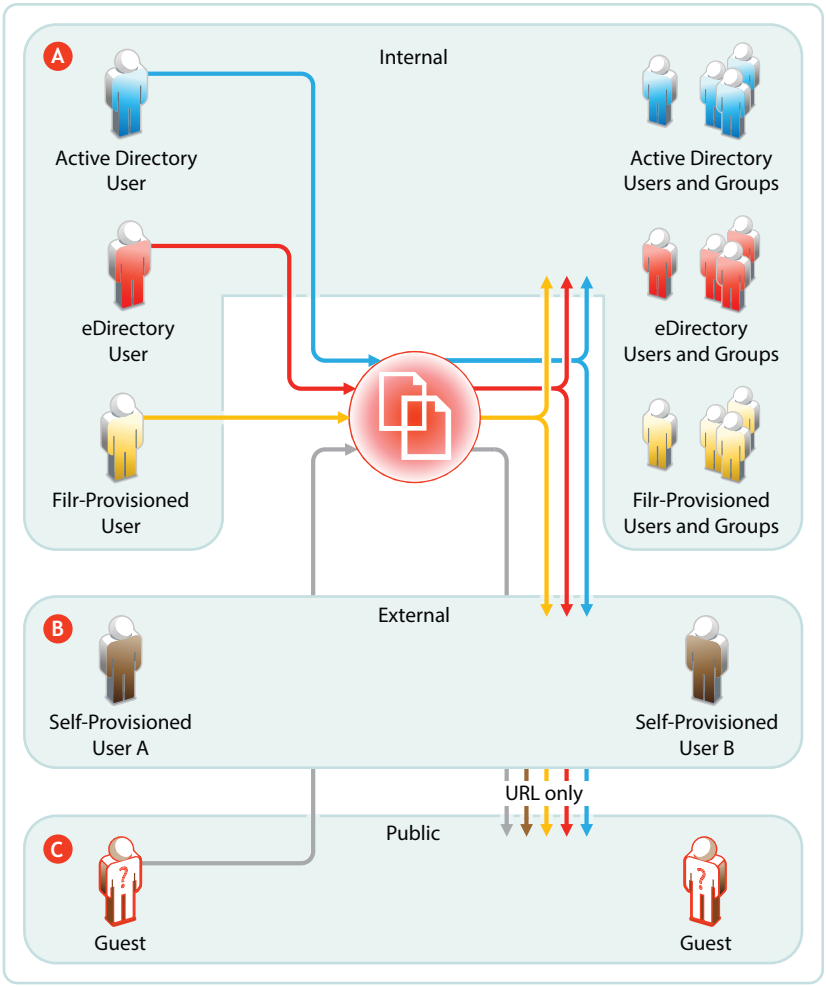
Letter	Details
A	Workstations and devices running Filr software access Filr using REST protocols that facilitate authentication and other access requests. Browsers use HTTPS to communicate with Filr.
B	Filr communicates with Novell file servers using NetWare Core Protocol (NCP) requests.
C	Filr communicates with Windows servers using the Common Internet File System (CIFS) protocol.
D	Other system protocols handle communication between Filr and the MySQL and Search appliances.

12 Sharing through Filr

Sharing lets users grant other users (internal or external) access to files that they own. If allowed by Filr administrators, users can also share files that they have received share invitations for.

Figure 12-1 presents a high-level overview of the sharing functionality available in Filr. The sections that follow provide more detail.

Figure 12-1 *Sharing through Filr*



Letter	Explanation
A	Depending on the sharing privileges they are granted, internal users can share and collaborate with each other, with external users who have been invited to self-provision into the Filr system, and with the public. If re-sharing items is allowed, those who receive share invitations can also share. This means that eDirectory users can share files with Active Directory users and groups, that the reverse is also true, and that both of them can invite external partners or others to join the Filr system for collaboration and other purposes.
B	When External Sharing is enabled in Filr, external users who receive share invitations can self-provision into the Filr system and collaborate with internal and external users, using the Comments feature.
C	If Filr is configured to allow public sharing, and if a file is shared publicly through a system-generated URL, then anyone with that URL can access the file as a guest user and share it with any other user, including other public users. This re-sharing is not a function of Filr but a function of sharing the URL through email, social networking, and so on.

12.1 Setting Up Sharing for Users and Groups

Before users can share, they must have sharing enabled for them at the Filr system level, either individually or as a member of a group.

After that, sharing of My Files is enabled by default, but sharing of files in Net Folders requires an additional step.

12.1.1 Do Not Enable Sharing for All Internal Users and All External Users

Prior to Filr 2.0, the documentation stated that enabling sharing for `All Internal Users` and `All External Users` was an acceptable method of enabling sharing on the system.

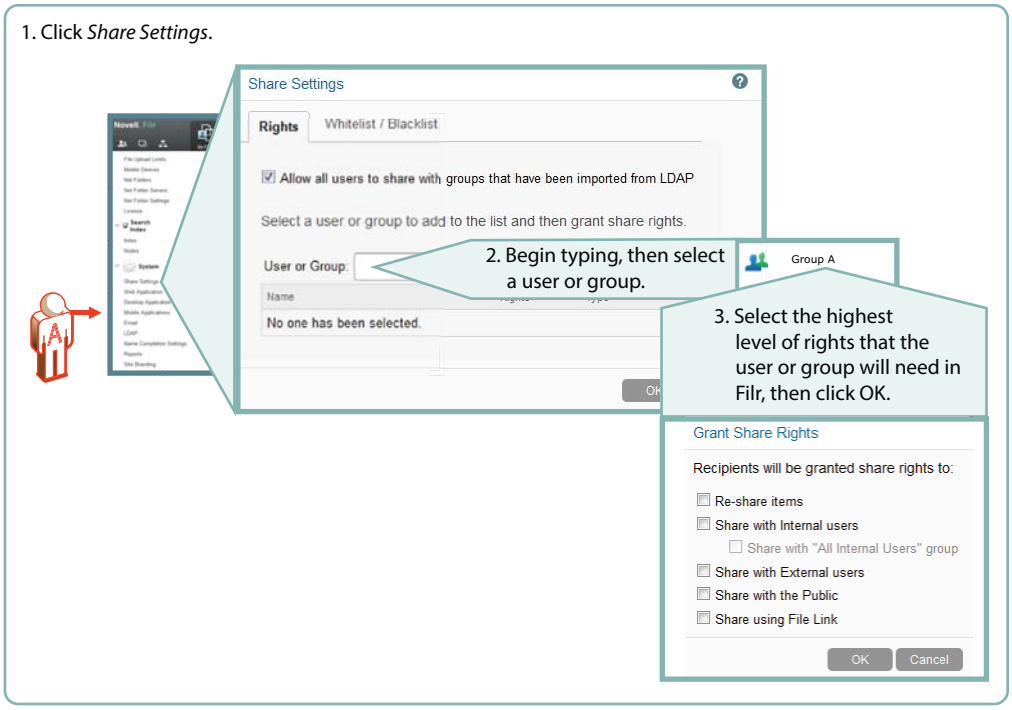
Unfortunately, this shortcut results in significant system overhead and often leads to serious performance degradation.

We strongly recommend that you enabling sharing only for specific users and/or groups, as outlined in the sections that follow.

12.1.2 System-Level Sharing Must Be Configured First

The first step in allowing Filr sharing to take place is to list the users and groups who are allowed to share in the Share Settings dialog. When you add the user or group, you also specify the upper limits of possible sharing rights for them. You can further restrict the rights, but you can't expand them beyond this limit.

Figure 12-2 *Setting Up System-Level Sharing Rights*

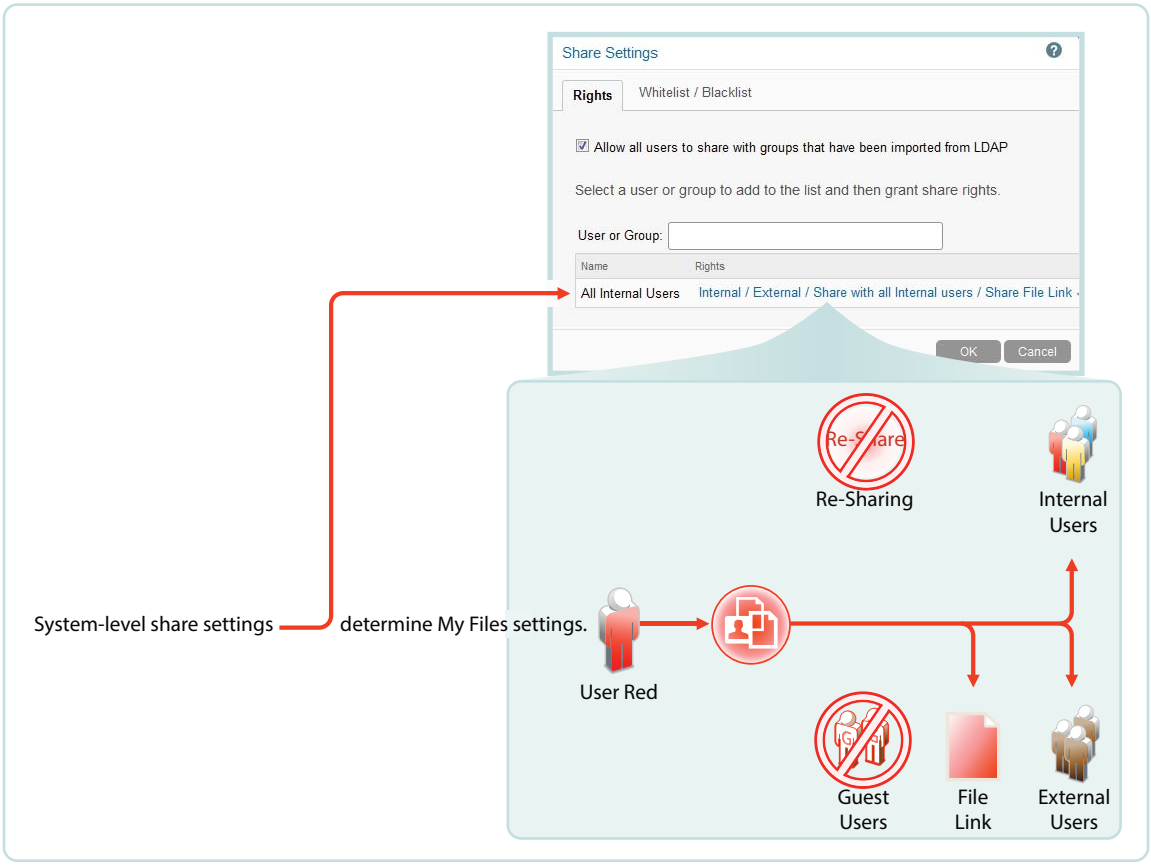


12.1.3 My Files Sharing Is Automatic

After sharing is enabled at the system level for users individually or as members of groups, then if those users have personal storage enabled, they can share their files and folders within the limitations set for the system.

Administrators can disable sharing of files and folders in My Files on an individual user basis.

Figure 12-3 *My Files Share Settings*



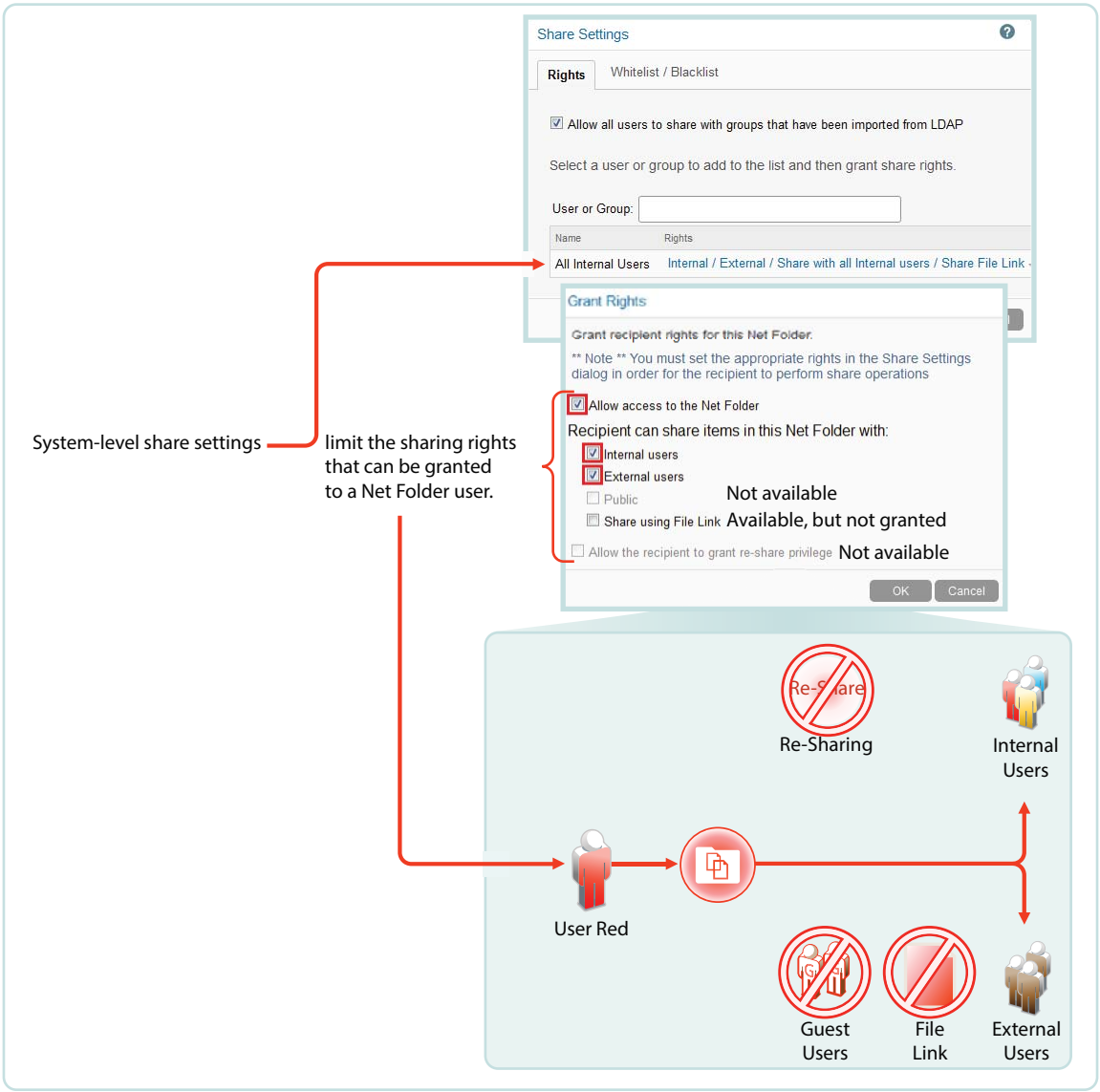
12.1.4 Net Folder Sharing Must Be Explicitly Allowed At Two Levels

Before the users or groups listed in the Share Settings dialog can share files in their assigned Net Folders, they must have sharing enabled on those Net Folders.

When enabling Net Folder access for a user or group, a Filr administrator can only assign up to the maximum sharing rights that are set at the system level.

In Figure 12-4, user red can only be assigned sharing rights that are allowed at the system level.

Figure 12-4 *An Example of Net Folder Sharing*



12.2 Understanding Sharing

12.2.1 My Files Sharing Vs. Net Folder Sharing

By default, users can share both files and folders in their **My Files** area; **Net Folder** sharing is limited to only files.

12.2.2 Sharing and Access Roles

When users send share invitations, they must designate the role that they want the user receiving the share to have for the file or folder being shared. The roles associated with sharing are the same as Net Folder roles.

Filr administrators who allow Net Folder sharing should understand the following foundational concepts.

- **Share Invitations Always Include a Shared-Access Role:** When users receive share invitations, they also receive one of three shared-access roles: Viewer, Editor, or Contributor. These involve the same rights as Net Folder roles.
- **Users Can't Share Roles That They Don't Have:** Users can grant only shared- access roles that either correspond to their roles or are more restrictive.

  For example, a user with the Contributor role can grant the Viewer, Editor, or Contributor shared-access role to other users as Filr system share and Net Folder share settings allow.

  On the other hand, a user with the Viewer role can only grant the Viewer shared-access role to other users.

  NOTE: Because users have all rights to their My Files area, they can share any role to a folder or file, provided that sharing is enabled on the system.

- **The Highest Role Wins:** If multiple users share the same item with a single user, the user receiving the share has the highest role that was granted along with the share.

  For example, if User B shares a file with User A and grants User A the Viewer role to the file, and then User C shares the same file with User A and grants the Editor role to the file, User A has Editor rights to the file.

12.2.3 Shared Access to Net Folders Is Always through a Proxy User

When Filr users access a Net Folder-based file in their Shared With Me folder, they access it through the proxy user assigned to the Net Folder where the file lives. File system rights that users do or do not have to shared items play no role when they are working within Shared with Me.

12.3 A Caution Regarding the Re-sharing Feature

Use caution when enabling file re-sharing. Removing one user's access rights to an item does not remove the access rights of other users with whom the item was re-shared.

For example, suppose User A shares an item with User B and grants re-share rights. User B then shares the file with User C. Even if User A revokes User B's access rights to the item, User C continues to have access to the shared item.

13 Filr Synchronization

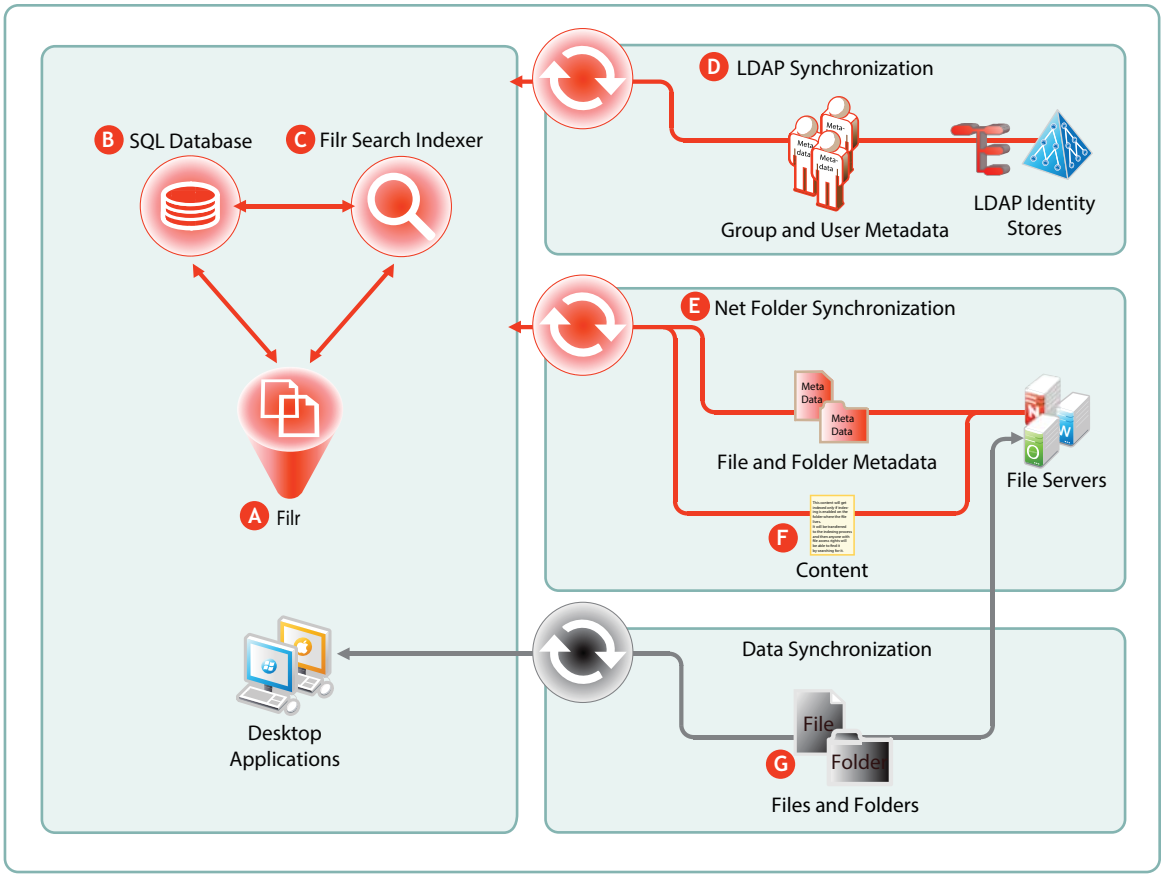
The synchronization of users, groups, files, and folders, along with the associated ACL rights, file contents, and so on, is central to Filr services. This section provides a high-level overview of the various synchronization processes in Filr 1.2.

13.1 Synchronization Overview

Figure 13-1 illustrates at a high level the information and content that get synchronized in Filr. The table that follows the figure describes some of the results and implications of the processes that take place.

The figure does not illustrate functional details. For example, it does not attempt to show the flow of LDAP metadata and file/folder metadata to Filr services for storage and indexing.

Figure 13-1 *What Gets Synchronized and Where*



Letter	Details
A	Filr relies on the SQL database and the Filr Search (Lucene) indexer in order to provide access to • Users and groups and • Files and folders
B	Filr stores metadata for users, groups, files, and folders in the SQL appliance or server.
C	After the metadata is retrieved and stored, Filr directs the Filr Search (Lucene) indexer to process it for viewing by administrators and users. Users, groups, files, and folders are only visible and accessible through Filr after their metadata is stored and indexed. For more details about the content indexing process, see Section 13.3, “Net Folder File Content Indexing Overview,” on page 87
D	Regular LDAP synchronization ensures that Filr is updated when users are added or removed and when group memberships changes in the LDAP identity store. it is usually sufficient to synchronize LDAP once a day, but some organizations require more frequent synchronization to keep Filr abreast of changes in their identity stores.

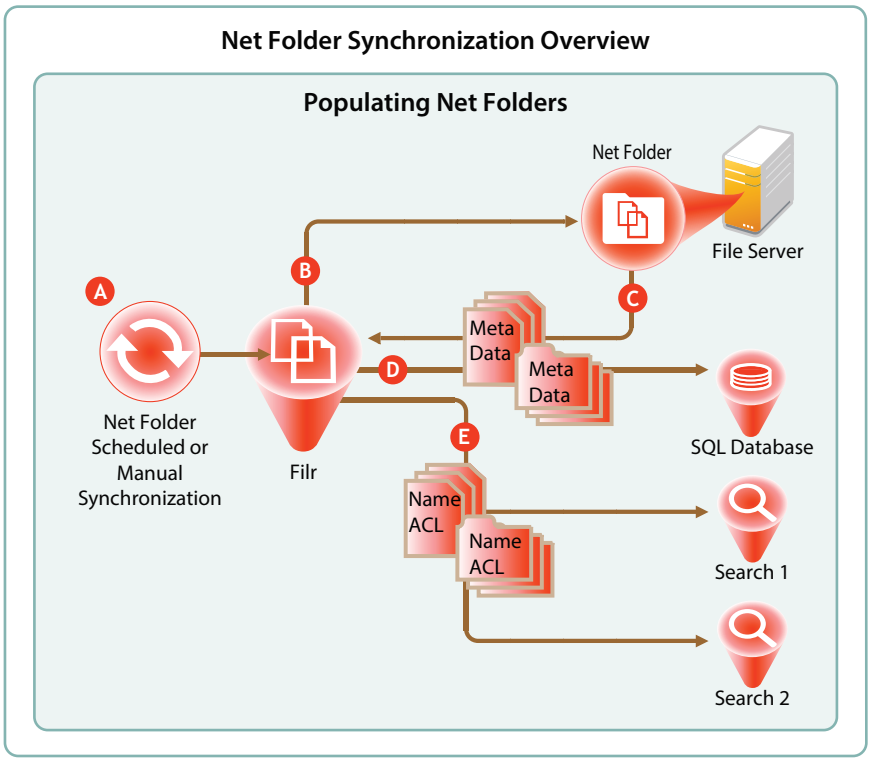
Letter	Details
E	Net Folder synchronization is highly configurable: ◆ **Schedules for Net Folder Servers:** You can set synchronization schedules for each Net Folder Server. The Net Folders associated with that server are then synchronized according to the general nature of the volume or share where they reside. ◆ **Schedules for Net Folders:** You can also set synchronization schedules for individual Net Folders that will override the server schedules and synchronize the folders either more or less frequently than the server schedule dictates. ◆ **Manual:** These are especially helpful when you create Net Folders to ensure that Filr users can browse and access the files and folders that they contain. ◆ **Just-in-Time Synchronization (JITS):** You can enable JITS so that as Filr users browse in Net Folders, file and folder metadata is synchronized with Filr. For more details about the synchronization process, see Section 13.2, “Net Folder Synchronization Detail Overview,” on page 85
F	For users to be able to search file content, folders must have content indexing enabled. For folders that are enabled for content indexing, Filr retrieves the content for each file and directs the indexer to process it for searchability.
G	By default, Net Folders don’t allow data synchronization with desktop applications. This prevents users from getting a local copy of sensitive files on the organization’s file servers. However, the download functionality can be enabled.

13.2 Net Folder Synchronization Detail Overview

IMPORTANT: My Files > Personal Storage doesn’t require a synchronization of metadata because the files are stored and managed on the Filr appliance itself. There is no synchronization with a back-end file server.

My Files > Home Folders function exactly like all other Net Folders from a synchronization standpoint.

Figure 13-2 *Net Folder Synchronization*

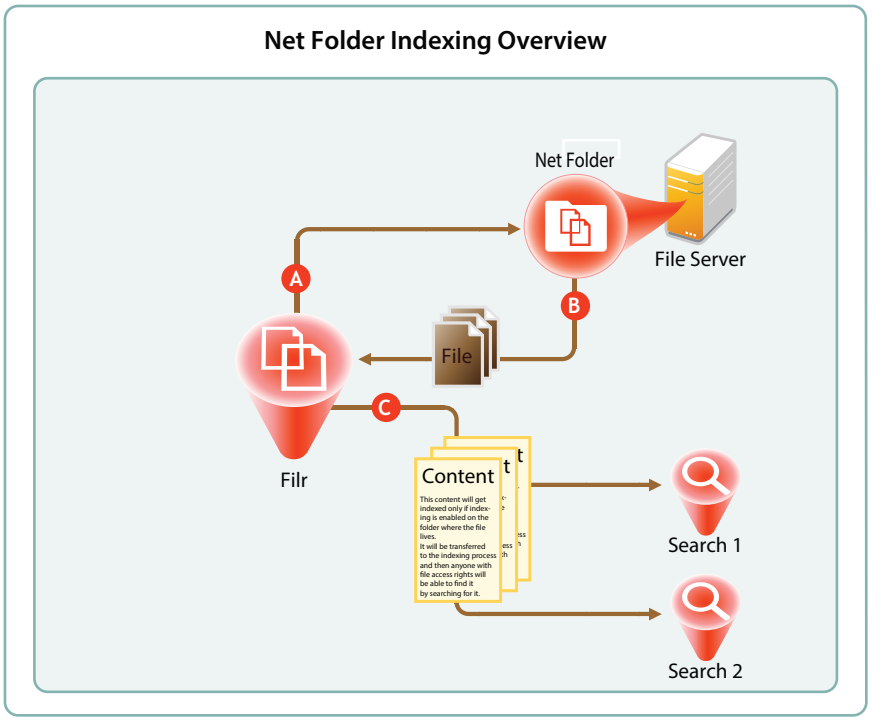


Letter	Details
A	Full Net Folder synchronizations occur according to individual Net Folder schedules, or if no schedule is defined for the Net Folder, then they occur according to the associated Net Folder Server's synchronization schedule. If no schedule is set, then it falls to Filr administrators to manually synchronize them.
B	When a Net Folder Synchronization is triggered, the Filr appliance connects to the specified Net Folder location on the target file server.
C	Filr then walks the directory structure, collecting meta data (name, size, dates, ACL information, etc.) about each folder and file as it goes.
D	Filr stores the collected meta data in the SQL database.

Letter	Details
E	Then Filr sends the folder and file names and ACL information to each Filr Search appliance to be indexed. This makes it possible for users to search for folder and file names, provided that they have sufficient rights on the file system to see them. The majority of Net Folder synchronization work occurs on the File appliance.

13.3 Net Folder File Content Indexing Overview

Figure 13-3 *File Content Indexing*



Letter	Details
A	For content indexing, Filr first requests copies of all of the files contained in the Net Folder.
B	After a file is copied to the Filr appliance, up to the first 1.1 MB of file content is extracted by Stellent, the technology that provides HTML rendering of file content in Filr.

Letter	Details
C	Filr then sends the extracted content to each Search appliance for content indexing. **IMPORTANT:** Content indexing is powerful and useful functionality. It is also very CPU- and IO-intensive because each file is processed separately. It is therefore important to carefully consider which Net Folders contain files that organization members must be able to search for specific content.

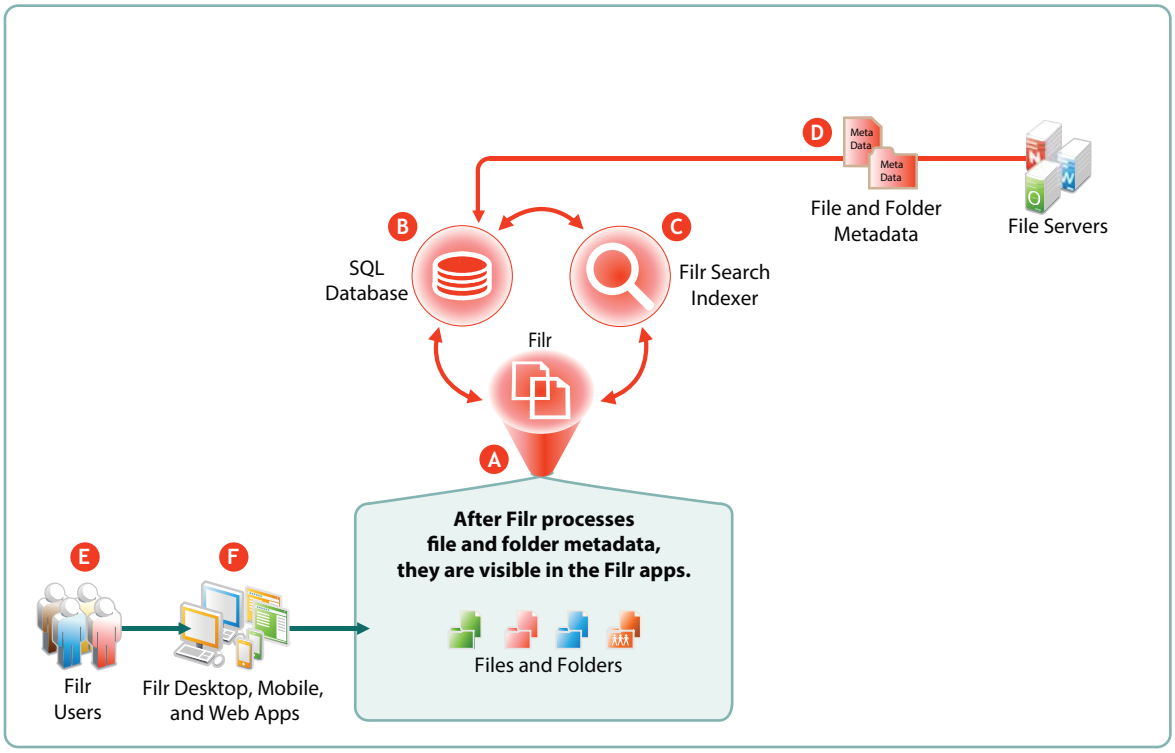
14 File and Folder Access in Filr

Most organizations store and manage their data in files and folders on network file servers.

Filr lets users see, access, and work with their assigned files and folders.

14.1 How Filr Makes Files and Folders Visible to Users

Figure 14-1 *Filr Processes Metadata to Make Files and Folders Visible to Filr Users*



Letter	Details
A	Filr directs and coordinates the processing of metadata for files and folders.
B	Filr retrieves and stores the metadata in the SQL appliance or server.

Letter	Details
C	After metadata retrieval, Filr directs the Filr Search (Lucene) indexer to process it for viewing in the Filr apps.
D	My Files files and folders are automatically retrieved and processed. Net Folder files and folders must by synchronized through one of the methods listed in the description for Letter E in Figure 13-1 on page 83.
E	After the metadata is processed for users, files and so on, Filr users can see the objects in the Filr apps (Letter G).
F	Filr apps for desktops, mobile devices, and web access let Filr users interact with the files, folders, users, and groups that are made accessible through Filr.

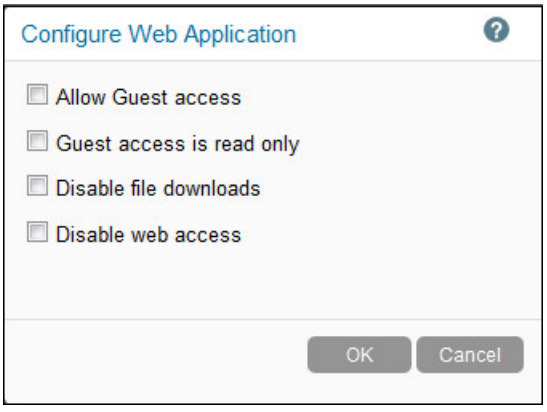
14.2 Web Application for Browsers

Web browser access to Filr is enabled by default. Filr users can browse and access files in their **My Files** and assigned **Net Folders** areas. They can also access files and folders that have been shared with them in **Shared with Me**, and they can see what they have shared in **Shared by Me**.

If file downloading is enabled, users can download files to their local drives for modification, and so on, and if they have the required Filr role and sufficient rights on the back-end file server, they can then upload the files back to the network with content changes intact.

Browser access is intuitive and convenient. However, the Filr 2.0 desktop applications are integrated with Windows Explorer and Mac Finder and are the recommended option for desktop users who need seamless and synchronized access with back-end file servers.

The Configure Web Application dialog (below) (**Administration Console > System > Web Application**) shows the controls that administrators have over web browser access to Filr.



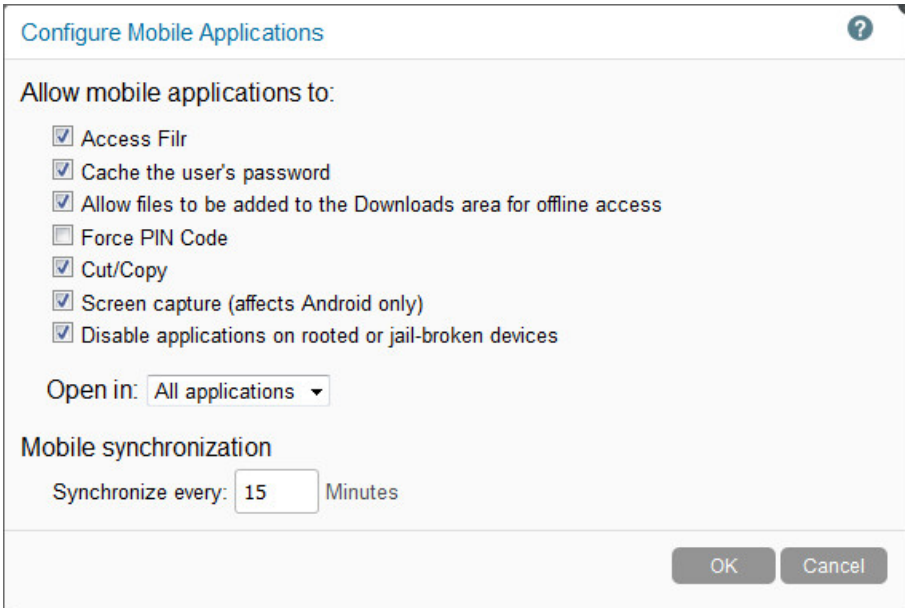
For Administrative instructions and information, see “Configuring User Access to the Filr Site” in the *Filr 2.0: Administration Guide*.

Information for web application users is in the *Filr 2.0: Web Application User Guide*.

14.3 Mobile Apps

Filr users who spend a lot of their time away from their offices and workstations find the Filr mobile apps very convenient and useful.

The Configure Mobile Applications dialog (below) (**Administration Console > System > Mobile Applications**) shows the controls that administrators have over mobile application functionality and access to Filr.



For Administrative instructions and information, see "Configuring User Access to the Filr Site" in the *Filr 2.0: Administration Guide*.

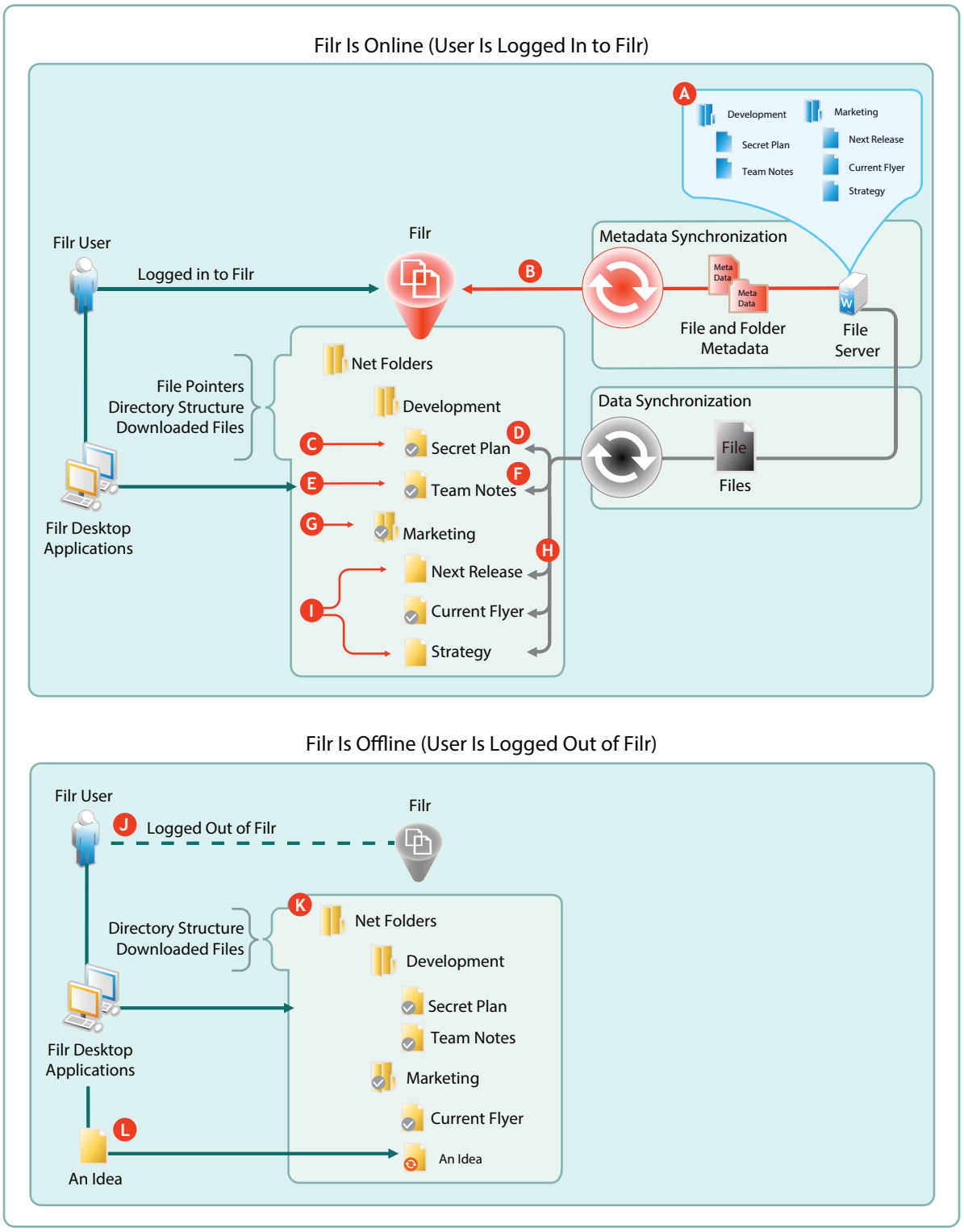
Information for mobile users is in the *Novell Filr Mobile App Quick Start*.

14.4 Desktop Applications

14.4.1 How the Filr 2.0 Desktops Work

As shown in Figure 14-2, what desktop application users see in Windows Explorer and Mac Finder varies, depending on whether they are logged in to Filr and what they have marked to be **Available Offline**, in other words, available when Filr is offline.

Figure 14-2 *Filr Desktops: Online Vs. Offline*



Letter	Details
A	The back-end Windows file server has files and folders in two parent folders: `Development` and `Marketing`.
B	The Filr administrator creates Net Folders for the `Development` and `Marketing` folders and synchronizes them with Filr. Although not shown in the graphic, at this point none of the folders or files have the overlay icon that indicates downloaded files that are synchronized with the back-end file server. (For more detail about Net Folder Synchronization, see Section 14.1, “How Filr Makes Files and Folders Visible to Users,” on page 89 and Section 13.2, “Net Folder Synchronization Detail Overview,” on page 85)
C	In Windows Explorer, the desktop user marks the `Secret Plan` file as **Available Offline**.
D	The file is downloaded to the local disk and the overlay icon displays on it. **IMPORTANT:** Because it is marked as **Available Offline** in Filr, the `Secret Plan` file is retained on the local disk and kept in sync with its counterpart on the back-end file server until it is marked **Online Only**.
E	Using an application on the workstation, the desktop user opens the `Team Notes` file.
F	The file is downloaded to the local disk and the overlay icon displays on it. **IMPORTANT:** The `Team Notes` file is not marked in Filr as **Available Offline**. Rather it is classified as a Cached file. This matters because it is subject to Filr's cache cleanup process, which removes inactive files from the local disk.
G	The desktop user marks the `Marketing` folder as **Available Offline**.

Letter	Details
H	The three files in the `Marketing` folder are downloaded to the workstation's hard drive and marked **Available Offline**. Although not shown in the graphic, at this point all of the files under the `Marketing` folder have the overlay icon indicating that they are downloaded to the local disk and synchronized with the file server. **IMPORTANT:** When a folder is marked as **Available Offline** or **Online Only**, the folder and all its children (all files, all subfolders, and all subfolder files) are marked the same way. For example, A subfolder is marked **Available Offline** and all its files are downloaded. Later, the subfolder's parent folder is marked **Online Only**. At that point, everything in the subfolder is marked **Online Only** and all of the files in the subfolder structure that were previously downloaded, are removed from the local disk.
I	The desktop user marks the `Next Release` and `Strategy` files as **Online Only**. The files are immediately deleted from the local disk and the overlay icons are no longer displayed.
J	The user logs out of Filr.
K	The **Online Only** files are no longer displayed. The folder structure remains in place.
L	While traveling and not logged in to Filr, the desktop user has an idea to share with the Marketing Team. Because the folder structure remains in place, the user creates a file named `An Idea` in the `Marketing` Net Folder. An overlay icon indicates that the file is not yet synchronized. However, when the user logs back in to Filr, the An Idea file will be copied to the back-end file server, the file will be marked as **Available Offline**, and the overlay icon will reflect that the file is in sync with the file server.

14.4.2 Net Folder Synchronization Is Crucial

Although visibility no longer requires downloading files to the local drives, Net Folder synchronization remains a critical factor because desktop users can only see files and folders that have had their metadata synchronized.

- **Manual Synchronization (Synchronize Now):** If allowed by an administrator for a given Net Folder, this options lets desktop users synchronize with back-end file servers on an as-needed basis.

- **Net Folder Synchronization Schedules:** Regularly scheduled Net Folder synchronizations can keep files and folders in sync with Filr, especially if file server content is fairly static.
- **Just-in-Time Synchronization (JITS):** Prior to Filr 2.0, JITS had very limited applicability to the desktop applications, but now it can be very valuable for browsing, especially when Net Folder content is constantly changing. See “Desktop Browsing Triggers JITS”.

14.4.3 Desktop Browsing Triggers JITS

Starting with Filr 2.0, if Just-in-Time Synchronization (JITS) is enabled for a Net Folder, then browsing in that Net Folder from a desktop, a mobile device, or a web browser always triggers JITS.

When a user browses to a folder, JITS is triggered, and the metadata for everything in the folder is synchronized with the back-end file server, stored in the SQL database, and processed by the Filr Search appliance.

For help with evaluating whether to enable JITS on a Net Folder, see “Planning the Synchronization Method” in the *Filr 2.0: Administration Guide*.

14.4.4 Files on Demand

The following points summarize what Files on Demand means:

- **Downloading for Visibility Is Not Required:** Before Filr 2.0, files and folders had to be downloaded to the local hard drive to be visible.

  Filr 2.0 desktop applications are integrated with Windows Explorer and Mac Finder so that Filr users see an integrated view of downloaded files and file pointers derived from metadata synchronization (see Section 14.1, “How Filr Makes Files and Folders Visible to Users,” on page 89).
- **Folder Structures Are Always Retained:** Whether users are online with Filr or logged out, the folder structures in Net Folders, Home Folders, and Personal Storage are always retained.

  While users are logged in, folders are synchronized to local hard drives and kept in sync with back-end file servers and the Filr appliance.

  As users work offline, they see the same folder structure as when they are online. Therefore, they can therefore create new files, move files and folders, and make other changes that are automatically synchronized when they log back in to Filr.
- **My Files—Personal Storage Files Are Automatically and Immediately Visible:** Because personal storage files and folders reside on the Filr appliance, they are automatically visible in Windows Explorer and Mac Finder in the **My Files** folder. Metadata synchronization is not required.
- **Net Folders (Including Home Folders) Are Visible After Metadata Synchronization:** After files and folders are synchronized, and when Filr users are logged in to Filr, all Net Folder-based files and folders that a desktop user is authorized to view are automatically visible in Windows Explorer and Mac Finder under **Net Folders**.
- **File Pointers and Files Appear Together:** The Filr 2.0 desktop applications provide a consolidated view that includes file pointers that are generated from file metadata synchronized to Filr and actual files in Filr folders on workstation hard drives.
- **Filr Minimizes Local Disk Space Usage:** Initially, all files and folders are **Online Only**, meaning that the local disk contains only file pointers that link to the Filr appliance and in turn, to back-end file servers.
- **Full Browsing Is Supported:** When users are logged in to Filr, they can browse through their assigned files and folders as though they were all physically present on local hard drives.

- **Users Control Which Files Are Downloaded:** Files are downloaded only when a local copy is needed.

  This saves network bandwidth, streamlines file synchronization, and reduces workstation disk space requirements.

  Users can download files to their local hard drives in one of two ways:

  - They can open them in an application

    Or

  - They can mark them as “Available Offline”

14.4.5 A Good Replacement for Mapped Drives

For many traditional Novell desktop users, the files-on-demand features in Windows Explorer and Mac Finder provide an excellent alternative to traditional mapped drives.

- **Full Browsing Support:** Users can browse network file systems just like with mapped drives.
- **Data Synchronization:** Changes made by desktop users and by others on the back-end file server are kept in sync.
- **Conflict Resolution:** If simultaneous changes by multiple users cause copies to get out of sync, Filr’s file-conflict-handling facilitates reconciling the differences.

15 Network Time and Filr

Filr appliances and the file servers that they point to should be in the same time zone and they should use the same reliable NTP time source.

Browsers and access devices can be in different time zones than the appliances and servers that they access because all time-stamp-associated actions are handled using UTC. However, if the desktop is not synced to a reliable time source, there could be some confusion. For example, a time stamp on the server might appear to be “in the future” when compared with the time on the desktop.

16 Users and Groups in Filr

16.1 Leveraging the Built-in Security of eDirectory and Active Directory

Novell recommends that you leverage the security features of eDirectory and Active Directory whenever possible.

Both of these directory services have extensive and proven experience with authorization and authentication services. They also provide security features, such as intruder detection, forced complex passwords, password expiration, password history, and so on.

Local user accounts that you create through Filr in the SQL database are certainly not insecure, but neither are they protected by the security features mentioned above.

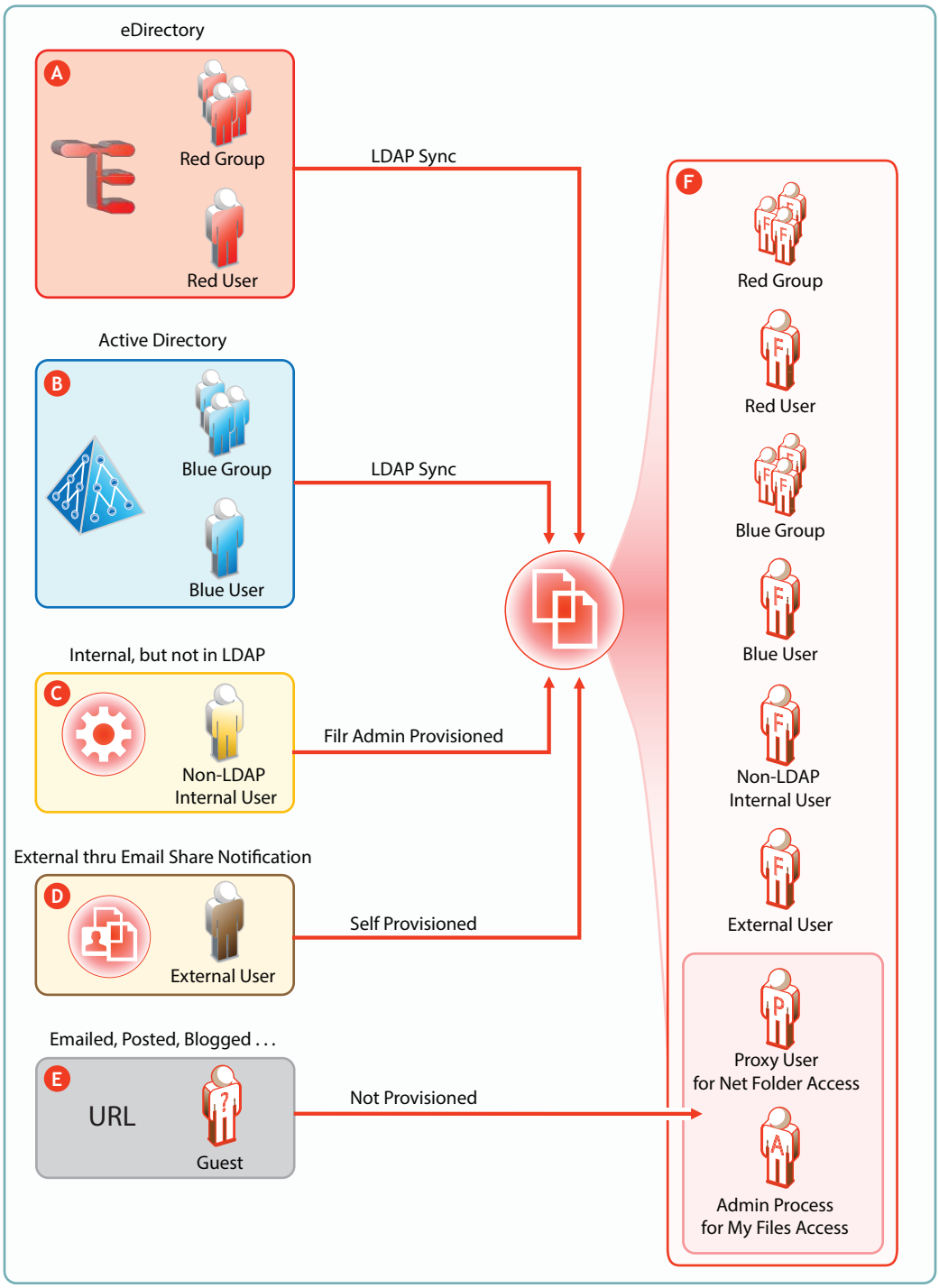
16.2 Provisioning Users and Groups

For users to access Filr, they must be provisioned on the Filr system. They can then be assigned access rights.

16.2.1 User Provisioning Overview

Figure 16-1 provides a high-level overview of the provisioning process that allows users and groups to access an organization’s internal data through Filr.

Figure 16-1 *Provisioning Users and Groups*



Letter	Details
A	eDirectory users are provisioned on Filr through LDAP/LDAPS synchronization. Synchronization is one-way. Password and other changes on the eDirectory side are handled in Filr without additional configuration. Password and other changes can be made to a user's Filr configuration. However, they are not synchronized back to eDirectory. Instead, they are overwritten by the configuration in eDirectory with each synchronization.
B	Active Directory (AD) users are provisioned on Filr through LDAP/LDAPS synchronization. Synchronization is one-way. Password and other changes on the AD side are handled in Filr without additional configuration. Password and other changes can be made to a user's Filr configuration. However, they are not synchronized back to AD. Instead, they are overwritten by the configuration in AD with each synchronization.
C	Filr administrators can also provision users on the Filr appliance. These are referred to as Local users in the documentation and Filr interfaces.
D	External User accounts are created when share invitations are issued through email from Filr. The users provision themselves with a password, and so on when they log in to Filr.
E	Public users (Guests) aren't provisioned with accounts on Filr. Public users are anonymous to Filr and are allowed access to shared files in Net Folders through the Proxy User assigned to the Net Folder they are accessing. For shared files and folders in My Files, Public users gain access through the Filr admin process.

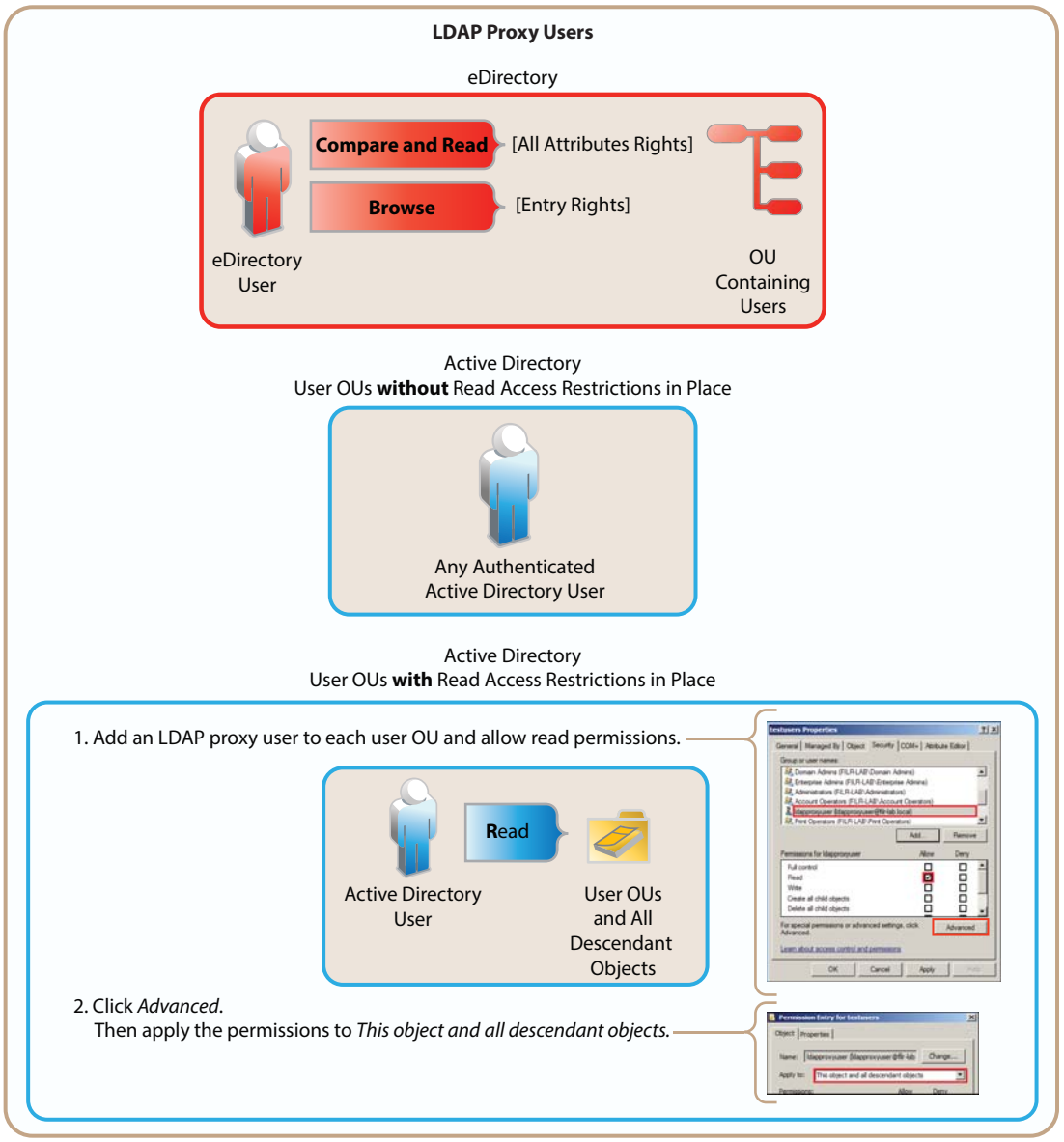
16.2.2 LDAP Proxy User Role and Rights

Filr synchronizes LDAP users by leveraging proxy users in the targeted LDAP directories that have sufficient rights to read the user and group information required by Filr.

Currently, eDirectory and Active Directory are supported as LDAP identity stores.

The rights required for LDAP synchronization are platform-specific, and for Active Directory they vary depending on whether read access restrictions are in place, as illustrated in Figure 16-2.

Figure 16-2 *Rights Required for LDAP Proxy Users*



16.2.3 Types of Filr Users

- **LDAP Synchronized:** Users and groups can be synchronized from an internal LDAP identity store.

  After users and groups are provisioned through an initial synchronization, they have accounts in Filr that correspond to their original identities, but these are only secondary. By leveraging the rights of one or more LDAP proxy users in the directory, Filr synchronizes regularly to keep authentication credentials current, update changes in home directory and file system rights assignments, and so on.

- **Filr Admin Created:** Users and groups can be created by Filr administrators.

  Admin-created groups are managed as part of the Filr system. They can be assigned personal storage, but access to Net Folders and other users' home directories happens only through Filr-based sharing.

- **External, Self-Provisioned:** Users can be invited to participate through share invitations.

  When they respond to the invitations, they are given the opportunity to self-provision an account on the Filr server.

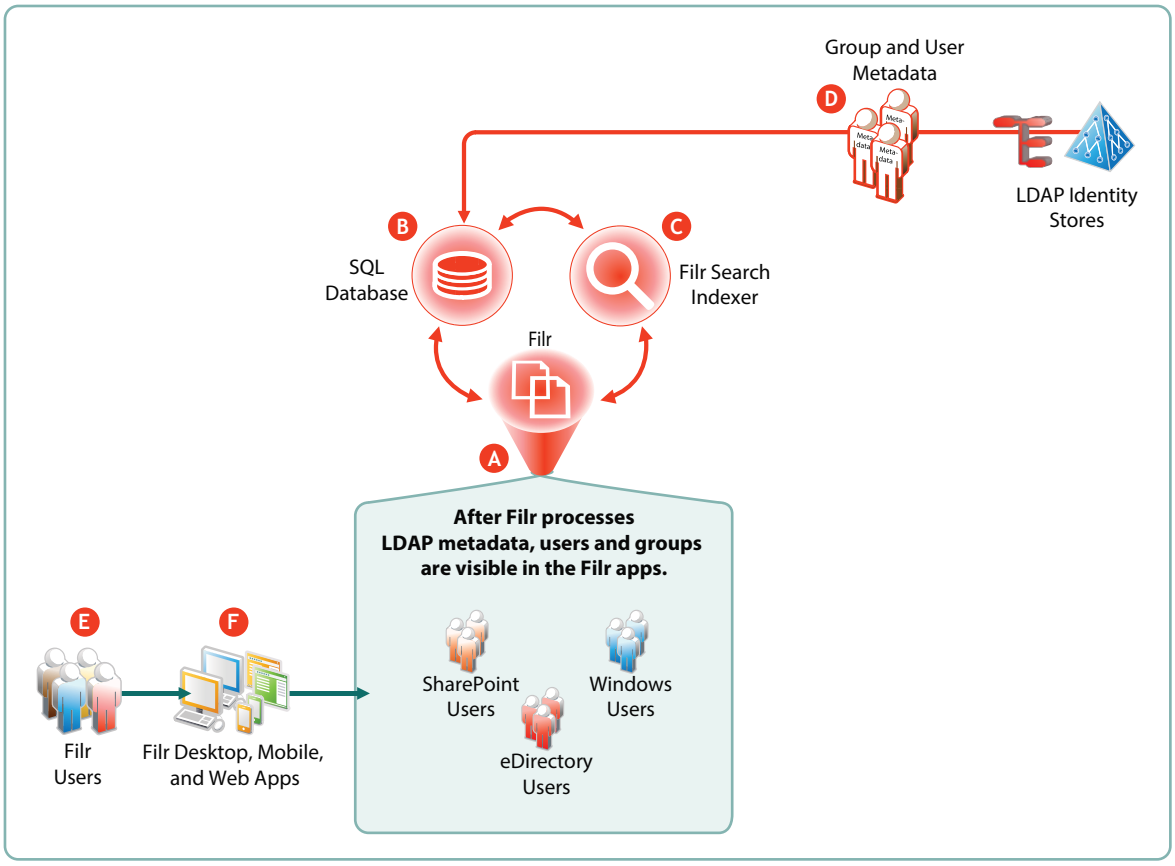
  After they are provisioned, they can then be granted personal storage and other permissions similar to those enjoyed by internal users.
- **Guest Users:** When Filr administrators allow it, Filr users can share the URLs to files in Net Folders and My Files, making them available to the general public. Those who access files in this way are referred to as “Guest” users. Guest users are not provisioned and anonymous from a Filr perspective.

16.2.4 The Role of Groups in Filr

Users can be assigned rights on Filr as members of groups, including as members of either the `All Internal Users` group or the `All External Users` group, which includes those whose accounts were created as a result of an email share invitation.

16.3 How Filr Makes LDAP Users and Groups Visible

Figure 16-3 *Filr Processes Metadata to LDAP Users and Groups Visible to Filr Users*



Letter	Details
A	Filr directs and coordinates the processing of metadata for users and groups.
B	Filr retrieves and stores the metadata in the SQL appliance or server.
C	After metadata retrieval, Filr directs the Filr Search (Lucene) indexer to process it for viewing in the Filr apps.
D	Organization Users and groups are either synchronized from the LDAP identity stores (shown) or created directly in Filr (not shown).
E	After the metadata is processed for users and groups, Filr users can see them in the Filr apps (Letter G).
F	Filr apps for desktops, mobile devices, and web access let Filr users interact with the users and groups that are made accessible through Filr.

16.4 Key Points About User Visibility in Filr

The following are key points to consider and understand regarding user visibility in Filr.

- **LDAP Synchronization Is Key:** As explained in Section 16.3, “How Filr Makes LDAP Users and Groups Visible,” on page 103, LDAP metadata must be imported and processed to make user and group objects visible.

  After the initial LDAP import, user and group metadata in Filr must be kept in sync with back-end LDAP identity stores, as explained in Section 13.1, “Synchronization Overview,” on page 83.
- **All Filr System Components Must Online:** For Filr users to appear in the various dialogs and lists, the Filr appliance, the Filr Search appliance, and the SQL database must all be online.
- **Who Can See Whom:** For various reasons, such as security, large numbers of users, and so on, it might be necessary to limit user visibility.

  Starting in Filr 2.0, administrators can restrict which users can see each other. See “Limiting User Visibility ” in the *Filr 2.0: Administration Guide*.

A Documentation Updates

In addition to version and content changes throughout the guide, the following overview sections include major substantive changes for Filr 2.0.

June 23, 2016

Section	Summary of Changes
◆ Figure 12-1 on page 77	Revised to show that sharing is not available for external users, beginning with Filr 2.0.

May 12, 2016

Section	Summary of Changes
◆ Section 12.2, “Understanding Sharing,” on page 81	Revised the explanation regarding shared-access rights. Changed to shared-access roles and corrected previous statements comparing them with Net Folder roles. Functionally, they are identical.

February 22, 2016

Section	Summary of Changes
◆ Figure 2-9, “Example of a Small Filr Deployment,” on page 24 ◆ Figure 2-10, “Example of a Large Filr Deployment,” on page 26, ◆ Figure 10-6, “Proxy User Rights Summary,” on page 73, ◆ Figure 11-1, “Protocols Used in Filr Installations,” on page 75,	Updated graphics to reflect OES 2015 NSS AD integration.

February 9, 2016

Section	Summary of Changes
Section 4.8, “Filr Roles and NSS File System Rights Might Not Match,” on page 48	New section.
Chapter 7, “Filr Search Appliance—Accessibility, and Searchability,” on page 55	Added more detail to explanations and refined the presentation order.
Section 10.4.1, “Net Folder Proxy Identities,” on page 71	New section.
Figure 13-1, “What Gets Synchronized and Where,” on page 83	Reworked graphic and explanation.
Chapter 14, “File and Folder Access in Filr,” on page 89	New Section.
Section 16.2, “Provisioning Users and Groups,” on page 99	Reworked content, starting with this section.